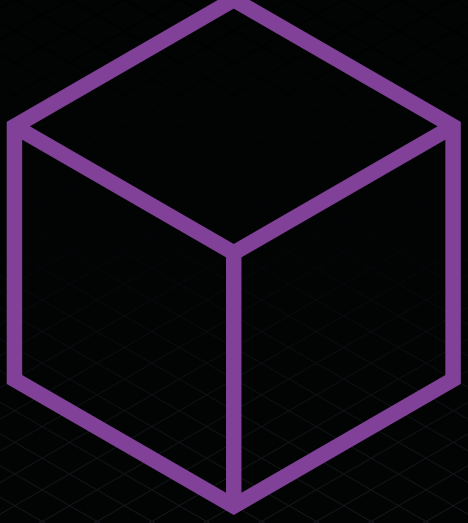
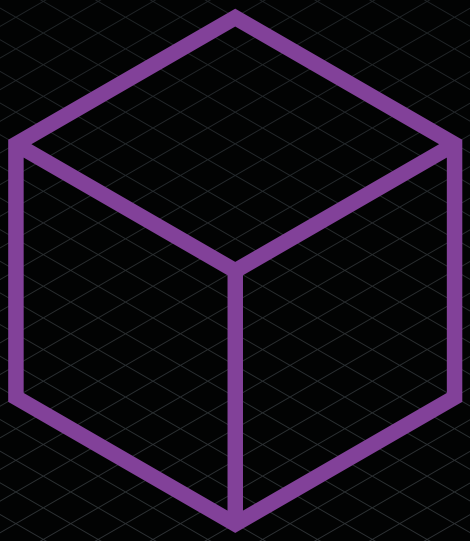
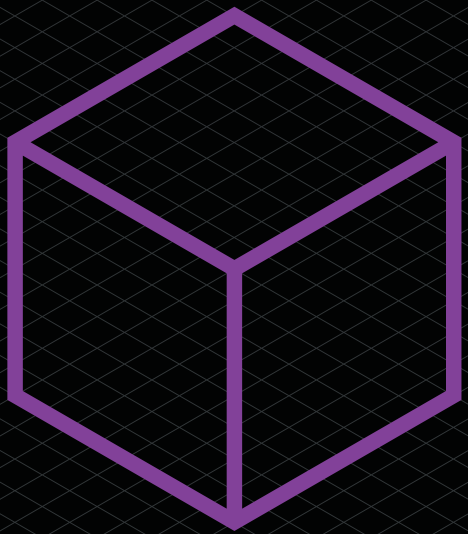


Part 1: Developing Technologies

Section 4

Types of Cryptoassets





Section 4: Types of Cryptoassets, Defi and On-Chain Compliance

Marc Piano, Harney Westwood & Riegels LLP (Cayman Islands).

Introduction

This section looks at different types of cryptoassets: in Part A: Central Bank Digital Currencies **(CBDCs)**, Part B: stablecoins and Part C: developments in the Decentralised Finance **(DeFi**) space and the adoption of the Financial Action Task Force **(FATF)** recommendations in respect of Virtual Asset Service Providers **(VASPs)** and on chain compliance.

Part A: Central Bank Digital Currencies

This section looks at CBDCs and new forms of private money as general concepts, considers their potential distinction from other forms of virtual assets, and legal issues for legal practitioners to consider.

What is 'money'?

Briefly, 'money' is that which can serve as a store of value, a unit of account and a medium of exchange.

In most economies, money takes the form of a fiat currency. This is money backed by a government and declared to be "legal tender" (which means that it can be used to settle debts or financial obligations). For example, under section 1(2) of the Currency and Bank Notes Act 1954 **(CBNA)**, all bank notes issued by the Bank of England constitute legal tender in England and Wales. Under section 2(1A) of the Coinage Act 1971, gold coins are legal tender for payment of any amount, nickel and silver coins in denominations of more than 10 pence are legal tender for any amount not exceeding GBP10, such coins in denominations of less than 10 pence are legal tender for any amount not exceeding GBP5, and bronze coins are legal tender for any amount not exceeding 20 pence.

The two forms of money in the UK are central bank money and private money. The Bank of England provides a brief overview of these in its 2021 discussion paper on new forms of digital money.

Central bank money represents liabilities of the central bank. For the public, this takes the form of cash (bank notes and coins). Under section 1(3) of the CBNA, bank notes may be exchanged at the Bank of England for bank notes of lower denominations. For commercial banks, this takes the form of central bank reserves. How these work is beyond the scope of this guidance.

Private money is commercial bank money, i.e. people's money deposited at commercial banks and loans created by commercial banks. The Bank of England notes that: "Around 95% of the funds households and businesses hold that are typically used to make payments are now held as commercial bank deposits rather than cash."[72]

What are CBDCs?

The Bank of International Settlements (BIS) defined CBDCs in its 2018 paper on the topic **(CPMI-MC (2018))** as: "potentially a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks"[73].

As set out in the BIS 2020 Report[74], CBDCs may be wholesale-only or general purpose.

72 BOE June 2021 Discussion Paper, section 1.1
73 Bank of International Settlements, March 2018, p 1 <https://www.bis.org/cpmi/publ/d174.pdf>
74 "Bank of International Settlements, 2020 <https://www.bis.org/publ/othp33.pdf>

Wholesale-only: As with electronic central bank deposits, wholesale digital token CBDCs would only be accessible by pre-defined users (i.e. qualifying financial institutions) and may (but is not required to) be combined with the use of distributed ledger technology, with the aim of enhancing settlement efficiency for a range of transactions including but not limited to retail payments, transfers, cross-border payments, and transactions involving securities and derivatives. Such wholesale-only CBDCs could also be used as a backing or settlement asset for other payment or stablecoin services, such as payment services or stablecoins (including synthetic CBDCs discussed below) offered by the relevant institution.

General purpose: these may be token-based or account-based. These operations are described in the Consensys white paper[75]:

> *"In a token-based system, the CBDC is created as a token with a specific denomination. The transfer of a token from one party to another does not require reconciling two databases, but is rather the near-immediate transfer of ownership, very much like handing over banknotes from one person to another.*
>
> *"In an account-based system, the central bank would hold accounts for users of the CBDC, and would handle the debit and credits between users itself."*

A token-based CBDC would likely require relevant accounts and their controllers to be verified and permissioned in order to receive and transact with CBDC tokens, together with some form of reporting and record-keeping system of transactions occurring in that account. Unlike bank notes where ownership is determined by possession, ownership of CBDC accounts and held tokens is likely to be determined by control of the private key to the account or its equivalent.

A general purpose CBDC, whether token-based or account-based, requires an infrastructure comprising the issuing central bank, operator(s) of the system infrastructure, participating payment service providers (PSPs) and banks, who may be responsible for creating and permissioning relevant accounts for CBDC tokens and reporting and record-keeping requirements as mentioned above. The BIS 2020 Report notes there could be overlaps in roles, such as the issuing central bank operating the system infrastructure[76].

In its March 2020 discussion paper **(the BoE March 2020 Discussion Paper)**, the Bank of England (the BoE) considers the potential impact of "disintermediation" through the introduction of CBDCs (i.e. the conversion of deposits held at commercial banks to CBDCs and the consequential reduction in the banking sector's balance sheet) as part of a wider range of complex policy and practical factors, noting that: *"If disintermediation were to occur on a large scale, that would either imply a large fall in lending or would require banks to seek to borrow significantly more from the Bank of England. This could have profound implications for the structure of the banking system and the [BoE's] balance sheet."* [77]

In short, CBDCs could reduce the role of commercial banks in the financial system, and managing the demand for CBDCs over bank deposits is a critical CBDC design factor.

What is the status of development and implementation of CBDCs?

As of May 2021, around 80% of central banks globally were exploring use cases involving CBDCs, with 40% already testing proof-of-concept programmes[78].

The Eastern Caribbean Central Bank (the monetary authority for Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St Kitts and Nevis,

75 "Central Banks and the Future of Digital Money", Consensys AG, January 2020, pp 17-18
76 BIS 2020 Report, page 4
77 "Central Bank Digital Currency: opportunities, challenges and design", Bank of England, 12 March 2020, Chapter 5.2
78 "About 80% of Central Banks Are Exploring CBDC Use Cases, Bison Trails Report Says", Coinbase, 19 May 2021

Saint Lucia, and St Vincent and the Grenadines) introduced its CBDC, DCash, on 31 March 2021 for public use[79].

The People's Bank of China has been researching its Digital Currency Electronic Payment (DC/EP) **(DCEP)** since 2014 and conducting small-scale trials in several cities, most recently in October 2020[80]. The PBOC intends to conduct a large-scale trial at the Winter Olympics in Beijing in February 2022[81].

The United Kingdom published terms of reference[82] for an HM Treasury and BoE CBDC taskforce in April 2021 to ensure a strategic approach to, and to promote close coordination between, the UK authorities as they explore CBDC, in line with their statutory objectives. In late September 2021, HM Treasury and the BoE announced the membership of the CBDC Engagement and Technology Forums to help progress the taskforce, which consists of senior stakeholders from industry, civil society and academia responsible for gathering strategic input on policy considerations and functional requirements pertaining to CBDCs[83]. CBDCs are also considered by the BoE as part of the BoE June 2021 Discussion Paper.

Design and operation of CBDCs will vary by central bank requirements, but a key consideration acknowledged by both the BIS and BoE is CBDC compliance with relevant anti-money laundering and countering the financing of terrorism frameworks. Research and discussions are ongoing around the use of CBDCs in cross-border payments, and this is considered briefly in more detail below.

What are "new forms of private money"?

The Bank of England defines "private money" in the BoE June 2021 Discussion Paper as mainly taking the form of deposits in commercial banks *"that is, claims on commercial banks held by the public. This 'commercial bank money' is created when commercial banks make loans."*[84]

The BIS 2020 Report notes that:

> *"Central banks support commercial bank money in various ways, by: (i) allowing commercial banks to settle interbank payments using central bank money; (ii) enabling convertibility between commercial and central bank money through banknote provision; and (iii) offering contingent liquidity through the lender of last resort function. Importantly, while cash and reserves are a liability of the central bank, commercial bank deposits are not."*

The key point to note is that private money, and any tokenised forms of private money, are not to be considered as CBDCs, as they are not issued by central banks. More likely, tokenised forms of private money will be deemed to be stablecoins and regulated accordingly (see Part B).

The BIS 2020 Report also considers "synthetic CBDC", under which PSPs issue liabilities matched by funds held at the central bank. Although these PSPs would act as intermediaries between the relevant central bank and end user, the BIS does not consider such liabilities as CBDCs, as the end user does not hold a claim against the central bank, only against the PSP[85].

Such arrangements, whether offered by qualifying financial institutions or other non-central bank entities (such as large technology companies), may constitute stablecoins, discussed in Part B, and may be subject to one or more legal and regulatory regimes in the relevant jurisdiction.

79 "DCash – an ECCB initiative – About the Project", Eastern Caribbean Central Bank
80 "Background and Implications of China's Central Bank Digital Currency: E-CNY", Jiaying Jiang Karman Lucero, Stanford Law School, 6 April 2021
81 "China Ramps Up CBDC Pilot Plans Ahead of 2022 Winter Olympics", CBDC Insider, 6 August 2021
82 "Terms of Reference (ToR), April 2021 - Central Bank Digital Currency (CBDC) Taskforce", HM Treasury, April 2021
83 "Membership of CBDC Engagement and Technology Forums", Bank of England, 29 September 2021
84 BoE June 2021 Discussion Paper, section 1.1
85 BIS 2020 Report, page 4

What are the properties of CBDCs?

For the purposes of this guidance, the key distinctions between CBDCs and other forms of virtual assets are that CBDCs are unlikely to be treated the same as other form of virtual assets for legal and regulatory purposes, because: (i) conceptually and by their intended function, they are, or are intended to be, representations of fiat currency; and (ii) practically, they are centrally issued and controlled by the issuing central bank instead of banks and other third parties (and such non-CBDC issuances are likely to be deemed be stablecoins for legal and regulatory purposes).

The BoE March 2020 Discussion Paper[86] notes that whilst distributed ledger technology may offer potentially useful innovations, there is no presumption that CBDCs inherently require DLT.

CBDCs are "programmable money". This means that the behaviour of CBDC accounts or tokens – alone, or in combination with smart contracts or third-party data oracles – can be programmed with instructions beyond those required merely to facilitate or restrict CBDC movement between accounts. The July 2021 white paper on the People's Bank of China's **(PBOC)** CBDC project notes that this can include functionality enabled through deployment of smart contracts that do not impair the CBDC's monetary function[87]. Such instructions could include limits on holdings, expiration dates, automated inflation or deflation rates, recipient or transaction restrictions and direct implementation of other forms of public or monetary policy.

The main design properties are: (a) account-based or token-based CBDCs; (b) direct pass-through (remuneration) of central bank interest rate adjustments on CBDC accounts, which can include negative rates; (c) structuring and tiering of remuneration (if any); and (d) soft and/or hard limits on CBDC holdings. Both the BIS and BoE consider the arguments for and against these structuring considerations in CPMI-MC (2018) and the BoE March 2020 Discussion Paper.

The "programmable money" element of CBDCs can theoretically facilitate policy implementation at a more granular level. For example, BNY Mellon notes that "*the CBDC wallet application can be programmed in a way such that funds contained within can only be spent in designated areas and also have a certain expiry date — an exercise almost impossible to implement with physical notes and coins"*.[88] We would note that this approach may require some form of location-based geographical and spending restrictions, and/or linking a CBDC wallet to a holder's verified residential address or other form of digital identity, to be effective. The PBOC has already experimented with CBDC expiration dates.[89] Theoretically, this means that CBDCs could be programmed to encourage or discourage use in certain types of transactions, in alignment with national policy and behavioural objectives.

Can CBDCs be used for cross-border payments?

Central banks are designing CBDCs pursuant to domestic mandates and public policy objectives. These influence a range of design, structuring and operational considerations. CBDC interoperability will be a key element that determines whether CBDCs are suitable or even technically capable of facilitating cross-border payments.

The BIS published a dedicated paper on this topic in March 2021 **(the BIS mCBDC Paper)**, introducing the concept of "multi-CBDC arrangements" **(mCBDC)**[90]. This paper acknowledges that improving cross-border payments efficiency acts as an important motivation for CBDC research and sets out three conceptual models of mCBDC interoperability to facilitate CBDCs being used in cross-border payments:

86 BoE March 2020 Discussion Paper, Chapter 6
87 "Progress of Research & Development of E-CNY in China", Working Group on E-CNY Research and Development of the People's Bank of China, July 2021, Section 3.2.7
88 "China and the dawn of digital currency", Geoff Yu (BNY Mellon), Aerial View, November 2020
89 "China's Digital Currency Is About To Disrupt Money", Enrique Dans, Forbes, 7 April 2021
90 "Multi-CBDC arrangements and the future of crossborder payments", BIS Papers No 115, Bank of International Settlements, March 2021

— developing common international standards, allowing compatible CBDC exchange between national CBDC systems;

— linking multiple CBDC systems through a shared technical interface or a common clearing mechanism (which may be decentralised); and

— integrating multiple CBDCs into a single mCBDC.

The BIS mCBDC Paper concludes by encouraging central banks to collaborate in CBDC development to identify unintended barriers, and to aid efficiency in enabling CBDC conversion as part of enabling CBDC cross-border payments. BIS's position is that this approach is preferable to widespread use of private global currencies but acknowledges the importance of safety in the CBDC design process. Development in this area is ongoing and this guidance will be updated as CBDC design models are finalised and tested.

Will CBDCs replace cash and existing banking and payment infrastructure?

CBDCs do not automatically imply either retail accessibility and use, nor replacement of existing cash, banking and payment infrastructures. The BIS 2020 Report emphasises as a foundational principle that CBDCs should complement existing central bank money and co-exist with robust private money to support public policy objectives. On cash, the BIS 2020 Report states: *"Central banks should continue providing and supporting cash for as long as there is sufficient public demand for it."*[91]

This position appears to be reinforced at the level of government policy. For example, the G7 document, Public Policy Principles for Retail Central Bank Digital Currencies (the **G7 PPP**), published in October 2021, is explicit in both Principle 9 on digital economy and innovation[92] and Principle 10 on financial inclusion[93] that CBDCs will coexist alongside cash.

Nonetheless, the possibility that CBDCs may eventually replace cash has been hypothesised, together with possible implementation mechanics. In a blog article dated 5 February 2019[94], the International Monetary Foundation describes a process by which a cash economy could transition to CBDCs through the use of negative interest rates. This involves separating the monetary base into cash and CBDCs, then applying a negative interest rate policy on cash as against conversion into CBDCs. Combined with dual acceptance of cash and CBDCs as a means of payment, this could incentivise a relatively gradual transition to CBDCs by making them a preferable form of money to cash. The BoE also notes the possibility of CBDCs replacing cash in the BoE June 2021 Discussion Paper: *"In principle, a CBDC could be used, in conjunction with a policy of restricting the use of cash. If the interest rate on the CBDC could go negative, this could soften the effective lower bound on interest rates and lower the welfare loss associated with the opportunity cost of holding cash."*[95] The BoE goes on to note that: *"In practice, however, the UK authorities remain committed to ensuring access to cash to those that need it."*

This important caveat is consistent with the stated policy positions set out in the G7 PPP: that as at the date of this guidance CBDCs will not replace cash, at least not among the G7, and there are currently no indications that this position is likely to change for the foreseeable future.

Hypothetically, if CBDCs were to replace cash in whole or in part, their programmable nature could have a profound impact across and between society, human behaviour, economic activity, monetary and public policy and the relationship

91 BIS 2020 Report, section 3.1
92 "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)", G7, October 2021, page 12
93 G7 PPP, page 13
94 "Cashing In: How to Make Negative Interest Rates Work", Ruchir Agarwal and Signe Krogstrup, IMFBlog, 5 February 2019
95 BoE June 2021 Discussion Paper, section 4.5

between governments, central banks, financial institutions, businesses and citizens. Discussion of these elements is well outside the scope of this guidance. Even if governments were to adjust any current publicly-stated policy positions and encourage a transition from cash to CBDCs, there is a confluence of as yet unresolved considerations around cross-border payments, compliance with anti-money laundering and data protection laws, responsibility and accountability for provisioning CBDC account access, and a lack of widespread infrastructure and acceptance. Together, these factors are likely to heavily influence CBDC design factors and mean that any envisaged transition from cash to CBDCs is unlikely to proceed at pace or at an international scale in the short to medium term.

CBDCs distinguished from other firms of virtual assets and practical legal considerations

As noted above, CBDCs are, or are representations of, fiat money and constitute legal tender. This means that CBDCs are likely to be explicitly or implicitly excluded from relevant local laws and regulations governing other forms of virtual assets and/or VASPs so that CBDCs can achieve their intended purpose.

For example, the FATF, the global standard-setting body for anti-money laundering and countering the financing of terrorism standards, explicitly acknowledges this position in its draft updated guidance on a risk-based approach to virtual assets and VASPs (considered separately, later in this section) (the Updated FATF Guidance)[96], as does the Financial Stability Board (FSB) in its final report and high-level recommendations on "Global Stablecoin Arrangements" (the FSB Stablecoins Report)[97], considered in more detail in Part B, below.

Legal practitioners should be aware of the distinctive treatment of CBDCs as against other forms of virtual assets for legal and regulatory purposes. Although recognised as fiat currency and legal tender by the relevant government, the design and implementation of CBDCs and their use in transactions may give rise to additional analysis, advice and transactional considerations, such as cross-border acceptance, compliance with local anti-money laundering and countering the financing of terrorism laws, additional representations and warranties around relevant properties for account-based CBDCs, acceptability of relevant CBDCs as a means of payment in cross-border transactions and settlement and completion mechanics.
This section of this guidance will be updated and expanded on in future, as the development and implementation of CBDCs progresses.

Conclusion

CBDCs constitute a new form of "programmable money". Although they are "virtual assets", being assets that are virtual, their intended function lends to their exclusion from the operation of laws and regulations intended to cover other forms of virtual assets. A sufficient number of central banks are investigating or developing CBDCs to warrant close scrutiny of developments in this area, given the potential impacts of CDBCs across multiple spheres of consideration beyond the scope of this guidance. The stated public policy of a number of governments, combined with a range of discrete and sometimes overlapping design, implementation and compliance considerations, do not lend to any indication that CBDCs, when introduced, are or are likely to replace cash in the short to medium term. Legal practitioners should be aware of CBDCs as a concept, their likely distinction from other forms of virtual assets for legal and regulatory purposes, and development of coordinated policies around cross-border acceptance of CBDCs, which will be relevant should clients seek adoption or acceptance of CBDCs in relevant transactions as a range of legal and regulatory issues are concomitant with such intentions.

96 "Updated guidance on a risk-based approach to virtual assets and virtual asset service providers", Financial Action Task Force, October 2021, paragraph 17
97 "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Final Report and High-Level Recommendations", Financial Stability Board, October 2020, Glossary definition of "digital asset", page 5

Part B: Stablecoins

This section provides a high-level overview of so-called stablecoins (stablecoins) and considerations for legal practitioners.

What is a stablecoin?

There is no consensus definition of a stablecoin. This guidance adopts the definition of a stablecoin as used by the FSB in the **FSB Stablecoin Report** (the FSB Stablecoin Report) as *"a cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets"*.[98]

This definition encompasses a range of stablecoins, broadly divided two categories: i. asset-backed stablecoins and ii. algorithm-based stablecoins. Distinguishing features between stablecoin models include design, operation and associated contractual rights. Some stablecoins may operate as a hybrid, being asset-backed as well as utilising an algorithmic stabilisation mechanism.

i. Asset-backed stablecoins

Asset-backed stablecoins represent value by reference to an underlying reserve which may consist of one or more fiat currencies, precious metals, securities such as bonds, other virtual assets or a portfolio of several assets.

Examples of asset-backed stablecoins include:

- Fiat-backed stablecoins, such as Tether (USDT, backed by the US Dollar), EURS (backed by the Euro), USD Coin (USDC, backed by the US Dollar);
- Commodity-backed stablecoins, such as Digix (DGX, backed by physical gold), Tiberius Coin (TCX, backed by a basket of precious metals) and SwissRealCoin (SRC, backed by a portfolio of Swiss commercial real estate); and
- Virtual asset-backed stablecoins, such as MakerDAO (DAI, backed by other virtual assets collateralised in smart contracts) and Synthetix (SNX, which can be backed by other virtual assets, but can also be backed by fiat currency).

ii. Algorithmic stablecoins

Algorithmic stablecoins are not linked (or wholly linked) to underlying reserve assets. Instead, such stablecoins deploy an algorithm or protocol which acts as the "central bank", increasing or decreasing supply in accordance with the rules of the algorithm, which may be by reference to relevant third party data feeds (known as oracles), and the rules of which may be changed by the applicable (usually decentralised) governance process. The algorithm rules may reference a peg of market supply of the relevant stablecoin itself, or a peg based on one or more other virtual assets which are not themselves held in reserve. If demand increases or decreases, then the algorithm calculates the increase or decrease of token supply to maintain a stable market value.

Examples of algorithmic stablecoins include Basis (BAC, which uses an automated stability mechanism to maintain supply to keep the token's value relative to the US Dollar) and Frax (FRAX, which uses underlying partial collateralisation together with a base stabilisation mechanism, whilst also allowing additional fractional stability though further policy changes that do not affect the pegging of the FRAX token as determined by the base stabilisation mechanism).

As at the date of this guidance, algorithmic stablecoins have relatively little adoption in the market. Fiat-backed stablecoins are the primary form of stablecoin in use.

98 "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Final Report and High-Level Recommendations", Financial Stability Board, October 2020, Glossary definition of "stablecoin", page 5

Whether or not a cryptoasset constitutes a stablecoin will be determined by regulation, regardless of the underlying technological or economic characteristics of the asset regardless of intended use, referenced assets, price determination and/or algorithmic adjustments, and whether fully centralised, partially-distributed or highly-distributed.

Absent a common definition, both the FSB Stablecoins Report and the International Organization of Securities Commissions **(IOSCO)** report[99] (the **IOSCO Stablecoins Report**) broadly agree on three underlying properties that distinguish stablecoins from other forms of cryptoassets:

- a stablisation mechanism to stabilise the price of the stablecoin, compared to other non-stabilised cryptoassets;
- the technology used/the programmed functions and activities, such as governance, issuance, transfer, redemption and destruction (i.e. if distributed ledger technology is used, it is more likely to use a permissioned rather than permissionless protocol so that eligibility and participation criteria can be determined and controlled); and
- the eligibility criteria for participation, which in part may depend on the level of centralisation and control over the stablecoin's lifecycle and operability.

As noted in this guidance's section on CBDCs, virtual assets issued by central banks will be a form of central bank money and thus fiat currency, and are therefore likely to be explicitly excluded from categorisation as a cryptoasset under relevant laws and regulations to enable them to operate as intended and to reflect their nature as a form or representation of fiat currency. This treatment of CBDCs should be distinguished from stablecoins issued by commercial banks or other third parties (such as large technology companies) and intended as a means for payment that are linked to either that bank's or third party's own deposits or that bank's claim against central bank deposits; such stablecoins will constitute cryptoassets and not CBDCs as they are not issued by central banks. The potential legal and regulatory treatment of stablecoins is considered below.

What is the purpose of a stablecoin?

Fundamentally, stablecoins purport to offer price stability relative to the often extreme price volatility and fluctuation commonly seen in other forms of virtual assets such as cryptocurrencies. Many stablecoins are intended to function as a form of money by meeting the traditional criteria of money as[100] offering a store of value, unit of account and medium of exchange. This does not presume that all stablecoins are intended to function as a form of money – the intended purpose and actual use depends in each case on the relevant arrangements, such as where a stablecoin is created as a representation of collateralised cryptoassets (which may include cryptocurrencies) used to secure a loan. Further, although a stablecoin may be created and offered as a form of money, its utility depends on acceptance as a means of payment between parties – as stablecoins do not constitute fiat currency they do not have the benefit of recognition as legal tender and are not required to be accepted as a means of payment.

In the BoE June 2021 Discussion Paper[101] (the **BoE June 2021 Discussion Paper**), the BoE noted the potential for stablecoins to be issued by commercial banks to facilitate payments by retail customers. Stablecoins may also be issued by private non-bank third parties backed against that third party's own assets, such as the Facebook Diem project.

Stablecoins may be created for a variety of purposes, including on a standalone basis for development of use cases by third parties, as a means of payment for products or services offered by the issuer or ecosystem participants, as a payment rail for a payment services ecosystem, to act as a benchmark (possibly by reference

99 "Global Stablecoin initiatives – Public Report" The Board of the IOSCO, March 2020, page 5
100 "What Is Money?", International Monetary Fund, Finance & Development, September 2012
101 "New forms of digital money – discussion paper", Bank of England, 7 June 2021, section 5

to the relevant underlying assets, in which case they may be subject to relevant financial services regulation around benchmarks), or to act as a form of money within the relevant ecosystem, wider protocol on which the stablecoin operates, or sector (if cross-chain compatible).

Another function of stablecoins is to credit yield generation in DeFi protocols. This involves the relevant smart contract (or network of smart contracts) in that protocol receiving cryptoassets from a transferor (i.e. such assets are "staked" and otherwise unavailable for use by the original transferor) and putting them to work – such as allowing the transferred cryptoassets to be used as collateral for borrowing or lending out – with the yield such cryptoassets generate being credited in a stablecoin held by the user of the protocol. This approach allows protocol participants to take the benefit of the yield earned on the underlying transferred cryptoassets directly into another asset that can be used as a means of payment or otherwise sold or traded.

A common feature also seen in many DeFi protocols is the liquidity pool token **(LP tokens)**. This is a token representing a pro rata share of assets transferred to a liquidity pool and carries the right to receive the yield generated by the underlying cryptoassets staked in the liquidity pool, and the holder has the benefit of such right from holding the LP Token. LP Tokens can themselves be staked in other liquidity pools to generate additional yield. Although LP Tokens are not intended to function as a means of payment in and of themselves, their design, representation of an underlying basket of assets and redemption mechanics could lead them to fall under the definition of a stablecoin in some legal and regulatory frameworks and this element needs careful consideration by lawmakers, drafters and legal practitioners when advising clients on relevant projects, operations or transactions.

Legal and regulatory landscape, development and considerations

The collapse of TerraUSD in May 2022 attracted significant attention and regulatory scrutiny around stablecoins and their role.

Stablecoins, whether as standalone projects or as part of a wider business line or operation (whether cryptoasset-specific or not), present complex legal and regulatory challenges requiring consideration due to their potential range of properties and purposes. Given the rapid development and adoption of some stablecoins by some financial institutions and large non-financial institutions (such as Facebook's Diem project), global regulatory standards and local implementation continues to develop as at the date of publication of this guidance.

Legal analysis and advice in this area may need to encompass one or more regulatory frameworks, accommodate potential regulatory overlap and will require fact-specific analysis, including awareness of emerging local and international legal and regulatory developments.

Regulatory development

Financial stability

A key acknowledgement across many of the reports by global supervisory bodies concerning stablecoins is their potential to become systemically important and may, therefore, present systemic risk. This is a welcome acknowledgement that stablecoins may play a critical role in financial services and payment services in particular, and shows that supervisory bodies are factoring the rapid evolution of the design, deployment and adoption of stablecoins into regulatory development within their area of oversight.

Application of CPMI-IOSCO PFMI

The transfer function of a stablecoin (which in practice is a feature of the vast majority of stablecoins) is already deemed by IOSCO to be a financial markets infrastructure

(FMI) function[102]. FMI is defined as "a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions". A stablecoin participant facilitating the stablecoin transfer function will be subject to the CPMI-IOSCO Principles for Financial Market Infrastructures **(PFMI)**[103]. A detailed consideration of the PFMI themselves is outside the scope of this guidance.

FSB Stablecoin Report

The FSB Stablecoin Report sets out 10 high-level recommendations around regulatory, supervisory and oversight requirements for stablecoins from a financial stability perspective. The recommendations call for *"regulation, supervision and oversight that is proportionate to the risks, and [which] stress the value of flexible, efficient, inclusive, and multi-sectoral cross-border cooperation, coordination, and information-sharing arrangements among authorities that take into account the evolving nature of GSC arrangements and the risks they may pose over time"*.[104]

A key expectation communicated by the FSB is that: *"[Stablecoin] arrangements are expected to adhere to all applicable regulatory standards and address risks to financial stability before commencing operation, and to adapt to new regulatory requirements as necessary."*[105]

Although the FSB does not anticipate that every stablecoin inherently poses systemic risks, it does consider that *"such instruments may have the potential to pose systemic risks to the financial system and significant risks to the real economy, including through the substitution of domestic currencies"*.[106]

All 10 recommendations are worth reading in full, as the FSB Stablecoin Report is the work product of a G20 mandate to the FSB to examine regulatory issues raised by stablecoin arrangements and to advise on multilateral responses. This means that the recommendations are likely to be incorporated into each jurisdiction's regulatory framework and/or inform regulatory treatment of stablecoins and stablecoin-related projects.

In October 2021, the FSB published a progress report on the implementation of the recommendations (the **FSB Update Report**)[107]. The report noted that *"while the current generation so-called stablecoins are not being used for mainstream payments on a significant scale, vulnerabilities in this space have continued to grow over the course of 2020-21"*[108] and that *"jurisdictions have taken or are considering different approaches towards implementing"* the 10 recommendations arising out of the original FSB Stablecoin Report. Overall, implementation remains at an early stage, and given this combined with the rapid evolution of the stablecoin landscape, the FSB appears concerned that "differing regulatory classifications and approaches to stablecoins at jurisdictional level could give rise to the risk of regulatory arbitrage and harmful market fragmentation"[109].

The UK government regulatory approach to cryptoassets and stablecoins

On 7 January 2021, Her Majesty's Treasury **(HMT)** published a consultation document encouraging feedback on the government's approach to cryptoasset regulation, with a focus on stablecoins (the **HMT Consultation**)[110]. This is a comprehensive consultation

102 "Consultative report – Application of the Principles for Financial Market Infrastructures to stablecoin arrangements", Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, October 2021, section 1.3.3
103 "Principles for financial market infrastructures", Technical Committee of IOSCO, Committee on Payment and Settlement Systems, Bank of International Settlements, April 2012
104 FSB Stablecoin Report, page 2
105 FSB Stablecoin Report, page 2
106 FSB Stablecoin Report, page 7
107 "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Progress Report on the implementation of the FSB High-Level Recommendations", Financial Stability Board, 7 October 2021
108 FSB Update Report, Executive Summary (page 1)
109 FSB Update Report, section 2 (Progress in implementation at jurisdictional level), page 12
110 "UK regulatory approach to cryptoassets and stablecoins: consultations and a call for evidence", HMT, 7 January 2021

document and worth reviewing for an indication of policy thinking and potential direction of travel in other jurisdictions. The consultation period ran from 7 January 2021 to 21 March 2021 and published its response to the consultation in April 2022[111].

The UK government intends to apply the principle of "same risk, same regulatory outcome" in developing regulations governing stablecoins[112] and will maintain an agile approach to reflect international discussions and the rapid development of stablecoins within a framework of objectives and broader considerations set by HMT and the UK Parliament[113]. This means defining "the scope of the regulatory perimeter and the objectives and principles applicable under that new regime" instead of prescriptive legislation or regulation[114].

In line with this approach, the Financial Services and Markets Bill **(FSMB)** was introduced to the UK Parliament on 20 July 2022. The FSMB introduces the concept of "digital settlement assets" **(DSAs)**, defined as:

> *"a digital representation of value or rights, whether or not cryptographically secured, that—*
>
> *(a) can be used for the settlement of payment obligations,*
>
> *(b) can be transferred, stored or traded electronically, and*
>
> *(c) uses technology supporting the recording or storage of data (which may include distributed ledger technology)"*[115].

DSAs clearly include the concept of stablecoins.

The FSMB extends the Bank of England's oversight of payment systems under the Banking Act 2009 to both payment systems using DSAs and DSA service providers, and payment systems regulations under the Financial Services (Banking Reform) Act 2013 to payment systems using DSAs[116]. The FSMB also empowers the Treasury, in consultation with the Financial Conduct Authority, the Bank of England and, where relevant, the Prudential Regulatory Authority and the Payment Systems Regulator,[117] to make regulations in connection with: payments that include DSAs, payment systems that include arrangements using DSAs, recognised DSA service providers, and service providers connected with or in relation to such systems and services, including in the event of their insolvency[118]. As at the date of this publication, such regulations are not yet available.

In the absence of the regulations, the HMT Consultation includes some high-level requirements which may form part of any authorisation regime and are set out in section 3.23. These include capital and liquidity requirements, accounting and audit requirements, reserve asset maintenance and management, and orderly failure and insolvency requirements among other requirements. As discussed in the next few paragraphs, the UK government considers that a systemic stable token arrangement "could be assessed for Bank of England regulation in the same way that current payment systems and service providers are (i.e. when potential disruption could lead to financial stability risks"[119], extending this criteria to stablecoins performing a retail or wholesale payment system function[120]. A stablecoin arrangement with "significant potential" to be systemic at launch would need to be captured from launch by such regulation[121], echoing the FSB Report.

111 "UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence",
112 HMT Consultation, section 2.1
113 HMT Consultation, section 2.3
114 HMT Consultation, section 2.5
115 FSMB, Part 1, Chapter 2, section 22(2)
116 FSMB, Part 1, Chapter 2, section 21
117 FSMB, Part 1, Chapter 2, section 22(8)
118 FSMB, Part 1, Chapter 2, section 22(1)
119 HMT Consultation, section 3.31
120 HMT Consultation, section 3.32
121 HMT Consultation, section 3.32

The concept of systemic risk can extend to other participants in stablecoin arrangements, such as wallet providers where wallets are used at scale, meaning they may also be caught within a future regulatory framework[122].

Seeking to capture stablecoin arrangements including issuers or participants that are not based in operating from the UK, the UK government is considering whether "firms actively marketing to UK consumers should be required to have a UK establishment and be authorised in the UK", with options ranging from UK presence and authorisation, through to conducting activity in the UK and determining whether UK authorisation is requirement, or no location requirements[123]. This may also extend to location requirements for systemic stablecoin arrangements[124]. As at the date of this report, there are no further details available in the FSMB or the government's response to the HMT Consultation feedback. This approach may also be considered by governments and regulators in other jurisdictions, giving rise to the possibility of stablecoin issuers and other participants in stablecoin arrangements requiring multiple authorisations, although some regulatory regimes may recognise authorisation or its equivalent in other jurisdictions operating a suitable or equivalent regime. Legal practitioners should be aware of the development of regulatory regimes when advising clients and the possibility of full licensing requirements or treatment of licensees in other jurisdictions on either an exemption or "lighter touch" basis.

General considerations

Constituent components of stablecoin arrangements may be subject to different regulatory treatment depending on its role within the stablecoin ecosystem, whether the stablecoins themselves are systemically important or not.

For example, the BoE June 2021 Discussion Paper (which sets out helpful legislative development context in Box H) expects that:

> *"Payment chains that use stablecoins should be regulated to standards equivalent to those applied to traditional payment chains. Firms in stablecoin-based systemic payment chains that are critical to their functioning should be regulated accordingly."*[125]

The BoE also notes that the need to consider different regulatory regimes for systemic and non-systemic stablecoin arrangements, which could include "clarity of regulatory expectations for industry, the need for minimum standards across all stablecoins used for payments, impacts on competition and innovation, and how to ensure a smooth transition between future regimes for non-systemic and systemic stablecoins", including managing any "cliff-edge" effects between regimes if a stablecoin grew to be systemic over time[126].

On stablecoins themselves, the BoE's position is that:

> *"Where stablecoins are used in systemic payment chains as money-like instruments they should meet standards equivalent to those expected of commercial bank money in relation to stability of value, robustness of legal claim and the ability to redeem at par in fiat."*[127]

This BoE June 2021 Discussion Paper considers different regulatory models for meeting the Financial Policy Committee expectations[128], noting that some stablecoin issuers already operate under electronic money regulations (which may need enhancements)[129].

122 HMT Consultation, section 3.36
123 HMT Consultation, section 3.38
124 HMT Consultation, section 3.39
125 BoE June 2021 Discussion Paper, section 5.1
126 BoE June 2021 Discussion Paper, section 5.3.5
127 BoE June 2021 Discussion Paper, section 5.2
128 "Financial Stability Report, Financial Policy Committee Record and stress testing results – December 2019", Bank of England, December 2019. These expectations are that: "Payment chains that use stablecoins should be regulated to standards equivalent to those applied to traditional payment chains. Firms in stablecoin-based systemic payment chains that are critical to their functioning should be regulated accordingly." and "Where stablecoins are used in systemic payment chains as money-like instruments they should meet standards equivalent to those expected of commercial bank money in relation to stability of value, robustness of legal claim and the ability to redeem at par in fiat."
129 BOE June 2021 Discussion paper, sections 5.3.1 and 5.3.5

As with the FSB Stablecoin Report, the BoE envisages a proportionate and risk-based approach and aims to implement any regulatory models so that users can substitute between different forms of money without consequence for their level of protection[130].

BCBS proposed capital requirements

As a brief comment, it is also worth noting the BCBS's Consultative Document on the prudential treatment of cryptoasset exposures (the **Basel Consultation Document**)[131]in relation to stablecoin. In short, this proposes new guidance on the application of current rules to stablecoin holdings by applicable financial institutions (i.e. banks) to capture the risks relating to stablisation mechanisms (with further consideration for capital add-ons).

The Basel Consultation Document proposes that stablecoins which "have a stabilisation mechanism that is effective at all times"[132], based on a "redemption risk test" and a "basis risk test" set out in SCO60.12 to SCO60.1, be eligible for inclusion in 'Group 1b' cryptoassets. By contrast, all other stablecoins will fall into 'Group 2a' cryptoassets (that fail to meet the classification conditions but pass the Group 2a hedging recognition criteria) or 'Group 2b' (that fail to meet the classification conditions and fail the Group 2a hedging recognition criteria). Algorithm-based stablecoins or those stablecoins that use protocols to maintain their value are not eligible for Group 1[133].

The Basel Consultation Document's treatment of stablecoins relates to stablecoin holdings, rather than stablecoins issued by the relevant financial institution. It proposes that 'Group 1' cryptoassets be eligible for capital treatment generally based on the existing Basel III framework exposure to 'Group 2' cryptoassets (i.e. those not falling to be classified under Group 1a (tokenised traditional assets) or Group 1b (stablecoins) will be subject to a conservative prudential treatment based on a 1250% risk weight applied to the maximum of long and short position of each type of cryptoasset. The intention is for the capital to be "sufficient to absorb a full write-off of the cryptoasset exposures without exposing depositors and other senior creditors of the banks to a loss"[134]. At a minimum, this approach requires banks to hold risk-based capital at least equal in value to their Group 2 cryptoasset exposures, with additional risk-based capital holding requirements where such exposure includes short positions. This approach may inform the design and reserve decisions of banks seeking to issue their own stablecoins backed by one or more virtual assets held other than in a 1:1 reserve ratio.

No stablecoin in any group will be an eligible form of collateral in itself for the purposes of recognition as credit risk mitigation, as "the process of redemption adds counterparty risk that is not present in a direct exposure to a traditional asset"[135].

Local law

As indicated above, regulators and international bodies are working to identify the risks posted by stablecoins and develop principles for stablecoin-specific regulatory regimes. However, even where regulatory regimes dedicated to Stablecoins have not yet been implemented, stablecoin arrangements may be subject to existing law and regulation.

As noted below, this will include existing financial services regulation. Some stablecoins will meet the definition of "electronic money" and need to be regulated under relevant financial services legislation (such as the Electronic Money Regulations 2017 and the Payment Services Regulation in the UK) (see 5.3.4 of the BoE June 2021 Discussion Paper). Some stablecoin models could be structured as bank deposits,

130 BOE June 2021 Discussion Paper, section 5.3.5
131 "Consultative Document – Prudential treatment of crypto asset exposures", Basel Committee on Banking Supervision, Bank of International Settlements, June 2021
132 Basel Consultation Document, "Refinement of the classification conditions", page 3
133 Basel Consultation Document, "Introduction", page 1
134 Basel Consultation Document, section 3, page 18
135 Basel Consultation Document, section 2.1, page 13

in which case the issuers would need to be regulated as banks (see article 5 of the Regulated Activities Order 2001 for the UK, and recently published news articles on this possible approach in the United States of America[136]). These will be concerns for legal practitioners advising clients forming or involved in a stablecoin arrangement. As noted below, payment services regulation is also a relevant consideration.

It may be advisable to consult regulators, such as the FCA in the UK, if there is doubt as to whether a regulated activity is being carried out. Regulators are likely to scrutinise cryptoasset arrangements closely, so open and constructive cooperation would be advisable.

Counterparties to potential Stablecoin transactions will need to understand (and legal practitioners may need to advise on) matters such as:

— whether the stablecoin holder has a legal claim against an issuer or any other party by which they can redeem the stablecoin for fiat currency or some other asset

— the party against whom a stablecoin holder may claim

— the assets backing the stablecoin

— what happens if the stablecoin issuer or the person against whom a claim may be enforced fails, and which claims take priority in an insolvency situation

— data protection, anti-money laundering and legal and regulatory obligations of participants in stablecoin arrangements

— the role of other entities or participants in a stablecoin arrangement and the associated risks, e.g. is the client taking credit risk on the entity that holds the backing assets (if any)? What protections and procedures are in place to ensure there are no operational failures, e.g. errors in the ledger recording ownership?

Regard should be had to the stabilisation mechanism, properties and ecosystem participant role to determine whether existing banking, electronic money or payment/money transmission laws or other financial services regulation may apply in connection with the stablecoin arrangements and relevant activities.

Further, if the underlying assets constitute securities, the relevant stablecoin may be subject to local securities laws. The stablecoin arrangement may also constitute a money market or other form of collective investment vehicle (as noted in the IOSCO Stablecoins Report[137]), in which case the arrangement may be subject to regulation under local collective investment vehicle laws.

A business offering infrastructure or services connected with stablecoins may also be subject to local financial services regulation. As noted in the BoE June 2021 Discussion Paper[138]: *"If stablecoins are used to facilitate retail payments, regulation of payment services and critical payment system infrastructure would need to apply to ensure consumer protection and the overall resilience of the network of systems involved."* The position will vary by jurisdiction, but legal practitioners should consider whether a client's stablecoin-related operations fall under relevant financial services regulation in the same way that they might if such operations related to fiat currency.

Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT)

The FATF reported to the G20 on stablecoins from an AML/CFT risk perspective in June 2020[139] and its treatment of stablecoins forms part of the draft Updated FATF Guidance, first published in March 2021 and finalised and published on 28 October 2021. The FATF is explicit that [140]

136 "Biden Administration Seeks to Regulate Stablecoin Issuers as Banks", Wall Street Journal, 1 October 2021
137 IOSCO Stablecoins Report, pp 7-8
138 BoE June 2021 Discussion Paper, section 5
139 "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins", FATF, June 2020
140 Draft Updated FATF Guidance, Box 1

Careful analysis must be undertaken for each participant in a stablecoin arrangement or stablecoin issuer to determine whether they constitute a "virtual asset service provider" subject to AML/CFT regulation under local AML/CFT laws. As a stablecoin is unlikely to be considered as legal tender under local law, its issuer may be subject to the FATF Standards as they apply to virtual assets and VASPs. At a minimum, this may require some form of registration with the local responsible supervisory body. This may impact transaction sequencing and timings – for example, a stablecoin issuer may need to be registered or licensed by the relevant local authority prior to commencing operations.

Parallel regulatory systems and regulatory overlap

Stablecoin arrangements and intermediaries may be subject to multiple regulatory regimes, and oversight by multiple regulatory or supervisory bodies, depending on the properties of the Stablecoin, role of the participants or intermediaries, and whether the stablecoin arrangements are deemed to be, or likely to be, systemically important.

Conclusion

Stablecoins are the subject of significant ongoing policy, legal and regulatory analysis by governments and the global regulatory community. As policy and regulation evolves and is adopted globally or implemented locally as appropriate, legal practitioners should closely monitor reports, guidance and statements from relevant authorities to understand the policy and regulatory direction of travel and advise clients accordingly.

The nature of stablecoins and the activities of related service providers means that participants in this area may be subject to regulatory oversight from more than one supervisory body and under more than one regulatory framework. This means participants require complex yet comprehensive analysis and advice from legal advisors with a deep and current understanding of the sector in particular and the legal and regulatory matrix in general. In the absence of bespoke and jurisdiction-specific stablecoin regulations, a client's obligations under existing laws and regulations and preparation for compliance with potential future regulatory frameworks should be carefully considered when advising on stablecoin issuance, offering stablecoins within jurisdictions or their acceptance as a means of payment, particularly if there is a cross-border element to the transaction.

PART C:
DeFi and The Case for On-Chain Crypto Compliance, through the use of Blockchain Technology

Joey Garcia, Isolas LLP (Gibraltar)

Part C considers global trends in the regulatory environment for Virtual Asset Service Providers **(VASPs)** and the interplay with developing concepts of Decentralised Finance (**DeFi)** along with on chain compliance.

1. DeFi

Global Regulatory VASP Standards

The Financial Action Task Force (FATF) Interpretative Note to Recommendation 15 (INR. 15) on New Technologies published in June 2019 has been widely recognised and acknowledged as a significant step in the development of standards in the virtual assets space. These updates were also welcomed by the United Nations Security Council in Resolution 2462 of March 2018[141], which called on Member States to assess and address the risks associated with virtual assets, and encouraged Member States to apply risk-based anti-money laundering and counter-terrorist financing regulations to VASPs and identify effective systems to conduct risk-based monitoring or supervision of VASPs.

141 https://undocs.org/en/S/RES/2462(2019)

The 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' aimed to ensure that countries apply the same, or if not higher standards of AML/CFT to VASP related activity as is applied to other regulated financial services industries. In essence, to apply a full range of AML/CFT preventative measures to an industry which was largely not subject to effective regulation, supervision or AML/CFT controls, while at the same time providing a wide global and cross-border payments infrastructure for the transfers of value in an unregulated context.

While the focus of the FATF Recommendations was around the strengthening of standards to clarify the application of AML and CFT requirements on virtual assets and VASPs, the requirements have been on the basis of "licensing or registering" such providers and subjecting them to supervision or monitoring without defining such standards. As a global and intergovernmental organisation which sets international standards that aim to prevent money laundering and terrorist financing, the FATF is not a regulatory authority or organisation and as such, the standards for such licensing or registration were not, and will not be defined by the FATF. Section 80 of the original Recommendations[142] included references to authorities imposing conditions that should allow for "sufficient supervisory hold" and which could *"potentially include, depending on the size and nature of the VASP activities, requiring a resident executive director, substantive management presence, or specific financial requirements"*. The updated 2021 Guidelines[143] refer to new "Considerations for licensing and registering VASPs" but the licensing and registration criteria are defined as criteria which "give national supervisors confidence that the concerned VASPs will be able to comply with their AML/CFT obligations". The updated Recommendations also note that jurisdictions "should encourage a culture of compliance with all of a jurisdictions' applicable legal and regulatory requirements. These may address a range of policy objectives, including those related to investor and consumer protection, market integrity, prudential requirements, and/or national and economic interesting, in addition to AML/CFT."

At present, there are dramatically different approaches being taken globally in respect of VASP regulation or registration and substantially different 'standards' of licensing, registration or regulation while maintaining the notable requirement for countries not to rely on any self-regulatory body for the purposes of supervision or monitoring. Many jurisdictions have aimed to capture VASP related activity within the scope of AML requirements and a registration process, while others have sought to bring the activity, or are aiming to bring the activity within the scope or prudential supervision with substantially different requirements.

To provide more specific detail, the second 12-month review of the revised FATF standards on virtual assets and VASPs covered the state of implementation by the public sector through the global network of the FATF. Of 128 jurisdictions which provided responses to the assessment on a self-assessment basis, and not subject to independent review or to an official FATF assessment, only 58 reported that they had necessary legislation to implement R15/INR/15, with 35 reporting that their regime was operational[144]. Only a minority of jurisdictions had conducted examinations, and even fewer were reported to have imposed any enforcement actions. 32 jurisdictions reported that they had not yet decided what approach to take for VASPs and therefore do not have an AML/CFT regime in place and have not commenced a legislative/regulatory process. Similarly of the 52 jurisdictions which reported that they had established regulatory regimes permitting VASPs, 31 had established only registration regimes and only 17 licensing regimes.

142 https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
143 Section 131 to 140 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html
144 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html#:~:text=Paris%2C%205%20July%202021%20%E2%80%93%20The,and%20virtual%20asset%20service%20providers.&text=The%20report%20finds%20that%20many,implementing%20the%20revised%20FATF%20Standards.

This creates specific considerations from a regulatory arbitrage perspective as operators in the space are in many circumstances highly mobile, or at times partially decentralised work forces aiming to establish principle operations in a secure environment from a legal and regulatory perspective. While some operators and businesses target the highest standards available, others clearly target jurisdictions where there are gaps in the activity captured within the scope of licensing or registration requirements, or where authorities have not developed the experience or knowledge to actively monitor such activity.

VASP 'activity': global Interpretations and implementations

While the standards for VASP registration or licensing are extremely wide and varied around the world, there are similar considerations in respect of the 'activity' captured. In the second 12-month review by the FATF, concluded in June 2021, of the 52 jurisdictions having established registration or licensing regimes, 15 noted that they had not covered all VASPs defined in line with the FATF definition. However, even these definitions, as set out below, are subject to broad questions of interpretation and enforcement.

For the purposes of a general summary, the FATF definitions of a VASP are as follows:

*"**Virtual asset service provider** means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:*

- *exchange between virtual assets and fiat currencies;*
- *exchange between one or more forms of virtual assets;*
- *transfer of virtual assets;*
- *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
- *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."*

These definitions did create some issues for countries which had sought to regulate VASP activity prior to the publication of these Guidelines in June 2019. One of these is Singapore, a hub of activity in the Asia region, which transposed the amendments to the Payment Services Act in January 2019. This did not capture custodian wallet providers, but steps are being taken to expand the definitions there for consistency with the FATF definitions. Similarly, from an EU perspective the 5th Anti Money Laundering Directive which brought a platform used to exchange fiat currencies and virtual currencies within the definition of an obliged entity but did not capture an exchange between different forms of virtual assets within scope.

This is in fact a very wide global issue from the perspective of regulatory consistency. The following are a few global examples of the approaches being taken:

In **Nicaragua**, the Regulation of Financial Technology Payment Service Providers (Resolution CD-BCN-XLIV-1-20 approved on September 23, 2020) defines "Financial Technology Payment Service Providers" as: *"Legal entities authorized by the BCN, engaged in providing payment services with digital wallets, mobile points of sale, electronic money, virtual currencies, electronic trading and exchange of currencies and/or funds transfers."* The activities subject to registration there related to the management of virtual platforms on which virtual assets are traded and to provide such virtual assets (suppliers).

In **Vietnam**, ranked first in the world in terms of adoption rates of individuals and users within Vietnam by the Global Chainalysis Adoption Index[145], there is as yet

145 https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index

no legal definition of a crypto currency or virtual asset although the State Bank of Vietnam has publicly announced a pilot project to form part of the strategy towards the development of a digital economy[146].

In the **Philippines**, the Bangko Sentral ng Pilipinas (BSP) issued circular 944 in 2017 establishing itself as arguably the first to formally regulate digital currency services, by capturing digital currency exchanges as remittance and transfer companies. They have since issued Circular 1108 in January 2021[147] and changed the scope of virtual assets regulation within the Philippines. The definition of a Virtual Asset Service Provider is now aligned with the FATF VASP definition but excludes the 5th limb of the FATF definition being the "participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset". This is because such activity and any activity relating to an Initial Coin Offering (ICO) falls under the regulatory purview of the Securities and Exchange Commission in the Philippines[148].

In **Thailand**, the Digital Asset Management Act BE 2561 was enacted in May 2018 and the Securities and Exchange Commission (SEC Thailand) was granted authority to regulate the space under separate categories: a Digital Asset Exchange, Digital Asset Broker, Digital Asset Dealer, ICO portal, and a Digital Asset Investment Advisory categorisation[149]. Restrictions are also in place in Thailand and the SEC approved new rules in June 2021 to prohibit regulated digital asset exchanges from providing services in relation to utility tokens and certain categories of cryptocurrencies[150]. This included meme tokens, fan tokens, non-fungible tokens (NFT) and digital tokens issued by digital asset exchanges or related persons. This restriction was introduced largely on the basis that they involve significant risk and are designed for speculative purposes creating significant market risk. The listing of any asset on any regulated platform is also subject to consent by the SEC.

In **Indonesia**, the Minister of Trade Regulation 99 of 2018 formally permitted the trading of cryptoassets in Indonesia as futures contracts, and brought such activity within the scope of the Commodity Futures Trading Supervisory Authority ("Bappebti"). Bappebti Regulation No5 of 2019 provided a regulatory framework for the operation of physical cryptoasset futures market. This essentially means that the trading activity may be regulated but its application or use as a payment instrument is prohibited in the jurisdiction. Generally speaking, the activities falling within the scope of regulation are defined as Cryptoasset Exchanges, Cryptoasset Clearing Agencies, Cryptoasset Traders, Cryptoasset Clients, and Cryptoasset Storage Providers, all subject to separate requirements under local law.

In the **UK** the registration requirements for VASP related activity is captured by the activity defined under Regulation 14A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs). In summary this captured cryptoasset exchange providers (both fiat to crypto and crypto to crypto) and custodian wallet providers. Whether these definitions are consistent with the FATF definitions, particularly in respect of concept of "safekeeping" and instruments enabling "control" of virtual assets or smart contracts to which the business is not a party, is beyond the scope of this section but analysis against the FATF VASP definitions, accompanying guidance and international consistency on the way that these activities are legislated for, is a relevant consideration.

Cross-border considerations, VASP activity and virtual asset categorisations

The examples from the jurisdictions above are provided only to demonstrate some of the issues in the international approaches and consensus around the regulation of the space. It also provides some high-level consideration factors for advisors in the

146 https://www.vietnam-briefing.com/news/vietnam-establishes-research-group-study-regulations-cryptocurrencies-
147 https://www.bsp.gov.ph/Regulations/Issuances/2021/1108.pdf
148 https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/FAQs_VASP.pdf
149 https://www.sec.or.th/EN/Pages/Shortcut/DigitalAsset.aspx#AUDIT
150 https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=8994

space. There are a number of jurisdictions that make the use of any form of virtual currency for any form of 'payment transaction', completely illegal. There are other countries where there are legislated for 'approved' cryptoassets that may be traded on a regulated market[151] as well as specific approval criteria. Authorities in other jurisdictions also take very different approaches as to when they deem licensed 'activity' to be conducted in that country. While many large and global operators in the space rely on principles of reverse solicitation, and to not actively soliciting business from certain countries, many do not consider these rules on a jurisdiction by jurisdiction international basis and the intricate details relevant for certain countries around the world are sensitive and should be considered when being serviced from the UK.

Also, importantly, the categorisation of a 'virtual asset' under local law may at times bring the activity within the scope of existing regulatory perimeters. The most obvious example of this is the USA where FinCEN issued interpretative guidance in 2013[152] to clarify the applicability of the regulations implementing the Bank Secrecy Act to persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies, and bringing such activity within the scope of money services businesses. However, there are many examples of this and virtual asset classifications around the world are generally not consistent with the Final Guidance on Cryptoassets[153] issued by the Financial Conduct Authority in July 2019 and registered firms in the UK will also need to consider the implications of the categorisation of an unregulated token in the UK in other jurisdictions where such assets may be acquired and used through the UK platform. The asset or indeed the service categorised in respect of the transaction hosted or serviced in the UK, may be treated differently at its destination or originating address, and this is something that may need to be considered.

The Regulated VASP and the evolution of Decentralised Finance (DeFi)

The context of VASP activity and the legislation of the FATF VASP definitions into local law, and how such activity has been defined is also particularly relevant in the context of the global DeFi developments.

DeFi is a very broad term for financial services which are disintermediated, with no centralised point of authority or single point of failure as they are built on the decentralised infrastructure of blockchain technology. There are many types of business models and structures, or decentralised applications (DApps), which aim to replace traditional forms of intermediation. The strongest proponents of DeFi often make underlying arguments relating to the concepts of financial inclusion and allowing access to such services to any person with access to a computer and an internet connection. The design of DeFi services are typically built on programmable and open architecture and are non-custodial by design so that assets issues or managed cannot be accessed, altered or moved by any party other than the account holder. The applications are also typically trust-less in the sense that there is no 'trust' required in any central counterparty or intermediary as the trust is in the logic of the rules determined by the logic and rules of the DeFi protocol in question. The design of DeFi infrastructure is for direct participation on a peer-to-peer or peer to platform systems, and all features and functionality are coded and once executed are immutable on the underlying blockchain in a tamper-resistant and transparent form. The lack or a centralised counterpart or responsible entity also creates new frontiers to the possibilities of efficient regulatory control or standards from a consumer protection perspective.

151 Bappebti also recently enacted Regulation No.7 of 2020 defining this list in Indonesia. http://bappebti.go.id/resources/docs/peraturan/sk_kep_kepala_bappebti/sk_kep_kepala_bappebti_2020_12_01_i6tg8tfb_id.pdf
152 https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
153 https://www.fca.org.uk/publication/policy/ps19-22.pdf

How relevant are DeFi developments to authorities and policy makers in the UK?

In the case of many (DeFi) initiatives, protocols, applications and developments, some jurisdictions are aiming to determine whether such activity is 'decentralised' in more than name only, or how the risks in the developing application of decentralised exchanges, and protocols can be identified, managed, monitored or mitigated. The UK position is interesting in the context of the DeFi Adoption Index, published by the blockchain analytics group Chainalysis.[154] The adoption index was calculated by reference to three component metrics:

(1) on-chain cryptocurrency value received by DeFi platforms weighted by PPP per capita;

(2) total retail value received by DeFi platforms; and

(3) individual deposits to DeFi platforms weighted by PPP per capita.

The UK was ranked 4th in the world under these metrics. It is ranked 3rd in the world behind the USA and China in terms of the value sent to DeFi in retail transactions and web visits to DeFi platforms. Of similar interest is the fact that the region of Central, Northern and Western Europe accounts for 25% of the global value of cryptocurrency value received, turning this into the world's largest cryptocurrency economy. Within this, the UK is by some way the largest contributor to that regional metric, accounting for around $170 billion of the value received during the period of July 2020 to June 2021. This is referenced under this section as 49% of this value is made up of value sent to DeFi protocols.

This is consistent with the DeFi trends around the world where Uniswap now accounts as the largest cryptocurrency service by transaction volume in the USA, outperforming Coinbase.com which is followed closely by another Dex, the dYdX exchange.

Decentralisation as a concept

The DeFi space has seen exponential growth since the first edition of this guidance, but the fundamental question of when a DeFi-based operation falls within the scope of registration or licensing requirements or outside of the wider scope of the VASP categorisation or definition is currently one of interpretation.

Unfortunately, there are many blockchain-based services that pursue the idea of decentralisation on the understanding that this automatically brings the activity within the concept of a 'software service' and not a virtual asset based service, or financial service, and outside of the scope of any form of regulation. One of the clearest examples of this was the Etherdelta decentralised exchange (Dex) which was the most popular order book exchange service a few years ago. The US judgement is a matter of public record[155] and cites various factors that distinguish Etherdelta from a real peer-to-peer trading platform. In summary, these included the fact that:

1. The EtherDelta defendant, Mr. Zachary Coburn, maintained a list of 'official token listings' that were available for trading, and would request certain information from that issuer, performing his own due diligence before the 'listing' could take place. This was despite the fact that any token that was ERC20 compliant could 'function' on the platform.

2. Orders on EtherDelta did not change the state of the Ethereum blockchain (so no 'gas fee' was applied on any trade). All orders were stored on EtherDelta's order

154 https://blog.chainalysis.com/reports/2021-global-defi-adoption-index
155 https://www.sec.gov/litigation/admin/2018/34-84553.pdf

book which was maintained on a centralised server maintained by EtherDelta (and not on the Ethereum Blockchain).

3. Mr Coburn would keep users appraised of key events, announcements on the platform's operations and deal with user questions directly. Similarly, public forums allowed for users and EtherDelta representatives to post questions and answers.

4. Perhaps critically, EtherDelta did not charge fees to the maker of a contract in order to incentivise orders to be placed but did charge a 0.3% fee of a transactions trade volume which was identified as the 'fee account'.

Although there is no 'test' for decentralisation as a legal concept, the FATF have noted that a peer-to-peer trading platform or peer-to-peer provider can be captured within the definition of a VASP but will not always be captured. If a Dex is seen to "conduct or facilitate" the activity as a business, on behalf of another person, it may be seen to be providing the services of an exchange and being itself categorised as an exchange or VASP. The reality is that there are a number of factors that should be considered before a determination may be made on the specific facts of that arrangement or service.

DeFi regulatory approaches, interpretations and approaches

In the UK the MLR's wording includes the definition of a cryptoasset exchange provider as a firm or sole practitioner who by way of business provides services relating to exchanging or *arranging or making arrangements* with a view to the exchange of one cryptoasset for another. The Joint Money Laundering Steering Group (JMLSG) have issued guidance[156] which refers to the broad definition and potentially including activities relating to a dedicated peer-to-peer platform. The guidance also refers to bids and offers traded at an outside venue through individual wallets or other wallets not hosted by the forum or a connected firm may not be captured. However, it is clearly noted that that such business models will be considered on a case by case basis and there is no binary test as to when such activity will or will not be caught by the requirements for registration. Software developers and providers are noted as being more likely to fall outside of the scope of the definition if they derive no income or benefit from consequent transactions.

The interpretation around *"arranging or making arrangements"* is of course not exclusive to the UK. At an EU level the proposed Markets in Cryto-Assets Regulation (MiCAR) defines the *"operation of a trading platform for cryptoassets"* as a Crypto Asset Service, making the business a Crypto Asset Service Provider (CASP). This activity is defined as managing a platform *"within which multiple third-party buying and selling interests for cryptoassets can interact in a manner that results in a contract"*. The execution of orders for cryptoassets on behalf of third party, and the reception and transmission of orders for cryptoassets are also defined CASP activities and could also have DeFi touch points and regulatory triggers subject to the interpretation of those provisions in Member States. Similarly, in other jurisdictions around the world, there is common use and reference to the word "facilitation" of trading activity. One example of this is Thailand where a Digital Asset Exchange is defined as a *"center or a network established for the purposes of trading or exchanging digital assets, which operates by matching orders or arranging for the counterparty, or providing the system or facilitating a person who wished to trade or exchange digital assets to be able to enter into an agreement or match the others…"*.

Of course, one key question is whether bringing all such activity within the scope of existing VASP, or financial services regulation is possible and enforceable. Who or what is the counterpart to such an action? Should the developer of the code be made responsible for the activity conducted on any protocol as this is wholly

156 Section 22: https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf

inconsistent with other technical infrastructures currently in operation around the world. Should the question of the 'controller' of any smart contract on which activity is conducted maintain a level of responsibility and accountability? The current updated version of the FATF guidelines[157] points towards "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements" falling under the FATF definition of a VASP where they are providing or actively facilitating VASP services. Of course, how these guidelines are considered and transposed into local law in different countries still remains to be seen. A relevant issue is that the most commonly cited reasons for the lack of implementation of the 2019 FATF guidelines across the respondent jurisdictions included an "apparent lack of VASPs based in their jurisdiction" and a "lack of expertise and understanding" regarding virtual assets and VASPs, as well as resource constraints and restrictions arising from the COVID-19 pandemic. This of course related to the guidelines relating to (primarily) centralised exchanges and custodians/wallet providers. The extent to which authorities are prepared to consider the intricate complexities of DeFi infrastructure and activity from a regulatory perspective will be a relevant factor in the transposition of these recommendations.

DeFi risks and new approaches

It also remains to be seen whether relevant authorities will adopt the use of the technology available to address the relevant DeFi related risks. These risks are well reported[158] and involve new forms of financial risk due to the transactional behaviour of users of the service, specific counterparty risk to the underlying code, as well as liquidity and market risk. There are also technical and operational risks, and some of these have historically led to DeFi rug pulls where developers effectively abandon a project by exploiting smart contract vulnerabilities and draining assets from liquidity pools, or altering smart contracts containing project vault business logic, and draining funds. However, critically there are significant legal compliance risks relating not only to the regulatory risk of the platform, but also to financial crime. While many DeFi projects propose to be motivated by the idealistic concepts of financial inclusion they are also used for illicit purposes. Some analytics and compliance companies such as Coinfirm[159] provide DeFi/DEX liquidity pool risk assessments and these reports show quite clearly the exposure to potentially material AML, CFT and sanctions risk indicator breaches. The liquidity pools of larger unregulated DEX platforms will often show direct links, through the wallet addresses used to interact with the DEX, of mixers and tumblers, hacks, terrorist financing, ransomware, darknet and deep web touch points, as well as sanctions breaches.

Different approaches may be taken to address such risks including the development of compliance oracle systems which restrict such transactions from being able to execute on any decentralised platform. Digital Identifiers (DIDs) are also a developing new form of identifier that enables verifiable digital identity, including KYC verification and wallet address white listing processes to allow only such verified individuals to interact with a decentralised platform. There are also proof of kyc broadcasts (with no personal data) capable of being broadcast to public blockchain so that the proof of KYC is published on-chain and access to the underlying data is available only through specific nodes with the relevant authority attached.

While this section will not be able to consider each of these solutions in detail, what is clear is that the application and use of the technology may also be used to address many of the compliance related risks which are the primary focus for most authorities at present.

Similarly, authorities will need to consider the management of risk through the centralised access points to DeFi infrastructure and the (centralised) CeFi<>DeFi bridges which are being developed to allow users of regulated platforms access to the underlying benefits of these systems and services.

157 Section 67: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html
158 World Economic Forum: (DeFI) Policy-Maker toolkit: https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit
159 Coinfirm – Blockchain Analytics

Conclusion

The standards of VASP regulation and frameworks being developed are evolving around the globe. Arguably there are gaps to be addressed in terms of providing a regulated ecosystem with which users are able to interact and use in a secure and reliable way. Many registration regimes are aimed at complying with FATF recommendations from a purely compliance basis and arguably not aimed at identifying some of the core underlying issues. These may relate to the integrity of the markets being developed, and applying appropriate market abuse standards, client asset protection and segregation, capital adequacy and insurance, or even listing and transaction monitoring requirements. Different jurisdictions are accelerating such developments and the questions for any financial centre aiming to provide a solid legal foundation for such platforms and developing businesses should be considered.

Similarly, the pace of the development of the technology, and in particular the DeFi space is accelerating at a faster pace than most authorities are able to monitor and develop. Providing clarity and certainty around such developments is key and exploring mechanisms and standards to address new risks in new digital ecosystems is also important. The application of new technology and innovative development arguably requires a level of innovation to take place at a policy and regulatory perspective on at least a research basis.

The DeFi question, and categorisation within the scope or outside of the scope of a VASP related activity also has implications beyond the interpretation of FATF Recommendations. The commonly referred to "Travel Rule" defined under Recommendation 16 has been transposed into legislation in many countries in different ways. While some jurisdictions capture all transactions from an originating VASP wallet address to any beneficiary address (whether a VASP or unhosted wallet), others have sought to comply with the FATF recommendations through both threshold limits, and exemptions for transactions with un-hosted (non-VASP) destination beneficiary addresses, or by introducing "risk scoring" requirements for destination addresses with which originator and beneficiary details may not be shared. Whether a DeFi-related operation constitutes a VASP or a cryptoasset service provider in the UK or not, may in and of itself already have implications for jurisdictions which have transposed the Travel Rule requirements in this way. Whether there is a requirement for such information to be shared or not, will also need to be considered depending on the categorisation of the underlying address as a VASP, cryptoasset service provider or neither. At present under the proposed provisions specific to cryptoasset firms in the UK, an originating provider is not expected to send information to an unhosted wallet[160]. However, whether a non-custodied wallet, relating to a DeFi platform constitutes a cryptoasset firm is potentially not yet completely clear.

2. On Chain Compliance

Joey Garcia, Isolas LLP (Gibraltar), Dr Shlomit Azgad-Tromer Co-founder, CEO and Chief Legal Officer of Sealance Corp

Introduction

The development of regulatory standards and compliance frameworks for an emerging and developing market is a critical factor, particularly when the technology being used and implemented is also developing.

A recent US example – a bankruptcy filing by Celsius, a digital asset lending platform – revealed the names and transaction history of nearly half a million depositors. The

160 Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory instrument 2022. Consultation. Section 6.27: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004603/210720_SI_Consultation_Document_final.pdf

Celsius case also illustrates a risk that arises from the transparency and traceability of the blockchain. The privacy standard in most public blockchains is based on pseudonymity, which can be easily pierced to track user activity and balance. As a result, data leaks of names and wallet addresses can cause privacy harms to blockchain users, since anybody with an internet connection can easily match the on-chain activity and wallet addresses of named Celsius users disclosed in the filing with the dates and amounts of every transaction on their wallet, exposing wallet owners to the risk of theft or extortion.

To mitigate this risk, digital asset holders employ additional privacy enhancing technologies to protect confidentiality of their financial information. The problem is that current techniques to manage illicit finance risk on blockchains rely on transparency and traceability in order to assess user identity. As a result, the same tools used to protect legitimate privacy interests on public blockchains can also frustrate government investigations into malicious activity.

One widely used privacy protocol was Tornado Cash, which was sanctioned in summer 2022 by the US Treasury Department's Office of Foreign Assets Control (OFAC) on the grounds that it had been used in connection with more than $7 billion in illicit financial activity. This puts innocent blockchain users in a bind: rely on privacy through pseudonymity – which can be compromised – or have their funds associated with criminal activity, increasing the risk that they could face penalties, funds could be blocked, or their risk profile increased, potentially limiting their freedom to transact.

Arguably, this potential clash between privacy and compliance is an outcome that can be avoided using technological advances that can harness the power of the blockchain to enforce compliance in a privacy preserving manner, such that it sustains financial confidentiality and privacy for consumers and users, while providing law enforcement and regulators the tools required to enforce compliance, view suspicious information and prevent illicit activity with selective disclosure designated to specific authorised agents. These emerging technologies could serve to strike a better balance between national security, crime prevention and the fight against illicit finance, on the one hand, and the right to privacy, on the other, while harnessing blockchain technology. for its own native compliance.

This section identifies two fundamental premises of financial regulators in designing regulation for crypto markets and argues that — although useful — they face limitations as crypto markets, and the associated decentralised network services ('Web3'), mature. First, financial regulators assume compliance in crypto could lean on the role of financial intermediaries, and that these intermediaries indeed exist in the decentralised financial system, and moreover, are able and fit to carry regulatory responsibilities and, accordingly, liability. Second, financial regulators lean on the transparency of transactions on the blockchain, facilitated by the pseudo-anonymous nature of the users' wallet addresses, as an essential feature of crypto compliance, assuming that the traceability of transactions and addresses is an exclusive means to identify users, through heuristics, given the prominence of blockchain analytics as a methodology designed to enforce compliance-based surveillance and big data techniques. This second assumption about traceability as an exclusive tool renders anonymous and privacy preserving technologies as means to facilitate money laundering. Recent examples of these trends include the actions against Tornado Cash, but also the Virtual Asset Guidance published in October 2021 by the Financial Action Task Force, several stablecoin and digital asset bills being considered by the US Congress and the Markets in Crypto-Assets regulations (MiCA). These and many other jurisdictions are currently considering how to bring digital assets into the regulatory perimeter that applies to financial services, often leaning on the two assumptions that the methodology for compliance and enforcement in crypto can be manifested by expanding the search for financial intermediaries and by enforcing blockchain transparency and traceability.

We would posit that both these assumptions are not adequate for the permissionless and decentralised ecosystem of crypto. Anonymity and privacy are considered means of illicit finance despite representing fundamental values, simply because

current compliance methodologies lean on transparency and heuristic based surveillance. Likewise, the search for financial intermediaries as agents of legal enforcement in a decentralised financial system of peer to peer transactions lacking intermediaries, is arguably designed to fail. Digital assets in Web3 often lack an institutional issuer since they are created by individual users interacting with a protocol, and often users trade among themselves and with protocols using an unhosted wallet without financial intermediaries. Because of these incorrect assumptions, our view is that current regulatory frameworks lack the ability to address permissionless financial environments that characterise the emergence of Web3, and as a result could lead to regulatory gaps as these environments evolve. However, the ability of emerging technology to address the risks correctly identified by relevant authorities and policy makers, through the adoption of the technology to embed on-chain compliance by adopting the same consensus principles that underlie blockchain technology to programmatically enforce compliance obligations. It is therefore on that basis worth exploring the merits of such programmable on-chain compliance as a rule-based, blockchain native approach to crypto compliance.

How Crypto Compliance Works Today

Crypto compliance today is largely a replica of anti-money laundering regulation in traditional finance, in that these requirements assume the existence of an intermediary gatekeeper standing at the entrance to the financial system and confirming and validating the identity of participants[161].

In the following, we identify two flawed premises underlying current approaches to regulating Web3: the search for intermediaries in a decentralised environment, and the assumption that traceability and transparency are exclusive means to regulate this space.

The Search for Intermediaries

Current financial regulations target financial intermediaries responsible for performing critical aggregation and settlement functions on behalf of customers. Since these financial intermediaries maintain their transaction records on private, internal ledgers, modern financial regulations have placed financial obligations on them to ensure that they act in the interests of their customers, and otherwise mitigate information and economic asymmetries. To comply with these regulatory obligations, financial institutions implement regulatory requirements through policies, internal compliance controls and monitoring processes. Recognising that Web3 disintermediates the provision of financial services, current regulatory approaches search for alternative individuals or entities upon which to impose these regulatory obligations. However, such approaches do not generally taken into account a clear understanding of the underlying technology and are likely to fail since the alternative intermediaries identified typically do not possess the information to comply with relevant obligations or are ill-suited to regulatory compliance because they are functionally very different from traditional financial intermediaries.

Blockchain Analytics

Because most of the blockchain ledgers today are pseudonymous, law enforcement currently leverages blockchain analytic services that use heuristic, best-effort matching of public transaction information with private information. These heuristic techniques critically rely on the transparency of the blockchain and use big-data

161 From a US perspective the first anti-money laundering regime to arise was the so-called Bank Secretary Act ("BSA"), a series of U.S. statutes and regulations that emerged in the 1970s, have evolved over the intervening years, and were most recently revised through the U.S. PATRIOT ACT. Legislated for a financial system managed by intermediaries, the BSA's initial purpose was to ensure that banks would collect information about their customers (and their customers' counterparties and transactions) that would provide law enforcement with information designed to provide intelligence for prevention of crime. The BSA establishes reporting and recordkeeping requirements for regulated banks and Money Service Businesses (MSBs), including the filing of suspicious activity reports ("SARs") with FinCen in Treasury. A second tenet of anti money laundering is the requirement to Know Your Customer ('KYC") that is sometimes referred to as Customer Due Diligence (CDD) and is rooted in the Patriot Act and its amendments to the BSA.

techniques to identify and inspect it into data that can fuel compliance and risk management.

The Case for On-Chain Compliance

We believe that current approaches to crypto compliance are inefficient and unsustainable. As argued in the following section, imposing intermediary requirements from ad hoc decentralised players creates grave cybersecurity and espionage risks, undermines consumer protection, and threatens national security as blockchain technology gains broader adoption. Furthermore, it conflicts with the rights to financial confidentiality and to privacy, and jeopardises the innovation of decentralised finance with its promise. On-Chain compliance would address these concerns and provide a better, privacy preserving and blockchain native approach to regulating crypto ecosystems.

Consumer Protection and Information Security Risks

Forcing an intermediary-based approach on the decentralised crypto ecosystem presumes the existence of reliable entities that can collect the information, report it to law enforcement and keep it safe from cyber attacks. However, this is a problematic presumption, since in the decentralised settings many of the intermediaries (especially as captured by the aforementioned expansive definitions) are themselves ad hoc players who may be nefarious, and even if well-meaning, are incapable of protecting sensitive personal and commercial information. In particular, the collection and retention of personal information (e.g. names and physical address) of members of the public should not be carried by entities that are not well equipped to protect it, and lack the training, the resources and the culture of compliance to do so in a safe way. Imposing an intermediary status on such entities substantially increases the risk of data theft and concomitant harm to law-abiding citizens.

When blockchain-based assets are used for payments, as the vision of stablecoins entails, current crypto regulation would arguably not be suitable, appropriate or be able to deal with the inherent risks in the appropriate way. The intermediary-based approach may impose AML obligations on merchants who would be required to collect the personal information of all customers who make payments using an unhosted wallet, in order to relay this information to the money service businesses (MSBs) and banks that serve these merchants. Blockchain-based asset holders would thus be effectively required to disclose their home address to merchants they transact with. This is not merely impractical, but also arguably dangerous as an invitation to extortion or home invasion, if the merchant is rogue or had its systems compromised by a cyber attack. This risk is aggravated by criminals' ability to observe wallets' balances on public blockchains, to identify 'juicy' targets. (Recall that blockchain analytics and its transparency-based heuristics rely on such information being broadcast on public and immutable blockchains.) In a world where cryptocurrencies are a major payment currency, as the future of stablecoins and CBDC entails, transparency of every transaction is not merely an individual risk for a data breach, it is a potential espionage risk in exposing national financial data to prying eyes. Indeed, the prudent regulatory path would be to require stablecoins and CBDC to keep financial confidentiality as traditional banks do, but to allow them on-chain compliance mechanisms, compatible with their nature as a smart contract in a Web3 environment.

Crucially, on-chain compliance would be enforced without compromising the financial privacy and security of cryptocurrency users. While identity information may be recorded on the blockchain ledger, it could be cryptographically protected and not publicly visible. Instead, sensitive personal information (direct or derived) would be visible only to authorised parties, subject to the predetermined policy.

Blockchain-Native Approach: Regulating DeFi

Instead of enforcing principles of traditional financial regulation on a decentralised financial system, on-chain compliance allows regulators to harness the power of the blockchain to enable stronger blockchain based enforcement that is compatible with Web3 infrastructure. One prominent example of the need for an on-chain, blockchain-native approach to compliance is DeFi. DeFi protocols can be distinguished from traditional market infrastructures in several ways. First, typically assets in DeFi are held directly by users in 'unhosted' wallets or through smart contract-based escrow rather than by a centralised service provider or custodian in an account on the asset owners' behalf. Second, settlement and execution are conducted by software (smart contracts) rather than financial intermediaries. Rather than relying on a centralised service provider, operator, or organisation that ultimately exercises discretion, DeFi protocols are governed by open-source code. DeFi is a decentralised financial arena, with no intermediaries. Users may create intermediary or proxy contracts that redirect calls and transactions to a modified contract as a way of updating an earlier contract but they are always self sovereign and hold their assets directly without a custodian.

In the absence of an entity that can serve as an intermediary, on-chain compliance could regulate and enforce compliance in DeFi as a natural, programmable upgrade to the smart contract. For example, on-chain compliance can be compatible with unhosted (self-custodied) wallets without entrusting any third party with control or custody of the funds. Once unhosted users are identified and verified by a legitimate now your customer (KYC) provider, programmable on-chain compliance can monitor the trade and automatically issue reports off the blockchain, without any intermediary intervening in the process. Even for the most sophisticated compliance reports such as SARs, red flag tests can be coded into an on-chain policy and provide jurisdictional compliance.

This would arguably align the concept of DeFi regulation with the compliance focused regulatory standards set out under the FATF Recommendations which continue to be transposed in national law and regulation around the world. It would also allow for the development and use of the technology to address the relevant risks which are prevalent in the DeFi ecosystem, without the approach of defining every decentralised network, protocol or service as a Virtual Asset Service Provider and bringing the activity within the scope of legacy frameworks and standards.

Modernising AML Rules

On-chain compliance is an opportunity to modernise AML rules utilising consensus rules running on a blockchain. Instead of struggling to harmonise KYC practices, or exposing the financial system to a central panopticon with the implications on cyber security compromised, on-chain crypto compliance provides an opportunity for financial institutions to rely on other institutions' attestations and use them for risk management without moving information or exposing it to the user. Sanctions can be enforced on-chain and updated in real time, to prevent any transaction from going through absent compliance. And reports can be administered automatically off chain, saving important time and providing law enforcement with better chances to prevent crime from happening. Saving the redundancy of duplicate KYC checks in every entry would reduce the compliance burden from the financial industry, improve customer and user experience, and allow compatibility of the AML infrastructure with the future of stablecoin and CBDC payments, with robust enforcement that does not rely on intermediaries.

Conclusion

The current tension between privacy and compliance represents an uneasy compromise in traditional financial services that will be tested as crypto markets evolve and achieve broader mainstream adoption. In this evolving ecosystem, it is clear that the current regulatory solutions, which rely upon financial intermediation and blockchain analytics premised on the immutable and transparent nature of the blockchain, will confront limitations; and that attempts to force the regulatory model on decentralised and peer-to-peer transactions will broadly sweep in innocent conduct and hamper innovation in this space. This paper has suggested an alternative solution that can harness the power of modern cryptography and blockchain programmability to overcome the seemingly binary choice between compliance and privacy. Regulators and law makers assessing approaches to govern this evolving space of financial activity should assess the possibilities of adopting these novel tools, to achieve higher efficiency for compliance on the one hand, and privacy and information security on the other.