DIGITAL CURRENCIES
Governance Group

Call for Evidence: Review of the UK's AML/CTF regulatory and supervisory regime

OCTOBER 14, 2021

Digital Currencies Governance Group (DCGG) is an international industry body with the aim to provide regulators with unbiased information, best practice knowledge and expert industry-related insights on policies concerning crypto-assets.

DCGG represents the full spectrum of key stakeholders in the ecosystem, including Tether – the biggest stablecoin issuer worldwide, Hermez – pioneer Layer 2 technology for scaling payments, Bitfinex – top tier digital assets exchange, Iden3 – avant-garde player in blockchain-based identity management, and others.

DCGG creates an open dialogue and encourages the communication between political representatives and digital currencies experts to ensure that legislation supports scale and innovation in the crypto-asset space.

GENERAL CONSIDERATIONS

Regulating an innovative and fast-paced area such as the markets for crypto assets is not a trivial regulatory task, and DCGG is grateful for the opportunity to submit our Members' feedback to the Government's review of the UK's Anti-Money Laundering (AML) regulatory framework. Our Members firmly believe that the new technologies, including in the areas of data storage, data governance, encryption, third-party disintermediation, which drive the growth in crypto assets, can be leveraged towards effective AML practices. Furthermore, having a proportionate evidence-driven approach will set the UK apart from other jurisdictions, attract talent and business and help the UK regain its FinTech Hub leading role.

Extent of the regulated sector

Question 12. What evidence should we consider as we evaluate whether the sectors or subsectors listed above should be considered for inclusion or exclusion from the regulated sector?

The proportional extension of AML requirements over new sectors, particularly sectors developed on the basis of new and still rapidly developing technologies such as DLT, should factor in the following:

- *Growth of the sector*: The rapid growth of crypto-assets calls for a proportionate approach in the sector. It should be acknowledged that while some platforms have reached global scale, most of the sector is driven by small experimental projects, whose development is essential for the continuous development of the products and their underlying technology.
- *Business models:* There is sometimes a tendency to assume that all business models in crypto-assets markets carry similar AML risk. Much like in Financial Services, this is not the case. Specifically, while there are some products which attract customers because of their privacy functionalities, there are many others where rigorous Customer Due Diligence is the norm. This nuance should be factored in the regulatory framework through a principles-based approach as much as possible.
- *Technological Advantages*: Regulatory framework as well as enforcement powers should factor in novel risk-mitigating technological innovations such as blockchain tracing capabilities or wallet freezing capabilities. There is huge potential for effective public private partnerships between law enforcement, regulators and the private sector.

- It has been demonstrated that regulation cannot anticipate innovation effectively - which is why rules should consider how best to be future-proof in all their increasing diversity, and their AML risk profile.
- One effective way to collect evidence which can inform legislative or regulatory change is to use the *FCA's Regulatory Sandbox*. It is possible - and there are precedents of this outside the UK - to set up a dedicated and streamlined Sandbox fast-track process, where, for example, crypto-asset service providers pilot their solutions to comply with the so-called Travel Rule. It is also possible to use the Sandbox approach to test how DLT can be used to support addressing AML risks, detecting suspicious transactions, ceasing illicit activity and share data with enforcement agencies.

Question 13. Are there any sectors or sub-sectors not listed above that should be considered for inclusion or exclusion from the regulated sector?

There are three sectors / sub-sectors which should be left out of scope for AML regulation for the time being:

1. While DCGG Members support transparency requirements levied on service providers and transactions between them, we strongly believe that no feasible technology exists to comply with transparency requirements between service providers and persons (i.e., those transacting via the so called un-hosted wallets). *Un-hosted wallets are the crypto equivalent of cash-in-hand, and as such should be left out of scope for the Travel Rule*. To this end, even if there are any transparency requirements, as the FATF proposes, CASPs should not be liable for the accuracy of data sent from un-hosted wallets.
2. *Decentralised Finance (DeFi):* DeFi is a new segment of markets for crypto-assets. These are, essentially, products (both tokens and services) where a computer programme (algorithm) takes the role of a central counterparty, and any changes to this system are done only when all participants in the system, collectively, decide so - via casting their digital votes. In DeFi, the service provider and the service customer can be, effectively, the same person. Often, there is no need for a central legal entity, and even if one exists, it does not have the same powers as it would in traditional finance. For example, compliance with AML rules is decided through vote-based changes in the algorithm. It is not done by a centralised, human-based, function. DeFi is hugely promising, but extremely new when it comes to supervision and regulation. Requiring DeFi projects to comply with regulation intended for centralised entities often means that the projects cannot exist. To this end, while we encourage close work with regulators to establish an appropriate regulatory regime, we believe DeFi should be left out of scope.
3. In a similar vein, *projects where there is no central entity with effective control, such as algorithmic stablecoins or public permission-less distributed ledgers (i.e., Bitcoin, Ethereum) should clearly be out of scope for AML requirements.*

Question 14. What are the key factors that should be considered when amending the scope of the regulated sector?

DCGG Members put forward the following key factors:

- How AML risk / incidents in the sector compares to AML risk in other sectors – for example, transfers of crypto assets vs. wire transfers differ considerably in the reliability of their traceability. Customer identifying information may not be stored on-chain, but law enforcement have other ways to get this information, and the greater reliability of blockchain data will yield a greater return from these efforts.
- *How the sector has reacted and adapted to address AML risk - for example, groups of VASPs, including Tether and Bitfinex, have collaborated to catalogue and share AML red flag indicators in an effort to mitigate the steep learning curve of this new type of value transfer.*
- *How the regulator will allow the industry to grow, and learn alongside it - for example, Tether and Bitfinex regularly work with law enforcement in numerous jurisdictions when presented with valid requests, and have held training sessions with participation from law enforcement.*
- How to harness the potential of the DLT technology as a force for good in addressing AML risk. Contrary to the popular belief that digital assets are best suited for criminal use, there have been many examples of law enforcement successfully tracking down criminals and the proceeds of crime by leveraging public blockchain information. Moreover, formalized cooperation between cryptoasset exchange providers and law enforcement can help cryptoasset exchange providers to become aware of and freeze illicit funds in real-time on a worldwide basis, something that is not possible in the traditional financial system.

HOW THE REGULATIONS AFFECT THE UPTAKE OF NEW TECHNOLOGIES

Question 39. More broadly, and potentially beyond the MLRs, what action do you believe the government and industry should each be taking to widen the adoption of new technologies to tackle economic crime?

Government regulators, law enforcement and crypto asset exchange providers have the opportunity to create public-private partnerships to allow valuable information to be delivered to law enforcement while respecting data-privacy laws.

The traceability of blockchain movements allows for real-time detection and flagging of illicit blockchain transfers. Groups consisting of crypto-asset exchange providers, blockchain tracing companies and private investigators already exist that have a purpose of flagging on a private forum illicit transfer so that crypto-asset exchange providers can freeze any flagged illicit funds. With the addition of regulatory mandated suspicious activity reports, such programs can be expanded to allow crypto-asset exchange providers to file SARs with regulators world-wide. Moreover, law enforcement could flag funds related to heinous or time-sensitive crimes in order to raise a global red-flag on suspicious activity. This could be very useful for time-sensitive crimes like child exploitation where haste could save the life and dignity of a child or hack/ransoms of major companies or utilities companies.

Another important step that can be taken for *ensuring AML/KYC compliance whilst preserving user privacy requirements consistent with the UK's data protection regime would be to allow for the use of Zero-Knowledge Proof (ZKP) technology*.

ZKP is an advanced cryptographic technique that allows any piece of information such as user identity, tax and/or regulatory compliance, to be verified by a trusted counterparty. A short cryptographic proof is provided, which can then be re-verified at any time at very low cost without the verifier needing to maintain custody of the underlying information or documents. ZKP can essentially serve as a "notary on the blockchain", which significantly reduces transaction costs and increases transparency when investigating potential Money Laundering and Terrorist Financing. ZKP assigns cryptographic codes to users over a long period of time, meaning that Customer Due Diligence does not need to be conducted by each institution separately. This is both cost-effective and secure since personal information is prevented from being spread across multiple institutions. However, if a transaction is suspicious, law enforcement can receive access to the identities behind the codes within minutes.

Use of ZKP, when applied correctly, allows for meeting AML/KYC/CFT compliance objectives and reducing the burden of proof. Many regulations are written in an unnecessarily prescriptive way that requires each intermediary in a payment transaction chain to have sight and custody of underlying documents. ZKP is a transformative technology that offers very substantial cost savings whilst enhancing both compliance and privacy. If the necessary legal and regulatory recognition were given to ZKP the benefits would accrue to all parties.

ZKP allows users to take full advantage of the data-based economy whilst securing their privacy. The adoption of ZKP by HM Treasury will make the UK a pioneer in a novel, cutting-edge technology that will trigger economic growth and establish the most effective safety procedures within its digital economy.

Gatekeeping function

Question 45. Is it effective to have both Regulation 26 and Regulation 58 in place to support supervisors in their gatekeeper function, or would a single test support more effective gatekeeping?

DCGG would support further harmonization and consolidation of the 'gatekeeping tests' across the industry. As some individuals may be subject to more than one of the gatekeeping tests and, as the various tests can lead to different information requested, the evaluations might lead to possible inconsistencies in the assessments. Furthermore, the current variable standards are not necessarily linked to the risk that the different sectors may pose. The current rules regarding the information sought for cryptoasset business registration applicants are already very rigorous and exhaustive, which can be a burden especially for smaller start-up businesses.

DCGG members welcome a harmonized approach to supervision and risk assessment based on clients, products and geographies. It would also be important to ensure that any cryptoasset business is not by definition considered risky due to their nature (centralized or decentralized) but that there is a consistent approach across the financial services industry.