GLOBAL
DIGITAL
FINANCE

July 29, 2019

VIA EMAIL:
consultation-02-2019@iosco.org

International Organization of Securities Commissions (IOSCO)
Calle Oquendo 12
28006 Madrid
Spain

Re:
Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms

Dear IOSCO Team,

Global Digital Finance (GDF) support efforts by global standard setters, national authorities and regulators to consult and work with the nascent global virtual asset industry. To that end, we are hereby providing input to the Consultation Paper (CP) regarding Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (CTPs).[1]

This response has been drafted and led by the GDF Advisory Council.[2] Please do not hesitate to contact our Executive Director, Teana Baker-Taylor (Teana@gdf.io) for further questions or comments. We would also like to hereby express that GDF members are open to present on any of the topics set out herein should IOSCO deem such to be useful. Our members include CTPs as well as data aggregators, AML and trade surveillance providers, custodians, legal advisors, auditors and other relevant parties to this response.[3]

About GDF

GDF is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets and digital finance technologies through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members—including some of the most influential digital asset and token companies, academics and professional services firms supporting the industry.

[1] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf
[2] https://www.gdf.io/people/
[3] https://www.gdf.io/members-directory/

GDF is proud to include Circle, ConsenSys, DLA Piper, Diginex, Hogan Lovells, Huobi and R3 as patron members.

The GDF Code of Conduct is an industry-led initiative driving the creation of global best practices and sound governance policies, informed by close conversations with regulators and developed through open, inclusive working groups of industry participants, legal, regulatory and compliance experts, financial services incumbents and academia. Code principles undergo multiple stages of community peer review and open public consultation prior to ratification.

To date, the following Code Principles have been ratified:[4]

- Part I - Overarching Code of Conduct
- Part II - Principles for Token Sales & Token Sale Service Providers
- Part III - Principles for Token Trading Platforms
- Part IV - Principles for Cryptoasset Funds & Fund Managers
- Part V - Principles for Token Comparison & Rating Websites

The following Code Principles are in the open public consultation phase:

- Part VI - Principles for Stablecoins & Stablecoin Issuers[5]
- Part VII – Principles for Security Token Offerings & Secondary Market Trading Platforms[6]
- Part VIII -Principles for Know Your Customer (KYC) & Anti-Money Laundering (AML)[7]

Several IOSCO members, including the ADGM, ASIC, AMF, ESMA, DFSA, FCA, MAS and SFC have been observers or active participants in prior GDF summits, where Code Principles were presented and pursuant to which they were finalised.

Consultation Inputs

Per the CP, the key considerations relate to:

- Access to CTPs;
- Safeguarding participant assets;
- Conflicts of interest;
- Operations of CTPs;
- Market integrity;
- Price discovery; and
- Technology.

[4] https://www.gdf.io/gdfcode/
[5] https://www.gdf.io/docsconsultations/part-vi-code-of-conduct-principles-for-stablecoin-issuers/
[6] https://www.gdf.io/docsconsultations/part-vii-code-of-conduct-principles-for-security-token-offerings-secondary-market-trading-platforms/
[7] https://www.gdf.io/docsconsultations/part-viii-code-of-conduct-principles-for-know-your-customer-kyc-anti-money-laundering-aml/

The CP cites the following initial questions that may aid this analysis and inform decisions related to appropriate regulatory approaches.

- Who can access the CTP?
- How does the trading system operate, and what are the rules of that system?
- Which crypto-assets are eligible for trading?
- How are crypto-assets priced on the CTP?
- What degree of transparency of trading is provided?
- How does the CTP seek to prevent market abuse?
- What clearance and settlement processes exist?
- How are participant assets held?
- What possible conflicts of interest exist?
- What cyber security and system resiliency controls are in place?

The CP notes that each of these questions relate to key issues and risks that may impact investors and fair, efficient and transparent markets.

1. Access to Crypto-Asset Trading Platforms

Access Criteria

The CP notes that access criteria differ between CTPs. Some restrict trading access to regulated intermediaries, others provide non-intermediated access to institutions and some CTPs provide non-intermediated access to retail investors. The latter approach is novel to CTPs as Trading Venues that provide non-intermediated access rarely provide such access to retail investors.

Participant Onboarding

The CP notes that where investors, particularly retail investors, have non-intermediated access to a CTP, an important consideration for regulatory authorities is who is performing the onboarding process. In some CTP models, the CTP may perform the on-boarding functions that would otherwise be performed by an intermediary. Where the on-boarding processes used by CTPs are limited or opaque, there may be a risk of the platform being used for illegal activities. This risk may be enhanced, for example, where the technology provides the ability to: (1) transfer funds anonymously between parties, and (2) mask the origin or destination of the flow of funds. In addition, there may be regulatory arbitrage if investors are permitted to access a CTP from jurisdictions where such activities are prohibited. Further, a consideration of whether CTPs are providing risk disclosures to investors that set out the risks of trading the types of products that may be available on a CTP are also important.

Toolkit

The CP proposes that if a regulatory authority is considering the issues and risks relating to participant access to CTPs and the on-boarding process, an assessment may include:

- A review of the CTPs' policies and procedures regarding access criteria;
- Consideration of allowing only intermediated access to CTPs;
- A review of the assessments made by CTPs of their participants for "appropriateness" from the perspective of:
    - KYC,
    - AML/CFT, and
    - Product suitability; and
    - Consideration of whether CTPs should provide risk disclosure, and, if so, assessing the adequacy of such disclosure.

GDF Comments

Over the past year GDF has extensively engaged with FATF,[8] including multiple responses to their Interpretative Note, by presenting at the FATF Private Sector Consultative Forum in Vienna in May 2019, and more recently by moderating key sessions at the V20 in Osaka in June 2019, where FATF was in attendance.

In the **April 7, 2019 submission to FATF responding to FATF's February 22, 2019 statement,** we expressed that Virtual Asset Service Providers (VASPs) operating in jurisdictions that have made statements about future AML/CFT policy direction, or that have already issued guidelines or legislation bringing such VASPs in the remit of AML/CFT regulation, are more likely to have started implementing normal course AML/CFT measures, including:

1. Risk assessments (R1)
2. Sanctions screening for customers and payments and reporting of sanctions breaches (R6 and R7)
3. Customer Due Diligence (R10)
    a. KYC
    b. EDD
    c. Surveillance and transaction monitoring - both fiat/crypto and crypto/crypto[9]
4. Record-Keeping (R11)
5. PEP name screening (R12)
6. Reliance on third parties, particularly with regards to CDD (R17)
7. AML staff training (R18)
8. SAR/STR reporting to local FIUs and law enforcement (R20).

We also noted that FATF's position set out in provision 7(a) of the February 22, 2019 FATF Statement that "with respect to preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs" will further accelerate this evolution.[10]

[8] All prior GDF submissions to regulatory CPs can be found on https://www.gdf.io/resources/ .
[9] As noted in our prior submissions to FATF which can be found on https://www.gdf.io/resources/ , the crypto asset industry has seen the emergence of specialised surveillance tools focussed on tracking the movement of assets through the crypto asset addresses.
[10] https://www.gdf.io/wp-content/uploads/2018/01/GDF-Input-to-the-FATF-public-statement-of-22-Feb-2019-FINAL.pdf

Since, on June 21, 2019, FATF issued its **final guidance mandating that Recommendations 10 to 21 be applied to VASPs by FATF member states.** Implementation of the FATF guidance by FATF member states will address many of the concerns set out by IOSCO in this section.

Like FATF we believe that VASPs are able to apply robust AML/ CFT measures. Accordingly, we do not subscribe to the view implied in the IOSCO toolkit above that only intermediaries can fulfill this function and not CTPs. Quite to the contrary, we believe that **the emergence of retail CTPs has been a major catalyst in the emergence and improvement of non-face-to-face onboarding technologies**, some of which are now superior to the human eye and, therefore, are starting to be adopted by mainstream banks and other licensed institutions. Without Fintechs' including CTPs, this evolution might not have occurred or might most certainly have occurred slower.

We also would like to reiterate a concern about **regulatory arbitrage** while member states adopt different timelines for implementing the FATF guidance. We elaborate on this concern under **9 below.**

2. Safeguarding Participant Assets

The CP notes that where a CTP holds participant assets, a key consideration for regulatory authorities is how such assets are held and safeguarded. This includes consideration of what arrangements are in place in the event of a loss, including a loss due to theft from, or the bankruptcy of, the CTP. Asset custody functions are not usually performed by Trading Venues but rather by intermediaries, custodians, transfer agents and clearing houses. As a result, the performance of these functions directly by CTPs raises new issues and potential risks for regulatory authorities to consider.

The CP adds that where the CTP offers custody, the risks that could arise include:

- Operational failure – the system may be compromised such that participant assets are lost or inaccessible (e.g., due to a cyber-attack).
- Theft, loss or inaccessibility of private keys - private keys are compromised (e.g., due to a cyber-attack or breach, or by an action of a CTP insider), lost or not accessible resulting in stolen or inaccessible assets.
- Co-mingling of assets – the assets of the CTP may be co-mingled with those of participants and/or participant assets may be pooled, thus in the event of a default, investor assets may not be fully protected.
- Inaccurate record-keeping - the CTP may not accurately reconcile records or properly account for assets.
- Insufficient assets to meet liabilities – the CTP may not maintain sufficient assets to cover participants' claims (i.e., the CTP is not able to meet withdrawal demands).

Toolkit

The CP proposes that if a regulatory authority is considering the issues and risks associated with the safeguarding of participant assets, an assessment may include:

- A review of the adequacy of the arrangements by a CTP that:
    - discloses participant ownership rights;
    - secures participant assets in a manner that protects them from theft or loss, including appropriate backup arrangements regarding access to the private keys of CTP wallets;
    - segregates participant assets (from CTP operator assets and/or other participant assets); and
    - maintains accurate and reliable records that are sufficient to confirm participant positions;
- Where the CTP uses a third party for custody of participant assets, the adequacy of measures taken by the CTP relating to the security of the assets held at the third party;
- A review of the arrangements in place to compensate participants in the event of a loss of assets, including, for example, insurance policies, compensation funds or other contingency measures;
- An examination of the methods of retrieval of participant assets held outside of the regulatory authorities' geographical jurisdiction; and
- A consideration of the adequacy of disclosure made by the CTP to its participants in regard to the above.
- Consideration of the imposition of:
    - capital requirements on CTPs that reflect the nature of the business of the CTPs, including where the CTPs perform intermediary functions;
    - ongoing monitoring of capital positions; and
    - performance of an independent audit of the CTP's financial position.

GDF Comments

GDF subscribes to the concerns expressed above and would point out that the **reliability of the books and records and the tracking of the assets is key.**

We would note that one of **the Big 4[11] and other auditors like Grant Thornton[12] have started auditing CTPs** and accordingly suggest that IOSCO may seek their observations in terms of nascent best practices in this regard.

Capital

As a number of CTP's begin to develop new advanced offerings, such as margin trading and or futures trading, GDF believes that **CTP's offering these sophisticated products should have a capital adequacy plan in place**, as in effect the CTP is lending (margin trading) and taking deposits (collateral taking). The amounts of leverage allowed varies across CTPs and therefore each CTP should adjust their risk management accordingly.

[11] https://www.coindesk.com/pwc-unveils-new-tool-for-auditing-crypto-transactions
[12] https://www.ledgerinsights.com/grant-thornton-cryptocurrency-audit/

If the CFT only offers a spot market place, then the CTPs capital strategy would only need be a simple model where the CTP holds full reserves. The CTP should also clearly state that it does not participate in any rehypothecation of clients assets.

We note that in most cases where lending is offered, automatic liquidation occurs at a collateralization ratio greater than 1, in most cases this is 1.5 times, with the collateral held immediately sold at the market price, thus mitigating the CTP's risk exposure, as the loan is immediately repaid by the disposal of the clients collateral. However, the CTP could be exposed to such risks as low liquidity (cannot immediately sell), large price decrease thus the collateral does not fully cover the loan (e.g. a large liquidation will force the price down further exacerbating the problem, especially in immature markets with shallow liquidly pools). Also, the technology solutions need to be sound, paired with robust operational standards around development, testing, implementation and monitoring.

We observe that in the absence of consistent global regulatory treatment, a number of industry participants have developed novel capital strategies. For example, the CTP Binance allocates 10% of trading revenues (from July 2018), to an insurance fund called "Secure Asset Fund for Users" (SAFU)[13]. The SAFU was more than capable of covering the $40 million stolen from Binance[14] in May 2019. Although Binance's financials are not public, CNBC reported a profit on $446 million in 2018,[15] therefore we can assume revenues are a factor of 10-30 greater than this amount. CTP Kraken operates a "proof of reserve" service to their clients.[16] This technical solution allows the client to independently check that the assets held in Krakens client account, match that of their records, at any time.

Insurance

We would also add to the above toolkit the importance of insurance cover. That said, we would pair this observation with the fact that there are some difficulties obtaining material insurance coverages as the global insurance market for crypto assets is limited in capacity and maturity. Large insurance companies are reluctant to price the risk, due to the small size of the overall market. In addition, to the limited capacity in the global insurance market, costs are quite high vis-a-vis like coverages for traditional assets.[17]

Regulatory coordination across IOSCO and the IAIS could be beneficial in this regard.

[13] https://www.binance.vision/glossary/secure-asset-fund-for-users
[14] https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin
[15] https://www.cnbc.com/2019/02/14/crypto-exchange-binance-profitable-despite-bear-market-cfo-says.html
[16] https://www.kraken.com/en-gb/proof-of-reserves-audit
[17] Some of our smaller members inform us that the challenges involved are largely that each individual custody provider's balance sheet size is too small. Therefore, one solution could be for a mechanism whereby smaller firms can group together to form, a type of syndicated pool that is more attractive to an insurer.

3. Conflicts of Interest

The CP notes that both Trading Venues and CTPs may have conflicts that arise from the commercial interests of the platform or venue, its owners and operators, the businesses that raise capital on the platform or venue, and the participants who trade on the platform or venue. Those CTPs that position themselves to provide end-to-end services including, for example, the admittance and trading of the crypto-asset, settlement, custody, market making and advisory services may have additional conflicts. Traditionally, these roles have been performed by independent parties. When CTPs provide such end-to-end services, any conflicts of interest that arise need to be mitigated to prevent potential market conduct and/or investor protection concerns.

Examples of potential conflicts can include:

- Proprietary trading and/or market making on the CTP by CTP operators, employees or affiliates - conflicts could include information asymmetry, market abuse and/or unfair pricing provided to participants.
- Providing advice to customers – this may be an inherent conflict where the CTP has a direct or indirect interest in a crypto-asset traded on the CTP, or its issuance.
- Preferential treatment – conflicts arise where preferential treatment is given to a subset of participants or to the owners/operators of the CTP, including system design and programming that determines how orders interact and execute.

Toolkit

The CP proposes that if a regulatory authority is considering issues and risks relating to conflicts of interest, an assessment may include:

- An evaluation of the policies and procedures of a CTP that are established to mitigate and manage the conflicts of interest of various stakeholders, including a review of:
    - the disclosure of all relevant details, including where a CTP or related parties, or the operator, employees, officers and/or directors of the CTP or its related parties, may have any financial interest in the crypto-assets traded on that CTP; and
    - policies and procedures regarding access to and the confidentiality of information about participants on the CTP, or other information that should be treated as confidential;
- Where a CTP or related parties, or the operator, employees, officers and/or directors of the CTP or its related parties, are permitted to engage in proprietary trading and/or market making on the platform, a review of:
    - the disclosure of relevant trading activities;
    - the separation of market making activities from trading activities or services provided to participants;

    - the transparency of policies and procedures that address, among other things, participant priority, the fair pricing of trades with participants and/or favorable execution of trades with participants; and
    - disclosure relating to whether an issuer of a crypto-asset or related party is a participant on the platform; and
- A review of the disclosure of steps taken to mitigate and manage any conflicts of interest.

GDF Comments

GDF subscribes to IOSCO's concern that conflicts of interest have been a significant issue. As noted in our prior **response to the Joint Canadian consultation**[18], CTPs should disclose if they are trading as principal, or if there are formal market maker agreements. In the absence of **disclosure of market making, proprietary and affiliated activity, or CTP surveillance and controls over the activity of conflicted parties** (such as a highly concentrated number of accounts, including those controlled by the ICO issuers themselves), it is hard to form an accurate understanding of volumes and prices.

This topic is also closely related to what is set out under **4. Description of CTP Operations, 5. Market Integrity** and **6. Price Discovery** below. We accordingly refer IOSCO to the comments we set out under these sections.

4. Description of CTP Operations

The CP notes that the order execution rules, as well as any cancellation procedures, should be disclosed to the regulator and to market participants, and should be applied fairly to all participants. The exchange or trading system's order routing procedures should also be clearly disclosed to the regulator and to market participants, applied fairly, and should not be inconsistent with relevant securities regulation (e.g., client precedence or prohibition of front running or trading ahead of customers).

Given that many CTPs support non-intermediated access, the extent to which information about CTP operations, including rules, policies and procedures that facilitate fair and orderly trading and investor protection is available and transparent, is an important consideration. The use of DLT may limit the ability to cancel or modify trades once verified on the ledger. Therefore, how CTPs handle error trades and cancellations and modifications are also important considerations.

Further, the technology underlying crypto-assets may raise some novel and unique issues, such as in relation to hard forks, airdrops and other asset issuances, which may

[18] https://www.gdf.io/wp-content/uploads/2019/05/IIROC-April-24-2019.pdf

present operational challenges for CTPs and their participants. Specifically, hard forks make previous versions of the protocol invalid and may create entirely new assets. Issues may arise when there is a lack of clarity about how forked crypto-assets are managed by the CTP. Where a CTP holds custody of a participant asset that can be forked, depending on the operational approach of the CTP, the participant may not have access to any new asset that results from the hard fork.

Toolkit

The CP proposes that if a regulatory authority is considering the issues and risks relating to the transparency of CTP operations to participants, an assessment may include a review of the disclosure related to:

- Order types and interaction;
- Price discovery and transparency of orders and trades on the CTP, including trading volumes and turnover;
- Fees charged by the CTP;
- Rules relating to the prevention of market abuse;
- The technology used by the CTP;
- Policies and procedures relating to error trades, cancellations, modifications and dispute resolution;
- The treatment of assets where the distributed ledger has undergone a hard fork, or other irreversible changes to the distributed ledger protocol that makes previously valid ledgers or transactions invalid;
- The treatment of airdrops, corporate actions or other comparable events; and
- Information about the crypto-assets that the CTP offers for trading, including:
    - initial and on-going criteria for selection;
    - the principals or issuing developers behind the crypto-assets;
    - the type and details of the DLT and/or protocol used;
    - any hacking vulnerabilities of the technology underlying the crypto-assets; and
    - the traceability of the crypto-assets.

GDF Comments

GDF subscribes to IOSCO's concerns about transparency of CTP operations, especially in the case of unregulated CTPs where there is **continued occurrence of large volumes of fake and wash trading.** Not infrequently new CTPs appear on coin market tracking websites and in a matter of days top volumes of the more established CTPs. This can only be explained through fake and wash trading.[19]

Further, as a result of the nascent nature of the market, notwithstanding best efforts by some to show "adjusted volumes", different websites show different trading volumes.[20]

[19] https://www.coindesk.com/for-15k-hell-fake-your-exchange-volume-youll-get-on-coinmarketcap
[20] https://coinmarketcap.com/rankings/exchanges/; https://coinmarketcap.com/rankings/exchanges/reported/; https://www.bti.live/exchanges/; https://www.cryptocompare.com/exchanges/#/overview

IOSCO may find the contents of the recent **Bitwise submission** to the SEC interesting in this regard[21] and well as **the efforts of the Blockchain Transparency Institute**, which amongst other efforts shows **"BTI Verified" CTPs".**[22]

5. Market Integrity

The CP notes that Effective monitoring of trading on CTPs may be challenging. The methods for the transfer of beneficial ownership on CTPs often differ from those on Trading Venues. Therefore, rules relating to manipulation or insider trading, and how to enforce such rules, may need to be assessed as new forms of manipulation may occur. Existing supervisory tools may also need to be considered to account for unique issues relating to crypto-assets, such as the high price volatility of crypto-assets relative to traditional financial assets, the possibility of trading 24 hours a day and the lack of consistent and stable sources of crypto-asset pricing to support market surveillance systems and activities.

Toolkit

The CP proposes that if a regulatory authority is considering issues relating to market integrity, an assessment may include a review of:

- Traditional market integrity rules with a view to their applicability to crypto-asset trading;
- The rules, policies or procedures in place to govern trading on the market;
- Mechanisms for monitoring the rules, policies or procedures;
- The trading hours of the CTP and how they may impact the CTP's ability to effectively monitor trading;
- The management of any information asymmetries; and
- The availability of updated information regarding factors that may impact the asset, the value of the asset, its developer or the technology used.

GDF Comments

GDF agrees that market integrity has been a significant issue and, accordingly, has recently launched a new working group with a view towards better understanding market practices in regards to improving market integrity, including available technology.

As also noted in the **prior response to the Joint Canadian consultation**[23], at current the regulated CTPs are engaging similar **market integrity surveillance** solutions and vendors to those used in traditional asset classes, as these vendors have extended their solutions to apply the market misconduct rule set to crypto assets.[24]

[21] https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf
[22] https://www.bti.live/exchanges/
[23] https://www.gdf.io/wp-content/uploads/2019/05/IIROC-April-24-2019.pdf
[24] See here relevant news: https://www.apnews.com/99e1f16676704fc28ca39867be8b7f1a ; https://business.nasdaq.com/mediacenter/pressreleases/1728735/gemini-to-launch-market-surveillance-technology-in-collaboration-with-nasdaq

6. Price Discovery

The CP notes that due to the early stage of development of the crypto-asset market, it may be premature to determine the appropriate level of transparency at this point in time. Accordingly, the level of transparency is an important issue to monitor.

Toolkit

The CP proposes that if a regulatory authority is considering issues and risks relating to price discovery, an assessment may include consideration of:

- Whether and what pre- and/or post-trade information is made available to participants and/or the public and, on what basis;
- The overall potential impact of pre- and post-trade transparency on order execution quality for participants and market quality generally;
- The market microstructure of the CTP (e.g., continuous auction, call market, reference price model); and
- The crypto-assets traded, including the liquidity of the crypto-assets and their characteristics.

GDF Comments

As noted under **3. Conflicts of Interest** above, in the absence of disclosure of market making, proprietary and affiliated activity, or CTP surveillance and controls over the activity of conflicted parties (such as a highly concentrated number of accounts, including those controlled by the ICO issuers themselves), it is hard to form an accurate understanding of volumes and prices.[25]

7. Technology

The CP notes that in order to provide an appropriate level of stability, regulatory authorities should require trading venues to have in place mechanisms to help ensure the resiliency, reliability and integrity (including security) of critical systems. While the prevention of failures is important, trading venues should also be required to be prepared for dealing with such failures and, in this context, establish, maintain and implement as appropriate a Business Continuity Plan.

Toolkit

The CP proposes that if a regulatory authority is considering issues and risks relating to system resiliency, integrity and reliability, an assessment may include a review of:

- The CTP's business continuity/disaster recovery plans to ensure continuity of services;

[25] Brave New Coin has a few indices that are supported by NASDAQ that may be useful in the price discovery process. https://bravenewcoin.com/enterprise-solutions/indices-program/blx

- Where appropriate, stress testing and/or capacity planning processes and results;
- Quality assurance procedures and performance monitoring of any critical systems that are provided or developed by third-parties (whether or not outsourcing agreements are in place);
- Governance and change management procedures;
- Independent systems reviews to assure that relevant technology standards are met and maintained as intended;
- Policies and procedures that support an appropriate governance structure that identifies key systems or assets that could be at risk;
- Physical or organizational measures to control and protect against cyber risks (e.g., vulnerability testing, penetration testing);
- Measures to detect cyber anomalies;
- Policies related to incident response; and • Business continuity plans and/or disaster recovery plans

GDF Comments

We would draw attention in this regard to our **prior paper on safekeeping of crypto assets,** which includes **security and operational considerations.**[26]

8. Clearing and Settlement

The CP notes that with respect to clearing, some CTPs may maintain and update the account balances of participants on that CTP. While a separate party, like an intermediary, may assume this role for traditional securities, some CTPs may integrate these services into its operations. In such cases, efficient and accurate internal accounting systems are important for CTPs, especially where they provide non-intermediated access and allow for automated participant withdrawals. If accounting systems are inaccurate or compromised, withdrawals might be made by without ownership of the assets.

Similarly, it is important to understand how transactions that occur on CTPs are settled. Due to the underlying technology and trading models of CTPs, it may be unclear whether traditional settlement mechanisms are necessary or utilized to effect transfers of crypto-asset ownership. For example, how settlement finality is reached when recording transactions in a distributed ledger is important and may vary. In addition, it is currently unclear whether there is a common understanding or agreement of when legal transfer of ownership occurs when crypto-assets are trading on CTPs.

GDF Comments

Settlement finality in DLT is still an evolving field, with several protocols seeking to adopt different consensus mechanisms in order to reduce the risk of 51% attacks.[27]

[26] https://www.gdf.io/wp-content/uploads/2019/02/GDF-Crypto-Asset-Safekeeping_20-April-2019.pdf
[27] Examples include Hedera Hashgraph https://www.hedera.com/ and Algorand https://www.algorand.com/.

Further, the probability of risk of settlement failure can be reduced through **waiting for n confirmations.** n depends on the crypto asset/ differs by blockchain and the conditions of the network. Well-governed CTPs implement policies to this effect and wait for a preset number of confirmations that varies per blockchain and gets adjusted based on conditions of the network before e.g. crediting the assets to the customer.

9. Cross-border Information Sharing

We take note of IOSCO's ability to collaborate cross-border. We would reiterate the importance of this as noted in our **prior submission to the Her Majesty's Treasury in the UK**.[28] Unlike brick-and-mortar based business models, such as those common in traditional finance and which can be more easily supervised and enforced against within the jurisdiction(s) they are physically located in, technology services, including but not limited to cryptoasset services, can be offered from any location. Lack of regulatory clarity and consistency as is currently prevalent in the case of cryptoassets, leads to various outcomes:

- Cryptoasset providers who want to comply with clear standards seek out jurisdictions where a license can be obtained and/ or where the regulatory regime has been adjusted to address the unique characteristics of cryptoassets, particularly jurisdictions that created new legislative regimes to attract such businesses and that are willing to take the risk to learn with them as they evolve;
- Cryptoasset providers that have no intention to apply higher standards of regulation unless and until regulatory consistency exists, will instead choose to operate from less regulated jurisdictions. In other words, regulatory discrepancy creates room for regulatory arbitrage, sometimes justified - e.g. if a jurisdiction is ostensibly advanced on understanding a new trend and adjusting its regulatory regime for it - and sometimes unjustified - e.g. if the key motive is to locate in the weakest link jurisdiction in order to enable untoward activity.

It should also be noted that as was the case for many other novel technology related business models (e.g. Amazon, Uber, AirBnB, WeChatPay, Alipay, etc), different jurisdictions have different standing rulebooks that may depending on the regulatory and political backdrop in that jurisdiction be easier or harder to reinterpret, change or adjust. Technology businesses being global or at least multi-jurisdictional (the latter is needed to scale), will typically choose to expand in markets where they feel they can make progress fastest, and will leave jurisdictions where they cannot.

This dynamic is playing out in the cryptoasset sector given regulatory discrepancy, including in the AML/ KYC/ CFT space - e.g. many jurisdictions have not yet applied standing AML ordinances, laws and regulations to cryptoassets, while others have. Platforms who locate in the former and who have not applied robust AML/ KYC/ CFT

[28] https://www.gdf.io/wp-content/uploads/2019/06/HM-Treasury-AMLD5-Consultation-Response_Final.pdf

standards have a revenue advantage over those in the latter. Regulatory discrepancy that continues for several years can be a lifetime for technology related businesses.

In sum, as the IOSCO CP exemplifies, it is important for regulators to be internationally coordinated, specifically on the policy-setting level and, where abuse is apparent, on the enforcement level.

We hope you may find our response helpful.