DIGITAL CURRENCIES
Governance Group

OECD public consultation on Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard

DIGITAL CURRENCIES GOVERNANCE GROUP RESPONSE

About Digital Currencies Governance Group (DCGG)

DCGG represents the interests of the crypto-asset ecosystem and advocates for an innovation-friendly regulatory environment that ensures safety for all market participants. DCGG seeks to facilitate an open dialogue and encourages communication between political representatives and digital currency experts to ensure that legislation supports both political objectives and innovation in the digital-asset space. To this end, DCGG regularly engages with policy-makers and regulators both at the EU and national levels. DCGG represents a broad spectrum of stakeholders in the crypto-asset ecosystem. Among our Members, Tether – currently the largest stablecoin issuer worldwide, Ledger – a leading custodian service provider, Bitfinex – a crypto-assets exchange.

Executive Summary

DCGG supports the aim of the Organisation for Economic Co-operation and Development (OECD) to establish a global framework for market participants in the crypto space and tax authorities aiming to curb tax fraud and enhance tax collection. We fear that the broad approach to the scope may place a disproportionate burden on the crypto-assets industry compared to more established traditional industries. There is a high risk of penalizing a majority of compliant users while keeping problematic transactions under the radar, creating a false impression of safety. We believe that a limitation of the scope and clarification of relevant definitions and exclusions can help adapt the rules to the nature and resources of Crypto-Asset Service Providers without compromising the collection of relevant tax information. Further, we encourage the consideration of the superior transparency and immutability capabilities of distributed ledger technologies to be explicitly encoded in the proposed Crypto-Asset Reporting Framework (CARF).

General Comments

Overly increasing the reporting burdens on crypto-asset centralised service providers risks making using and operating those services impossibly costly and pushing users out of those services towards more decentralised, unregulated options not falling under stringent Know Your Customer (KYC) / Anti-Money Laundering (AML) / TAX reporting regimes. This would have a counterproductive effect in terms of

transparency supervision, since it will become more difficult to monitor transactions, creating a race-to-the-bottom dynamic.

On the contrary, developing private and public sector capabilities to use advanced transparency techniques such as blockchain analytics creates efficiencies not available in traditional finance.

For example, even if exchanges were to effectively increase transaction monitoring, deposits and withdrawals to local, private (unhosted) wallets, will remain an option for users. If exchanges are required to provide records of all transactions from and to a user's local wallet, supervision could still be circumvented by creating indefinite numbers of additional local wallets.

Unless incentivised to use centralised exchanges, users can still complete transactions using their local wallets, which do not fall and will not likely be able to fall under the proposed reporting framework. In turn, potentially asking exchanges to block these transactions because they cannot be reported would threaten the very basis of their business and goes directly against the foundations of the crypto-assets community.

Finally, we would like to make a consideration on data protection and privacy. DCGG members adhere to the strictest security requirements in the treatment of their users' data. By the nature of distributed ledger technology, all wallet addresses and transactions are recorded on a public blockchain, although not connected with user data. The collection and reporting of user data linked to wallet addresses increase the risks of security breaches, exposing the history of transactions of identified individuals in a way that is fundamentally different from traditional finance. Therefore, the rules for crypto-asset reporting should consider the vulnerability of data privacy in the transparent environment of blockchain technology.

1. Does the CARF cover the appropriate scope of Crypto-Assets? Do you see a need to either widen or restrict the scope of Crypto-Assets and, if so, why?

Although we understand the ambition to have a broad scope that includes most transactions in all crypto-assets, we want to caution against adopting an approach which lacks the needed nuance.

Therefore, DCGG Members recommend differentiating between classes of assets based on their utilization, technological design and core characteristics to enable the targeting of the scope of exchange of information based on their different risk profiles, without undue burden on low-risk investments and transactions. Further, we specifically address the treatment of non-fungible tokens (NFTs)

We believe it is also important to talk about the range of transactions in scope.

The number of transactions that would need to be recorded under the suggested rules does not add additional safeguards, will be very costly to implement and impractical to process for tax authorities.

Some of our Members match about 1 million trades per 24 hours. That would be roughly 365 million trades per year. Transactions are not stored in dedicated data files per user, but rather in a combined database. We believe it is therefore necessary to limit the types of transactions that are required to be reported. The most effective way to achieve this would be to exclude internal transactions from the scope. These are the types of transactions that occur within the same exchange, and therefore generate no actual taxable income for the user. Instead, users' deposits and withdrawals from and to an exchange and end of year balances could be reported in a significantly more cost-effective way.

In addition to that, it is worth considering the exclusion of transactions from/to own accounts, where one user transfers funds from his account on one platform to another account of his on another platform.

Gas transactions are another good example. Gas refers to the fee, or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum blockchain platform. This information is already publicly available and can be retrieved via details the CASPs are already required to provide. Unless explicitly excluded from CARF, this would simply be duplicating data that is already publicly available. Far more efficiently, the competent authority can develop capabilities to systematically collect and analyse publicly available information.

Other types of crypto-asset transactions might fall in the scope of this framework, but should not, include the so-called affiliates. These are existing customers who refer new people to join the platform and in exchange receive a very small bonus for each trade these people make. The amounts of the bonus are trivial, however, the reporting for all the trades and bonuses received could result in over a billion entries per year in total. This would add enormous administrative and financial burdens to the Reporting CASPs, without even being relevant for the purpose of capital gains.

Finally, stablecoins pegged to fiat currency, which can expect minimal gains or losses, present a low risk from a tax compliance perspective.

4. An NFT is in scope of the FATF Recommendations as a virtual asset if it is to be used for payment or investment purposes in practice. Under the Crypto-Asset Reporting Framework, an NFT would need to represent value and be tradable or transferable to be a Crypto-Asset. On that basis it is expected that relevant NFTs would generally be covered under both the CARF (as a Crypto-Asset) and the FATF Recommendations (either as a virtual asset or a financial asset). Are you aware of any circumstances where this would not be the case, in particular, any NFTs that would be covered under the definition of Crypto-Assets and that would not be considered virtual assets or financial assets under the FATF Recommendations or vice versa?

Reporting on NFTs can prove problematic in terms of determining their Fair Market Value. In addition, there can be situations where NFTs are reportable under CARF despite their underlying asset (such as property or artwork) not being an asset reportable under CRS. We believe that regulators should focus on the underlying assets, rather than attempting to cover a wide range of NFTs. In addition, in many situations it can be difficult to distinguish whether an NFT is held for investment or non-investment purposes, which further highlights the extent to which reporting can be problematic.

Intermediaries in scope

1. Do you see a need to either widen or restrict the scope of the intermediaries (i.e. Reporting Crypto-Asset Service Providers)?

While we highly appreciate the clarifications provided in the Commentary to the draft rules regarding the scope of Crypto-Asset Service Providers, we would like to see the definition of Reporting CASP further defined in the rules themselves. It would also be very helpful to include in the commentary a non-exhaustive list of intermediaries and ancillary service providers of the crypto market that should be excluded from

reporting obligations due to the fact that they do not have access to part or all the relevant data. This is the case of infrastructure and hardware providers such as providers of physical wallets. This clarification of the exclusion is also particularly important with regard to Due Diligence obligations, as these providers are not in a position to obtain data from users towards a self-certification and determination of Reportable User status.

Reporting Requirements

1. Do intermediaries maintain valuations on the equivalent Fiat Currency fair market values of Crypto-Assets? Do you see challenges in reporting on the basis of such fair market value? If yes, what do you suggest to address them?

Regarding valuation on transactions in fiat currency, challenges can emerge due to intra-day volatility. Furthermore, some tokens do not trade against a "base" fiat pair (e.g. BTC/ETH), in which cases getting a fair market value in fiat terms becomes difficult and inconsistent across exchanges. Moreover, for illiquid tokens it will be hard to apply valuation reporting rules and report the fair market value. One could use alternative benchmarks such as the last traded price but to apply this consistently and on a large scale will put an excessive operational and administrative burden on the reporting entities. This is another reason why reporting users' deposits and withdrawals from and to an exchange and end of year balances is a more effective and efficient process.

2. Are there preferable alternative approaches to valuing Relevant Transactions in Crypto-Assets?

One could use alternative benchmarks such as the last traded price but to apply this consistently and on a large scale will put operational and administrative burden on the reporting entities. This is another reason why reporting users' deposits and withdrawals from and to an exchange and end of year balances is a more effective and efficient process.

4. Regarding Reportable Retail Payment Transactions, what information would be available to Reporting Crypto-Asset Service Providers pursuant to applicable AML requirements (including the FATF travel rule, which foresees virtual asset service providers collecting information on originators and beneficiaries of transfers in virtual assets) with respect to the customers of merchants in particular where the customer does not have a relationship with a Reporting Crypto-Asset Service Provider, for whom it effectuates Reportable Retail Payment Transactions? Are there any specific challenges associated with collecting and reporting information with respect to Reportable Retail Payment Transactions? What measures could be considered to address such challenges? Would an exclusion of low-value transactions via a de minimis threshold help reducing compliance burdens? If so, what would be an appropriate amount and what measures could be adopted to avoid

circumvention of such threshold by splitting a transaction into different transactions below the threshold?

A key challenge here is differentiating between retail payment transactions, and transactions for other purposes, e.g. investment. Legal certainty and technical standards to do so are not available, for example in the EU.

It might be possible to, therefore, lower the reporting burden which such a requirement would pose by the exclusion of low-value transactions via a threshold, e.g. in line with FATF's USD/EUR 1000 CDD threshold.

Yet, DCGG members challenge the merit to include retail payment transactions in the CARF altogether. Existing transactions monitoring and blockchain analytics technology are better suited to address this transparency requirement.

Other Comments

Impact on Decentralized Finance

Decentralized crypto systems (DeFI) are an important part of the crypto-asset space. We fear that not addressing it properly in the proposed framework may lead to significant difficulties in application and enforcement. By its very nature, the crypto market trends towards decentralization.

Simply regarding DeFi as a loophole to transparency in crypto-asset market, and attention to close this loophole with tools available to traditional finance would require exchanges to keep full track of all transactions prior to a deposit in a local wallet. It would be the crypto equivalent of a bank requiring a customer to keep receipts of how and when a specific bank note was acquired, and all receipts associated with all prior transactions the note was involved in. The cost of processing of information would notably overburdening the resources of crypto-assets services providers. It is also doubtful that these efforts can be effective.

If regulators substantially increase the reporting requirements faced by centralized, regulated services, such as established exchanges, and force them to implement increasingly complex onboarding processes, many users will simply turn away from these services to decentralized options, such as non-custodial services and peer-to-peer transactions.

This would penalize the majority of compliant users and create a false impression of safety, while keeping problematic transactions under the radar.

We would like to see further assessment of the role of DeFi and a reconsideration of reporting obligations imposed on centralised systems to ensure a proportionate and comprehensive approach. Hence, we support the creation of a framework that would instead incentivise the flow of users toward complying and centralised entities, where the level of monitoring and reporting of crypto-asset transactions is unparalleled.

Conclusion

The crypto-asset industry holds an enormous potential for economic progress and innovation. Placing a disproportionate compliance burden on it would jeopardize that potential, by failing to consider the nascent state of the industry and the difference in resources from the traditional financial industry. The amount and nature of transactions and the way the data is processed make it particularly burdensome for the industry.

The risk of imposing burdensome requirements on a fast-paced, digital-native industry is that these can be quickly circumvented. We can learn from geographies where restricting the ways in which crypto-assets can be used has only resulted in users turning to third-party exchanges, OTC trading and P2P transactions. Instead of being able to better control crypto transactions, the result is governments losing oversight of who uses crypto-assets and for what purposes.

We call on OECD Members to take this impact into consideration by limiting the reporting requirements to a more robust and attainable range and further calibrating the definitions and exclusions contained in the rules.