UK FINANCE

KPMG

The future regulation of unbacked cryptoassets in the UK

December 2022

UK Finance

UK Finance is the collective voice for the banking and finance industry.

Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

KPMG LLP

The views and opinions expressed herein are those of UK Finance members and do not necessarily represent the views and opinions of KPMG.

KPMG LLP, a UK limited liability partnership, operates from 22 offices across the UK with approximately 15,300 partners and staff. The UK firm recorded a revenue of £2.43 billion in the year ended 30 September 2021.

KPMG is a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organization or to one or more member firms collectively.

KPMG firms operate in 145 countries and territories with more than 236,000 partners and employees working in member firms around the world. Each KPMG firm is a legally distinct and separate entity and describes itself as such. Each KPMG member firm is responsible for its own obligations and liabilities. KPMG International Limited is a private English company limited by guarantee. KPMG International Limited and its related entities do not provide services to clients.

Contacts

If you have any questions about this report please contact:
Rhiannon.Butterfield@UKFinance.org.uk

Information on UK Finance can be found at:
www.ukfinance.org.uk

Please contact Corporate Affairs for press queries or general information:
info@ukfinance.org.uk

For information about membership of UK Finance, please contact:
membership@ukfinance.org.uk

Table of contents

Executive summary

UK Finance members believe in the value of an economy that is global in terms of its reach and participants. Members recognise the value of different forms of money and a widening asset base: this will support consumers, businesses and financial institutions and ensures a long-term innovative and thriving financial services ecosystem. The developments and changes surrounding cryptoassets and the application of their underlying technology offer many opportunities for the UK to remain competitive in fintech. If the UK can get the regulatory framework right for these new products and services, it will continue its role as a global leader in financial innovation.

As we wrote in our recent response to the Treasury Select Committee, the work on the Future Regulatory Framework (FRF) gives the UK a greater opportunity to be able to regulate cryptoassets in a clear and proportionate way, best suited to meet the needs of consumers and businesses.

We are supportive of the UK's aspirations to advance in the cryptoasset space and become a 'hub'. However, significant delays in this advancement, or conflicting messaging on behalf of the government and the regulators, could negatively impact these aspirations, considering the pace of innovation and the highly competitive nature of the industry across jurisdictions.

Our intention in this report is therefore to assist relevant stakeholders in marrying the UK's regulatory frameworks to the novel world of unbacked cryptoassets.

The existing regulatory frameworks, though not perfectly suited to these new innovations, are nevertheless a helpful starting point.

The scope of unbacked cryptoassets has been selected as it is one of the key components of the ecosystem that is yet to be comprehensively addressed from a policymaking perspective. Moreover, recent market turbulence in this area has further highlighted the need for action.

Our report addresses the regulatory considerations for unbacked cryptoassets from the perspective of consumer protection, market integrity and effective competition – i.e. the FCA's operational objectives[1]. It does not consider the financial stability implications as these are already being extensively analysed by other authorities.

To help in assessing the risks and innovation associated with unbacked cryptoassets, we firstly consider how these assets interact with financial services' cross-sectoral regulatory requirements (such as financial resilience, operational resilience, financial crime and governance).

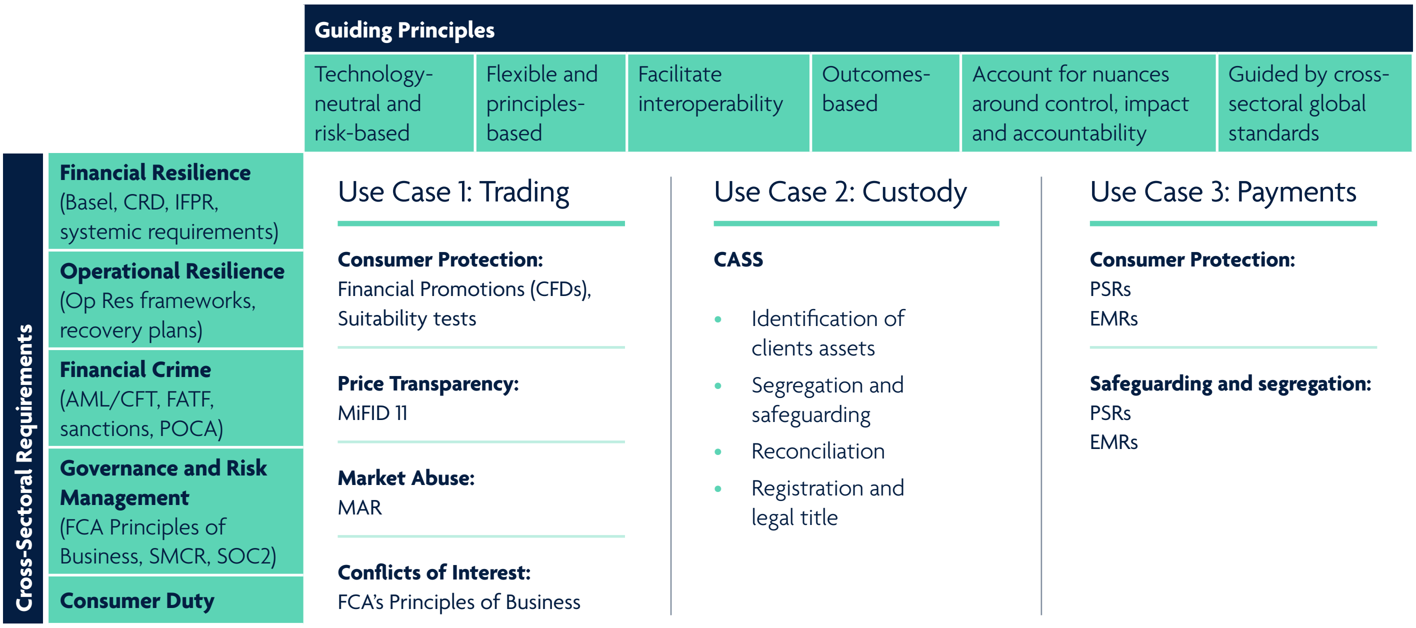
We then analyse three specific use cases – trading, custody and payments – under which we consider:

1. What risks or harms do regulators typically try to address in relation to this activity?
2. What tools are used to address similar risks in traditional finance?
3. What challenges and opportunities are encountered when applying these tools to cryptoassets?
4. What novel risks are raised by the cryptoasset ecosystem?

We note that, across the use cases, existing regulations and tools – e.g. Client Assets Sourcebook (CASS), Markets in Financial Instruments Directive (MiFID), Market Abuse Regulation (MAR), Payment Services Regulation (PSR) – should form the foundation of the approach. However, these regulations will then need to be amended and adapted to sufficiently map to cryptoassets, something which may be aided by the new flexibility proposed in the Financial Services and Markets (FSM) Bill. Our report discusses various nuances around these potential amendments but stops short of reaching definitive recommendations (as further analysis is still required). This process supports the principle of 'same risk, same regulatory outcome', that has been outlined by the government[2] and the Bank of England (BoE).[3]

As consultations continue, it is fundamental that policy makers continue to engage with industry participants as well as seek international alignment to ensure effective coordination across different jurisdictions. This will facilitate the development of an efficient regulatory framework and allow firms based in the UK to interact with the wider global market.

Overview of our approach



Guiding Principles

Technology-neutral and risk-based	Flexible and principles-based	Facilitate interoperability	Outcomes-based	Account for nuances around control, impact and accountability	Guided by cross-sectoral global standards

Cross-Sectoral Requirements

- **Financial Resilience** (Basel, CRD, IFPR, systemic requirements)
- **Operational Resilience** (Op Res frameworks, recovery plans)
- **Financial Crime** (AML/CFT, FATF, sanctions, POCA)
- **Governance and Risk Management** (FCA Principles of Business, SMCR, SOC2)
- **Consumer Duty**

Use Case 1: Trading

Consumer Protection:
Financial Promotions (CFDs), Suitability tests

Price Transparency:
MiFID 11

Market Abuse:
MAR

Conflicts of Interest:
FCA's Principles of Business

Use Case 2: Custody

CASS

- Identification of clients assets
- Segregation and safeguarding
- Reconciliation
- Registration and legal title

Use Case 3: Payments

Consumer Protection:
PSRs
EMRs

Safeguarding and segregation:
PSRs
EMRs

[1] https://www.fca.org.uk/publications/business-plans/2022-23
[2] Source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088774/O-S_Stablecoins_consultation_response.pdf
[3] http://www.bankofengland.co.uk/speech/2022/november/jon-cunliffe-keynote-speech-and-panel-at-warwick-conference-on-defi-digital-currencies

Introduction

In April 2022, the UK's city minister announced that the government would develop a strategy to ensure the UK becomes the "global technology hub for cryptoassets and blockchain"[4].

The announcement also proposed new stablecoin legislation, reform to existing tax guidance, an FCA-led crypto regulatory tech sprint and a new financial market infrastructure innovation sandbox. This fell within a broader timeline of government and regulatory cryptoasset announcements and developments – which is described in full later in the report.

The UK has experienced rapid adoption regarding the number of UK adults that own or have owned cryptoassets. In 2022, UK Finance consumer research found that 11 per cent of UK adults owned a cryptoasset[5] – while the 2022 HMRC consumer survey[6] indicated this figure sat at around ten per cent. This represents an increase from 5.7 per cent in 2021 according to data from the FCA.[7] Moreover, HMRC expects this number to grow again in 2023.

In recently tabled amendments to the Financial Services and Markets Bill, the government proposed a definition of cryptoassets as "any cryptographically secured digital representation of value or contractual rights that – (a) can be transferred, stored or traded electronically, and (b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)". This definition is deliberately broad to account for all elements of the nascent and evolving ecosystem.

Indeed, there are many different elements and activities in this ecosystem and our report does not attempt to cover them all. Instead, it will only focus on **unbacked cryptoassets** – i.e. those that are not fully-backed by fiat currencies or high-quality liquid assets (i.e. HQLA) – as these constitute a key component that is yet to be comprehensively addressed from a policymaking perspective.

In this context of increasing consumer adoption – as well as increasing market turbulence (marked by the failure of several prominent centralised platforms) – our report includes proposals and considerations to support the development of a coherent regulatory framework. The content of this report was aided by the facilitation of several workshops with industry stakeholders and UK Finance members.

The report will analyse these assets via **cross-sectoral requirements** as well as three specific retail use cases – **trading, custody** and **payments**.

[4] HM Treasury, Government sets out plan to make UK a global cryptoasset technology hub (2022)
[5] UK Finance consumer crypto survey, Dec 2022
[6] HMRC, Individuals holding cryptoassets: uptake and understanding (2022)
[7] FCA, Cryptoasset consumer research note, 2021

USEFUL DEFINITIONS

When the UK's Crypto Asset Taskforce published its first report[8] in 2018, it established a taxonomy which has since been used by HM Treasury (HMT), the FCA and the BoE. This report concluded that there are three distinct categories of cryptoasset:

1. **Exchange tokens or payment tokens** – often referred to as 'cryptocurrencies' such as Bitcoin, Litecoin and equivalents. They utilise a distributed ledger technology (DLT) platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens but are used as a means of exchange or for investment.
2. **Utility tokens** – which can be redeemed for access to a specific product or service that is typically provided using a DLT platform.
3. **Security tokens** ('tokenised securities') – which amount to a 'specified investment' as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order (RAO).[9] These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or financial instruments under the EU's Markets in Financial Instruments Directive II (MiFID II).

Under these categories, unbacked cryptoassets are typically made up of category one and two (**exchange tokens or payment tokens** and **utility tokens**) and are currently unregulated in the UK. The FCA[10] has further described unbacked cryptoassets as "crypto assets (that) offer limited or no rights for the token holder and are usually issued in a decentralised manner. Users treat unbacked crypto assets as speculative instruments rather than mediums of exchange".

Category three (**security tokens**), on the other hand, already fall within the regulatory perimeter – as they are subject to the raft of existing regulations that apply to traditional securities (i.e. MiFID, MAR). As such, these are not in scope of our report.

There is also a fourth category of asset – **stablecoins** – which are cryptoassets backed by a fiat currency or another type of traditional asset class (debt instruments/precious metals). These also fall out of scope for this report, as the UK government is already establishing its regulatory approach (please see the section below on the Current UK Regulatory Landscape.) Please note that we are not including any reference to algorithmic stablecoins here.

Some additional key concepts that are relevant for this report include:

Blockchain: A blockchain is a digital system for recording the transaction of assets that uses cryptography to store information securely and immutably in multiple places simultaneously. Unlike traditional databases, distributed ledgers have no central data store or administrative functionality – and require consensus to update the state of the ledger. Blockchain is a subset of distributed ledger technology (DLT) – the technology that underpins all assets in the crypto-ecosystem.

Cryptoasset wallets: A cryptoasset wallet stores cryptoassets. It enables users to transact on blockchains.

Keys: Keys allow participants to send and receive cryptocurrency. There are 'public' keys and 'private' keys which operate as a pair.

Public keys: An alphanumeric string of characters that is the public address of the wallet. Other parties can send digital assets to this public address (similar to a sort code and account number). A user can provide the public key to a third-party as part of a transaction, however the third-party cannot access or transact assets within the wallet.

Private keys: An alphanumeric string of characters that initiates a transaction. This string can be represented in its raw form and/or as a QR code or mnemonic phrase. The private key is unique to each public key and cannot be reproduced if lost or stolen. Digital assets are controlled using the unique private key associated with the public addresses in which the digital assets are held.

Consensus mechanisms: A consensus mechanism is the process by which a blockchain agrees on and updates the state of the ledger through a network of validators. The most common mechanisms are either proof-of-work or proof-of-stake.

Additional concepts that are referred to throughout this report are defined in Appendix 1: Glossary of Terms.

[8] HM Treasury, FCA, Bank of England, Cryptoassets Taskforce: final report (2022)
[9] House of Commons, The Financial Services and Markets Act 2000 (Regulated Activities) Order (2001)
[10] FCA, Cryptoassets (2022)

Current UK regulatory landscape – Overview

The UK has so far implemented limited regulation of the crypto ecosystem, focusing on certain elements within it. Until recently, most of these elements (beyond the security tokens already discussed) have remained distinctly outside of the regulatory perimeter – with only the requirement for crypto firms to become authorised under AML/CFT regulations.[11]

However, as the government continues to pivot towards becoming a 'global hub for cryptoasset technology', this perimeter is evolving. Most significantly, in July 2022 through the Financial Services and Markets Bill HMT proposed bringing stablecoins within existing e-money and payment services regulation. And, later in 2022 or early 2023 the Cryptoasset Task Force (comprising the BoE, FCA, HMT and Payment Systems Regulatory (PSR)) is expected to publish a consultation on wider cryptoassets.

Overall, UK regulators are seeking to keep pace in managing the risks that digitalisation is bringing to consumers and markets, but also to encourage innovation to support the benefits that digitalisation and cryptography can provide. All of this is within the context of the wider Future Regulatory Framework review which aims to 'deliver bespoke UK-orientated regulation that is primarily focused on delivering growth, innovation and competition'.[12]

A timeline of significant developments to-date is included below. The full description of each of these milestones is included in Appendix 2.

[11] FCA, Guidance on Cryptoassets (2019)
[12] HM Government, The Benefits of Brexit (2022)

2024

Q1: MiCA begins applying to in scope firms

2023

H1:

- FSM Bill to be finalised spring 2023
- HMT consultation on wider cryptoasset regulation expected

September: HMT publishes amendments to regulation on AML/CFT/Transfer of Funds comes into force – extending FATF's travel rule to cryptoassets

July:

- HMT introduces Financial Services and Markets Bill – enabling creation of FMI sandboxes and proposing to bring stablecoins within existing e-money regulations
- Law Commission's report (28 July 2022) around future reforms relating to the law re digital assets

March: FCA publishes notice reminding firms of existing obligations (e.g. Principles for Business)

2022

January: HMT publishes response to consultation proposing to strengthen rules on misleading crypto promotions

2021

January: FCA ban on the sale of crypto derivatives and exchange traded notes (ETNs) to retail customers becomes effective

2020

January: FCA requirement for firms carrying out cryptoasset activity in the UK to be compliant with AML/ CFT requirements

2019

July: FCA publishes guidance on cryptoassets – clarifying boundary of the regulatory perimeter

Designing a regulatory framework – Guiding principles

The UK should act quickly in order to guarantee it remains internationally competitive in this area – i.e. becoming a competitive crypto-hub, while maintaining a robust regulatory environment. A principles-based and outcomes-based approach may facilitate this – sentiment which has been reflected in the FCA's recent strategy.[13]

In considering the regulatory framework that could be developed for cryptoassets, it was agreed during workshops with UK Finance members that the following design principles be considered:

- The framework should be **technology-neutral and risk-based** to facilitate a level playing field between competing offerings (i.e. bank and non-bank) – and should be applied proportionately to the risk posed.
- The framework should be **flexible and principles-based** to better adapt to the heterogenous product landscape and rapidly changing technology. This would create the conditions for regulatory agility from which the UK has often prospered.
- The framework should **facilitate interoperability** between systems and services.
- The framework should be **outcomes-based** to ensure consumer protection, competition and market integrity, and bake in the Consumer Duty principles.
- The framework should account for nuances around **control, impact and accountability** within a decentralised context.
- The framework should be **guided by cross-sectoral global standards** and aligned to any global common taxonomies.

As already outlined above, given the highly developed financial services regulatory framework in the UK, we recommend using existing regulation as the starting point for this approach. This is also in line with the principle that frameworks should be technology-neutral.

However, some parts of existing frameworks could prove inappropriate for the specificities of unbacked cryptoassets. In their current state, they may not deliver the intended outcomes or manage the identified risks of these innovative assets. Therefore, a wholesale implementation of existing frameworks may not be pragmatic and amendments should be discussed.

As part of this discussion around potential amendments, we should assess the approach taken in other jurisdictions (such as the EU's Markets in Cryptoasset Regulation, MiCA) and consider applying the most appropriate proposals to the UK context. Not only will this help to best position the UK from a competitive perspective, but it will contribute to further international and global alignment. UK Finance is already undertaking such analysis of the MiCA Regulation to ensure that we can be clear of what would work well and less well for the UK.

The proposals made in the Financial Services and Markets Bill[14] to revoke and modify retained EU law, provide an opportunity to adapt existing legislation and regulation in the most appropriate and measured way for the UK (notwithstanding those areas where the UK is keen to maintain equivalence, such as with the Single Euro Payments Area (SEPA) Rules).

[13] FCA, Our Strategy (2022)
[14] House of Commons, Financial Services and Markets Bill (2022)

Designing a regulatory framework – Approach used

This report addresses regulatory considerations for the unbacked cryptoasset ecosystem from the perspective of consumer protection, market integrity and effective competition – i.e. the FCA's operational objectives.

This report does not consider the financial stability implications of the growth of the cryptoasset market. This is already being considered by relevant institutions, including the Financial Stability Board (FSB), the International Monetary Fund (IMF) and the Basel Committee for Banking Supervision (BCBS).

The report also does not consider the relevant taxation regime.

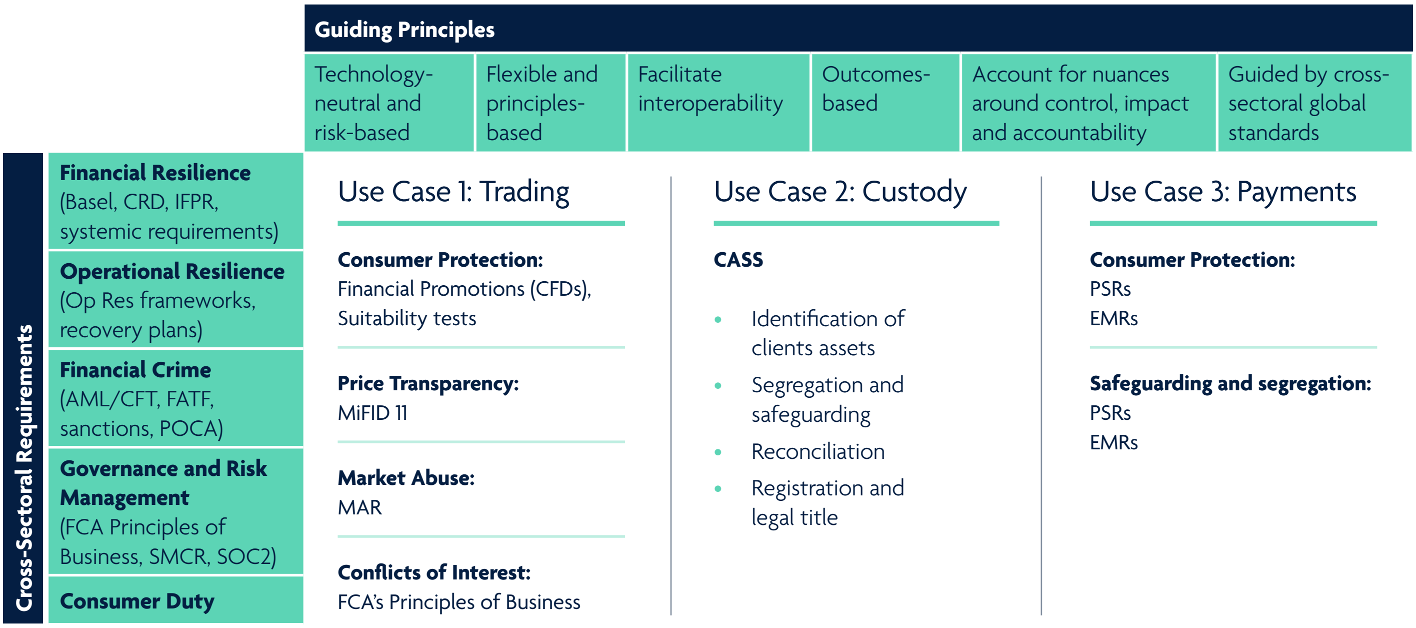
To help in assessing these regulatory considerations, we firstly address how these assets interact with financial services' cross-sectoral requirements (e.g. financial resilience, operational resilience, financial crime and governance).

We then analyse our three specific use cases – trading, custody and payments – under which we consider:

1. What risks or harms do regulators typically try to address in relation to this activity?
2. What tools are used to address similar risks in traditional finance?
3. What challenges and opportunities are encountered when applying these tools to cryptoassets?
4. What novel risks are raised by the cryptoasset ecosystem?

Through this analysis, we initiate discussion points around what potential amendments may need to be made to existing UK regulation to sufficiently map to unbacked cryptoassets. However, we stop short of reaching definitive conclusions – as further analysis is still required.

Overview of our approach



Guiding Principles

- Technology-neutral and risk-based
- Flexible and principles-based
- Facilitate interoperability
- Outcomes-based
- Account for nuances around control, impact and accountability
- Guided by cross-sectoral global standards

Cross-Sectoral Requirements

- **Financial Resilience** (Basel, CRD, IFPR, systemic requirements)
- **Operational Resilience** (Op Res frameworks, recovery plans)
- **Financial Crime** (AML/CFT, FATF, sanctions, POCA)
- **Governance and Risk Management** (FCA Principles of Business, SMCR, SOC2)
- **Consumer Duty**

Use Case 1: Trading

Consumer Protection:
Financial Promotions (CFDs), Suitability tests

Price Transparency:
MiFID 11

Market Abuse:
MAR

Conflicts of Interest:
FCA's Principles of Business

Use Case 2: Custody

CASS

- Identification of clients assets
- Segregation and safeguarding
- Reconciliation
- Registration and legal title

Use Case 3: Payments

Consumer Protection:
PSRs
EMRs

Safeguarding and segregation:
PSRs
EMRs

Designing a regulatory framework – Cross-sectoral requirements

The regulatory framework has developed in the UK such that, at a high level, there are common requirements across the financial sector for all intermediaries that engage with customers. Rather than repeating the analysis of these requirements under each use case, this section addresses these requirements upfront, as they could apply to all cryptoasset service providers (CASPs) that provide unbacked cryptoassets.

CONSUMER DUTY

In the UK, the FCA has recently signalled its intention to raise the level of consumer protection in the retail financial services market with the introduction of the Consumer Duty. This new principle introduces the obligation that a firm must act to deliver good outcomes for retail customers.

The Consumer Duty currently applies to the regulated activities and ancillary activities of all authorised firms[15] in relation to products and services affecting prospective and actual retail customers.

In short, there are now cross-cutting rules requiring firms to act in good faith, avoid causing foreseeable harm, and enable and support customers to pursue their financial objectives. If CASPs were to come into scope of the Duty, they would need to determine how to map and implement this onto products where price is driven entirely by supply and demand. They could, for example, aim to demonstrate compliance by evidencing the provision of clear guidelines and Terms & Conditions to ensure that consumers are able to make informed decisions.

Consumer Duty is seen as one of the first instances of outcomes-based regulation in the UK, with expectations of outcomes such as inclusive design, fair price and value and customer understanding. As such, good practice is still developing across the financial sector. However, it could prove to be a valuable case study, as future regulation could likely take a similar approach.

FINANCIAL RESILIENCE

The current regulatory framework imposes varying requirements on intermediaries for financial resilience, such as levels of capital or liquidity. These requirements range from the Basel Framework/on-shored Capital Requirements Directive for banks, Investment Firms Prudential Regime for trading venues and capital requirements contained within the Payment Services Regulation.

Depending upon the nature of the CASP, similar requirements could be applied to cryptoassets in proportion to the risks they pose. A prudential framework would also need to consider or account for:

- varying levels of volatility in cryptoassets
- the operational organisation of a CASP – including how functions and services are organised (i.e. whether there should be formal separation of trading and custody)
- the specifics pertaining to the service provided – e.g. within a trading context, will the CASP function bilaterally (that is, being counterparty to each transaction) or multilaterally (by matching buy-and-sell orders)?
- The extent of any off-chain transactions (which do not leverage any of the security features of the blockchain, and instead expose users to credit and counterparty risk and increased operational risk).

Additionally, as the IMF28[16] has pointed out, as entities or activities become systemic, they should then become subject to additional requirements comparable to those for traditional systemically important institutions (i.e. more intensive supervision, safety and soundness requirements, stress testing, and recovery/resolvability assessments). Systemic importance may be measured for a firm as a standalone entity or through risks posed through material integration with traditional financial institutions.

It's worth noting that, although the holding of unbacked cryptoassets on the balance sheet by traditional banks is not a use case in this report, the considerations above are also reflected in the BCBS' consultations on the prudential treatment of cryptoassets.[17]

Although the FSB and other authorities have acknowledged that the level of interconnection between cryptoassets and traditional finance is currently limited, they still point out that this needs to be accounted for before the level of interconnection has grown to the size that would pose a financial stability risk.

[15] FCA, Financial Services Register (2022)
[16] https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715
[17] Bank of International Settlements, Prudential treatment of cryptoasset exposures – second consultation (2022)

OPERATIONAL RESILIENCE (INCLUDING CYBER SECURITY)

The UK's operational resilience framework aims to ensure that consumers have ongoing access to their financial assets and financial services. The framework now requires many financial services firms to prevent, adapt and respond to, recover and learn from operational disruption. The framework is implemented in proportion to the impact of the harm that could be caused by an outage from that firm, either given the firm's size or the importance of the services that they deliver.

In theory, the decentralised nature of blockchain means that there is no one single point of failure. As such, the technology should offer high operational resilience. However, in practice, blockchains can operate on permissioned ledgers (as opposed to permissionless) where there is a gatekeeper who limits access and consensus to pre-authorised users (arguably negating some of the benefits of using DLT).

Alternatively, they can involve centralised intermediaries that employ a combination of on-chain and off-chain activity to deliver their services. We have also seen examples of decentralised blockchains being impacted by issues of centralisation based on their having a relatively small pool of validator nodes. This can consequently introduce points of heightened vulnerability – such as bridges. As these entities typically hold large amounts of digital assets on behalf of clients, this makes them an attractive target for cyber criminals. Enhanced operational resilience requirements are therefore necessary to ensure protection over these assets.

The FSB[18] proposes that CASPs should be required to establish effective contingency arrangements (including robust and credible recovery plans, where warranted) and business continuity planning, in proportion to the financial stability risk that may be posed by their activity.

Within the traditional finance sector, regulators are showing increasing concern around the resilience risks posed as a result of the concentrated use of a small number of critical service providers (such as cloud service providers) and are proposing regulatory oversight. As this issue is also pertinent to the cryptoasset ecosystem, these proposals should be welcomed by CASPs.

FINANCIAL CRIME

There is a highly developed regulatory framework aimed at preventing financial services firms being used to facilitate financial crime. CASPs in the UK are already required to comply with AML/CFT regulations and register with the FCA. HMT has also recently amended the regulations to implement the Financial Action Task Force's (FATF) "Travel Rule" and clarify its application to cryptoassets.

Moreover, beyond the specific remit of financial services, other requirements such as sanctions, the Proceeds of Crime Act (POCA) and criminal anti-bribery prohibitions already apply to CASPS – as they do to all other players both in and out of the regulatory perimeter.

Nonetheless, further work is still required to determine how other financial crime legislation, regulation and supervision can continue to apply to cryptoassets and the ecosystem to ensure full coverage.

The inherent data-rich environment and the emergence of DLT and blockchain analytics firms (and the continuing improvement of their capabilities) provide an opportunity for market participants and regulators to better understand the risk profile of the wallets they are interacting with. Due to the public nature of blockchain transactions and despite the pseudonymity of the wallets themselves, transactions can be traced through 'clusters' to identify the types of activity that a wallet has participated in. For example, a wallet which has sent money to a 'cluster' associated with the sale and purchase of illicit substances on the darknet can be flagged by a blockchain analytics tool as doing such. Similarly, wallets which attempt to obfuscate their activity by using 'mixers' will also be flagged as participating in suspicious behaviour. In many ways, the insight provided by these tools means that, for financial crime purposes, digital assets can be investigated more comprehensively than cash transactions.

Nonetheless, some digital assets are designed with a more overt focus on privacy. These so-called 'privacy coins' achieve this by obfuscating the blockchain data. Whereas standard public blockchains display the data of pseudonymous wallet addresses, the blockchains of privacy coins are encrypted and unintelligible. This means that wallet addresses, balances, and transactions are hidden to all participants except those who possess a 'view key' (something which can only be granted by the executor of a transaction). This feature inhibits blockchain analytics firms from analysing the activity of privacy coins' blockchains. It is also why privacy coins have become the digital asset of choice for illicit activity.

Challenges also remain due to the nature of the cryptoasset ecosystem particularly given that cryptoasset users in the UK are not limited to the use of CASPs regulated within the UK. Further international cooperation and development of cryptoasset regulation and supervision is a necessity if the UK's regulatory framework is to more effectively address the risks posed. Regulatory expectations do not always take this into account, for example placing an onus on FIs to police customer payments despite regulatory guidance lacking detail to support this.

GOVERNANCE AND RISK MANAGEMENT

Currently, there are varying requirements for governance and risk management across the sector. At a minimum, a threshold condition for authorisation[19] by the FCA or PRA includes being a 'fit and proper' person, with the FCA requiring a firm's management to have adequate skills and experience.

The FCA's Principles for Business[20] require firms to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems. Many firms are now also required to comply with the Senior Managers and Certification Regime, which codifies accountability and responsibility.

[18] FSB, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report (2022)
[19] FCA, Early Stages (2021)
[20] FCA, Principles of good regulation (2022)

It would be hard to argue against the proportionate application of these requirements to CASPs. This could pose a challenge to many smaller CASPs which have developed in a way that does not conform to traditional governance structures and risk management processes.

However, CASPs are starting to apply some existing assurance techniques to their processes. This includes SOC2, which is an attestation that the entity in question has an operational control framework to mitigate risks pertaining to the management of data. A SOC 2 Type 1 report attests that the firm has an appropriately designed control framework. A SOC 2 Type 2 report is an attestation that the controls have operated effectively over a six-month period.

The FSB proposes that regulators should require cryptoasset issuers and service providers to have in place and disclose a comprehensive governance framework. This framework should provide for clear and direct lines of responsibility and accountability for the functions and activities being conducted. The FSB also proposes that regulators should require CASPs to have an effective risk management framework that comprehensively addresses all material risks associated with their activities.

Applying these requirements or frameworks to decentralised finance (DeFi) structures poses even greater challenges given the inability to identify the person and /or entity accountable for regulatory compliance. See more in the section on Additional Considerations.

Designing a regulatory framework – Use case deep dives

USE CASE ONE: TRADING

Now that the cross-sectoral requirements – spanning across all use cases – have been discussed, the individual nuances around each specific use case can be addressed. As explained earlier in the report, this will involve addressing (i) what harms regulators are trying to address, (ii) the tools they use to address these in traditional finance, (iii) the particular challenges and opportunities of applying these tools to cryptoassets, and (iv) any novel risks posed by cryptoassets.

To begin with, we look at trading.

The trading use case constitutes the facilitation or execution of an exchange involving unbacked cryptoassets with other unbacked cryptoassets or fiat. For the purpose of this report, we will focus on retail spot trading only and not derivatives/options.

There are three key methods of trading unbacked digital assets:

1. **Using a self-hosted wallet through a decentralised exchange.** Please refer to the section on DeFi in Additional Considerations for more. To self-host a wallet, an end user would need to utilise the appropriate software/hardware to store their public and private keys.
2. **Trading unbacked cryptoassets through an intermediary (i.e. a centralised exchange).** A retail customer can do this by setting up an account through the website of the centralised exchange and then transferring fiat currency into this account to commence crypto trading.
3. **Peer-to-peer trading using a centralised facilitator.** These platforms are called 'peer-to-peer' because the centralised entity is not involved in processing the exchange, but simply acts as a connecting intermediary (i.e. similar to a bulletin board). The purchase of digital assets in this case happens as a direct exchange between the buyer and seller.

It's important to note that centralised cryptoasset exchanges that facilitate the buying and selling of unbacked cryptoassets provide much wider services than traditional securities exchanges – including settlement, clearing, custody, asset issuance, market making and proprietary trading.

There are also the additional nuances around consumers trading directly with each other (without the need for an intermediary or CASP) – which are not directly considered in this use case. However, regulators would need to consider if this should fall within the regulatory perimeter and, if so, how it could be regulated.

CONSUMER PROTECTION

The trading of cryptoassets is unique and dissimilar from trading within traditional finance. With cryptoassets, a retail customer can interact directly with the exchange – whereas, in traditional finance, customers usually only interact through various intermediaries (e.g. brokers, banks). Indeed, this kind of differentiation is one of the philosophical priorities for many cryptoasset exchanges, which see their role as being to facilitate the democratisation of financial services for consumers.

With the trading of traditional financial instruments, current regulation imposes requirements on intermediaries to ensure sufficient consumer protection. These requirements include ensuring customer comprehension of the relevant risks involved. Specifically, intermediaries must make an assessment of the customer's risk profile and investment needs, and only facilitate access to products which are deemed suitable and appropriate.

The UK government is already updating the financial promotions regime to incorporate cryptoassets, so that advertising of cryptoassets is "fair, clear and not misleading". In traditional finance, FCA already requires, among other measures,[21] the sellers of contract for differences (CFD) to retail consumers to have a standardised risk warning noting the percentage of the firm's retail client accounts that make losses – something which could be extended to crypto firms.

The EU's newly agreed Markets in Cryptoassets regulation (MiCA) introduces specific similar requirements around the assessment of cryptoasset suitability for customers – including a consideration of customer experience, knowledge, objectives and ability to bear losses. If assessments around cryptoasset suitability and appropriateness were required by UK regulation, these could potentially be built into the interface/website that retail clients interact with when trading with crypto exchanges. Some exchanges have already implemented questionnaires that could potentially fulfil this requirement. It will be important to note whether the EU deems them compliant under MiCA's technical standards.

[21] FCA, Contracts for Difference (2019)

Recent FCA research[22] also highlighted more effective ways of ensuring consumers make more suitable decisions on their investments by introducing 'positive frictions' in the self-certification process such as requiring the consumer to submit evidence for self-certification of being a high net worth or sophisticated investor.

However, it is acknowledged that even the most sophisticated controls such as the above may still prove to be ineffective.

PRICE TRANSPARENCY

For markets to work well and efficiently, trading needs to be orderly and transparent so that investors can see where to get the best price with sufficiency clarity around spread.

In the traditional finance world, to meet the above objective, on-shored MiFID II requires exchanges and other intermediaries which facilitate trading (such as investment banks) to report their trades to data reporting service providers. This ensures that investors in the market can see where to get the best price for their assets. MiFID II also supports the idea of a consolidated tape (or ticker tape) which would allow investors to get this information in one place – although this has not happened yet due to issues with uniformity of data and the lack of consensus around cost-sharing in production and distribution of the data.

Currently, the crypto trading market is fragmented but 'oracles' are starting to appear that could become crypto's answer to a consolidated tape. Oracles are a network of data providers which reach consensus on a particular datapoint and provide that data on any particular blockchain. For example, a group of data providers can provide a price feed for any particular asset. The majority of these data providers must agree on the value of the data being provided for the data to be recorded onto the blockchain. This decentralised method of data sourcing provides a unique solution for instances where the integrity of data being relied upon is in question. The ability to leverage a decentralised network of data providers (oracles) – in combination with additional solutions like Smart Order Routing – might mitigate this concern.

The FSB17 proposes that CASPs facilitating trading be required to ensure their operations are resilient and should maintain clear and transparent operating rules.

A framework for reporting trades and transactions that could be built upon is the OECD's statutory reporting requirements for CASPs, released in October 2022 as the updated Crypto-Asset Reporting Framework (CARF) and Amendments to the Common Reporting Standard (CRS).[23] This framework defines three types of transactions which CASPs are required to report:

1. exchanges between relevant cryptoassets and fiat currencies;
2. exchanges between one or more forms of relevant cryptoassets; and
3. transfers (including reportable retail payment transactions) of relevant cryptoassets

These definitions could be leveraged to achieve wider and more-general transparency objectives.

MARKET ABUSE

Market abuse arises in any circumstance where financial market investors are unreasonably disadvantaged (either directly or indirectly), by other participants, through the use of non-publicly available information, distortion of price setting mechanisms or the dissemination of misleading information.

In traditional finance, the on-shored Market Abuse Regulation (MAR) tries to prevent market abuse by outlawing certain behaviours and expects firms to manage conflicts of interest. Regulators also monitor transaction reporting to detect market abuse.

Outlawing certain behaviours

MAR categorises three types of market abuse offences:

- Insider dealing
- Unlawful disclosure of inside information
- Market manipulation, such as front running, wash trades and pump and dumping

MAR expects trading firms and venues to try to prevent these market abuse offenses and have controls to detect them.

These same offenses can be undertaken when trading in cryptoassets. And in fact, MiCA introduces obligations that align to traditional MAR requirements, to address such abuse in cryptoasset markets. These rules include:

- Requiring issuers, offerors or persons seeking admission to trading to inform the public as soon as possible of inside information which directly concerns them
- Prohibiting market manipulation (e.g. giving misleading signals of supply, demand or price or securing the price of a cryptoasset at an artificial level)

Under MiCA, CASPs that are authorised for the operation of a trading platform, must inform their competent authority when they identify cases of market abuse or attempted market abuse.

However, beyond these traditional concerns, the crypto world also introduces novel types of market abuse.

For example, firstly, there can be attempts to manipulate the consensus mechanisms of distributed ledgers (i.e. through so-called "51 per cent"[24] or "Sybil" attacks) – which can put the value on the entire blockchain at risk. If an attacker is able to gain control of a majority of network nodes (or hash power), they could then deliberately change the ordering of transactions and enable a "double spend".

[22] FCA, Beyond disclosure for high-risk investments: slow down and think (2022)
[23] OECD, Crypto-Asset Reporting Framework and Amendments to Common Reporting Standard (2022)
[24] A 51% attack on a blockchain network is characterized by control of over half of the network's computer power – referred to as a hash rate.

The recent shift of popular blockchain Ethereum's consensus mechanism from proof-of-work to proof-of-stake complicates this further. Proof-of-work is widely considered to be more secure than proof-of-stake as the distribution of energy and hash rate is distributed evenly. As such, proof-of-stake blockchains are more susceptible to 51 per cent attacks as it is easier to control 51 per cent of validator nodes compared to 51 per cent of the hash rate.

A recent study[25] showed that, among the top ten proof of stake platforms by market capitalisation, the top ten validators held between 17 per cent and 88 per cent of the stakes, while the top 50 held between 47 per cent and 100 per cent of the stakes.[26]

This complexity is further compounded by the fact that node operators can use VPNs to hide their location, making it difficult to detect if nodes are being concentrated in one geographical location.

Secondly, due to the public nature of the most popular blockchains, transactions which are in the queue to be processed can be seen by any observer. This raises a complex dilemma, one which is referred to as 'maximal extractable value' (MEV). MEV is a concept by which miners/validators can maximise their profit (and affect market prices) by determining the order of transactions on the blockchain which are due to be processed. One may submit a higher fee to accompany their transaction in order for it to be processed faster. Market abuse can emerge in instances where bots scan blockchain transactions for arbitrage opportunities, front-running on-chain activity and responding accordingly. Whilst this information is available to all, the vast majority of retail users are not aware of how to leverage it, creating an information asymmetry effect in the market.

If MAR was applied to cryptoassets in the UK, it would need to be updated and extended to take account of these novel risks and examples.

On the other hand, in some respects, regulating market abuse could prove to be easier than in traditional finance due to the transparent, data-rich nature of the blockchain – as long as all activity is occurring on-chain. For example, entities registered with the regulator could provide their public key address to allow for real-time monitoring.

Management of conflict of interests

The FCA's 8th Principle of Business[27] requires firms to manage conflicts of interest fairly, both between the firm itself and its customers, and between customers.

This is done in a variety of ways including functional (e.g. Chinese walls) and legal separation of services, conflicts of interest registers and disclosures to clients.

In the context of cryptoassets, MiCA requires CASPs to have robust policies to identify, prevent, manage and disclose conflicts of interest. In particular, they should have specific procedures in relation to when they place cryptoassets with their own clients and when the proposed price for placing cryptoassets has been overestimated or underestimated.

Similarly, the FSB17[28] proposes that CASPs be required to make available to users and relevant stakeholders (including customers), all necessary information regarding how they operate, how they transact, the risk features of their products, and how they manage and mitigate any potential risks in an understandable manner for the intended audiences. This should include, as appropriate, the governance structure and procedures related to the main activities offered and important conflicts of interest emanating from cryptoasset activities.

As discussed previously, many CASPs do offer multiple services (such as issuance, exchange, lending, and storage), which could allow them to take advantage of information and trade against their own customers. It seems sensible then that robust governance and disclosure requirements should be put in place to address these potential conflicts of interests. Or moreover, it could be considered whether CASPs be required to formally undergo a functional or legal separation of exchange and custody services (as suggested by the FSB).

Detection of market abuse by regulators

The current regulatory framework requires exchanges and investment firms to report their transactions in traditional financial instruments to regulators. The regulators use these reports to detect and investigate suspected market abuse.

ESMA is already studying how data fields in DLT transactions compare with those required in MiFIR reporting. One challenge may be the pseudonymous nature of DLT transactions. However, CASPs operating in the UK are now required to comply with KYC requirements under AML regulations, so transactions should be linked to an identifiable customer.

There are also additional possibilities for addressing this information need. Regulators are already exploring the growing functionality of blockchain analytics (see previous Cross-Sector requirement on financial crime) and ways to access off-chain crypto data.[29] As such, this could be investigated further and incorporated into the regulatory framework.

Summary:

Looking at the trading use case our analysis shows that some regulatory requirements, like the financial promotions regime, are already due to apply to unbacked cryptoassets. Suitability tests like those expounded in the EU MiCA Regulation could also be applied, possibly built into websites/interfaces or through 'positive frictions' like the FCA's suggested self-certification processes. And defining the trading of cryptoassets or the safeguarding of cryptoassets as a regulated activity, would require firms to comply with the FCA Principles of Business. Meanwhile, defining cryptoassets as financial instruments could bring them into CASS and the on-shored MiFID and MAR regimes.

[25] London School of Economics, Cryptocurrencies and Decentralised Finance (DeFi) (2022)
[26] Governance of "Decentralised" Finance: Get up, Stand up! – speech by Carolyn Wilkins | Bank of England
[27] FCA, Handbook (2022)
[28] Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report – Financial Stability Board (fsb.org)
[29] ESMA Reference PROC/2022/09 – Notice of a call for tenders (Crypto off-chain data)

USE CASE TWO: CUSTODY

The second use case to be addressed is custody.

During the recent FCA Crypto Sprint, defining what "custody" is in a digital asset context was identified as a particular challenge by participants. Participants noted that there was currently a wide range of business models, standards, and services among existing cryptoasset custodians, and that regulators should use existing regulation where possible.

For the sake of this report, cryptoasset custody will be defined as "the safekeeping of the private key on behalf of self or others". A private key is a sophisticated form of cryptography that represents control or ownership (or both) of a user's cryptoassets and enables the user to access their assets to transact. For a more detailed description, please refer to Appendix 1: Glossary of Terms.

As control or ownership of cryptoassets is determined by who holds the corresponding private keys, they are far more important than a password could ever be. If a key is lost or stolen, the assets cannot be recovered even by their rightful owner (it is recognised that there will be enhanced consumer education considerations on this point, as many retail consumers may not appreciate this point of differentiation from traditional finance).

There are several types of custody model being employed within the crypto ecosystem.

Personal custody or non-hosted/non-custodial wallets are in effect a form of custody where there is no third-party providing any service. Beneficial owners (clients) access these services directly to secure/safeguard their own cryptoassets, giving them full control. The assets can be stored in hardware or software wallets. This is analogous to holding cash in your leather wallet. As no intermediary exists – this model is out of scope for this report.

Full and minority-controlled custody can therefore be categorised as hosted or custodial. Custodial wallet services offer varying levels of control. Some providers have partial control over assets – with the ability to execute, transfer and sign transactions; and block or recover assets/private keys on behalf of a client with their instruction. However, these providers would not have full control to initiate a transaction on behalf of a client if the custodian does not have the client's private key in their possession to enable the transaction's release.

Custodians may provide additional services beyond the safekeeping or holding of assets on behalf of clients, which include but are not limited to reconciliation, settlement, corporate actions, maintaining bank accounts and fund management.

Across financial services, whenever assets are custodied with an intermediary, a risk of financial harm to consumers is introduced whereby they may lose the ability to access their assets. This could come as the result of operational outages (including cyber-attacks), asset theft, or insolvency of the intermediary.[30] Please refer to the earlier section of the report – Cross-sectoral requirements – for relevant measures specifically in relation to financial and operational resilience and the prevention of financial crime. In fact, the IMF[31] has noted that wallets are the components of the ecosystem that are most exposed to cyber risk. Furthermore, cryptoasset exchanges and other locus points for consumer custodial holdings remain an ongoing target for crypto hacks.

In relation to insolvency, the bankruptcy filing of systemic institutions during the 2008 financial crisis raised concerns around how safe the assets held on behalf of clients actually are, and if they can even be identified in a swift manner. This led to a strengthening of the client assets (CASS) rules in the UK.

Participants in the FCA Crypto Sprint suggested that regulators apply CASS rules as a basis for building a regulatory regime for the custody of cryptoassets.

There are four fundamental principles to CASS:

- Identification of client assets
- Segregation and safeguarding
- Reconciliation, and
- Registration and legal title (legal title to a safe custody asset is appropriately registered and maintained as belonging to a client)

These principles could be extended to cryptoasset custody – and accompanied by additional checks and balances e.g. CASS audits. It is worth noting that these CASS principles already feature prominently and are mirrored closely in the EU's MiCA. Furthermore, some cryptoassets exchanges, for example, already undertake voluntary 'proof-of-reserves audits' (cryptographic accounting procedures) to demonstrate that they do still hold the assets they claim to.

Within the context of CASS, Crypto Sprint participants noted how a further challenge was the bearer nature of private keys and emphasised the need for custodians to apply robust operational and governance controls to help prevent loss and misuse. Regulators must also clarify who remains liable in instances where loss of key still happens to occur.

Beyond the specifics of CASS, the FSB17 also more generally proposes that authorities should supervise and regulate custodial wallet service providers, proportionate to their risk, size, complexity and systemic importance, in order to address operational, reputational, financial and consumer/investor protection risks that may arise from the storage of users' private keys. Regulations should assess the adequate safeguarding of customer assets, for example, through segregation requirements (including in the case of default/bankruptcy of the custodial wallet service providers).

[30] There also exists in the UK the Dormant Asset Scheme, which currently enables banks and building societies to access dormant funds and channel them towards good causes. In 2021, following a consultation, the government announced its intention to expand the scheme to include certain assets from the pensions, insurance, investment and wealth management and securities sectors to be used for public benefit, whilst protecting the original asset owners' legal right to reclaim the amount that would be due to them had a transfer into the scheme not occurred. It is not clear whether in the future cryptoassets might come under scope of such a scheme, or how that might work in practice if the private keys are not custodied.

[31] IMF, Regulating the Crypto Ecosystem: The Case of Unbacked Cryptoassets (2022)

IDENTIFICATION OF CLIENT ASSETS

To support the application of CASS, a custodian should be able to identify where client assets arise in their business. Despite the pseudonymous nature of cryptoassets meaning that owner identity is inherently difficult to verify, given the fact that all CASPs are now subject to AML regulations, KYC checks should nonetheless already be being undertaken.

As things stand, some cryptoasset custodians hold all client keys in one central combined wallet, with ownership allocated via a back-end database. If the CASS framework were to be applied to these assets, the FCA would then likely expect the CASP to implement adequate systems and controls around the maintenance of these databases.

SEGREGATION AND SAFEGUARDING

CASS rules require custodians to ensure that client assets are registered appropriately and are held separately to the custodian's own assets. This is achieved by having segregated client accounts, contractual arrangements (which specify whether assets can be reused or rehypothecated) and appropriate record keeping.

Similar controls could be implemented within cryptoasset custody by requiring different wallet addresses for clients versus the CASP itself. CASPs could also provide a higher level of security by using cold wallets alongside hot wallets. Hot wallets are connected to the internet and are therefore exposed to a higher level of cyber risk. This is not the case for cold wallets, for which the private keys are stored on a device which is not connected to the internet.

As discussed, crypto custodians often maintain linked databases to record the breakdown of client assets in a wallet. To mirror CASS requirements, there may need to be requirements facilitating for trusted third parties to be granted access to these databases in the event of insolvency.

Finally, in situations where cyber or operational processes are delegated to third parties, the IMF has noted that the wallet provider should remain responsible for any incidents that occur in the third parties with clear outsourcing requirements in place. The FCA's Consumer Duty also extends to third parties and the distribution chain.

RECONCILIATION

CASS rules require regular reconciliation of the custodian's records to ensure that the account of what is held on behalf of clients corresponds with the firm's obligations towards these clients. In theory, due to the unified and immutable nature of DLT, this reconciliation should be redundant in a cryptoasset context. Moreover, the blockchain ledger would also be transparent and accessible to third parties such a regulators or insolvency administrators.

However as discussed above, in practice, records of client's assets can actually be maintained in offline databases. As such, the requirement for reconciliation may still be necessary.

REGISTRATION AND LEGAL TITLE

In traditional finance, the custodian may hold client assets itself or appoint a sub-custodian. In either case, the original custodian is required to ensure that legal title to a safe custody asset is appropriately registered and maintained as belonging to a client.

In a cryptoasset context, no clear distinction between legal and beneficial ownership exists, as these details are not recorded on the underlying DLT. This consequently introduces legal and contractual ambiguity in the event of an insolvency. A clear legal and regulatory framework is needed to ensure the appropriate separation and protection of client assets following the default of a wallet provider – and to ensure that these clients are not treated as unsecured creditors (as has been the case in some recent examples[32]).

The FSB also proposes that service provider should be required to provide full and accurate disclosure to any client for whom it is providing custody services of the terms and conditions of the custodial relationship and the risks that could be faced by the client if the custodian were to enter bankruptcy. This should include, if appropriate, information on whether or not client assets are protected and segregated properly.

Summary:

The FSB proposes that authorities should supervise and regulate custodial wallet service providers, proportionate to their risk, size, complexity and systemic importance. In the UK, it has been suggested that regulators apply CASS rules as a basis for building a regulatory regime for the custody of cryptoassets. This would provide a framework for identification of client assets, segregation and safeguarding, reconciliation, and registration and legal title.

[32] Wall Street Journal, Coinbase Says Users' Crypto Assets Lack Bankruptcy Protections (2022)

USE CASE THREE: PAYMENTS

The final use case to be addressed is payments.

A payment in the context of digital assets pertains to the transfer of digital assets from one party to another in exchange for a good or service.

Unbacked cryptoassets are not widely used in the UK for payments due to their volatile nature and the perceived complexity of transactions. Further, spending on cryptoassets is classed as a capital gain taxable event by HMRC.[33]

However, where a customer wants to make a cross-border payment, the use of cryptoassets may be more attractive. This has been seen with the recent success of SWIFT's 'connecting digital islands' experiments, which looked to integrate digital currencies into the world's existing payments ecosystem. At present it might be argued that the use of unbacked cryptoassets for payments is only a nascent use case but looking ahead to possible future scenarios of increased use is in line with the regulators' ambitions to anticipate market developments.

In both the domestic and international scenarios for payments, a CASP intermediary acts similarly to a payment service provider (or, in some cases, more specifically a merchant acquirer) as they enable a transfer of value from one party to another through a 'system' or an e-money firm. In the UK, for fiat payments this 'system' is either a regulated payments system (e.g. Bacs, CHAPS, Faster Payments) or card payment system (e.g. Visa, Mastercard).

It is worth noting that, in the international scenario, there is the additional complexity of varying requirements across jurisdictions which would have implications on consumer outcomes.

CONSUMER PROTECTION

In traditional finance, a possible risk to consumers of using payment institutions or e-money issuers is that the money paid by the consumer (to the intermediary) does not get successfully transferred on to the end beneficiary due to outages, fraud, settlement failure, or the insolvency of the intermediary.

To mitigate this risk, the UK Payment Services Regulations (PSRs) and e-Money Regulations (EMRs) impose capital, safeguarding, outsourcing, accounting and audit requirements onto these intermediaries. These payment and e-money firms must also be authorised by the FCA and comply with FCA regulations pertaining to AML/CFT and operational resilience. Specifically in cases of insolvency, a new special administration regime was introduced in November 2021 so that funds can more efficiently be returned to consumers (as compared to using standard administration processes).

As discussed earlier in the report, the government is in the process of amending the PSRs and EMRs to bring stablecoins into scope through the Financial Services and Markets Bill. This Bill gives HMT the power to bring "digital settlement assets" used for payments into the UK regulatory perimeter.

Given the nascent nature of the cryptoasset market, the Bill gives HM Treasury a power to amend this definition in the event that there are new features, underlying technology or usage of these assets. This will allow for the regulation to continue to have the intended effect.

The Bill currently defines a 'digital settlement asset' 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).

Due to the general wording used in this definition, it may not need to be amended to incorporate the use of unbacked cryptoassets.

Given this, questions are opened up as to whether being an intermediary facilitating the use of unbacked cryptoassets to make payments would qualify as a payment service, with corresponding regulation under the PSRs and EMRs. If it did, tailoring would need to occur to account for specific and novel risks. For example, under PSR and EMRs ongoing capital requirements are calculated based on factors such as 'a scaled amount representing the firms' average monthly payment volume'. In the case of unbacked cryptoassets, this would need to be supplemented with a significant volatility add-on to account for the rapid price swings, legal uncertainty and enhanced operational risks (due to the nascent infrastructure) or the custodying or backing of multiple asset types to issue a token.

In addition to the new Consumer Duty (mentioned at the start in the overarching themes section), there are developing/nascent consumer protection considerations for a crypto payments use case: work to unlock the wide opportunities of Open Banking and increase account-to-account retail transactions (A2ART); and work to introduce new consumer protections measures for authorised push payment (APP) scams. While neither would directly impact on crypto firms today, it is arguable that the precedent set in terms of the consumer experience of payments/transacting could set high expectations.

In September, the PSR (through the Joint Regulatory Oversight Committee – JROC) pulled together a Strategic Working Group (SWG) to explore how to 'unlock' the wider opportunities of Open Banking payments. In essence, the PSR is seeking to increase choice for merchants. A series of detailed sprints with industry stakeholders was launched to unpick a whole variety of issues connected with increasing the use of account-to-account (often initiated via open banking) payments for retail (A2ART). If the regulators' vision for A2A payments were to be realised it may see an uptick in the volume of Faster Payments/payments through the New Payments Architecture (NPA) for retail use (i.e. consumers making in person point-of-sale and online purchases with retailers paying direct from their bank account).

The focus of this work is currently on A2A payments via the interbank rails (e.g. Faster Payments) given the focus on Open Banking. However, in principle, consumers might in future use a payment initiation service provider (PISP) or equivalent to initiate a stablecoin or even crypto

[33] Subject to it falling outside the current CGT exempt threshold in any given tax year (at present up to £12,300)

payment (subject to the offering of the PISP and merchant). In which case, the very detailed discussions now underway in the payments industry about how to possibly provide for consumer purchase protection, liability and dispute mechanisms (as separate from the usual remit of payments firms whose responsibilities usually end with the correct transmission of the payment), are presumably representative of issues that may well arise in due course for crypto firms also. Taking an early view on how some of those complex issues might be addressed, for example, through standards, voluntary codes and cross-industry collaboration, may help to mitigate the challenges and ensure better and safe uptake of such new payment options for consumers and merchants. In addition, seeking to leverage the potentially richer data available through some of the underlying technologies of crypto may help to address some of the difficulties faced in supporting consumers with purchase or other disputes.

The second area of note is APP scams. In October 2022, the PSR published proposals designed to reduce the rates of APP scams and enhance the consumer outcomes. Current suggestions are for mandatory reimbursement within 48 hours amongst other elements. While crypto firms may be some way off coming into scope of such rules, it is again worth considering how such high levels of consumer protection might function in future scenarios where perhaps consumers have been scammed into making crypto transfers to pay for goods/services. For all parts of the industry, there also needs to be consideration of how crypto firms and traditional finance firms can work together on risk management and the protection of consumers. Further collaboration between traditional banks and payment firms and crypto firms is also likely to enable a better understanding of how criminals might exploit the on-off ramps between the different parts of the sector for multi-generation type scams and other consumer harms. Some traditional firms have already been seen to be blocking some crypto activity in order to protect customers. Ongoing collaboration and the appropriate consumer protection regulations may help to mitigate such actions in the future.

SAFEGUARDING AND SEGREGATION

Under the PSRs and EMRs, firms are required to safeguard customers' funds by either placing them in a segregated account (distinct from the institution's own working capital and other funds), or covering them with an appropriate insurance policy or comparable guarantee. Although the often-volatile nature of unbacked cryptoassets assets could make acquiring such a policy or guarantee difficult, regulators could focus on the segregation requirement as well as additional redeemability rules.

If applied to unbacked cryptoassets this segregation requirement could be met (i) by keeping the assets in different wallets to the firm's own wallet, (ii) by using a third party, or (iii) by converting funds to another cryptoasset.

Summary:

Although a payments use case for unbacked cryptoassets is perhaps more nascent, the regulatory considerations share the same focus as that of stablecoins, namely the PSRs and EMRs. Both of these regulations are likely to be reviewed in the next 12–18 months as part of the Future Regulatory Framework analysis and therefore an opportunity is available to ensure an effective application of rules for consumer protection and safeguarding and segregation. In addition, early consideration may be helpful of emerging expectations of 'payments providers'. These will sit alongside the Consumer Duty, and might apply to unbacked cryptoasset service providers, for example, around purchase protection, reimbursement and fraud data sharing.

Designing a regulatory framework – Additional considerations

Beyond the specific elements described in each of the three use cases, there are some additional considerations which unbacked cryptoassets present in the regulatory context. Once again, the analysis points introduced here do not reach definite conclusions, but rather aim to stimulate further discussion and consultation so that they can eventually be factored into the final regulatory framework in an effective way.

DECENTRALISED FINANCE (DEFI)

According to IOSCO,[34] DeFi is "the provision of financial products, services, arrangements and activities that use DLT to disintermediate and decentralise legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions". As such, DeFi allows for user-directed, non-custodial economic transactions via smart contracts. These interactions are peer-to-protocol (i.e. between the user and the software).

Even if certain DeFi transactions 'sound' similar to transactions in the traditional financial system, they are fundamentally different because they are (a) facilitated entirely by the user, (b) run solely by software, and (c) devoid of traditional financial intermediaries.

DeFi brings novel challenges in a regulatory context because compliance cannot be imposed in the same way as in the traditional financial system without the typical entities or individual(s) able to be held accountable.

According to the FSB, "among crypto-asset activities provided by DeFi protocols, there exist a variety of governance structures, some of which may obfuscate the identification of a governance body or otherwise impede the application of regulation. In some other cases, there may be individuals/entities responsible for the operation of an activity that have not adequately disclosed their roles." As such, regulators need to establish ways to identify who exercises effective control of the protocol or provides access to the protocol, and to find ways of making them accountable.

Moreover, the FSB also notes that while DeFi protocols claim governance to be entirely distributed; in reality, governance is often concentrated in a small group of participants (developers, investors or governance token holders). Other international regulatory bodies (including the OECD[35]) have also noted that there may be some concentration in governance of DeFi protocols – e.g. the 'decentralisation illusion' where a majority of participants band together.

The FSB proposed framework suggests that DeFi protocols should not undermine robust governance and accountability arrangements. Authorities should require compliance with rules and regulations for effective governance irrespective of the structures of activities and technology used to conduct the cryptoasset activities. However, stakeholders have warned that this framework could risk impeding the innovative technology.

A potential solution that regulators are currently exploring is the idea of embedded supervision – which allows authorities to directly interact with distributed networks, enabling them to monitor compliance in real-time by viewing blockchain transaction data. The European Commission is currently tendering for a project with the objective of establishing how and what data can be gathered from DeFi protocols on the Ethereum public blockchain in real time, how this can be used for effective supervision of DeFi activity and, if not, what critical data may be missing.

And yet, although theoretically appealing, the IMF's view28[36] is that such an approach would initially be limited to authorities with the relevant resources and expertise, and a high initial investment could be required, with ongoing costs of maintenance and training.

Instead, a member of the Bank of England's[37] Financial Policy Committee has suggested starting by designing industry-led codes of conduct that could include practices such as regular audits of the code, and disclosure of how rights to change the code are determined. This is consistent with the most recent report by the European Union Commission on DeFi Policy Considerations[38] that proposes introducing a voluntary compliance framework – where protocols and users freely choose to adhere to some policy requirements in order to obtain different forms of public support.

[34] IOSCO, Decentralised Finance Report (2022)
[35] https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf
[36] https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715
[37] Bank of England, Governance of "Decentralised" Finance: Get up, Stand up! - speech by Carolyn Wilkins (2022)
[38] European Commission, Decentralised Finance: Information Frictions and Public Politics (2022)

More stringently, other European regulators[39] are strongly advocating that the providers and users of DeFi be held accountable for ensuring that these smart contracts operate within the legal framework and fulfil relevant obligations.

UNDERLYING TECHNOLOGY

Regarding the underlying technology itself – DLT – there are several factors that should be taken into account.

Firstly, DLT comes in two forms – either decentralised and public, or centralised and private. Whereas public 'permissionless' DLT allows any user to add nodes to the network, a private 'permissioned' infrastructure has a gatekeeper who limits access to pre-authorised users.

The use of DLT in financial services can deliver may benefits. DLT's smart contracts allow for the codification of stakeholders' rights, obligations and ownership and produce a single source of truth. As a result, the need for bilateral reconciliation is eliminated, along with many other inefficiencies encountered in legacy systems (e.g. the processing gap between front and back-office functions, settlement risk, the need for capital buffers, a lack of transparency).

However, the use of DLT also presents new challenges and risks.

The IMF28[40] has pointed out how these risks differ depending on whether the DLT is private or public. Private blockchain risks include fragmentation, concentration, financial stability risks, too-big-to-fail systems and single point of failure risks. On the other hand, public blockchain risks include 51 per cent attacks, and MEV. Both types of DLT introduce new risks related to counterparty issuance.

As a result of the various risks, the Basel Committee's second consultation on the prudential treatment of cryptoassets,[41] incorporates an 'add on' to risk weighted assets. The Committee notes that, as the infrastructure is still relatively new, it may pose additional unknown risks or could alter the risk profile of traditional assets.[42]

Finally, the IMF has also pointed out how certain types of consensus mechanisms generate frictions with broader policy objectives. For example, proof-of-work consensus is extremely energy-consumptive and consequently does not sit comfortably alongside the ESG agenda. On the other hand, alternative types of consensus (such as proof-of-stake) could generate security, concentration or financial inclusion concerns. The IMF has illustrated this by describing how, although the shift from proof-of-work to proof-of-stake would improve energy efficiency and scalability, it could also create excessive concentration of decision-making powers on crypto exchanges and wallet services providers, which may increase market integrity risks.

When MiCA[43] comes into force in 2024, it will require cryptoassets to disclose their carbon footprint. The EU is also working on a scheme to grade/label blockchains according to their energy efficiency, and potentially even include minimum energy efficiency requirements.

More generally, the FSB17[44] has proposed that authorities should require cryptoasset issuers and service providers to disclose any material risks associated with the underlying technologies, such as cyber security risk, as well as environmental and climate risks and impacts, as appropriate and in line with jurisdictional legal frameworks.

STAKING

In short, staking is a way of earning rewards for holding certain cryptoassets, and it has important regulatory implications.

For the benefit of this report, we split staking into the following two categories:

Staking as a validator on a proof-of-stake blockchain. This is when a participant 'locks up' cryptoassets for a set period of time to help support the operation of the blockchain. Blockchains that have consensus mechanisms[45] based on proof-of-stake, require validators or 'stakers' to provide capital (generally in the form of the blockchain's native token) to the public network. These 'stakers' are incentivised to do so as they receive fees and newly minted tokens as a reward for producing new blocks and securing the network, proportional to the amount they have staked. This process also disincentivises bad actors from acting against the interest of the system as their own capital is at risk.

As an additional consideration, this staking process can sometimes be delegated out (in a decentralised manner) or managed through 'pools' operated by centralised entities, both of which have secondary implications.

Staking as an entity (individual or corporate) as a means to receive passive income. This second form of staking does not involve providing capital to secure a blockchain. However, it is a way for token holders to earn income by lending out their token – either to a centralised exchange or to a decentralised application within the DeFi ecosystem.

Regulators should be cognisant of the of the distinction between the two forms of staking outlined above. Staking as a validator is essential for the security of any blockchain. As such, should regulation around staking become too stringent, regulatory arbitrage opportunities can lead to a geographical concentration of validators which may compromise the security of the blockchain of the cryptoasset in question.

However, there are specific risks that need to be accounted for in regard to staking. For example, there is the potential for users to lose their stake (i.e. have their stake 'slashed') when an incorrect or missing attestation arises during the consensus process.

Moreover, there are also market abuse and conflict of interest considerations. For example, exchanges are often the largest holders of an asset and therefore can have disproportionate control of applications when engaging in proof-of-stake consensus.

[39] Politico, Digital Bridge: Race for chips – Decentralized finance – US tech gets political (2022)
[40] https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715
[41] Bank for International Settlements, Basel Committee publishes second consultation document on the prudential treatment of banks' cryptoasset exposures (2022)
[42] https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715
[43] European Council, Digital finance: agreement reached on European crypto-assets regulation (MiCA) (2022)
[44] Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report – Financial Stability Board (fsb.org)
[45] Investopedia, What Are Consensus Mechanisms in Blockchain and Cryptocurrency? (2021)

Conclusions

Overall, in the regulation of these cryptoassets, the UK needs to move in a more agile (but informed) way, in order to avoid falling behind other jurisdictions. The longer it takes for the government and regulators to agree upon and begin implementing a coherent approach, the more firms are deciding to establish their business elsewhere.

The FRF offers a significant opportunity for the UK to achieve this agility. Through the analysis of our three use cases, as well as our proposed regulatory guiding principles and additional considerations, this report has demonstrated how, in order to address risks and harms in the crypto market, existing regulations and tools can be leveraged. Defining cryptoassets as financial instruments could bring them into CASS and the on-shored MiFID and MAR regimes.

However, despite acting as a valuable starting point, these regulations may need to be significantly amended and adapted to sufficiently map cryptoassets and account for the novel risks raised. In our report, we have discussed some of the specific considerations that would need to be accounted for.

Alternatively, defining, for example, the trading of cryptoassets or the safeguarding of cryptoassets as a regulated activity, would require firms partaking in these activities to be authorised by the FCA. Then firms would need to comply with the FCA Principles of Business which contain high level principles such as maintaining adequate financial resources, observing proper market conduct and treating customers fairly.

In order for the UK to achieve its goal of becoming a 'crypto hub', it's important that policy makers continue to engage with industry participants to promote a mutual understanding of objectives, perspectives and experiences. It is also important to avoid inadvertently creating a 'halo effect' around these assets, with unrealistic expectations of what constitutes consumer protection – as pointed out by ex-FCA Chair, Charles Randell.[46]

Policy makers should also continue to seek international alignment in their approach and be guided by global frameworks wherever possible.

Together, these elements will facilitate the development of an effective and efficient regulatory framework.

In order for the UK to achieve its goal of becoming a 'crypto hub', it's important that policy makers continue to engage with industry participants to promote a mutual understanding of objectives, perspectives and experiences.

[46] https://www.fca.org.uk/news/speeches/risks-token-regulation

Appendix 1: Glossary of terms

Unbacked cryptoassets	Cryptoassets that offer limited or no rights for the token holder and are usually issued in a decentralised manner. Users may treat unbacked cryptoassets as speculative instruments rather than mediums of exchange
Exchange or payment tokens	Cryptoassets that utilise a DLT platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens but are used as a means of exchange or for investment
Utility tokens	Cryptoassets which can be redeemed for access to a specific product or service that is typically provided using a DLT platform
Security tokens	Cryptoassets which amount to a 'specified investment' as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order (RAO). These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or financial instruments under the EU's Markets in Financial Instruments Directive II (MiFID II).
Stablecoins	Cryptoassets backed by a fiat currency or another type of traditional asset class (debt instruments/ precious metals.
DLT/Blockchain	A blockchain or DLT is a digital system for recording the transaction of assets that uses cryptography to store information securely and immutably in multiple places simultaneously. Unlike traditional databases, distributed ledgers have no central data store or administrative functionality – and require consensus to update the state of the ledger. DLT is the technology that underpins all assets in the crypto-ecosystem.
On-chain/Off-chain	The phrase 'on chain' refers to activity which takes place on the blockchain. Correspondingly, the phrase 'off chain' refers to activity which takes place off the blockchain.
Bridges	A bridge is a blockchain application which facilitates the transfer of assets between different blockchains.
Node	A computer connected to a blockchain network that supports the network through validation and relaying of transactions on the blockchain. It also maintains a full copy of the blockchain.
Consensus Mechanisms (Proof-of-work and proof-of-stake)	A consensus mechanism is the process by which a blockchain agrees on and updates the state of the ledger through a network of validators. These mechanisms can be either proof-of-work or proof-of-stake. A proof-of-work consensus mechanism does this through validators (miners) solving complex mathematical problems which requires hardware and energy. The first miner to solve the problem is rewarded the block fee, and as other miners agree on the solution provided by the original miner, further confirmations are added to the state of the blockchain.
Hash Rate	A hash rate is the speed at which proof-of-work validators (miners) can process potential solutions to the mathematical problem which is to be solved in order to process the block of transactions. Hash rate is generated by specialised hardware using electricity.
Miners	Miners are entities which process transactions/blocks on a proof-of-work blockchain by solving complex mathematical problems.
Smart Contracts	Smart contracts are applications which handle transactional logic on the blockchain (i.e. when X happens, do Y). They are 'self-executing' lines of code, where the terms of a transaction are automatically verified and performed via the blockchain network.

<table>
<tr><td><b>Keys</b></td><td colspan="2">Keys allow participants to send and receive cryptocurrency without requiring third-party verification of blockchain transactions. There are 'public' keys and 'private' keys which operate as a pair.</td></tr>
<tr><td><b>Private Key</b></td><td colspan="2">An alphanumeric string of characters that initiates a transaction. The private key is unique to each public key and cannot be reproduced if lost or stolen. Digital assets are controlled using the unique private key associated with the public addresses in which the digital assets are held. The theft, loss or destruction of a private key is irreversible, and those private keys would not be able to be restored.</td></tr>
<tr><td><b>Public Key</b></td><td colspan="2">An alphanumeric string of characters that is the public address of the wallet. Other parties can send digital assets to a public address (similar to an email address). A user can provide the public key to a third-party as part of a transaction (i.e. request for funds), however the third-party cannot access or transact assets within the wallet.</td></tr>
<tr><td><b>Transaction Cluster</b></td><td colspan="2">A series of transactions on the blockchain which can be grouped together due to their proximity between wallet addresses (e.g. wallets that regularly interact with each-other).</td></tr>
<tr><td><b>Mixers</b></td><td colspan="2">Mixers are applications which send transactions through a series of wallets to hide the origin of the digital assets being transferred.</td></tr>
<tr><td rowspan="6"><b>Wallet</b></td><td colspan="2">A wallet stores private and public keys. It enables users to transact on blockchains and see balances and transactions related to the wallet.

A hot wallet is a wallet which is connected to the internet (i.e. Desktop, Online, Mobile). A cold wallet is one which is not connected to the internet (i.e. Hardware, Paper).

A wallet may be a:</td></tr>
<tr><td>Desktop</td><td>Wallets downloaded and installed on a PC or laptop. They are only accessible from the single computer in which they are downloaded.</td></tr>
<tr><td>Online</td><td>Wallets run on the cloud and are accessible from any computing device in any location. While they are more convenient to access, online wallets store private keys online and are controlled by a third party, making them more vulnerable to hacking attacks and theft.</td></tr>
<tr><td>Mobile</td><td>Wallets run on an app on a mobile device that can be used anywhere including retail stores. Mobile wallets are usually much smaller and simpler than desktop wallets because of the limited space available on a mobile device.</td></tr>
<tr><td>Hardware</td><td>Wallets that store private keys on a hardware device like a USB. Although hardware wallets make transactions online, they are stored offline, delivering increased security.</td></tr>
<tr><td>Paper</td><td>The term 'paper wallet' can simply refer to a physical copy or printout of the public and private keys. It can also refer to a piece of software used to securely generate a pair of keys, which are then printed.</td></tr>
</table>

Appendix 2: Current UK regulatory landscape – Detailed timeline

This section includes a detailed description of each of the timeline milestones represented in the section 'Overview of UK Regulatory Landscape'.

July 2019: The FCA published PS19/22 – Guidance on Cryptoassets[47]

This policy statement clarifies the types of cryptoassets that fall within the FCA's regulatory remit and the resulting obligations on market participants. In summary, it notes that:

- Exchange tokens fall outside of the perimeter
- Utility tokens fall outside of the perimeter, unless they qualify as e-money (i.e. some stablecoins) – at which point, they are regulated under EMRs
- Security tokens (i.e. those that qualify as specified investment under RAO) fall within the perimeter
- Where an FCA-authorised firm carries on unregulated activity – while that activity may not require a permission in itself, it's possible that some FCA rules (e.g. Principles for Business, SMCR) may still apply
- Any firms using cryptoassets to facilitate regulated payments, must ensure that they have the correct permissions

January 2020: FCA requirement for firms carrying out cryptoasset activity in the UK to be compliant with AML/CFT requirements[48]

- Includes requirement to be registered with the FCA in order to continue carrying on business
- FCA responsibility under this regime is limited to AML/CFT registration supervision and enforcement only. Does not provide customers with protections of the Financial Ombudsman Service or the FSCS

January 2021: FCA ban on the sale of crypto derivatives and exchange traded notes (ETNs) to retail consumers becomes effective[49]

January 2022: HMT publishes response to consultation proposing to strengthen rules on misleading crypto promotions[50]

- Proposes to regulate cryptocurrency adverts, with the intention of bringing the promotion of "qualifying cryptoassets" within the scope of the Financial Services and Markets Act 2000 (FSMA) and the FCA. As part of this:
  - A person must not, in the course of business, communicate an invitation or inducement to engage in an investment activity or claims management activity unless that communication (i) is made by an authorised person; (ii) has been approved by an authorised person; or (iii) is exempted under the Financial Promotions Order (FPO)
- Until the legislation comes into force, the Advertising Standards Authority (ASA) has been issuing enforcement notices

March 2022: PRA issues 'Dear CEO' letter on prudential framework for crypto assets[51]

- Aims to operate as an interim approach until international frameworks (e.g. BCBS) are finalised (expected end-2022)
- Proposes:
  - Strong risk controls
  - Pillar 1 framework considerations
    - Direct holdings of cryptoassets likely classified as an intangible asset – and therefore result in full deduction of any direct holdings from CET1
    - For market risk, a capital requirement of 100% of the current value of the firm's position should be used. Diversification and hedging frameworks should be conservative (e.g. the commodity framework). Most counterparty credit risk crypto exposures will likely be mapped to 'other risks' category for SA-CCR purposes

[47] https://www.fca.org.uk/publication/policy/ps19-22.pdf
[48] https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime
[49] https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers
[50] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1047232/Cryptoasset_Financial_Promotions_Response.pdf
[51] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2022/march/existing-or-planned-exposure-to-cryptoassets.pdf

- Pillar 2 framework considerations
    - Firms should set out considerations of risks in their ICAAP
    - Separately assess activities for at least market risk, credit risk, counterparty credit risk and operational risk
- Also consider extent to which products, market participants or legal structures expose them to risks not generally considered in existing Pillar 2 assessments

March 2022: FCA published notice reminding firms of existing obligations[52]

- Notes that all FCA regulated firms must observe Principles for Business[53]
    - Principle 10 requires a firm to arrange adequate protection for clients' assets. As part of this, the FCA's Client Assets Sourcebook[54] (CASS) provides detailed rules to follow when holding regulated assets in custody
    - Where cryptoassets are specified investments[55] (i.e. security tokens), firms carrying out regulated activities involving custody of these assets are likely to be subject to the CASS regime
- While currently no specific prudential treatments – there are still regulatory obligations. Firms subject to the new investment firm prudential regime (IFPR), have obligations (under MIFIDPRU 7)[56] to assess and mitigate the potential for harm to clients, to the markets in which the firm operates and to itself, that could arise from all of their business. This applies whether or not that business consists of MiFID investment business, other regulated activity or is unregulated. It also applies irrespective of operating on an agency basis, principal basis, or in some other capacity. This therefore includes cryptoassets business, however firms conduct that business
- Other firms subject to FG20/1: Assessing adequate financial resources[57] should consider that guidance when assessing and managing risks and exposures from cryptoassets. Where a firm accounts for a cryptoasset as an intangible asset, it will likely need to deduct this asset from its regulatory capital

July 2022: HMT introduced FS and Markets Bill[58]

- Proposes bringing stablecoins within existing e-money and payment services regulation
    - Potentially may use an HQLA backing model
- Introduces regulatory sandboxes to experiment with the use of DLT in financial market infrastructures
    - Participants can experiment with trading and settling crypto while having certain reg requirements suspended
    - Each sand box will be created by a specific statutory instrument
    - Andrew Griffith's amendment to the Bill gave HMT and the FCA powers to regulate unbacked cryptoassets
- Law Commission's report (28 July 2022) around future reforms relating to the law regarding digital assets: The Law Commission published proposals and sought views from legal experts, technologists and users, examining how existing personal property law does – and should – apply to digital assets. The Commission's proposals are designed to ensure that the law remains dynamic, highly competitive, and flexible, so that it can support transactions and other arrangements involving the technology.

Sept 2022: HMT amendments to regulation on AML/CFT/ transfer of funds came into force[59]

- Addresses the Financial Action Task Force's (FATF) "Travel Rule" – requiring that countries ensure financial institutions send and record information on the originator and beneficiary of a wire transfer, and that this information remains with the transfer or related message throughout the payment chain
- Expands this to cryptoassets:
    - Includes de minimus threshold of EUR 1000
    - Only one of the originator's address, date and place of birth, and passport number to be sent with a cross-border transfer that is above the de minimis
    - Only applies to intermediaries that are cryptoasset exchange providers or custodian wallet providers
    - For un-hosted wallet transfers, cryptoasset businesses will only be expected to collect this information for transactions identified as posing an elevated risk of illicit finance. The minimum factors that firms should consider when making such a determination of risk will be set out in the legislation

H1 2023: HMT consultation on wider crypto-asset regulation expected

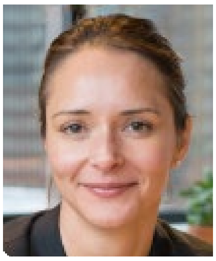
- HMT may potentially use the EU's MICA[60] as a crib sheet
    - UK FSM Bill to be agreed in summer 2023 (which would establish the stablecoin framework);

Q1 2024: MiCA to begin applying to in-scope firms

[52] https://www.fca.org.uk/news/statements/notice-regulated-firms-exposure-cryptoassets
[53] https://www.handbook.fca.org.uk/handbook/PRIN.pdf
[54] https://www.handbook.fca.org.uk/handbook/CASS/
[55] https://www.handbook.fca.org.uk/handbook/glossary/G1117.html
[56] https://www.handbook.fca.org.uk/handbook/MIFIDPRU/7/1.html?date=2022-07-29
[57] https://www.fca.org.uk/publications/finalised-guidance/fg20-1-assessing-adequate-financial-resources
[58] https://bills.parliament.uk/bills/3326
[59] https://www.legislation.gov.uk/uksi/2022/860/introduction/made
[60] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

CONTRIBUTORS

UK FINANCE



Jana Mackintosh
Managing Director, Payments and Innovation

Phillip Mind
Director, Digital Technology and Innovation

Rhiannon Butterfield
Principal, Payments and Innovation

Will Lee
Analyst, Payments and Innovation

KPMG

John Hallsworth
Partner, Open Finance and Fintech

Rob Smith
UK Head, Financial Services Regulatory & Risk Advisory Services

Ian Taylor
Head of Crypto & Digital Assets

Sinchan Banerjee
Director, Digital Assets Consulting

Kate Dawson
Director, Regulatory Insights Centre

Bronwyn Allan
Manager, Regulatory Insights Centre

Maz Shakibaii
Assistant Manager, Digital Assets Consulting

This report is intended to provide general information only and is not intended to be comprehensive or to provide legal, regulatory, financial or other advice to any person. Information contained in this report based on public sources has been assumed to be reliable and no representation or undertaking is made or given as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of UK Finance or any of their respective members, officers, employees or agents shall have any liability to any person arising from or in connection with any use of this report or any information or views contained in this report.