Gregory Chan*

ANTI-MONEY LAUNDERING LAWS: A THORN IN THE SIDE OF THE FOUR ASIAN TIGERS

Abstract

The Four Asian Tigers are often characterised by their surge of economic growth, and have come to represent rapid industrialisation albeit with a dash of authoritarianism. Indeed, the economies of Hong Kong, Singapore, South Korea and Chinese Taipei had undergone an unprecedented level of development in an extremely short span of time following decolonialisation, causing the World Bank to dub them "The East Asian Miracle". Yet, as the world moves into the digital age, new hurdles present themselves on the horizon for these mammoths to overcome. Of these, one of the tallest, and perhaps most unpredictable, seems to be the increasingly disruptive nature of decentralised digital assets ("DDA"). Since the launch of Bitcoin in 2008, the use, development and activity of DDAs has been growing at an unprecedented rate across the globe. With a global market cap of over $1 Trillion USD in crypto-assets alone, DDAs undoubtedly would play a significant role in the modern global economy.

Yet, despite the huge potential around these assets, policy-makers have become particularly wary of these DDAs. The emphasis on their decentralised nature has presented them as a way for users to undermine the traditional regulatory mechanisms. Particularly here, DDAs have gained notoriety as tools for assisting in money-laundering, and bypassing state-imposed economic sanctions. Studies by the International Federation of Accountants here note 5 common ways these occurs: (1) predicating crime, (2) converting illegally obtained digital assets into tangible assets, (3) hiding transactions through anonymised services, (4) layering numerous exchanges of assets from tangible to intangible to mask transactions, and (5) the integration and legitimisation of income. In light of these concerns, regional harmonised approaches seem to be taking centre stage. In Europe, significant discussion has been placed around the recent Markets in Crypto-Assets Regulation. On the other side of the Atlantic, the United States seems to be working on similar provisions, following the recent leak of the draft bill regulating DeFi and Decentralised Autonomous Organisations ('DAO"). Yet, such a harmonised approach seems to be lacking in Asia. Instead, competition between the Asian Tigers to attract investors has resulted in starkly individualised approaches among them, each looking to out-position the other to take advantage of these new developments. However, this disharmonised and fragmented approach ultimately led to cracks appearing in the regulatory firewall, often through policy oversights.

This paper will thus take a comparative, and law-economics based approach towards the law governing DDAs across these 4 high-income economies, particularly the laws governing transnational anti-money laundering mechanisms, and the place of DDAs in the law of sanctions among these nations. It primarily considers this from the perspectives of DDAs as a tool, and their impacts on how nation-states craft anti-money laundering laws ("AML"). While it ultimately concludes that the fragmented approach is acceptable given the current

* King's College London, LLB. gregory.chan@kcl.ac.uk. All information contained in this paper represents the view and opinion of the author, and does not necessarily represent the views of the publishers or affiliated organisations. Any errors are solely the fault of the authors.

situation, greater cooperation between both private and public stakeholders is imperative towards the development of the law of sanctions.
In doing a comparative analysis within these economies, this paper looks at 2 key areas within AML on digital assets. Firstly, it considers the extent of which regulatory mechanisms (such as disclosure of identities) interact with these DDAs within the local economies. Then, it considers how sanctions target DDAs, and the relevant AML laws. A further dimension that is also explored is the role of Virtual Asset Service Providers ("VASPs") within these economies, and the nature of the set of rights which are attached to these DDAs. It then discusses how this domestic legislation would interact with the growing body of international law instruments that have been in the works, including the guidelines introduced by the Financial Action Task Force ("FATF"), and the United Nations International Institute for the Unification of Private Law. It is then argued here that the crux of the interaction between the law of sanctions and domestic legislation on DDAs lies in the conversion between DDAs and tangible assets. The role of AMLs should then look to combat the conversion of "dirty" assets as a whole.
Ultimately, the comparative analysis concludes with a brief discussion of mechanisms to strengthen and, to an extent, harmonise international laws in this field. Firstly, the doctrine of comity between nations should once more be reaffirmed and strengthened. This ensures mutual recognition of regulatory attempts between these economies mutually strengthening AML legislation through the Courts in a bottom-up, but also a top-down regulatory perspective. This similarly extends to provisions around regional cooperation across the private sector, and mechanisms where these economies can implement to encourage such cooperation. Secondly, a discussion is had about the use of corporate standards for future regulatory work; concerns that AML might be too reactive, or "out-of-date" is rather prominent. Hence, futureproofing through working with various stakeholders to develop comprehensive frameworks to encapsulate the relevant features and novelties with DDAs would prove invaluable. Such would then allow these economies to fully utilise DDAs to their full potential while ensuring compliance with the law of sanctions.

JEL CLASSIFICATION: F39, F50, G28, K29, P10, P59

SUMMARY

1 Introduction

In recent years, Decentralised Digital Assets ("DDAs") has become the talk of the town. The advent of cryptocurrencies stemming from the now infamous Bitcoin Manifesto[1] has spiralled into over countless new currencies built on unique variants of blockchain technologies.[2] In the public sector, central banks have begun bilateral and multilateral discussions and initiatives to venture into the world of Financial Technology ("FinTech") and DDAs, embracing these technological developments in various ways.[3] Indeed, DDAs have undoubtedly caused significant disruptions within the global financial market in a myriad of ways. However, as with new developments, growing concerns have been raised over their use. Given the anonymity and transboundary nature of the internet, coupled with the decentralised and deregulated nature of DDAs, one can definitely understand the fears policy-makers have over DDAs. This is made worse especially with the current peer-to-peer model of DDAs which seems to bypass the paper-trail of transactions policy-makers are attempting to preserve.

As such, it seems self-evident why DDAs are particularly difficult to stomach in the law of economic sanctions. Traditionally, economic sanctions are used as a punitive measure against State's wrongful conduct. In practice however, the imposition of economic sanctions is rare, usually extremely targeted and only used in serious and extreme cases. Most recently, the 2022 invasion of Ukraine prompted a series of sanctions against Russia and Belarus, designed to narrowly target those in the upper ranks of the Russian government.[4] Similarly, in sanctions imposed against Argentina during the Falklands War, general trade sanctions were limited; instead, the targeted sanctions on the arms supply aimed to mitigate the conflict on the ground when it was deemed that the conflict would be resolved through gunfire.[5] Even when sanctions are enacted through United Nations Security Council ("UNSC") resolutions, they are generally designated against key figures,[6]

---

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) 1,6. <https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf> accessed 5 December 2022.

[2] Xian Rong Zheng and Yang Lu, 'Blockchain Technology - Recent Research and Future Trends' (2021) 16(12) Enterprise Information Systems, <https://www.tandfonline.com/doi/full/10.1080/17517575.2021.1939895> accessed 3 December 2022.

[3] For instance, see here regarding Project BENJA, a partnership between Deutsche Bank, Hashstacs Pte Ltd, Bursa Malaysia, the UBS Group AG, the Union Bank of Philippines, and the Monetary Authority of Singapore: <https://stacs.io/wp-content/uploads/2021/05/Project-Benja-Public-2021.pdf> accessed 21 March 2023. There are similar projects in the field such as Project Genesis by the government of Hong Kong and the BIS Innovation Hub: <https://www.bis.org/publ/othp58.htm> accessed 1 December 2022.

[4] Ruth Endam Mbah and Divine Forcha Wasum, 'Russian-Ukraine 2022 War: A Review of the Economic Impact of Russian-Ukraine Crisis on the USA, UK, Canada, and Europe' (2022) 9(3) Advances in Social Sciences Research Journal 144.

[5] N Piers Ludlow, 'Solidarity, Sanctions and Misunderstanding: The European Dimension of the Falklands Crisis' (2021) 43(3) The International History Review 508 <https://doi.org/10.1080/07075332.2020.1791226> accessed 2 December 2022.

[6] Gary C Hufbauer and Barbara Oegg, 'Targeted Sanctions: A Policy Alternative' (2000) 32(1) Law and Policy in International Business 11.

or limiting a State's means to continue wrongful conduct.[7] In that regard, while sanctions seek to punish, States largely use them to target those involved and directly responsible for the State's actions rather than the general populace.

Of course, there have been sanctions imposed which are aimed at the wider populace in an attempt to incite societal pressure against the ruling government. Notable examples of this include overall trade sanctions made against the Democratic People's Republic of Korea ("DPRK") since its first nuclear launch program in 2006,[8] which covered general travel and trade, as well as the sanctions against Iran for its Nuclear Program.[9] While the DPRK's situation is unique, with a more tightly controlled government masking the effects of the sanctions to the general populace, the sanctions in Iran tell a different story. The Iranian sanctions caused a weaker currency, resulting in individuals suffering a higher cost of living as the price of exports increased.[10] Further, many oil and gas multinational corporations operating in Iran were forced to leave the country despite them being major players within the Iranian economy.[11] This exodus cost significant job shortages and many had no livelihoods amidst the inflation occurring in the country.[12] While the actual effect of these sanctions remains arguable in pushing Iran to signing the Joint Comprehensive Plan of Action,[13] they nonetheless showcase the societal impact of sanctions on a State's populace.

The imposition of these sanctions is, at its core, a top-down approach by the State. Within the State imposing sanctions, domestic laws are drafted to prevent corporations and individuals from engaging with trade with a particular State. Often, a breach of sanctions carries criminal liability within the sanctioning State's jurisdictions.[14] The United States has even gone so far as to call upon international law enforcement for assistance in prosecuting a foreign national accused of breaching sanctions within their

[7] Tom Ruys, 'Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework' in Larissa van den Herik (ed), *Research Handbook on UN Sanctions and International Law* (Edward Elgar Publishing 2016) 5. <

[8] John Crook, 'North Korea Rejects Past Nuclear Commitments, Tests Another Nuclear Weapon, and Provokes Additional UN Sanctions.' (2009) 103(3) American Journal of International Law 597.

[9] Mehdi Khalaji, 'Great Expectations: Iran after the Deal' (2015) 38(3) The Washington Quarterly, 61 <https://www.tandfonline.com/doi/abs/10.1080/0163660X.2015.1099025> accessed 2 December 2022.

[10] Ali Feghe Majidi and Zahra Zarouni, 'The Impact of Sanctions on the Economy of Iran' (2020) 8(4) International Journal of Resistive Economics, 49 <http://www.oajre.ir/article_125414.html> accessed 2 December 2022.

[11] Nikolay Kozhanov, 'U.S Economic Sanctions Against Iran: Undermined by External Factors' (2011) 18(3) Middle East Policy 144.

[12] Orkideh Gharehgozli, 'An estimation of the economic cost of recent sanctions on Iran using the synthetic control method' (2017) 157 Economic Letters 141 <https://www.sciencedirect.com/science/article/abs/pii/S0165176517302331> accessed 3 December 2022.

[13] For a discussion of sanctions following a joint comprehensive plan of action, see Farhad Rohan and others, 'The Impact of Implementing Sanction by the Party of the Six Countries (5+1) in the Joint Comprehensive Plan of Action in Exercising the International Upstream Oil Agreements from the Point of the View of Iran's Legal System' (2021) 13(24) Civil Jurisprudence Doctrines 163.

[14] See, for example, in South Korea, Art 27(1)-(8) of the Foreign Exchange Translation Act imposes criminal liability for breach of sanctions. More broadly, discussed in Nicolas Angelet, 'Criminal Liability for the Violation of United Nations Economic Sanctions' (1999) 7(2) European Journal of Criminal Law and Criminal Justice 89.

jurisdictions.[15] Of course, the enforcement of sanctions is significantly easier when trade is conducted through tangible goods and with legal tender. Tracking the paper (or electronic) trail of the movement of money has never been easier. Anti-money laundering ("AML") mechanisms adopting modern technological innovations have been increasingly applied to tackle breaches of sanctions.[16] For instance, embracing machine for transaction monitoring learning to identify suspicious patterns has strengthened AML laws globally.[17] These developments are undoubtedly to be applauded, as States seem to be moving with the rapid development of technological trends through the years.

As a whole, sanctions can only be enforced if there is sufficient oversight to monitor ongoing transactions. Conversely however, DDAs have been designed to avoid third party oversight within transactions with its peer-to-peer model. While one might consider this to be the role of DDA custodians, there is similarly difficulty with this position. These custodians, more commonly known as 'wallets', and operate as a platform for individuals to interact with their DDAs, as well as transfer DDAs to and from other users.[18] However, due to the sheer number of custodians, the inability of them to track transactions, as well as terms regarding the ownership of these assets, these custodians cannot be regarded as central institutions. The same can be said for exchanges, servers, nodes, as well as other 'custodial' platforms.[19] Instead, these should be regarded as services which other holders of these assets provide. While ownership of the DDA remains with the true owner, the DDA custodian acts as a platform to utilise these assets as though they were tangible. With so many different custodians, it further undermines any attempt at creating a regulatory environment. As a result, certain countries have been reported to have used DDAs to commit "cybercrimes", utilising these DDAs as a mechanism to avoid sanctions which were imposed on them.[20] Such practical considerations undoubtedly exemplify the importance of this discussion.

Despite these hardships, four strong economies which have a history of embracing and taking advantage of technological developments are taking this challenge head on. Characterised by the surge of rapid economic growth in wake of attaining independence,

[15] AFP, 'Singaporean wanted by US over North Korea is in Singapore: Police' *Alarabiya News* (Singapore, 6 November 2022) <https://english.alarabiya.net/News/world/2022/11/06/Singaporean-wanted-by-US-over-North-Korea-is-in-Singapore-Police> accessed 30 November 2022.
[16] David Cortright and George A Lopez, *Smart Santions: Targeting Economic Statecraft* (Rowman & Littlefield publishing, 2002).
[17] Gökberk Bayramoğlu, 'An Overview of the Artificial Intelligence Applications in Fintech and Regtech' (2017) 1 The Impact of Artificial Intelligence on Governance, Economics and Finance, 291 <https://link.springer.com/chapter/10.1007/978-981-33-6811-8_15> accessed 2 December 2022.
[18] Richard Walker and others, 'The unique and complex consideration of digital asset custody' (2021) 13(2) Journal of Securities Operations & Custody 2, 150.
[19] See, a discussion here in Harry Leinonen, 'Decentralised Blockchained and Centralised Real-Time Payment Ledgers: Development Trends and Basic Requirements' in Jakub Górka (ed), *Transforming Payment Systems in Europe* (Springer Link 2016).
[20] See, for instance, the case of North Korea at: DPRK Cyber Threat Advisory, 'Guidance on the North Korean Cyber Threat' (Government of the United States of America, 2019) <https://www.cisa.gov/uscert/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf> accessed 2 December 2022.

the Four Asian Tigers once more seem poised to embrace these new disruptions. Dubbed as the "East Asian Miracle" by the World Bank,[21] it would seem that these economies are once more attempting to be global leaders within the FinTech World. Indeed, one can similarly argue that Singapore, South Korea, Hong Kong, and Chinese Taipei have all been vying to be the London or New York of the East - the financial hub for the region.[22] Thus, their abilities to be able to take advantage of these new technologies would likely give them the necessary edge in the competition in this era of digitisation. Unfortunately, such competition has similarly resulted in starkly individualised approaches to be adopted between these countries, as they look to out-position the other. Unfortunately, where there is disharmony among nations despite the transboundary nature of the issues, there is a growing concern of cracks appearing in the regulatory firewall appearing in these assets.

This paper will thus take a comparative approach to the regulatory framework of DDAs across the Four Asian Tigers. In particular, it will comment on three areas within their regulatory framework - its definition of DDAs, its climate for DDA investors operating within their countries, internal Anti-Money Laundering ("AML") provisions and transboundary regulations and compliance with sanctions. Finally, it will analyse the position of each country and discuss potential areas for a harmonised framework to be adopted within this field.

As a brief disposition, Section II will discuss and comment on the laws found within each of the Four Asian Tigers in two areas – the general regulatory framework of DDAs, and how DDAs interact with AML and economic sanction legislation. Section III then takes a comparative view and discusses the position of these economies in three sub-sections – their taxonomies, treatments of DDAs, and compliance with existing international frameworks. Section IV discusses potential reforms that can be taken in moving towards a harmonised approach. Section IV concludes.

2 An overview of DDAs across the Four Asian Tigers: a comparative approach

As briefly alluded to earlier, DDAs have been treated significantly differently across the jurisdictions of the Four Asian Tigers. While it can be said that all these economies have a seemingly pro-DDA attitude, it is worth exploring them in greater detail to understand the nuances behind their policy-making. In that regard, this section seeks to provide an overview of the regulatory framework around DDAs.

[21] Nancy Birdsall and others, 'The East Asian miracle : economic growth and public policy : Main report (English)' (26 September 1993, World Bank Reports) <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/975081468244550798/main-report> accessed 4 December 2022.
[22] Darryl S L Jarvis, 'Race for the money: international financial centres in Asia' (2011) 14 Journal of International Relations and Development, 60.

To that end, there are three key themes which it will follow through its analysis. First, the jurisdiction's taxonomy surrounding digital assets. Second, internal domestic AML provisions and mechanisms surrounding DDAs. Finally, transboundary frameworks and compliance with international obligations. It is ultimately hoped that these three key areas will provide a holistic overview of DDAs and the law of sanctions in these jurisdictions.

2.1 Singapore

2.1.1 The regulatory framework of DDAs in Singapore

Beginning first with the small island State of Singapore. Singapore is not unfamiliar with embracing technological developments as a means to boost its economy. Since gaining independence 1965,[23] the government has been seeking to take advantage of the "latest trends" in the market. Beginning with the Civil Service Computerisation Program in the 1980 which saw the first adoption of information and communication technologies,[24] Singapore continuously adapted to the technological developments with initiatives such as SingPass[25], the Smart City project.[26] Most recently, Singapore launched GovTech - a government branch dedicated to leading digital transformation in the country.[27] Given this, it seems clear that the government is dedicated to embracing technological change, rather than shunning them away.

This trend has similarly carried over to the realm of DDAs. With Singapore touting itself as the "FinTech Hub of Asia", the country has been particularly receptive to DDAs. The Monetary Authority of Singapore ("MAS") has been extremely active in discussing technological trends in the financial world. Adopting a wide definition of DDAs, s.2 of the Payment Service Act 2019 ("PSA") hence defines them under the umbrella term "digital payment tokens", which are expressly mentioned to include cryptocurrencies.[28] In particular, the PSA writes that:

[23] Reuben Ng, Paul Wong and Si Qi Lim, 'Singapore: 50 Years of Science and Technology' (8 August 2018, Global-is-asian, Lee Kuan Yew School of Public Policy) <https://lkyspp.nus.edu.sg/gia/article/singapore-50-years-of-science-and-technology> accessed 21 March 2023.
[24] Kwok Cheong Lee, 'Civil Service Computerisation - the Singapore experience' (Expert Group Meeting on Integrating Information Systems Technology in Local Regional Development Planning, 31 October 1988). <https://dr.ntu.edu.sg/bitstream/10220/485/1/AMIC_1988_OCTNOV(VOL_1)_11.pdf> accessed 3 December 2022.
[25] Jezon Ow, 'The future of healthcare in Singapore. How an integrated use of A.I., Internet-of-Medical things (IoMT), Blockchain-based technologies, and Cloud-computing-based Medtech and Digital Health solutions will radically address medical data integrity concerns' (1 November 2021). <https://ssrn.com/abstract=3965116> accessed 3 December 2022.
[26] Ahm Shamsuzzoha and others, 'Smart city for sustainable environment: A comparison of participatory strategies from Helsinki, Singapore and London' (2021) 114 Cities.
[27] Woo Jun Jie, 'Technology and governance in Singapore's smart nation initiative' (HUP 2018).
[28] Monetary Authority of Singapore, 'Digital Payment Tokens' (November 2021, Government of the Republic of Singapore) <https://www.mas.gov.sg/-/media/MAS-Media-Library/who-we-are/mas-gallery/MAS-Gallery/Digital-Payment-Tokens.pdf> accessed 5 December 2022.

> "digital payment token" means any digital representation of value (other than an excluded digital representation of value) that
> (a) is expressed as a unit;
> (b) is not denominated in any currency, and is not pegged by its issuer to any currency;
> (c) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt;
> (d) can be transferred, stored or traded electronically; and
> (e) satisfies such other characteristics as the Authority may prescribe.

The PSA similarly distinguishes digital payment tokens from the concept of "e-money" through the "official currency" requirement in the Act.[29] This is particularly welcome amidst the pseudo "peer-to-peer" instantaneous bank transfer technology such as PayLah and PayNow which is particularly prevalent in the small island State.[30] For digital custodians and intermediaries, s.6 of the PSA requires digital payment token service providers to obtain a licence from MAS prior to operation. These licences carry further obligations for service under the PSA. These include the obligation of licensee to notify the authorities of certain events (s.15 PSA), obligation of licensee to provide information to Authority (s.16 PSA) and the obligation of licensee to submit periodic reports (s.17 PSA). Further, under the recent Financial Services and Markets Act 2022, the MAS has the authority to conduct inspections on these service providers to ensure compliance with these provisions. Hence, despite the nature of DDAs being fundamentally decentralised, the Singaporean Government seems to be attempting to claw power back from these custodial platforms back to the central authorities.

Despite the attempts of such a wide umbrella term, it must be noted that "digital payment token" under the PSA excludes digital securities, distinguishing them from the realm of these tokenised assets.[31] These digital securities are instead regulated under the Securities and Future Act 2001 ("SFA"); the criteria laid out under the s.2 of the SFA provide an exhaustive list to determine whether a DDA is a token under the FSA, or a tokenised security under the SFA. Such similarly reflects the ongoing policies of the MAS to be pro-DDA, but hostile towards cryptocurrencies and forms of digital property.[32]

[29] S.2, Singapore Payment Service Act 2019 <https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220> accessed 21 March 2023.
[30] See the statistics provided in: Statista, 'Singapore: Leading e-payment services by age 2022' (December 2022). <https://www.statista.com/statistics/1106658/singapore-leading-e-payment-services-by-age/> accessed 7 December 2022.
[31] Monetary Authority of Singapore, 'A Guide to Digital Offering', (26 May 2020, Government of the Republic of Singapore) paras. 1.2, 2.1 <https://www.mas.gov.sg/-/media/MAS/Sectors/Guidance/Guide-to-Digital-Token-Offerings-26-May-2020.pdf> accessed 30 November 2022
[32] Monetary Authority of Singapore, 'Yes to Digital Asset Innovation, No to Cryptocurrency Speculation' - Opening Address by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Green Shoots Seminar on 29 August 2022, (29 August 2022, Government of the Republic of Singapore) <https://www.mas.gov.sg/news/speeches/2022/yes-to-digital-asset-innovation-no-to-cryptocurrency-speculation> accessed 29 November 2022.

Indeed, it seems that MAS is looking to adopt a "wait-and-see" approach before making a clear distinction in these assets; to "look beyond labels and examine features and characteristics of each token".[33]

From a practical perspective, this distinction might explain the decisions of the Courts to allow proprietary injunctions of non-fungible tokens where they were regarded as securities rather than a form of payment tokens.[34] The position however, is currently unsettled for cryptocurrencies, where the Apex Court in *Quoine Pte Ltd v B2C2*[35] declined to comment on whether "[bitcoin], may even be regarded as a species of property capable of attracting trust obligations." despite citing the United Kingdom's Jurisdiction Taskforce's analysis on crypto-assets[36] which concluded that crypto-assets could be treated as having a proprietary character.[37] Nonetheless, as cryptocurrencies were suggested to form part of the legislation of digital securities or a 'security-based derivative contract',[38] it is likely that they would be caught under this Act, and cement its proprietary character.

A final category that must be discussed is 'stablecoins', given its unique position in Singapore's regulatory environment. While traditional cryptocurrencies such as Bitcoin and Ethereum are predominantly floating and speculative, stablecoins are described as a fiat currency, backed by a different form of asset.[39] In the private sector, the most common crypto-assets known as stablecoins are Tether Gold (Ticker: XAUT) and Paxos Gold (Ticker: PAXG) are backed with gold.[40] The MAS seems to have special considerations for these coins, and is even looking to promote them despite their hostile approach towards traditional cryptocurrencies.[41] However, an analysis of the proposed changes indicates that these requirements once more suffer from attempts to 'centralise' these

[33] (n 30). See also: Monetary Authority of Singapore, *Money at a Crossroads: Public or Private Digital Money?* - Summary of Panel Remarks by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at IMF Seminar on Money at a Crossroads on 18 April 2022" (18 April 2022) <https://www.mas.gov.sg/news/speeches/2022/money-at-a-crossroads-public-or-private-digital-money> accessed 2 December 2022.
[34] *CLM v CLN* [2022] SGHC 46. However, the term "digital securities" was not mentioned through the decision, nor was the Securities and Futures Act 2001. However, the reasoning from the judgement is similar to the distinction made between DPTs and securities.
[35] *Quoine Pte Ltd v B2C2* [2020] SGCA(I) 02.
[36] ibid para 57 and para 143.
[37] UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019) The LawTech Delivery Panel 21, 22 [85] <https://resources.lawtechuk.io/files/4.%20Cryptoasset%20and%20Smart%20Contract%20Statement.pdf> accessed 1 December 2022.
[38] Kenneth Pereire and Lin YingXin, 'KGP Legal LLC' in Joasis N Dewey (ed), *Blockchain & Cryptocurrency Laws and Regulation 2023* (Global Legal Insights 2022).
[39] Makiko Mita and others, 'What is Stablecoin? A Survey on Price Stabilization Mechanisms for Decentralised Payment Systems' 8th International Congress on Advanced and Applied Informatics (2019) 60 <https://ieeexplore.ieee.org/abstract/document/8992735> accessed 2 December 2022.
[40] Akanksha Jalan, Roman Matkovskyy and Larisa Yarovaya, '"Shiny" crypto assets: A systemic look at gold-backed cryptocurrencies during the COVID-19 pandemic' (2021) 78 International Review of Financial Analysis <https://doi.org/10.1016/j.irfa.2021.101958> accessed 7 December 2022.
[41] Monetary Authority of Singapore, *MAS proposes measures to reduce risks to consumers from cryptocurrency trading and enhance standards of stablecoin-related activities* (26 October 2022, Government of the Republic of Singapore); Monetary Authority of Singapore, *Consultation Paper: Proposed Regulatory Approach for Stablecoin Relate Activities* (Government of the Republic of Singapore, October 2022).

fundamentally 'decentralised assets'. Proposed regulations include oversight of the issuers of the currency stablecoins are pegged to, disclosure obligations, as well as background checks for users and holders of these currencies.[42] It is also worth noting that express wording that MAS to describe decentralised stablecoins is "well-regulated and securely backed."[43] In essence, such regulations would place users of stablecoins in a similar position as using traditional currencies, rather than anything unique or different. Such would consequently have stablecoins lose their unique identities within the DDA framework.

Ultimately, the position of DDAs in Singapore seems to have been flipped on its head. On one hand, the country seems to be extremely positive towards incorporating and embracing DDAs as a whole, believing it to constitute the next generation of payments. Yet, it cannot accept concepts of decentralisation and ownership of DDAs, and seeks to shelter this novel financial instrument under a regulatory climate of obligations. While this may yield benefits to ensure a less volatile, less speculative and more certain markets for greater use in international trade, such a framework unfortunately seems to undermine the whole purpose of DDAs as a peer-to-peer model. Nonetheless, for the purposes of AML and compliance with sanctions, such regulatory oversight would, at first glance, seem beneficial.

2.1.2 AML laws and economic sanctions of DDAs in Singapore

Having delved into the Nation-State's position on DDAs' one can then consider its implications on AML laws. To briefly summarise the position above, the laws governing DDAs in Singapore are split into two categories. First, digital payment tokens under the PSA, where tokens operate as a form of 'decentralised currency' exchanged on licensed online platforms complying with the relevant obligations. Examples of these digital payment tokens generally include the traditional cryptocurrencies - Bitcoin, Etherum. Second, digital securities traded under the SFA which stem from securities-based contracts on the blockchain. These include tokenised commodities, as well as modern innovations such as blockchain-based green bonds,[44] and bank-backed debt instruments,[45] to name a few. In both instances however, Singapore's MAS was similarly quick to refer to the Terrorism (Suppression of Financing) Act 2002 ("TSFA"), as well as international instruments such as UNSC within their guidance documents for their anti-AML provisions.[46] These key pieces of legislation in Singapore include the:

[42] ibid.
[43] ibid.
[44] Project Benja, *An MAS Financial Sector Technology & Innovation (FSTI) Scheme Proof-of-Concept* (2020-2021) <https://stacs.io/wp-content/uploads/2021/05/Project-Benja-Public-2021.pdf> accessed 4 December 2022.
[45] Monetary Authority of Singapore, *MAS Partners the Industry to Pilot Use Cases in Digital Assets* (31 May 2022, Government of the Republic of Singapore) <https://www.mas.gov.sg/news/media-releases/2022/mas-partners-the-industry-to-pilot-use-cases-in-digital-assets> accessed 28 November 2022.
[46] Statista (n 30), para 3.2.2.

1. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992,
2. MAS Notice PSN01 'Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services),
3. the MAS Notice PSN02 'Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service)';
4. and the MAS Notice SFA04-N02 'Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Markets Intermediaries'.[47]

For digital payment tokens, obligations under the FSA require DDA custodians registered in Singapore to conduct regular risk assessment procedures, which includes customer and beneficiary due diligence.[48] Further, MAS has similarly informed these service providers that they have obligations to report suspicious transactions under AML regulations, and comply with sanctions against terrorism activities listed under the Combating the Finance of Terrorism ("CFT") provisions.[49] Where transactions are carried out by entities under CFT provisions, the TSFA similarly requires custodians to disclose these transactions to the MAS.[50]

These AML provisions are particularly thematic, given that they are largely contingent on obligations around the provisions of the licence granted to service provided. For instance, where these licences impose rather onerous disclosure obligations on DDA custodians, their AML framework becomes contingent on the appropriate verification of the identities of persons who operate on these custodians. Such seems to suggest a stringent top-down approach for custodians operating and providing services in Singapore. Similarly, to attempt to dissuade unlicensed DDA custodians from operating, the s.4(4) of the FSM has laid out particularly onerous fines for institutions who do not comply with these provisions.

Unfortunately, a majority of the provisions surrounding digital payment tokens in Singapore are silent on their compliance with international obligations and international law instruments; the exception being express reference to UNSC resolutions.[51] Nonetheless, s.15 FSM does note that the MAS has the final say on determining the compliance of DDA custodians with the State's international law obligations under the broader header of the "public interest". The MAS has recently exercised this power

[47] Kenneth George Pereire and Lin Yingxin, 'The Virtual Currency Regulation Review: Singapore' in Paul Anderson (ed), *The Virtual Currency Regulation Review* (The Law Reviews 2022).
[48] s.16 Financial Service and Markets Act 2022. More specifically, referenced in: Monetary Authority of Singapore, "Prevention of Money Laundering and Countering the Financing of Terrorism - Banks". (24 April 2015, MAS Notice 626). <https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/notices/AMLD/notice-626/MAS-Notice-626-last-revised-on-1-March-2022-1.pdf> accessed 25 November 2022.
[49] Statista (n 30). See also: s. 45 of the *Terrorism (Suppression of Financing) Act* 2002
[50] Cf s.16(3) of the *Finance and Securities Market Act* 2022.
[51] Statista (n 30), para 3.2.2.

following the global sanctions imposed against Russia, despite the lack of a UNSC resolution imposing sanctions on Russian authorities.[52] In effect, such requires DDA custodians to restrict their client's ability to transfer assets to Russian beneficiaries.[53] As such, it is evident that Singapore's mode of handling digital payment tokens is rather traditional, and falls along the lines of how sanctions are enforced on domestic companies within the physical world.

For digital securities governed by the SFA, the situation remains significantly simpler. While the FSA itself does not make express provisions for governing the trade of decentralised securities, the Singaporean Government makes blanket umbrella bans against the trading of these assets against sanctioned countries. For instance, global sanctions imposed against Russia include a blanket ban for financial institutions to create business relationships with the relevant Russian banks. On that basis, DDA-securities traders in Singapore would be unable to tap on decentralised tokenised securities based in Russia, such as the Atomyze token.[54] However, for countries sanctioned by UNSC resolutions, Singapore's domestic legislation enforcing these provisions operates differently. Sanctions against Iran,[55] Libya,[56] Yemen,[57] among other countries, do not mention a general ban for the use of DDA-securities. Perhaps this could be explained by the different economic developments these countries enjoy - Russia having a more significantly developed digital infrastructure and hence, requiring express provisions. Similarly, some of these countries have express bans on DDAs and do not embrace tokenised securities.[58] However, closer analysis of the imposed sanctions indicate that these are narrow targeted sanctions imposed by the country on certain individuals or activities. In that regard, the lack of express prohibitions for DDAs is thus unnecessary, and would fall outside its scope.

As a whole, Singapore's regulatory climate surrounding AML and compliance with economic sanctions of DDAs can be said to be twofold. First, the restriction of the trading of security-based DDAs seems to flow from their obligations to comply with overall international sanctions. Where international sanctions are broad, compliance with them requires the overall prohibition of trading on these platforms. This position holds true for

[52] Peace and Security, 'Russia blocks Security Council action on Ukraine' *UN news* (26 February 2022) <https://news.un.org/en/story/2022/02/1112802> accessed 29 November 2022.
[53] Monetary Authority of Singapore, *Targeted Financial Sanctions: Financial Measures in relation to Russia* <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions> accessed 2 December 2022; Ministry of Foreign Affairs, 'Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine' (5 March 2022, Government of Singapore) <https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions> accessed 2 December 2022.
[54] See, for instance, Éva Réka Keresztes and others, 'Exploratory Analysis of Blockchain Platforms in Supply Chain Management' (2022) 10(9) Economies, 206.
[55] United Nations Act (Chapter 339), United Nations (Sanctions - Iran) Regulations 2019.
[56] United Nations Act (Chapter 339), United Nations (Sanctions - Libya) Regulations 2021.
[57] United Nations Act (Chapter 339), United Nations (Sanctions - Yemen) Regulations 2015.
[58] Younis A Younis, Abdulsalam Sami and Salme Naje, 'Blockchain and Cryptocurrencies in Libya: A Study', ICEMIS'21: The 7th International Conference on Engineering & MIS 2021, New York, United States, October 2021) <https://dl.acm.org/doi/abs/10.1145/3492547.3492594> accessed 2 November 2021.

digital payment tokens, where blanket statements and regulations have been imposed on these DDAs custodians. Conversely, the lack of guidance found within domestic AML legislation indicates that the country is largely reliant on digital custodians conducting their independent due diligence in accordance with regulations, and only intervening in extreme cases. Such similarly follows the "wait-and-see" trend which the MAS has been practising on the distinctions between digital securities and payment tokens. After all, it cannot be denied that these sanctions are often only imposed in extreme and rare cases. Hence, such an approach may allow more flexibility for the MAS to provide appropriate guidance where necessary and at a short-term notice, but also give DDA custodians means for their own discretion. While concerns might arise pertaining to legal certainty, the MAS' current approach seems to indicate that the small nation State is attempting to best embrace this novel technology, albeit through centralising the ongoing decentralisation efforts

2.2 South Korea

2.2.1 The regulatory framework of DDAs in South Korea

Not unlike the Singaporean story, the Republic of Korea (South Korea) has a history of embracing technology at every step of its development. Although it had been regarded as one of the poorest nations in the world in the 1960s after the Korean War, the country's transformation into a high-tech economic leader in the region had prompted many to dub them "The Miracle on the Han River".[59] This development was largely attributed to then President Park Chung Hee. With the economy dominated by family-run conglomerates in the past,[60] then President Park worked with these families on a close personal level, providing them economic support in exchange for socio-political approval.[61] As a result, some of these conglomerates have now become household names, which includes technology-heavy firms Samsung, Hyundai and LG.[62] This similarly propelled South Korea's economy towards becoming one of the most respected across East Asia.

In the present day, South Korea has similarly adopted a mammoth role in DDAs. Prior to its collapse, South Korea formed the home-base for the Terra-LUNA token, which had

[59] Vincent Koen and others, 'Sustaining the Miracle on the Han River', (25 October 2021, Organization for Economic Co-operation and Development). <https://www.oecd.org/country/korea/thematic-focus/sustaining-the-miracle-on-the-han-river-103653fa/> accessed 3 December 2022.
[60] Eleanor Albert, 'South Korea's Chaebol Challenge' (4 May 2018, Council on Foreign Relations), <ahttps://www.cfr.org/backgrounder/south-koreas-chaebol-challenge> Accessed 3 December 2022.
[61] Pyŏng-guk Kim, Byung-Kook Kim and Ezra F Vogel, *The Park Chung Hee Era: The Transformation of South Korea* (Harvard University Press 2011).
[62] Terry Campbell and Phyllis Keys, 'Corporate governance in South Korea: the chaebol experience' (2002) 8(4) Journal of Corporate Finance 373 <https://doi.org/10.1016/S0929-1199(01)00049-9> Accessed 4 December 2022.

a market value of over USD $20 billion.[63] Similarly, recent initiatives by the legislature include the South Korea's Act on Reporting and Using Specified Financial Transaction information 2021 ("RSFTI") showcase its willingness to adapt in the financial sphere. The RSFTI currently forms the backbone of the legislature around DDAs in South Korea and provides the Taxonomy which the Republic uses in its subsequent legislation. The RSFTI is similarly seeking to pave the way for the upcoming Digital Assets Basic Act 2023 ("DABA") which will be the leading statutory instrument for the regulation of digital assets in South Korea.

While DABA remains the long-term plan, it is nonetheless worth looking at the framework which the RSFTI has set out for DDAs. Under the RSFTI, South Korea's taxonomy on DDAs designated the term "digital assets" as the umbrella term for all intangible assets. These include e-currencies, Central-Backed Digital Currencies ("CBDCs"), as well as Decentralised Autonomous Organisations ("DAOs"). Under these "digital assets", there is a further subset which has been dubbed "virtual assets". These virtual assets are where cryptocurrencies and NFTs are governed.[64] For Korea, such a distinction seems particularly important due to their use of "critical digital assets" within national security infrastructure.[65] Hence, for the remainder of the paper, the phrase DDAs when used in the context of South Korea's regulatory framework will refer to its use of "virtual assets". For further reference, the definition of "virtual assets" was particularly broad under the RSFTI, and reads as follows:

> "electronic certificates of economic value (with the exception of electronic currency, etc. as defined under the Electronic Financial Transactions Act) that can be traded or transferred electronically."[66]

However, what is particularly interesting within the DDA framework is that "virtual assets" seems to only cover NFTs and cryptocurrencies. While these are the most common forms of DDAs, modern DDAs can encompass a significantly wider range of assets. These include decentralised tokenised securities such as green bonds or commodities, distributed ledger technologies, non-convertible intangible assets, among other matters.[67] At first glance, it would seem that these assets would, by default, fall under the wide term of "virtual assets" under the RSFTI. However, they are instead covered by the Financial Investment Services and Capital Market Act ("FISCM"), which provides its own

[63] Riccardo De Blasis and others, 'Intelligent Design: Stablecoins (In)stability and Collateral During Market Turbulence' (30 June 2022). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217910> accessed 4 December 2022.
[64] Meejeong Hwanga, Kookheui Kwonb, 'Development of an Identification Method for Vital Digital Assets Selection on Nuclear Cyber Security'' (Transactions of the Korean Nuclear Society Spring Meeting, Jeju Island, Korea, 17-18 May 2018), 3 <https://www.kns.org/files/pre_paper/39/18S-134황미정.pdf> accessed 2 December 2022.
[65] Junyoung Son, Jonggyun Choi and Hyunsoo Yoon, 'New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants' (2019) 7 IEEE Access, 78379-78390
[66] s.3(3) Act on Reporting and Using Specified Financial Transaction information 2021.
[67] Andria van der Merwe, 'A Taxonomy of Cryptocurrencies and Other Digital Assets' (2021) 41(1) Review of Business 30.

sets of regulations to securities. As such, it becomes self-explanatory why commentators are concerned about the potential conflicting legislation would create unpredictability and legal uncertainty within the digital asset market within South Korea.[68] Nonetheless, if one were to look at the current President of South Korea, Suk-Yeol Yoon's election mandate which includes the regulation of DDAs, it would seem that "virtual assets" would exclude security tokens.[69] Hence, it is likely that security tokens within South Korean legislation would fall under the FISCM, and governed by the relevant securities legislation found within the State.

While South Korea's DDA framework remains significantly younger than Singapore's current approach, it nonetheless remains important to understand how these different tokens are governed within Korea, both for users and custodians. For DDA custodians, South Korea has adopted a similar position to Singapore, requiring mandatory registration of all virtual asset service providers ("VASP") under the Korean Financial Intelligence Unit. Upon registration, they will be granted a licence to operate within the Republic.[70] Unlike Singapore however, there seems to be less of a regulatory framework surrounding VASPs, with its core obligations merely to verify customer identity, report on suspicious transactions, and follow anti-money laundering guidelines.[71]

Perhaps most crucially for VASPs, the registration process requires compliance with the Korea Information Security Management System ("K-ISMS") under the Act on Promotion of Information and Communications Network Utilisation and Information Protections (as amended in 2008). The K-ISMS is a certification based on the industry standard ISO 27001:2002, managed by the Korea Internet and Security Agency that is meant to ensure adequate protection of personal data. The K-ISMS regulations further requires users to register their personal details on VASP sites, using a real-name verifiable account. Using this, the State can then act to ensure the sites' ability to protect the data from cyber-threats through this top-down system. Consequently, while adhering to K-ISMS then removes the layer of anonymity surrounding VASPs, it nonetheless provides an additional layer of protection for peer-to-peer transactions. However, it must be emphasised that adherence to the K-ISMS framework is not unique to cryptocurrency exchanges. Almost all

[68] Han-Jin Lee, Sung Yun Kang and Mooni Kim, 'Opening the floor for global discussions: regulatory transition around digital assets in South Korea' (International Financial Law Review, 30 September 2022) <https://www.iflr.com/article/2aowsnrfgsb8r3avrw075/sponsored/opening-the-floor-for-global-discussions-regulatory-transition-around-digital-assets-in-south-korea> accessed 2 December 2022.
[69] Ik-Hwan Cho, Young Man Huh and Bumkyu Sung, 'New Administration's National Agenda on Financial Services Sector' (11 May 2021, Kim & Chang) <https://www.kimchang.com/cn/insights/detail.kc?sch_section=4&idx=24980> accessed 1 December 2022.
[70] Keundug Park and Heung-Youl Yoom, 'Proposal for Customer Identification Service Model Based on Distributed Ledger Technology to Transfer Virtual Assets' (2021) 5(3) Big Data Cognitive Computing 31 <https://doi.org/10.3390/bdcc5030031> accessed 1 December 2022.
[71] ibid.

sites which stores personal data, such as Amazon,[72] Google,[73] and Microsoft[74] all require K-ISMS compliance. Hence, such regulations form the core minimum operating requirements in Korea.

This is undoubtedly a stark departure from the full disclosure and reporting obligations which Singapore and the MAS imposes on digital payment token providers. Nonetheless, South Korea seems to wish to tap upon the "decentralised" nature of these technologies as much as possible; hence, imposing minimum obligations as opposed to a full regulatory regime. Interestingly, it seems that the overall notion of decentralisation is, in Korean culture, linked to the popular view on democracy. The 'more' decentralised something is, the more democratic the people believe it to be.[75] As such, the country's rather lax stance towards managing DDAs seems like a natural conclusion.

2.2.2 AML laws and economic sanctions of DDAs in South Korea

Despite the minimal regulatory interference which South Korea has on virtual assets providers, the emphasis on AML and compliance with sanctions remains a core pillar within South Korea's regulatory framework. Undoubtedly, attempts to preserve the decentralised nature of these assets despite them being designed to undermine these policies, and still finding a balance for strong AML policies, and sanction-compliant framework is to be applauded.

Beginning with VASP's obligations, the RSFTI was designed around strengthening AML provisions and international economic sanctions within the realm of virtual assets, while similarly ensuring VASP compliance with these regulations. Under the RSFTI, there are two core obligations for VASPs. Firstly, the "Travel Rule", for VASPs to record the originator and beneficiary's information in a transfer of DDAs.[76] Secondly, the "segregation rule", requiring VASPs should isolate these recorded transactions where they are suspicious in nature.[77] These rules operate in tandem and seek to ensure a degree of anonymity within these transactions, but also ensuring no foul play is amidst.

Beginning first with the Travel Rule, this essentially requires VASPs to record transactions about the virtual asset transfer, providing the virtual asset originator's

[72] See at: <https://aws.amazon.com/compliance/k-isms/> accessed 27 November 2022.
[73] See at: <https://cloud.google.com/security/compliance/k-isms> accessed 27 November 2022.
[74] See at: <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-korea-k-isms> accessed 27 November 2022.
[75] Jae Hyun Lee and Jaekwon Suh, 'Decentralisation and government trust in South Korea: Distinguishing local government trust from national government trust' (2021) 8(1) Asia & the Pacific Policy Studies 68 <https://doi.org/10.1002/app5.317> accessed 2 December 2022; Jong Soon Lee, 'The politics of decentralisation in Korea', (1996) 22(3) Local Government Studies 60 <https://doi.org/10.1080/03003939608433830> accessed 3 December 2022.
[76] Kibae Kim, 'Global Standards Mapping Initiative (GSMI 2.0): Standalone Paper, South Korea' (November 2021, Global Blockchain Business Council), 5.
[77] Lee & Ko, 'Amended Act on Reporting And Using Specified Financial Transaction Information Now Governs Virtaul Assets' (13 March 2020, Legal500) <https://www.legal500.com/developments/thought-leadership/amended-act-on-reporting-and-using-specified-financial-transaction-information-now-governs-virtual-assets/> accessed 3 December 2022.

information about their beneficiary as a means for information sharing.[78] This is starkly different from obligations to record and report such information to a top-down body, and leaves power in the hands of the citizens rather than the governments. Yet, it seems that the obligation is reversed for beneficiaries. If a transaction is suspicious, beneficiaries have an obligation to report these transactions to the relevant authorities under the RSFTI.[79] When these suspicious transactions are reported, VASPs then trace the relevant wallet addresses and wallet-to-wallet transactions history to match them with real-name-verification obligations under the K-ISMS framework, then allowing for surveillance units to trace the transactions of the senders.[80] Such undoubtedly exemplifies the level of trust which the Korean government has with its people. After all, respect goes both ways. Where the government seems to trust the populace, it becomes natural that the populace returns the favour.

In that regard, one thus easily identifies the importance of the "segregation rule" under the RSFTI. Following reporting obligations, it seems that the State is rather careful to ensure that only key personal information is reported; hence, segregating the suspicious activity from the remainder of the records kept by VSAP. This is similarly exemplified in the process that VASPs use to track these transactions. Despite having and requiring real-name-verification for users who sign up, VASPs only when there is a notion of suspicious activities. Hence, this protects the information of others on the platform, while allowing for a degree of regulatory oversight with minimal interference in the virtual asset marketplace.

Before delving into the interaction between virtual asset regulations and sanctions regime, it is similarly quintessential to understand South Korea's sanctions regime independently. As a State with a history of imposing sanctions on their not-too-distant neighbour - the Democratic Republic of Korea all the way back since the Korean War,[81] one undoubtedly expects this regime to be a firm one. Indeed, under the Article 5 of the Foreign Trade Act, the Minister for Trade, Industry and Economy has the discretion to impose general and specific trade embargos against nations "when it is necessary to perform duties to maintain international peace and security under treaties on trade…and generally accepted international laws and regulations".[82] An emphasis should be had on the latter words of international law, which shows respect for UNSC resolutions that impose sanctions, and similarly abiding by them when necessary. Similarly, financial sanctions can be imposed by the Minister of Strategy and Finance under the "Guidelines for payment and receipt permits for the Implementation of Obligations for the

[78] See at: <https://www.fsc.go.kr/eng/pr010101/22526> accessed 4 December 2022.
[79] National Assembly of Korea, *Act on Reporting and Using Specific Financial Transaction Information*, No 17299, Amended on 19 May 2020, Enforced on 20 May 2020.
[80] (n 75).
[81] Nazanin Zadeh-Cummings and Lauren Harris, 'The Impact of Sanctions against North Korea on Humanitarian Aid' (2020) 2(1) Journal of Humanitarian Affairs 9 <https://doi.org/10.7227/JHA.033> accessed 1 December 2022.
[82] Foreign Trade Act, Art 5(4). Also note the additional requirement of ensuring the maintenance of international law. Translated at <https://elaw.klri.re.kr/eng_service/lawView.do?hseq=37529&lang=ENG> accessed 2 December 2022.

Maintenance of International Peace and Security.".[83] Though labelled as "Guidelines", this remains an enforceable derivative legislation which imposes punitive fines when there are prohibited transactions with a term of imprisonment (maximum 3 years) or a fine (maximum KRW 200 million).[84]

Unfortunately, there seems to be a dearth in the legislation of economic sanctions and DDAs; there are no mentions of their applicability within the respective acts which governs virtual and digital assets. While Article 15(2) of the RSFTI does make a brief note about disallowing transactions that finance terrorism, as well as abiding by recommendations from international organisations with regards to virtual assets, such an approach seems too general, and not specific towards virtual assets. This top-down blanket approach by the government also does not make itself privy to the uniqueness of virtual asset technologies, such as blockchain-based transparency.[85] In that regard, an assumption can be reasonable that these sanctions would operate similar to those in Singapore, falling under the Minister of Strategy and Finance and the Financial Service Commission where these assets are treated as financial instruments.[86] Applying this to South Korea's virtual asset infrastructure, any decisions pertaining to the use of sanctions on virtual assets would likely require a harmonised approach to be taken by all VASPs, as well as the Minister for Trade, Industry and Economy to similarly enforce general trade sanctions and prevent the exchange of virtual assets for tangible goods. Hence, although decentralisation preserves characteristics, a unified approach must be adopted across these decentralised bodies.

Overall, the provisions surrounding AML regulations, and economic sanctions of virtual assets seem to be in their infancy in South Korea. Nonetheless, the strong framework which the country has set for itself has placed it on the right path towards ensuring compliance with their relevant international law obligations. Nonetheless, more work is to be had in the field of compliance with economic sanctions to ensure appropriate legal certainty within international law obligations. After all, user-trust can only go so far.

[83] Financial Action Task Force, *Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism*, (26 June 2009, Organisation for Economic-Cooperation and Development) 49 <https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Korea.pdf> accessed 21 March 2023.

[84] *Foreign Exchange Transactions Act*, Art 27(1)-(8). Translated at <https://law.go.kr/LSW/lsInfoP.do?lsiSeq=191033&viewCls=engLsInfoR&urlMode=engLsInfoR> accessed 2 December 2022.

[85] Juan F Galvez, Juan C Mejuto and Jesus Simal-Gandara, 'Future challenges on the use of blockchain for food traceability analysis' (2018) 107 TrAC Trends in Analytical Chemistry 222.

[86] YangJay-Son, Kim Tae Yeun and Lee Tae Ho, 'Banking Regulation in South Korea: Overview'. (Thomson Reuters Practical Law, 1 November 2022) <https://uk.practicallaw.thomsonreuters.com/w-032-4691?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 3 December 2022.

2.3 Hong Kong

2.3.1. The regulatory framework of DDAs in Hong Kong

The Special Administrative Region of Hong Kong ("HKSAR") has a rather unique position in its overall governance structure. Originally a British Colony, the governance of the region was transferred to the People's Republic of China ("PRC") on the 1st of July 1997.[87] However, as part of the agreement, HKSAR was allowed to have its own economic and governance independent from mainland PRC. As a result, the HKSAR economy saw significant success as foreign investors viewed it as a pathway to expanding in Asia while China was still opening up.[88]

As a result, the influx of western influence had similarly brought an advent of technology to HKSAR, in turn, fostering a strong culture of embracing new developments to promote economic development. Even in its early days, the USD $5 Billion Innovation and Technology Fund established in 1999 by the government sought to promote the integration of technology. This fund subsequently continued and even expanded, with over USD $40 Billion injected as of July 2022.[89]

Recently, there has even been a strong push towards working with mainland PRC and facilitating mutual development between the regions. The Lok Ma Chau Loop is one example of this - currently being developed as part of the Hong Kong-Shenzhen Innovation and Technology Park initiative to further push for greater technological advancements and sharing of information between the economies.[90] As such, it should be a foregone conclusion that HKSAR is particularly receptive towards DDAs, with public private partnerships set up to explore and take advantage of these new technologies in a sustainable manner.[91]

The regulatory framework in HKSAR is led by the Financial Action Task Force, which has just passed the new Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 ("MLCTF") around DDAs, coming into force on 1 January 2023.[92] In essence, the MLCTF adopts a similar definition of DDAs to those in Korea. It uses the term "virtual assets" and defines them as an intangible representation of an asset which has economic value. More specifically, the Art 53ZRA of the MLCTF notes that a virtual asset is defined as:

[87] Joint Declaration on the question of Hong Kong. 1985.
[88] Amy Ang, 'Hong Kong: Securities Regulation after 1997 Handover' (CORE publishing, 1 January 2020) <https://core.ac.uk/download/pdf/8766482.pdf> accessed 2 December 2022.
[89] Innovation, Technology and Industry Bureau, *Hong Kong: The Facts. Innovation, Technology and Industry* (July 2022, Gov.Hk) <https://www.gov.hk/en/about/abouthk/factsheets/docs/technology.pdf> accessed 5 December 2022.
[90] See at: <https://www.hsitp.org/en/about-us/index.html> accessed 27 November 2022.
[91] Project Genesis by the government of Hong Kong and the BIS Innovation Hub: <https://www.bis.org/publ/othp58.htm> accessed 1 December 2022.
[92] Gov.Hk, *Government welcomes passage of Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022*. (7 December 2022, Gov.HK Press Release) <https://www.info.gov.hk/gia/general/202212/07/P2022120700263.htm> accessed 8 December 2022.

(1) In this Ordinance -
  (a) A cryptographically secured digital representation of value that
    (i) Is expressed as a unit of account or a store of economic value;
    (ii) Either -
      A) Is used, or is intended to be used, as a medium of exchange accepted by the public, for any one or more of the following purposes -
        I) Payment for goods or services;
        II) Discharge of a debt;
        III) Investment; or
      B) Provides rights, eligibility or access to vote on the management, administration or governance of the affairs in connection with, or to vote on any change of the terms of any arrangement applicable to, any cryptographically secured digital representation of value;
    (iii) Can be transferred, stored or traded electronically; and
    (iv) Satisfies other characteristics prescribed by the Commission under subsection (3)(a); or
  (b) A digital representation of value prescribed as a virtual asset by notice published under subsection (4)(a)
(2) A digital representation of value is excluded from the definition of *VA* in subsection (1) if -
  (a) It -
    (i) Is-
      A) Issued by a central bank, or by an entity that performs the functions of a central bank or by an entity authorised by a central bank on its behalf; or
      B) Issued by a government of a jurisdiction, or by an entity authorised by the government of a jurisdiction and acting pursuant to an authority to issue currency in that jurisdiction;
    (ii) Is a limited purpose digital token;
    (iii) Constitutes securities or a futures contract;
    (iv) Constitutes any float of SVF deposit of a stored value facility as defined by section 2 of the Payment Systems and Stored Value Facilities Ordinance (Cap. 584); or
    (v) Satisfies other characteristics prescribed by the Commission under the subsection (3)(b); or
  (b) It is a digital representation of value prescribed not to be a virtual asset by notice published under subsection (4)(b)

This is a particularly extensive definition of virtual assets under the MCLTF, which is undoubtedly to be applauded. Within it, there are clear signals that indicate HKSAR is embracing VAs. Art 53ZRA(1)(a)(A)(ii)(b) shows an understanding of on-chain governance mechanisms which have been employed recently as a mechanism for decentralised governance.[93] Further, it is also worth noting that the use of virtual assets as decentralised debt instruments, as well as investment instruments, are all found within the definition of virtual assets under Art 53ZRA(1)(a)(A)(ii)(a)(II)-(III). This is a stark difference from the positions of Singapore and South Korea where these financial instruments are governed by securities-based legislation.

Finally, it is similarly worth noting elements which are excluded from the definition of a virtual asset. Art 53ZRA(2)(a)(i) which covers CBDCs, and Art 53ZRA(2)(a)(iii) on securities and future contracts are of relevance. On the former, this is a clear recognition that these central bank digital currencies are a distinct form of virtual assets; Singapore and South Korea are currently silent on its classification. Of the latter however, a distinction seems to have been made between the use of these assets by investors (Art 53ZRA(1)(a)(A)(ii)(a)(II)-(III)), and the design of the assets by issuers. When issuers engage in the dissemination of virtual assets, such as through Initial Coin Offering, these assets would be considered to be securities and outside the scope of virtual assets.[94] Conversely, when such assets are traded by users at a later stage, they would constitute an investment under Art 53ZRA(1)(a)(A)(ii)(a)(II). Unfortunately, such a distinction seems to create some uncertainty within the current regulatory framework, particularly in the realm of the secondary markets on the applicable laws. Nonetheless, the practical reality is that service providers do not engage in the initial setting up and issuance of tokens, but rather, merely act as a custodian when these companies engage in such activities. Hence, while clarity is preferred, the current situation remains adequate given the circumstances.

Overall, HKSAR's legal framework surrounding the use of digital assets is indeed robust. Accounting for technological developments and understanding the nuances behind DDAs are efforts that should be applauded. Indeed, the distinctions made within virtual assets between its issuance and subsequent use creates a practical framework, clearly delineating the role of VASPs and private entities within HKSAR.

2.3.2 AML laws and economic sanctions of DDAs in Hong Kong

With such a broad definition of DDAs in HKSAR under the all-encompassing term "virtual assets", there would inevitably be obligations and requirements for VASPs to comply with. These licensing provisions can be found under Art 53ZRH - 53ZRS. VASPs operating within

[93] Wessel Reijers and others, 'Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies' (2021) 40 Tapoi 821 <https://doi.org/10.1007/s11245-018-9626-5> accessed 8 December 2022.
[94] Securities & Futures Commission of Hong Kong, *Regulatory approaches to Authorized Institutions' interface with Virtual Assets and Virtual Asset Service Providers*, (5 September 2017, IOSCO Publishing) <https://www.iosco.org/library/ico-statements/Hong%20Kong%20-%20SFC%20-%20Statement%20on%20initial%20coin%20offerings.pdf> accessed 1 December 2022.

HKSAR are required to apply for a licence under Art 53ZRK, which contains requirements for the granting of a licence for the operation of a VASP. Broadly, they include, AML and anti-terrorism financing policies, compliance with reporting and disclosure obligations, cyber security, appropriate risk management regulations, among others.[95] These form the baseline requirements for VASPs operating in HKSAR. However, Art 53ZRK is not an exhaustive list, and the regulatory authority has the general discretion to consider a myriad of other factors before granting licence for VASPs to operate.

It is similarly worth additionally considering the circular put out by the HKSAR Monetary Authority, which highlighted three core themes for the regulatory approach which HKSAR has been taking with regard to VASPs - supervision, AML and financial crime risk, and investor protections. For the purposes of this paper, only AML provisions will be considered.[96] Under these AML provisions, there are two core obligations which VASPs have to fulfil. First, VASPs are required to require users to engage in DDA activities through their verified bank accounts. This is akin to real-name verification used in South Korea, and identification requirements in Singapore. Second, VASPs are required to maintain business relationships with banks for the purpose of risk-assessments, customer and VASP due diligence, and maintain capital requirements under traditional banking legislations.[97] Such links VASPs to traditional banks, hence allowing greater scrutiny when it comes to user's activities in the realm of DDAs while also giving VASPs the opportunity to tap on the greater resources which these banks have. In that regard, such similarly ensures greater compliance mechanisms with international standards for AML protection.[98] Indeed, there are strong indications that banks would have a greater role to play in the realm of DDAs. Studies around the incorporation of the SWIFT banking network into the realm of DDAs are currently ongoing.[99] However, where the legislation requires VASPs to actively engage with banks, such integration would undoubtedly promote greater information sharing and capacity building to strengthen the overall AML framework.

From this framework, HKSAR's policies towards the AML framework can be said to focus on the implementation of gap-filling mechanisms. Where VASPs act as digital custodians and operate as trading platforms, they often have their own policies and security measures in place to prevent illegal and illicit activities. However, to harmonise these policies with national and international obligations, mutual cooperation and between VASPs and larger institutions would allow VASPs to maintain a level of discretion with their technical

[95] Art 53ZRK(5) Anti Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022.
[96] Hong Kong Monetary Authority, *Regulatory approaches to Authorized Institutions' interface with 1 Providers*, (Government of Hong Kong, 28 January 2022) <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220128e3.pdf> accessed 1 December 2022.
[97] Securities & Futures Commission of Hong Kong (n 94).
[98] Financial Action Task Force, 'Easy Guide to FATF Standards and Methodology: Virtual Assets: What, When, How?' (undated, FATF-Gafi) <https://www.fatf-gafi.org/media/fatf/documents/bulletin/fatf-booklet_va.pdf> accessed 1 December 2022.
[99] Practical Law Finance, 'SWIFT Reports: CBDCs and Tokenized Assets Can Integrate into International Financial Ecosystem' (Thomson Reuters Practical Law, 12 October 2022) <https://ca.practicallaw.thomsonreuters.com/w-037-2021?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 30 November 2022.

expertise in the matter, while similarly strengthening the overall regulatory framework. This two-pronged approach is similarly reflected within their policy paper to tap into the existing financial markets worth over US$4.5 Trillion.[100] In that regard, the role of VASPs is thus exemplified within HKSAR's markets, with greater discretion placed upon them.

While the laws around virtual assets and DDAs within HKSAR are certain, the position with sanctions is particularly unique due to its relations with the People's Republic of China ("PRC"). Under the original Sino-British Agreement, HKSAR was allowed a degree of autonomy and independence in their legislative powers.[101] As a result, HKSAR cannot, as its own independent State, unilaterally sanction another. Instead, Chinese foreign policy is adopted. In that regard, the regime for sanctions in Hong Kong falls under the United Nations Sanctions Ordinance (Cap. 537) and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) which covers sanctions imposed under obligations to the United Nations. However, outside of these legislations, there is a dearth in the imposition of sanctions or trade embargos outside of these obligations. Further, it is similarly key to note that these Acts expressly exclude sanctions made against the PRC. Hence, HKSAR should be said to have limited powers in this area.

However, turning to the PRC's foreign policy and their history of sanctions related to DDAs, one would inevitably observe a particularly contradictory position if compared to HKSAR. The PRC has outlawed the use of DDAs in its entirety.[102] Instead, all intangible currencies were replaced by the CBDCs currency known as the "e-CNY".[103] Yet, in HKSAR, CBDCs are excluded from the definition of a virtual asset.[104] Hence, there seems to be a large conflict-of-laws position surrounding the virtual assets which creates legal uncertainty. On one interpretation, one can presume that virtual assets are completely outlawed, with international transactions illegal. On the other through a narrower lens, virtual assets fall outside the scope of the law of sanctions within the PRC. Undoubtedly, the latter position is untenable, and creates numerous gaps in the law for many to bypass sanctions. However, the former position also conflicts with HKSAR's pro-digital asset policies. In that regard, one could perhaps identify that the reason for VASPs to have such wide powers in HKSAR is to allow VASPs discretion to abide by international obligations independent of the domestic laws. Further, where VASPs work with banks who similarly often operate transnationally and across jurisdictions, they would be able to tap onto the regulatory framework in foreign jurisdictions. In that sense, VASPs would be able to tap

[100] Financial Service Treasury Bureau, *Policy Statement on Development of Virtual Assets in Hong Kong*, (October 2022, Government of Hong Kong) <https://gia.info.gov.hk/general/202210/31/P2022103000454_404805_1_1667173469522.pdf> accessed 29 November 2022.
[101] Galvez et al. (n 85).
[102] Cong Yun and Yun Chen, 'The impact of regulatory ban on connectedness of cryptocurrency market' (2022) Applied Economics Letters, <https://doi.org/10.1080/13504851.2022.2141440> accessed 28 November 2022
[103] Jiaying Jiang and Karman Lucero, 'Background and Implications of China's Central Bank Digital Currency: E-CNY' (11 January 11 2021) <http://dx.doi.org/10.2139/ssrn.3774479> accessed 1 December 2022.
[104] Art 53ZRH (2)(a)(i)(A) Anti Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022.

upon international obligations in foreign jurisdictions, and transpose these regulations towards end-users in HKSAR. Hence, the wide discretion which VASP and banks enjoy within HKSAR may be preferable given the unique position which HKSAR has.

As a whole, one can thus sum up HKSAR's position with regards to DDAs as one which is rather broad. HKSAR seems to be looking to prioritise and embrace the technology behind DDAs. The trend seems to follow that they believe VASPs to be in the best position to determine their independent appropriate risk-management for AML and sanction legislations. Hence, the emphasis is placed on private due diligence obligations. Conversely, there are similar obligations for these VASPs to work with larger financial institutions to encourage capacity building in AML, as well as compliance with international law obligations through tapping on these transnational corporations.

2.4 Chinese Taipei

2.4.1 The regulatory framework of DDAs in Chinese Taipei

At first glance, Chinese Taipei seems to be in the same boat as HKSAR - its position in international law is in itself unique and largely complex, enjoying greater autonomy but also greater conflicts with the PRC than that of HKSAR. Beginning with a brief history,, the Qing Dynasty was overthrown by the Kuomintang Party in 1912, led by Chiang Kai Shek. In its wake, they formed the Republic of China.[105] Fast forward to 1927, the Chinese Communist Party declared a civil war against the Kuomintang, forcing them to flee in 1949 to a neighbouring offshore island known as Formosa to establish their own government.[106] Later that year, on 1 October 1949, the Kuomintang declared Formosa as its independent country, under the original banner of the Republic of China, forming Taiwan.[107] However, to this day, the PRC has not recognised this claim; conversely, it forms part of its foreign policy that countries dealing with the PRC should similarly reject recognition of Taiwan, requiring the international community to dub it "Chinese Taipei".[108] Despite the ongoing hostilities and political tension which lasts to this day,[109] the PRC has seemingly left Chinese Taipei largely alone,[110] allowing them to develop their own robust infrastructure through the years.

As a result of this period of autonomous governance, Chinese Taipei has flourished economically, growing to become the 22nd largest GDP in the world boosted by its world-

[105] Xiaoyuan Liu, 'Chiang Kai-Shek's (Invisible) Marathon to the West' (2010) 17(1) Chinese Historical Review 24 <https://doi.org/10.1179/tcr.2010.17.1.24> accessed 30 november 2022.
[106] Michael Lynch, *The Chinese Civil War: 1945-1949* (Bloomsbury Publishing 2022).
[107] ibid.
[108] Christopher Hughes, *Taiwan and Chinese Nationalism* (Routledge Publishing 1997).
[109] Yinghua He, Ulf Nielsson and Yonglei Wang, 'Hurting without hitting: The economic cost of political tension' (2017) 51(C) Journal of International Financial Markets, Institutions and Money 106.
[110] ibid.

class semiconductor industry and innovation incubators.[111] Hence, it is not unfamiliar to the role of modern technological developments. In 2013, merely five years after Bitcoin's release when the asset was only valued at USD $350 each, the central bank in Chinese Taipei was quick to issue a press release indicating that crypto assets will fall under the banner of "virtual commodity".[112] Subsequently that year, banks were disallowed from allowing individuals to trade crypto-assets.[113] In that regard, the early years saw a significant degree of scepticism towards the use of these assets by Chinese Taipei. This scepticism has seemingly carried over to the modern era, where the economy has recently announced plans to disallow the purchasing of cryptocurrencies with credit cards.[114] In that regard, one inevitably sees the reluctance of the economy to engage in this novel financial technology.

It was, however, only recently in 2019 at the Asia Blockchain Summit, that Taiwenese legislator Jason Hsu announced the country's plans to become a "crypto-nation".[115] Following that announcement, Chinese Taipei revamped its legislation completely, introducing a new framework for DDAs in the country. Indeed, VASPs within the region were governed to fall under the broader term "financial institutions" under the amendments to the Money Laundering Control Act ("MCLA"). Under Art 5, this placed VASPs in the same operating conditions as traditional banks, requiring them to implement internal control and audit systems, risk assessment reports, as well as traditional AML and terrorist financing legislation.[116] Particularly notably however, there are no specific rules or regulations for VASPs to be registered or licensed in Chinese Taipei; instead registration and licensing requirements for VASP fall under the general requirements for financial institutions.[117] Instead, the position when it comes to DDAs within Chinese Taipei is largely focused on supervision of AML and sanction-compliance, rather than overall regulatory oversight.[118]

Unfortunately, apart from this Chinese Taipei's position around DDAs, as well as an overall taxonomy of DDAs the issue seems rather lacklustre. The government has made no

[111] John Mathews and Mei-Chih Hu, 'Enhancing the Role of Universities in Building National Innovative Capacity in Asia: The Case of Taiwan' (2007) 35(6) World Development 1005
[112] UK Jurisdiction Taskforce (n 37).
[113] ibid.
[114] Sandali Handagama, 'Taiwan Set to Ban Crypto Purchases Using Credit Cards: Report' (22 July 2022). <https://www.coindesk.com/policy/2022/07/22/taiwan-set-to-ban-crypto-purchases-using-credit-cards-report/> accessed 29 November 2022.
[115] Rachel Wolfson, 'Crypto Congressman Jason Hsu On Taiwan Becoming A Blockchain Island And Crypto Nation' (*Forbes*, 29 August 2018) <https://www.forbes.com/sites/rachelwolfson/2018/08/29/crypto-congressman-jason-hsu-on-taiwan-becoming-a-blockchain-island-and-crypto-nation/?sh=4490a0ec49b7> accessed 3 December 2022.
[116] For a translated version, accessed at <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131> accessed 6 December 2022.
[117] See, a list of 24 VASP service providers licensed under the rules for financial institutions at <https://www.fsc.gov.tw/userfiles/file/(111_9_2更新)已完成洗錢防制法令遵循聲明的虛擬通貨平台業者名單.pdf> accessed 2 December 2022.
[118] Cheng Hwa Lee, Heng-Li Yang and Shiang-Lin Lin, 'The Key Evaluation Criteria of Blockchain Technology Implementation' (2021) 24(4) 科技管理學刊 [Journal of Science and Technology Management] 1

indication on establishing a formal definition for DDAs, but rather has taken a negative approach to define security tokens, and having everything outside its scope to form "virtual commodities".[119] More recent legislation in the 2021 Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction ("RGAVCT") similarly takes a broad approach. In particular, Art 2(2) reads:

> 2. "A virtual currency" refers to a digital representation of value with the use of cryptography and distributed ledger technology or other similar technology that can be digitally stored, exchanged, or transferred, and can be used for payment or investment purposes. However, virtual currencies do not include digital representations of NTD, foreign currencies, currencies issued by Mainland China, Hong Kong, or Macao, securities, and other financial assets issued in accordance with laws.

This definition is particularly broad and general, not really reflecting the nuances of DDAs, instead, placing great emphasis on the technology which is used in the issuance of these assets. However, there are greater nuances when it comes to DDAs. For instance, CBDCs which run on these technologies are inherently covered by this legislation despite having a fundamentally different characteristic entirely, and treated differently across other jurisdictions. This trend seems to follow the publicity which the Taiwanese media has given to DDAs, where a majority of its comments around DDAs were made around the umbrella term of cryptocurrencies such as Bitcoin, rather than modern developments surrounding DDAs.[120] As such, and perhaps owing to the general infamy of cryptocurrencies,[121] the full nature of DDAs has not been fully appreciated by the economy. Even domestic commentators have called for more robust developments in the field of DDAs.[122] Hopefully however, this would similarly serve as a wake up call for the economy to better develop its DDA-based infrastructure, less it gets left behind by the rest of the region.

In that regard, one can say that the Chinese Taipei economy still seems to be finding its footing and position over the application of DDAs. While certain members of the

[119] Abe Sung, Eddie Hsieung, 'Cryptoassets & Blockchain in Taiwan' (*Lexology*, 19 December 2019), <https://www.lexology.com/library/detail.aspx?g=75c285a8-d738-4052-b1a3-bcface3d31d4> accessed 2 December 2022.

[120] Hsin-Ke Lu and others, 'A study on adoption of bitcoin in Taiwan: using big data analysis of social media' (International Conference on Communication and Information Processing, November 2017), 32. <https://doi.org/10.1145/3162957.3163046> accessed 3 December 2022.

[121] Gourang Aggarwal and others, 'Understanding the Social Factors Affecting the Cryptocurrency Market' (International Conference for Internet Technology and Secured Transactions). <https://doi.org/10.48550/arXiv.1901.06245> accessed 1 December 2022.

[122] Editorial, *Nation lags world in crypto controls* (21 November 2022), <https://www.taipeitimes.com/News/editorials/archives/2022/11/21/2003789312> accessed 2 December 2022.

legislature might be intrigued by the idea of embracing these new technologies,[123] the overall position seems to indicate significant reluctance of incorporating DDAs into the general economic ecosystem. Hence, it would seem that Chinese Taipei has a limited role in DDAs.

2.4.2. AML laws and economic sanctions of DDAs in Chinese Taipei

While not much can be said surrounding the treatment by regulators and policymakers in Chinese Taipei, their focus on AML provisions is nothing to scoff at. Indeed, the treatment of VASPs under the wider category of financial instruments undoubtedly allows the economy to use a tried and tested system for the regulation of this new industry.[124] Such similarly allows for a more certain legal framework, for both legislators and lawyers with experience in this field, but also for end-users who would be familiar with these legislations.

The current MCLA framework for financial institutions in Chinese Taipei imposes the following obligations against Financial Institutions:

1. Maintenance of records of transactions (Art 8), alongside reporting obligations (Art 9)
2. Reporting suspicious transactions (Art 10)
3. International cooperation (Art 11)

It must be emphasised that these regulations are not unique to DDAs, but apply to all financial institutions operating in the economy. What seems intriguing however, is that these provisions fall into a similar category as the legislation put by Singapore. In essence, by grouping VASPs together with financial institutions, it promotes a top-down governance of DDAs, which seems to frustrate the notion of "decentralisation" of these assets. For instance, in the maintenance of records and transactions, Art 8 of the MLCF is particularly detailed to require financial institutions to maintain these transactions for "at least five years". However, it is silent on the methods of record keeping, instead, looking to "consult with relevant industry associations" to determine the scope of the record. For DDAs however, this may create significant controversy over the scope of the records, and whether they would include an individual's personal and sensitive information. In that sense, two conflicting approaches can be adopted: first, full disclosure of these personal information, using real world verification data obtained under due diligence provisions under Art 7. Alternatively, it could adopt the position of South Korea, and record the unique wallet addresses to preserve individuals' data, and only match wallet details to real world data when a transaction is deemed suspicious. In that regard, there is a significant degree of uncertainty in the strength of AML laws in Chinese Taipei.

[123] UK Jurisdiction Taskforce (n 37).
[124] Under Article 5(2) of Money Laundering Control Act, there is an express requirement that virtual asset service providers are subject to similar rules and regulations as traditional financial institutions.

There was an effort to answer these questions by Chinese Taipei. Art 7(1) of the RGAVCT specifies that customer due diligence includes a reporting of the transactions from both the originating party, and the beneficiary. Art 7(2) then goes further to explain that the official national identification number, address, date and place of birth, and wallet information should be included in the report. This is indeed a positive first step for regulatory initiatives for DDAs in Chinese Taipei. However, the questions regarding the extent of the reports submitted to the relevant authorities, whether the specific transaction chain, or the entire transaction history of an individual deemed suspicious, remains unanswered. Further, the legislation is similarly silent on how this personal information would be treated by the relevant authorities. In that sense, one can conclude that the Taiwanese position is similar to that in Singapore.

A further comment should be made about the role of sanctions by Chinese Taipei, especially given its unique position in international law. Unlike HKSAR, Chinese Taipei has its own independent regime of enforcing sanctions. Most recently, following the Ukrainian invasion, Chinese Taipei has imposed similar sanctions to the Western world,[125] whereas the PRC has remained silent and neutral on the issue. Similarly, it seems evident that Chinese Taipei is acting compliant with UNSC sanctions, despite the region not being part of the international organisation.[126] While it is hopeful that Chinese Taipei is independently to be following the trends and ensuring compliance in international law despite being in a grey area itself, the dearth of literature, coupled with partial recognition of the State,[127] indicates that the imposition of sanctions are largely voluntary.

The law however, is equally murky when it comes to DDAs in Chinese Taipei. Not only is the MCLA silent on the position of sanctions, especially with regard to DDAs, but there seems to be a dearth in the legislative action surrounding sanctions of DDAs in Taiwan. The only reference to "sanctions" can be found in Art 4(7) of the RGAVCT, that prevents VASPs or DDA custodians from engaging in business relations with organisations under the Counter-Terrorism Financing Act. However, Art 4 of this Counter-Terrorism Financing Act merely focuses on targeted sanctions, as opposed to general trade sanctions made against another sovereign nation. In that sense however, one can make a reasonable assumption that under Art 4(7) of the RGAVCT, the cessation of business relationships would extend to individuals or organisations of a sanctioned country. This interpretation should follow Art 1 of the Counter-Terrorism Financing Act on the purpose of sanctions in general, namely, the "[preservation] of international security, [and the protection of] fundamental human rights".

[125] Ministry of Foreign Affairs fort the Republic of China (Taiwan), *The Republic of China (Taiwan) government strongly condemns Russia's invasion of Ukraine in violation of the UN Charter, joins international economic sanctions against Russia*, (25 February 2022, Government of the Republic of China (Taiwan) <https://en.mofa.gov.tw/News_Content.aspx?n=1328&s=97420> accessed 2 December 2022.
[126] Reuters Staff, *Taiwan tells U.S. it is complying with North Korea sanctions,* (19 May 2020 Reuters). <https://www.reuters.com/article/us-northkorea-missiles-taiwan-usa-idUSKBN22V0F6> accessed 3 December 2022.
[127] Randall Newnham, 'Embassies for Sale: The Purchase of Diplomatic Recognition by West Germany, Taiwan and South Korea', (2000) 37 International Politics, 259.

As a whole, it is rather unfortunate that there is a significant dearth of legislative action around the role of DDAs within Chinese Taipei. However, it seems only recently that the legislature has shaken off its regulatory chill and begun to realise that greater work needs to be done across DDAs in the country. Nonetheless, the current trend surrounding the regulatory action in the country seems rather similar to Singapore, emphasising a more top-down approach towards DDAs in the region.

3 A comparative view

Before delving into this analysis, it is helpful to give a summary of the positions of these economies with regards to DDAs. From the analysis above, Singapore seems to be taking the most heavy-handed approach towards regulating DDAs, treating them as yet another asset with its top-down obligations on users as well as VASPs (or digital payment token services as known there). However, the other economies seem to be embracing the decentralisation and technology behind these assets, giving VASPs wider discretion. Of note, HKSAR and South Korea have seemingly taken up a "minimum core obligations" approach, leaving much discretion towards VASPs to regulate their own behaviour while imposing a minimum standard for them to adhere to. HKSAR has even gone a step further to impose an obligation for VASPs to work with established financial institutions to promote mutual capacity building measures. Conversely, Chinese Taipei's regulatory environment for DDAs seems to currently be in its infancy; requiring VASPs to abide by traditional rules which govern financial institutions. However, it is hoped that the Digital Assets Act 2023 in Chinese Taipei will clear the air and bring some clarity to the field soon.

Utilising this, this section will delve into a comparative analysis of how DDAs are treated within their jurisdictions, and their interactions with the beginnings of international law in DDAs. In particular, it focuses on the three areas which it identified - the taxonomy, internal policies, and compliance with international AML obligations. In that regard, a key overarching theme in the following analysis will be the interaction of these independent legislations within the wider regional, and international DDA and AML frameworks. While it notes that the disharmony surrounding DDAs seems particularly worrying, the current reality of DDAs makes this fear largely unfounded.

3.1 Taxonomy of DDAs

As with each snapshot of each country, this section will begin first to compare and analyse the framework of each nation's treatment of DDAs. Such a comparison will allow one to determine if there are legislative gaps in the framework surrounding DDAs, and potentially point out areas where there is an inconsistency with the laws surrounding DDAs alongside its international obligations. Having already considered the individual position of each economy, this section will first begin with the definition adopted by the international

community. Namely, the United Nations International Institute for the Unification of Private Law ('UNIDROIT'). Under their Working Group 3, the definition which they have adopted can be found across 'Category 1' and Category 2' based DDAs.[128] They include:

> **Category 1**: transferable code constituting a representation of:
> (i) a moveable tangible
> (ii) an immovable tangible
> (iii) a tokenised currency, of which two fundamentally distinct categories
> - privately tokenised fiat funds (e.g., the utility settlement coin)
> - central bank digital currency (CBDC)
>
> (iv) an intangible financial asset
> (v) an intangible non-financial asset (e.g., IP)
>
> **Category 2:** transferable code constituting a representation of an asset that is not a Category 1 asset.[129]

Examples of Category 1(iii) assets under UNIDROIT's definition include the Utility Settlement Coin project by Fnality.[130] Examples of Category 2 assets include Bitcoin, and Non-Fungible Tokens ('NFTs'). However, the UNIDROIT working group noted that there is a further third category of 'stablecoins' which was not reflected, listing examples including KPM Coin, Diem, and Dai (MakerDAO).[131] There is similarly an additional category which UNIDROIT has mentioned in their working paper, but not expressly codified - a category 3 for Stablecoins.[132] However, there is some confusion over how this new category would operate, compared to "privately tokenised fiat funds". Considering these crypto-assets with a different framework from stablecoins (under the proposed Category 3) even though they serve similar purposes only creates confusion. However, this category 3 presently does not stand, and stablecoins fall under the provisions laid out in Category 1.[133]

There are three core distinctions with the definition laid out by UNIDROIT, and the interpretation of DDAs by these nations. First and importantly, the UNIDROIT working paper expressly acknowledged that CBDCs form part of the umbrella of DDAs. Conversely, three of the Four Asian tigers (missing Chinese Taipei) excluded CBDCs from their definition of DDAs. This position adopted by them seems preferable. While CBDCs may be

[128] United Nations International Institute for the Unification of Private Law, Digital Assets and Private Law Working Group, Issues Paper, Study LXXXII – WG3 – Doc 2 (rev 1), adopted 2 July 2021
[129] ibid 54.
[130] See at <https://www.fnality.org/home> accessed 2 December 2022. Discussed in (n 140), 40.
[131] ibid 57-8.
[132] ibid.
[133] ibid 40.

decentralised,[134] they do not have the same risk profile as DDAs for AML provisions. First, CBDCs are issued by the State, and often backed by a fiat currency - the State's national currency. Where these tokens are issued by the States, States can program AML safeguards within them that would be unseen to the naked eye.[135] Such has indeed already been implemented in other State-distributed DDAs. Decentralised and tokenised green bonds from Project Benja have safeguards to ensure that the funds are only used for their purpose as a blockchain-based carbon credit scheme.[136] In that regard, the programming of internal AML measures such as mechanisms to track the currency would be possible.[137] As such, the position of Singapore, South Korea and HKSAR is undoubtedly preferred. CBDCs should not fall under the traditional scope of DDAs in the law of sanctions.

Second, DDAs within UNIDROIT's framework includes decentralised securities under Category 1's "digital representation of a movable tangible". This seems to include commodity backed tokens as well as digital securities; a distinction was not made within the UNIDROIT working papers.[138] Conversely, across the Four Asian Tigers, there have been express provisions made where decentralised securities fall outside the scope of DDA provisions, and are instead governed under the same traditional categories as non-digital securities. At this juncture, it is hence worth noting that nations have been working together with the International Council of Securities Association ("IOSCO") to put forth developments across DDA security-based legislations.[139] Indeed, the IOSCO has been working with various nations, including the Four Asian Tigers, on developing a harmonised framework in the realm of security-based DDAs.[140] Similarly, one can thus assume that UNIDROIT will soon take a step back in this field, given that the organisations have a long history of cooperation in this field.[141] However, further consideration by the IOSCO should be given to existing frameworks, such as the UNIDROIT Convention on Substantive Rules for Intermediated Securities (2013) and the UNIDROIT Legislative Guide on Intermediated

[134] For instance, as discussed by the Central Bank of Malaysia in: Nurjannah Ahmat and Sabrina Bashir, 'Central Bank Digital Currency: A Monetary Policy Perspective' (September 2017, Central Bank of Malaysia) <https://www.bnm.gov.my/documents/20124/826874/CB_Digital+Currency_Print.pdf> accessed 2 December 2022.
[135] For instance, as discussed by the European Union in: European Central Bank, *Exploring Anonymity in Central Bank Digital Currencies*, (December 2019, Issue 4 - In Focus, Eurosystem). 5-9 <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf> accessed 6 December 2022.
[136] Monetary Authority of Singapore (n 41).
[137] Bank for International Settlements, 'Central Bank Digital Currencies: System Design and Interoperability', (September 2021, Report 2, BIS Publishing) <https://www.bis.org/publ/othp42_system_design.pdf> accessed 3 December 2022.
[138] Reuters Staff (n 126), 27, 81.
[139] Jane Diplock, 'Securities Regulation - An International Perspective' (International Council of Securities Association, Tokyo, 30 October 2006). <https://www.iosco.org/library/speeches/pdf/securities_regulation_international_perspective_oct06_jd.pdf> accessed 3 December 2022.
[140] International Council of Securities Association, *IOSCO Decentralised Finance Report*, (March 2002, OR01/2022, IOSCO) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> accessed 2 December 2022.
[141] Rita Cunha, *Memorandum of Understanding (MMOU): An international Benchmark for Securities Enforcement*, (UNIDROIT Colloquium, 6-7 September 2010, UNIDROIT Secretariat). <https://www.unidroit.org/english/documents/2010/study78b/cem1-colloquium2010/cunha.pdf> accessed 4 December 2022.

Securities (2017). As such, one can thus expect the IOSCO to begin leading the field in this area; a consensus among the Four Asian Tigers towards their stance on DDAs is, in itself, thus promising.

Lastly, and particularly within the realm of DDAs, a word has to be said about the non-specificity of UNIDROIT's classification with regard to Category 2 assets. UNIDROIT's current position seems to best reflect the position in Chinese Taipei - the 'catch-all umbrella' category consisting of everything that is not a digital asset; a similar trend appears to be present where Category 2 assets were only described as including Bitcoin, or NFTs; more broadly speaking, assets which have seemingly garnered the most infamy and media attention.[142] Conversely, Singapore, South Korea and HKSAR all contain a more robust definition of DDAs within their national legislation. The importance of such a distinction indicates a broader and more nuanced understanding of these assets, which is similarly evident in subsequent legislation concerning digital payment tokens, virtual assets and virtual commodities respectively. In a practical setting, this disharmony would create a degree of legal uncertainty. End-users, investors and even issuers of DDAs would have to understand different nuances in classification of assets, and comply with different regulations as they operate in different regions.

As such, one can thus see the consequences surrounding a non-harmonised taxonomy of DDAs. Unfortunately, it seems that domestic legislations seem to be more robust, and have greater overall certainty as compared to their international counterparts. However, to achieve a strong overall framework and consistent regulatory environment for DDAs as they often operate in a transboundary setting, there needs to be a clear and consistent use of taxonomy for DDAs. Currently, it seems that only three out of the four powerhouses in the region are fully ready to embrace these assets.

3.2 Treatment of VASPs

DDAs are not the only matter which requires legal certainty. VASPs, and DDA custodians have a similarly large role to play in the regulatory process. After all, end-users would not be able to access their virtual commodities or virtual assets without a platform or interface, given the intangible nature of these assets. Indeed, for beneficiaries and receivers of DDAs, the crux of the mechanism which they utilise these assets lies in the conversion of intangible financial instruments, with tangible physical objects used to commit wrongful acts.[143] Hence, where VASPs act as the gatekeeper towards enforcing AMLs, the regulatory framework surrounding them should be discussed.

[142] Hwa Lee (n 118).

[143] See here, for example, the status of Russian Paramilitary Groups using digital assets to evade sanctions in: Peter Maroulis, Nick Grothaus and James Disalvatore, 'Online Crowdfunding Campaigns use Cryptocurrency to Support Russian Paramilitary Groups in Ukraine' (5 December 2022), <https://brief.kharon.com/updates/online-crowdfunding-campaigns-use-cryptocurrency-to-support-russian-paramilitary-groups-in-ukraine/> accessed 6 December 2022.

In the current international framework, the Financial Action Task Force ("FATF") has been working with UNIDROIT towards a regulatory framework. Generally regarded as the organisation in charge of international AML standards,[144] the FATF has been seeking to harmonise the laws surrounding DDAs globally. However, what is interesting is that within UNIDROIT Working Papers, the FATF has made a distinction between "tradability" of assets, and the "transfer of assets", going at odds with the UNIDROIT Secretariat.[145] This position was subsequently reflected within FATF[146] and UNIDROIT[147] reports - while 'trade' was defined as the exchanging of the intangible for a tangible, or recognised legal tender, 'transfer' refers to the exchange of digital assets from an originator to a beneficiary. Such a particularly nuanced view exemplifies the role of VASPs within the DDA ecosystem. In that light, the FATF has taken centre-stage in attempting to develop an international regulatory framework of VASPs.[148] Unfortunately, this important distinction seems to have been lost in translation within the legislative framework across the Four Asian Tigers, each treating them as one and the same term. However, such a distinction is particularly relevant in AML laws where the whole purpose of utilising DDAs is founded on a means of "cleaning dirty money". In that aspect, Singapore's heavy top-down approach can thus be said to be more effective in this last-leg, whereas South Korea, Chinese Taipei and HKSAR's more discretionary approach is better suited to facilitate transfers in DDA-based investments.

A second consideration lies in the risk-assessment framework posited under FATF guidelines. In essence, VASPs traditionally focuses on risk assessments of DDAs, customer due diligence, VASPs maintaining banking relationships, implementation of the "travel rule", internal controls, harmonising policies across foreign branches, reporting of suspicious activities and mechanisms for whistleblowing, as well as mutual cooperation across VASPs.[149] This is a particularly extensive set of top-down obligations which the FATF seems to impose on VASPs, which are consistent with many of the provisions found within these economies. Nonetheless, they seem to be largely harmonised under both FATF guidelines, as well as across the economies in the Four Asian Tigers. For instance, customer due diligence obligations across the four jurisdictions is largely harmonised with principles set out by the FATF - namely, that all end-users should disclose personal information to VASPs when using the data. Interestingly however, one area which all

[144] Navin Beekarry, 'The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law' (2011) 31 Northwestern Journal of International Law and Business 137.
[145] Digital Assets and Private Law Working Group, *Summary Report of the First Session*, Study LXXXII – W.G.1 – Doc. 4 (rev. 1), 17-19 November 2020. United Nations International Institute for the Unification of Private Law.
[146] Financial Action Task Force, *Virtual Assets and Virtual Asset Service Providers, Updated Guidance for a Risk-Based Approach* (October 2021, FATF/OECD) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 2 December 2022.
[147] Digital Assets and Private Law Working Group, *Master Copy of the Principles and Comments*, Study LXXXII – W G 5 – Doc 3 (rev 1) 7-9 March 2022, United Nations International Institute for the Unification of Private Law.
[148] ibid. Also note that UNIDROIT seems to be silent on the role of VASPs within their work.
[149] Beekarry (n 144).

jurisdictions have left to the discretion of VASPs lies in the mechanisms of their reporting obligations. This is in line with the FATF report, which seems to embrace various mechanisms for implementing AML reporting procedures.[150] However, guidelines have been provided in the consultation paper on red-flag indicators for VASPs to utilise.[151] Nonetheless, these guiding principles provide a strong framework for VASPs to tap upon, and to utilise as guidance, even if they are not bound by these principles. As such, one should applaud this extensive framework which the FATF recommends looks to mitigate and minimise any potential risk which may arise through DDAs.

However, it should also come as no surprise that there are definitely varying degrees of implementation of these standards. Singapore currently has the greatest "top-down" regulatory approach towards VASPs, complying with FATF guidance and even going further than that with reporting and record-keeping obligations imposed on VASPs operating in Singapore include mandatory periodic disclosure obligations.[152] While the FATF is currently silent on this, it instead adopts a "wait-and-see" framework where third party supervisors may request for certain information at given points in time.[153] Conversely, HKSAR, South Korea and Chinese Taipei are attempting to preserve anonymity, and, in line with standards set out by the FATF, only request for information when required. Such over-preparedness by Singapore might be detrimental for the use and growth of DDAs within Singapore, where anonymity in transactions has become a fictitious concept despite international standards not requiring such disclosure. Yet, having the relevant authorities hold information at the ready might similarly allow for the strengthening of AML obligations through more timely responses. This presents a precarious balancing act which would undoubtedly determine the future of DDAs in Singapore, and whether they would be widely adopted. Despite this disharmony however, the minimum obligations can be said to have been met.

Unfortunately, a word has to be said about the disharmony across capacity building obligations, and varying degrees of trust that central authorities take towards these VASPs. Currently, only South Korea, HKSAR and Chinese Taipei give VASPs a significant amount of discretion in their operation, merely providing requirements for the end goal of AML laws. This follows the position of the FATF, which similarly place an emphasis on promoting cooperation within the private Sector. Indeed, the FATF has even provided express recommendations which promote mutual capacity building and information sharing between VASPs and Banks.[154] Conversely, Singapore has taken a more regulatory approach towards defining each individual obligation, distinguishing them as a unique

[150] ibid 88.
[151] Financial Action Task Force, '*Virtual Assets, Red Flag Indicators of Money Laundering and Terrorist Financing*' (September 2020, FATF/OECD) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf> accessed 3 December 2022.
[152] Cf s.16(3) of the *Finance and Securities Market Act* 2022.
[153] Beekarry (n 144), 104 [7].
[154] ibid 82, 102.

entity in the market across seven different categories[155] Such a disharmonised framework is rather problematic, particularly when there are disparate standards which result due to developments in technology. Indeed, if too much regulatory oversight is imposed in the technological standards which these nations adopt, there would be concerns that VASPs lack discretion to upgrade their security framework in line with corporate standards. The situation is particularly worse for VASPs which operate exclusively in Singapore, where they would have no obligations to update their AML or protection frameworks, nor have foreign branches which they can tap on. This latter point is similarly made worse given the particularly onerous obligations Singapore imposes on VASPs operating transnationally.[156] As such, too much regulatory oversight would inherently leave VASPs operating in Singapore at a different technological standard from the rest of the region.

Such a disparate technological standards would, if left unchecked, lead to issues both within DDA technologies itself, as well as disharmonised regulatory standards. On the former, "splitting" within DDAs occurs where significant holders of a particular asset become incompatible with the larger pool of assets. This results in the particular asset splitting into two distinct forms of currencies, with these incompatible assets becoming its own unique currency. This was the case for Ethereum's hard fork, resulting in two different cryptocurrencies of Ethereum and Ethereum Classic.[157] Such incompatibility due to disparate technological standards might be cause for concern. On the latter, greater regulatory oversight over the operating standard of VASPs might similarly result in a stagnation of AML frameworks in these VASPs where top-down approaches do not adapt. Such further fragments the standards of VASPs within the region, creating an overall disharmonious technological framework.

Finally, the technical aspect surrounding DDAs and the importance of VASP's due diligence obligations should be discussed. At present, all four economies have obligations for VASPs to conduct due diligence studies on the particular DDA which they wish to offer; albeit to varying degrees. However, what is common between them, is that the core due diligence obligations seem to be merely limited to customer and beneficiary due diligence; only HKSAR imposes an additional obligation for VASPs to understand the underlying asset which they are offering. This obligation to understand the asset however, is of particular importance. While there is established precedent of DDAs being programmed to be able to fund projects which ensure public good, such as within the trading of smart carbon credits,[158] the reverse can similarly be done. Various organisations can issue DDAs programmed to fund wrongful conduct, such as the purchasing of arms in sanctioned

[155] Lim Chong Kin, Benjamin Gaw and Elizabeth Tong, 'Singapore' in Barbara Stettner and Bill Satchell (eds), *Global Legal Insights Fintech* (Global Legal Group Publishing 2019) 218.
[156] ibid 219-20.
[157] Chitturi Prasad and others, 'Quantifying Blockchain Immutability Over Time' (5th International Conference on Electronics, Communication and Aerospace Technology 2021) 715,720 <https://ieeexplore.ieee.org/abstract/document/9675947/> accessed 1 December 2022.
[158] Project BENJA and Project Genesis (n 3).

countries. In that regard, without proper due diligence on the asset, DDA issuers could potentially hide their malicious intentions within the code of the asset that is often overlooked by investors. This emphasis on the use of technology to bypass assets is not a novel concept, and has seen discussion across applications which are predominantly used by DDA-based investors.[159] In particular, the messaging platform "Telegram" has garnered a notorious history of being used to bypass sanctions.[160] As such, while the due diligence obligations within these economies are a good first step, HKSAR seems to be leading the field in this aspect.

Overall, the rules surrounding VASPs are rather broad and currently disharmonised across the region. Indeed, there are significant efforts to implement the international guidance provisions by the FATF to strengthen AML laws. However, where a country's attitude towards VASPs remains particularly top-down, there is a concern that these regulations would fall behind corporate standards, particularly when the rest of the region seems to be embracing these matters. As such, this disharmony in technological standards may become cause for concern going forward.

3.3 Compliance with international law obligations

The final area for consideration lies in the role of international law obligations which States have. In the area of AML and economic sanctions, this generally takes the form of compliance with UNSC resolutions in imposing sanctions against individuals, or general trade sanctions against nations. There is, unfortunately, no general framework for the imposition of unilateral sanctions against particular nations.[161] As such, compliance with international law obligations pertaining to sanctions is difficult to assess. This is especially true for HKSAR and Chinese Taipei, due to their political difficulties in assessing their foreign policies in light of pressures by the PRC. Hence, this subsection will primarily consider the application and enforcement of sanctions ordered by the UNSC.

From the snapshot of the Four Asian Tigers, it is particularly evident that they do comply with the relevant UNSC sanctions, and have mechanisms in place to enforce a sanctions regime. However, UNSC sanctions are traditionally more targeted, rather than operating as general trade sanctions.[162] This is largely owed to their design to prevent a State's continuous wrongful conduct, aiming to stem the means to their ends.[163] Oftentimes, the

[159] Leonardo Nizzoli and others, 'Charting the Landscape of Online Cryptocurrency Manipulation' (2020) 8 IEEE Access 113239-113245.
[160] Ehsan Lor Afshar, 'Banking the Bazl: Building a Future in a Sanctioned Economy' (2022) 9(1) Economic Anthropology 60.
[161] Marc Bossuyt, 'Consequences of Economic Sanctions on the Enjoyment of Human Rights' (2000, E/CN 4/Sub 2/2000/33, UN Sub-Commission on the Promotion and Protection of Minorities). [5] <https://www.ohchr.org/sites/default/files/Documents/Events/WCM/MarcBossuyt_WorkshopUnilateralCoerciveSeminar.pdf> accessed 1 December 2022.
[162] Francesco Giumelli, 'Understanding United Nations Targeted Sanctions: An Empirical Analysis' (2015) 91(6) International Affairs 1351 <https://doi.org/10.1111/1468-2346.12448> accessed 29 November 2022.
[163] ibid.

nature of these targeted sanctions, targeting a particular industry, would be easier to enforce. However, the opposite is true for DDAs. The current framework means that such targeted sanctions would allow DDAs to inherently fall through their provisions, particularly when they have a peer-peer framework. Hence, even with real-world verification measures, there would be no oversight actively preventing the transfer of DDAs into sanctioned countries. Especially if real world verification is only one-sided, VASPs and regulators would be unable to track the subsequent movement of DDAs once transferred to a country with a more lax regime. Following, DDAs can then be exchanged for tangible goods at a later stage once within the ecosystem of sanctioned countries, subsequently bypassing sanctions. The situation is especially worse when there is, at present, no international framework for VASPs to comply with. Indeed, all current legal obligations for VASPs and DDAs stem from the economies which they are operating in. Even if they were to trickle down from the international level at a later stage, it might still take time for States to legislate these international obligations into domestic law, and ensure VASP compliance. Hence, targeted sanctions, while potentially effective at the international level, might be inadequate if a framework governing DDAs are to be applied.

Despite these matters, the work of all Four Asian Tigers in the realm of economic sanctions is undoubtedly to be applauded. Singapore, in particular, has attempted to circulate advisors to ensure that VASPs do take note and be wary of the role of international sanctions, urging VASPs to prevent transactions to locations with IP addresses indicating sanctioned country.[164] Conversely, South Korea, HKSAR and Chinese Taipei have not made any statements surrounding the enforceability of these sanctions within the realm of DDAs. However, it would seem that as the remaining economies do have significant regulatory plans in the works, set to be enacted very soon. In that regard, it is hopeful that greater clarity on the interaction between DDAs and domestic regimes will come into play; even expressing references and acknowledgements of the transboundary nature of these assets would allow international law to take its roots within DDAs.

4 Towards a harmonised framework

Having identified the issues, this paper then seeks to set out solutions and guidance towards a harmonised regulatory framework. To that end, two principles can be tapped upon - that of comity between regulators, as well as mutual cooperation with the private sector.

[164] Monetary Authority of Singapore, *Guidelines to MAS Notice PS N-02 on Prevention of Money Laundering and Counter-terrorism Financing of Terrorism*, (16 March 2020, Government of the Republic of Singapore) <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines-to-PSN02-on-Prevention-of-Money-Laundering-and-Countering-the-Financing-of-Terrorism--DPT.pdf> accessed 2 December 2022.

Beginning first with comity, the role of international comity within digital assets is quintessential due to its fundamentally transboundary nature. In essence, international comity is the mutual respect between political and legislative entities across nations.[165] This includes decisions in both the judiciary,[166] as well as various legislative bodies. Indeed, the role of comity within the laws of DDAs cannot and should not be understated for various reasons. First, DDAs are inherently transboundary in nature. As such, they cannot be said to solely operate within each jurisdiction independently of each other. Conversely, there is an entire ecosystem of DDAs which would be affected by one economy's actions which may have an entire spillover effect within the industry. For instance, when the PRC made an announcement to ban the use of crypto-assets within its country, its value had plummeted drastically.[167] With an understanding of the volatility of these assets, such presents clear evidence that the unilateral action of one economy will frustrate the efforts of the global economy towards mitigating the risk-factor within these DDAs. Hence, the role of international comity cannot be stressed enough.

Undoubtedly, there exists a range of issues where the Four Asian Tigers practise international comity outside of DDAs. For instance, there has been discussion of the harmonisation of civil procedure rules, particularly across transboundary commercial disputes.[168] Similarly, the harmonised compliance with international law obligations is, in itself, a respect for the international legal order along the lines of comity. On this basis, it would be up to the economies to begin consultations with each other to best tackle the issue of DDAs within the region. Certain key themes of the talk should include the harmonisation of due diligence requirements for VASPs, both with regards to customer and DDA due diligence, the harmonising of licensing requirements for VASPs, as well as mechanisms to enhance and promote cross-border real world verification, particularly within the end-user experience (i.e. would both the originator and receiver of DDAs be able to view the others' personal data during the transfer, or merely be limited to the wallet addresses). In that regard, there is significant potential for mutual cooperation by policy-makers to determine the scope of a harmonised DDA framework within the region.

The same can be said for the adherence of DDAs to international standards. While there may be discussion of whether DDAs would fall under targeted sanctions by the UNSC or other international organisations, these economies should instead look towards integrating technologies in the interpretation and enforcement of these orders. This could be achieved through mere treaty interpretation standards, such as those suggested by

[165] Bryan Garner, *Black's Law Dictionary* (10th ed, Thomson Reuters Publishing 2014) 342.
[166] See, for instance, in: E*coBank Transnational Inc v Tanoh* [2015] EWCA Civ 1309, [2016] 1 WLR 2231 where the judiciary gave respect for exclusive jurisdiction clauses and did not want to frustrate the purpose of foreign judiciaries in granting an anti-suit injunction.
[167] BBC Editorial, 'Bitcoin falls further as China cracks down on crypto-currencies' (*BBC News*, 19 May 2021) <https://www.bbc.com/news/business-57169726> accessed 1 December 2022.
[168] James Spigelman, 'International Commercial Litigation: An Asian Perspective' (2007) 37 Hong Kong Law Journal 859.

Anja Ipp through Art 31(3)(c) of the Vienna Convention on the Law of Treaties,[169] which similarly applies within UNSC resolutions.[170] While Singapore has been noted to be leading the charge, South Korea, HKSAR and Chinese Taipei could similarly look towards Singapore as precedent for adopting such a wide view of sanctions and DDAs.

Secondly, and perhaps more briefly, the integration of corporate standards and the future proofing of regulatory work remains quintessential towards long term sustainability of AML mechanisms. While this notion has been briefly alluded to initially with respect to the FATF standards, more can definitely be done. The first step has already been taken by South Korea and HKSAR in embracing these technologies, giving appropriate discretion towards VASPs. HKSAR has even gone further to have VASPs work with larger financial institutions. Singapore and Chinese Taipei should thus look to these economies, and this is the first step towards developing a more robust and sustainable framework through the corporate world.

However, to proceed beyond this and move towards a harmonised framework, regional cooperation between financial institutions, central banking authorities, as well as VASPs need to move beyond a domestic level. Within this, a framework for inter-VASPs cooperation is quintessential to ensure that all VASPs are operating under similar regulatory standards, while giving them a platform to innovate and strengthen the AML framework. Of course, this is not to take away their individual innovations and stem competition, but rather, mutual cooperation within VASPs should be focused on enforcing AML standards at a regional level. Indeed, it is trite that end-users would have their own preference of VASPs which they engage with. However, to ensure there are no gaps within the regulatory firewall, these VASPs should operate harmoniously among themselves for matters such as end-user information disclosure, sharing of information pertaining 'blacklisted' individuals, as well as facilitating mutual strengthening of security functions. To that end, it is the regulatory bodies - central banks, larger financial institutions, and regulatory institutions - within these economies which have to facilitate such development. Else, it is unlikely that VASPs will take initiatives in this area, particularly where there is a general lack of incentive to do so after they fulfil the minimum obligations to comply with domestic law.

As a whole, these recommendations are intended to lay out a long-term sustainable framework to enhance AML measures within VASPs, and move towards an end-goal of the harmonisation of international trade law. However, to achieve such this, there is undoubtedly significantly more work that needs to be done, both at a domestic level, and a regional level. The first step towards achieving this aim however, seems to be to

[169] Anja Ipp, 'Regime interaction in investment arbitration: Climate law, international investment law and arbitration' (12 January 2022, Kluwer Arbitration Blog). <http://arbitrationblog.kluwerarbitration.com/2022/01/12/regime-interaction-in-investment-arbitration-climate-law-international-investment-law-and-arbitration/> accessed 30 November 2022.

[170] Efthymios Papastavridis, 'Interpretation of Security Council Resolutions under Chapter VII in the Aftermath of the Iraqi Crisis' (2007) 56(1) The International and Comparative Law Quarterly 83.

overcome the inertia, and begin a multi-faceted, multilateral dialogue in the realm of DDAs. Only through mutual cooperation and involvement of key stakeholders, tangible and effective change would arise.

To that end, perhaps lessons can be learnt from the European approach towards DDAs and VASPs. Under the recent Markets in Crypto-Assets Regulation ("MiCA") which is expected to come into force in February 2023.[171] As a regulation, the introduction of MiCA would create binding obligations on European Union ("EU") Member-States following its entry into force.[172] Very briefly, MiCA introduces a blanket definition to DDAs as "a digital expression of value or rights that can be transferred and stored electronically, using distributed registry technologies or similar technologies".[173] This harmonised taxonomy was established with consultation from the private sector (under the European Banking Authority") way back in 2019.[174] This taxonomy is hence undoubtedly to be applauded for this reason. The incorporation of private standards would allow for greater consideration of the nuances of DDAs such as the inclusion of "rights" within the definition. Further, while it must be noted that the use of a regulation as opposed to a directive signals a heavy-handed approach from this supranational organisation, perhaps such is required, given the transboundary nature of the asset and interconnectedness of Europe. In that regard, perhaps the economies of the Four Asian Tigers could look upon such a model to foster greater cooperation. More likely however, this would come at a later stage once these economies have a chance to properly consider the impact of MiCA following its enactment into EU legislation.

It must similarly be noted that MiCA is generally silent on AML provisions, with only a mere reference to the European Central Bank to handle all AML related legislation.[175] Additionally, the EU has not yet drafted a European-wide surveillance regime. The current position under the AMLD5 directive merely requires EU States to establish their own version of DDA-related AML provisions.[176] While this is rather unfortunate, many commentators note that with the introduction of MiCA and the overarching goal for harmonisation of DDA-related laws, a harmonised AML provision is only inevitable.[177] Nonetheless, for the Four Asian Tigers, what can be gleaned from this is that the harmonisation of AML provisions remains a long-term goal. Step-by-step harmonisation should first be considered before moving towards longer-term goals including AML

[171] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937' COM2020/593 final 24 September 2020.
[172] ibid 1.
[173] ibid 3.
[174] ibid 23.
[175] ibid 1.
[176] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for purposes of money laundering or terrorist financing, and amending directive 2013/36/EU [2018] OJ L 156/849.
[177] Koen Byttebier and Konstantinos Adamos 'Cryptoassets – a new frontier for money laundering and terrorist financing: legal changes to address the increasing AML risk' ahead-of-print [2022] Journal of Financial Crime <https://doi.org/10.1108/JFC-10-2022-0262> accessed 2 December 2022.

provisions. Undoubtedly, if the EU were to rush to harmonise through MiCA, this would be putting the cart before the horse - one would likely have to question whether its categorisation of what constitutes DDAs were truly effective in practice. Hence, perhaps it is due time that the Four Asian Tigers took the first step, and made the plunge into moving towards greater regional cooperation in this field.

5 Conclusion

Ultimately, DDAs present a novel financial technology, which has seen widespread adoption by both individuals within major and minor economies in recent times. However, as nations seek to take advantage of this new asset and out-position each other to attract investors, a disharmonious regulatory framework inevitably arises. Indeed, key culprits of this regulatory race include the four economic leaders in East Asia – Singapore, South Korea, HKSAR, and Chinese Taipei; also known as the Four Asian Tigers. Named after their and rags-to-riches story, each individual economy has had a history of embracing technological developments to get to where they are today. However, as they embark on the next step of their growth, each of these economies are vying to become world-class financial hubs within East Asia. To that end, they would inevitably have to address the controversial question of the particularly polarising financial instrument which has been gaining traction – that of DDAs.

In that regard, this paper sought to explore and take a snapshot of the current AML framework across thematic investigations into the regulatory framework of DDAs. In particular, it considers the position of these economies across three core issues within DDA regulation – their taxonomy and treatment of DDAs, rules and regulations surrounding custodians and service providers of these assets, and finally, their compliance and compatibility with international obligations, through the lens of AML laws and regulations. This area is particularly important given the current international climate and sanctions regime in place which DDAs seem to undermine; the lack of a central regulatory institution undoubtedly stroking much fear within both domestic and international policy makers. Unfortunately, despite the transboundary nature of these assets, there is clear disharmony both regionally across these economies, as well as under broader international law standards.

From the analysis conducted, one can identify that each of the economies seem to be taking a different thematic approach towards DDAs. Singapore seems to be the most stringent on matters pertaining to regulation, preferring to adopt a top-down, rather heavy-handed approach towards DDAs. Conversely, South Korea has taken the “minimum standards” approach, looking to strike a balance between maintaining the decentralised aspect of these assets, while setting up minimum core obligations for VASPs to follow, including the AML laws. HKSAR similarly embraces the technological developments under VASPs, urging stronger capacity building and information sharing measures and

encouraging cooperation within the private sector. Chinese Taipei however, has a rather new infrastructure surrounding DDAs, and the position of the legislative framework around DDAs has yet to be set.

These clear regulatory themes which these economies have adopted all find their grounding within the international legal framework set out by UNIDROIT and the FATF. What is particularly striking however, is that the domestic standards set out by these economies (with the exception of Chinese Taipei), seems to be more robust than the current taxonomy set out by UNIDROIT. In that regard, one can assume that international law would thus operate as a 'gap-filling' mechanism in the event that a new and novel instrument arises in the coming years. Similarly, the regulatory themes can all be found within the recommendations laid out by the FATF. Currently, HKSAR's framework is the most compatible with that of the FATF, particularly where the international task force has been looking to embrace evolving corporate standards of DDAs. Yet, while the HKSAR is best poised to take the lead in AML and regulatory compliance of DDAs, the high standards of regulations might not look the most attractive to investors and end-users. In that regard, a balance needs to be struck, drawing on the experiences of South Korea and Singapore, to further develop a harmonised framework in the region.

To that end, this paper makes two core suggestions in the realm of DDAs. First, an emphasis should be placed on the age-old doctrine of international comity, particularly within regulators. While competition among policy-makers across these regions undoubtedly spurs on regulatory innovation, and is beneficial to the overall standards surrounding DDAs, an emphasis should be placed on mutual cooperation towards a harmonised framework. This is especially the case where DDAs are known to operate in a transboundary manner. Mutual respect for the legislative systems within the region would set the ground for developing a unified taxonomy and regulations surrounding AML efforts within the region, removing the need for gap-filling mechanisms. Such similarly promotes regional cooperation, while strengthening the overall efforts of AML provisions. Secondly, this paper firmly believes that Chinese Taipei, South Korea and especially Singapore should follow the examples set out by HKSAR in embracing the rapid development of technologies, giving wider discretion towards VASPs. While, undoubtedly, top-down regulatory oversight on these institutions is required, it should come with a degree of trust that VASPs understand the market and are best positioned to address the wider policy concerns. In that regard, there is significant potential to allow and encourage VASPs to the table, both to provide their technical expertise on the matter, but similarly be allowed an opportunity to perhaps to accept the jurisdiction of international law in establishing an AML framework, while similarly enhancing the sanctions regime of the UNSC.