asifma

Growing Asia's Markets

ASIFMA Best Practices for Digital Asset Exchanges

June 2018

Disclaimer

The information and opinion commentary in this ASIFMA Best Practices for Digital Asset Exchanges ('Paper') was prepared by the Asia Securities Industry and Financial Markets Association (ASIFMA) to reflect the views of our members. ASIFMA believes that the information in the Paper, which has been obtained from multiple sources believed to be reliable, is reliable as of the date of publication. As estimates by individual sources may differ from one another, estimates for similar types of data could vary within the Paper. In no event, however, does ASIFMA make any representation as to the accuracy or completeness of such information. ASIFMA has no obligation to update, modify or amend the information in this Paper or to otherwise notify readers if any information in the Paper becomes outdated or inaccurate. ASIFMA will make every effort to include updated information as it becomes available and in subsequent Papers.

ASIFMA is an independent, regional trade association with over 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the US and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

Table of Contents

I. Introduction

1. Setting the scene

In 2008, an individual under the pseudonym Satoshi Nakamoto released a document called "Bitcoin: A Peer-to-Peer Electronic Cash System" which defined a decentralized system for exchanging value that is today referred to as 'Bitcoin'.

Bitcoin was not the first attempt at creating a virtual currency, but it was one of the early few to gain momentum and backing. Prior to Bitcoin, most previous attempts at creating virtual currencies relied on a central authority keeping a record of transactions to determine if one party still owned the money or had previously spent it. The central authority would confirm that the payer actually had the amount that they wanted to spend, which prevented one of the key issues namely, 'double-spending'.

Bitcoin differs from its predecessors in that it has no central authority governing the issuance or amount of the currency available. Instead, every single transaction is recorded digitally in a code format. This coded transaction is added to a 'block'. Every Bitcoin transaction block records who sent it, who received it etc. and is publicly viewable on an electronic, decentralized, distributed and public ledger– think about this like a long piece of paper that many people have a copy of, which shows every Bitcoin transaction and who sent it and received it. This ledger is known as the blockchain, with values represented by 'tokens' that are recorded in transactions on the Bitcoin blockchain.

Over the past decade, literally thousands of other cryptocurrencies have been launched hot on the heels of Bitcoin. Examples include Litecoin, Ethereum and Ripple. These altcoins vary in popularity, price, levels of anonymity and technical details.

Initially, Bitcoins were traded through enthusiasts bilaterally where Bitcoins were exchanged for fiat currency. Since then, numerous exchanges have been launched and now trade many of the thousands of cryptocurrencies that have been launched. The significant growth of cryptographic coins and tokens ('digital assets')[1] has brought with it a flourishing ecosystem of products and services, including systems that facilitate trading.

'Exchange' platforms can take a number of forms, including:

- centralized and decentralized systems;
- automated and/or brokerage models;
- peer-to-peer / swap technology platforms;
- bulletin board-type communication portals; and
- fiat / non-fiat gateways.

Each platform carries its own infrastructure, products / services, regulatory status, jurisdictional reach, risk profile and opportunities. A vast number of other applications and technology layers are also available or under development, either as standalone services or as a value-add.

[1] 'Digital assets' is used as a general term in this document to describe various tradeable assets based on blockchain / distributed ledger technology (or similar). It is not intended as a technical term.

This document focuses on **centralized digital asset exchanges**, although a number of principles can be applied more broadly.

Digital asset exchanges can act as the vehicle for a number of potential digital asset distributions and trades, including the following:

- ***Primary sales*** – The digital asset exchange acts as the gateway for the first issuance of an asset by the issuer to a purchaser, after which the asset may be traded again on that exchange or via other means.
- ***Secondary sales*** – The digital asset exchange facilitates trading of assets already previously issued.
- ***Air drops*** – The digital asset exchange allocates assets to users without payment, as part of incentive and/or community building initiatives.
- ***Earn drops / payments*** – The digital asset exchange allocates assets to users in exchange for a task, such as updating know-your-customer ('**KYC**') information, providing input on interface design etc.

Some, all or none of these may be under arrangements with issuers. A variety of other models also exist in different markets.[2]

The digital asset exchanges often wear multiple 'hats' as they serve as marketplaces, brokers, custodians and even proprietary holders of assets. This leads to the inherent risk of conflict of interest. This risk can also be exacerbated by individual conflicts of interest at the Board, Advisory Board and other governance levels. This risk must be addressed strategically and comprehensively, through appropriate segregation of functions, information barriers, data flow controls and appropriate selection criteria and procedures for officers, advisors and staff.

Overall, digital asset exchanges provide a valuable service to the market, by facilitating price discovery, liquidity and efficient trading. Despite the growth, there has been trouble in paradise. Some of the bigger exchanges in the region have suffered hacks resulting in hundreds of millions of dollars' worth of Bitcoin stolen from these exchanges. In addition, in many cases, there is a lack of due diligence and independent insight on many of the industry's new token sales[3] that have led to failures caused by fraud, manipulation and mismanagement. According to Fortune, "Nearly Half of 2017's Cryptocurrency 'ICO' Projects Have Already Died" or are believed to be outright scams (the OneCoin token sale in 2017 was nothing more than a Ponzi scheme that saw investors lose around USD350 million).

Customers that pose higher money laundering/terrorism financing ('**ML/TF**') risks present increased exposure and risk for banks. According to media reports, many banks have closed down the accounts of several digital asset exchanges. This is likely due to the uncertain regulatory frameworks applicable to digital asset exchanges in many countries and the risks associated with banking digital asset exchanges which require enhanced due diligence measures to be applied. The Reserve Bank of in India in April 2018 banned banks and other regulated entities from servicing businesses dealing in cryptocurrencies.

[2] A very brief high-level overview of token sales is also included in the Annex.

[3] The term 'token sale' is used generically to refer to the sale of digital assets by an issuer. These are sometimes also called 'initial coin offerings', 'ICOs', 'token generation events' and various other names depending on their nature and market practice.

As the industry becomes more mainstream, preventing systemic risk and ensuring investor protection are critical. This is especially important now considering the amount of money tied up in cryptocurrency and the relative immaturity of the industry. Infrastructure is crucial for the continued stable growth of the industry.

2. About these best practices

These best practices have been developed by ASIFMA and its members in consultation with various market participants, including professional advisors, technical experts and exchanges. Aimed at the digital asset exchanges and industry practitioners, the goal of these best practices is to guide the digital asset exchanges towards international best practices and highlight points for consideration in several key areas.

This document is structured as follows:

I. Introduction
II. Listing process
III. Market manipulation, pricing and liquidity
IV. Regulatory considerations: licensing and authorization
V. AML/CTF and KYC issues
VI. Custody
VII. Cybersecurity
VIII. Risk mapping
IX. Engagement with external stakeholders

These best practices are by no means exhaustive, and best practice continues to evolve. They are not law, nor have they been endorsed by any regulatory authority. As a jurisdiction-neutral document, it is subject to local legal and regulatory requirements. Any references to third parties or specific initiatives are for reference only and not an endorsement of any kind.

Professional advice should always be obtained. As a rapidly evolving area of technology, law and regulation, extreme care is required to ensure that controls remain up-to-date and relevant.

3. The path ahead

Transnational bodies and regulators around the world are still coming to grips with what 'effective' regulation of the digital asset sector entails. The G20, International Organisation of Securities Commissions, International Monetary Authority, Bank for International Settlements, Financial Action Task Force ('**FATF**'), local authorities and many others are maintaining a watching brief on the sector.

Certain jurisdictions already regulate digital asset exchanges, with more undoubtedly to follow. This must strike the right balance between innovation and risk mitigation, and sensitively navigate the differentiated nature of individual assets and platforms.

Beyond sensible regulation, there is a need for the large market 'infrastructure' that we would see in more traditional markets. This includes systems related to custody, screening and operational risk control. In addition, market data aggregation systems and controls are required to address whether

reported exchange figures are reliable. There remain very few 'institutional-ready' market data feeds in the market.

Finally, information asymmetry must be addressed. The increasing myriad of digital assets has made it difficult for any purchaser, institutional or otherwise to be able to keep up with and assess the relative merits, risks and value of the thousands of different digital assets in the market. This relies on:

- proper disclosure;
- data misuse controls, to prevent insider dealing;
- independent research reports; and
- ideally, independent rating agencies. Holders of cryptocurrencies have no rights as it relates to corporate governance or the underlying equity of the issuing company and independent assessment agencies might help to enforce good practices and transparency.

Further best practices and standards will evolve and ASIFMA looks forward to contributing to the dialogue on this important part of the digital economy.

II. Best practices for the listing process

Market practice on the listing of tokens currently varies amongst digital asset exchanges. For example, a number of exchanges do not make their token listing process publicly available. Where exchanges do make their token listing process publicly available, the information available and listing requirements often vary. Some exchanges state that they do not have a definitive set of criteria for listing tokens, while others have more detailed listing frameworks.

Although market practice currently varies, the following are examples of best practices:[4]

- **Listing process framework** - An exchange should make its listing process publicly available.

- **Application form** - Exchanges should obtain information from the applicant to help it determine whether the token should be listed.

- **Listing requirements and considerations** - While it is the exchange's commercial decision in listing a token, we consider it best practice for the exchange to set out any minimum listing requirements it has. In addition, there are merits for an exchange to set out the factors it will take into account in coming to a listing decision, as some exchanges have already done.

  Suggested key factors are set out below. The information can be provided by the issuer, public information and/or specialist advisors, but should be credible:

  - ***Token issuer business.*** Factors to consider include the history, background, business and performance, financial condition and prospects, operations and structure, procedures and systems.

  - ***Token applicant team.*** Factors to consider include the track record, experience, resources and disciplinary history of the team and group.

  - ***Token applicant governance considerations*****.** Factors to consider include whether there are mechanisms and controls in respect of updates to codes, system issues, conduct of users, disputes etc.

  - ***Technological considerations*****.** Factors to consider whether the token ecosystem has already been established, whether the token uses technology that has an open source code, whether the token ecosystem has well-documented peer review, and whether the token ecosystem has been tested by contributors outside the initial development team.

  - ***Token supply and liquidity considerations*****.** Factors to consider include the market capitalization of tokens, the trade velocity of tokens, whether the supply of new tokens are subject to any protocols, the number of exchanges which support the tokens (and the volume of trading), whether existing fiat and digital asset trading pairs already exist

[4] Please note that the points discussed in this section relate to centralised exchanges which list tokens at their own discretion, as the listing process for user voting systems would be different.

in respect of the token, and the jurisdictions in which the digital assets have been offered.

- ***Token demand considerations*.** Factors to consider include whether there is strong customer demand, whether there are contributors, whether there is a strong community base (e.g., based on activities in forums, etc.), whether third parties such as venture firms or hedge funds have invested in the project, and whether the project has other corporate partnerships.

- ***Token ecosystem considerations*.** Factors to consider include whether there is a compelling reason for the token to exist (i.e., not purely for fundraising), and whether there are mechanisms to promote good behaviour or deter bad behaviour by holders/users.

- ***Token sale structure considerations*.** Factors to consider include whether there has been a fair distribution of tokens in the sale, whether the applicant team has retained a minority stake subject to lock-up conditions, and whether the sale has been conducted in a fair and transparent manner.

- ***Regulatory considerations*.** Factors to consider include whether the tokens can be traded in jurisdictions which the exchange operates in and whether it would affect the exchange's compliance obligations (e.g. AML/CTF compliance).

- ***Reputational risk considerations*.** Factors to consider include whether the listing of the token would bring a reputational risk to the exchange. For example, reputational risk could arise if the token ecosystem is linked to illegal activities, gambling, pyramid schemes and narcotics.

- **Legal opinion** – Exchanges should consider obtaining written legal advice in the form of a legal opinion or memorandum to confirm the legal and regulatory status of the tokens in the relevant jurisdictions (i.e., the jurisdictions into which the token has been sold) and the implications for the exchange. Exchanges may wish to set out guidelines on matters such as the form of the opinion, the scope of review, the issues to be addressed and the documents to be reviewed by legal counsel. Most or all issuers should have obtained a legal opinion regarding the characterization of their tokens in connection with their primary token sales, in which case the exchange could ask the issuer for copy of this opinion. Such legal opinion would be addressed to the issuer and provided to the exchange on a non-reliance basis. The advantage to this approach is that the exchange does not need to incur any additional expense to obtain a new opinion (whether on its own account or by passing through the cost to the issuer as a part of the listing fee). The disadvantage is that the exchange would not have formal legal recourse to the issuer's law firm in the event that the characterization of the token is incorrect. Alternatively, the exchange could obtain a legal opinion from its preferred external counsel. The advantage of this approach is that the exchange could rely upon the opinion. The disadvantage is that obtaining the opinion will take time and incur costs (which could be passed through to the issuer in the form of listing fees).

  Regardless of the approach adopted by an exchange, the exchange should ensure that it:
  - has reviewed the legal opinion as part of its due diligence process;

  - understands the legal analysis; and

- is satisfied with the legal counsel's scope of work and the assumptions/qualifications on which the opinion is based.

- **Issuer due diligence** – Exchanges should conduct reasonable due diligence and not fully rely on the legal opinion provided by the issuer. The level of due diligence would depend on the circumstances and may include, for example, compliance searches on the token applicant team individuals, due diligence on source code and review of internal procedures. Where appropriate, exchanges should verify the information provided by the issuer by clarifying inconsistencies with the issuer or other means such as obtaining independently sourced information. The team responsible for the due diligence should be competent and have the expertise to conduct the due diligence (for example, it should consist of individuals with relevant technological, business, legal and regulatory expertise to perform due diligence on the issuer effectively). Adequate records, including relevant supporting documents and correspondence, should also be maintained by exchanges. These records may include the due diligence plan, details on the due diligence procedures, the results of due diligence performed and assessment of such results[5].

- **Listing fees** - Some digital asset exchanges do not accept payment for listing, while some may charge applicants a listing fee. While the level of fees to be charged is a commercial decision, it is best practice to charge a flat rate for all applications to avoid giving the impression that the exchange's listing decision are determined or influenced by the amount of money an issuer is willing to pay for listing a cryptographic token.

- **Other internal controls** - Exchanges should implement internal controls such that decisions makers in the listing process do not divulge confidential information or use such information for their own gains.

- **Listing rules** - Exchanges should ensure that there are terms or other arrangements in place with the applicant that sets out, at the minimum, the responsibilities and continuing obligations of the applicant (e.g. notification of a material change in the issuer's business) and the circumstances in which a token listing may be suspended or de-listed.

A note about 'stablecoins'

A number of exchanges list or otherwise utilize digital assets that attempt to maintain a stable price as against a reference asset (e.g. a particular fiat currency). Each of these digital assets carries different features and risks. The structure that they adopt to achieve their stable price also differs – by way of example only, they could be based on market consensus alone, operate as structured products or money market funds, be asset-backed, reflect debt instruments or stored value facilities, or use third party price stabilization activities.

Extreme care is required in using stablecoins. Whilst they can serve a valuable purpose offering a less volatile class of asset, many are likely to be regulated products. In certain jurisdictions, price stabilization activity could also constitute unlawful asset price manipulation. Customers may also be confused as to which assets they hold (fiat vs. stablecoin), particularly if the names are similar.

[5] We note that this is an area of emphasis for regulators. In Hong Kong, for example, the Securities and Futures Commission ('SFC') has sent letters to exchanges warning them they should not trade in digital assets that are 'securities'. We understand that one area of the SFC's focus is on the diligence that has been done on the digital assets that are listed.

Proper governance and controls are critical to ensure that any assets or other mechanisms supporting the stablecoin in fact exist. The key protections that exchanges should adopt include:

- ensuring that stablecoins are subject to rigorous due diligence before being onboarded onto the platform, including obtaining all necessary legal and advice, akin to any other digital asset;
- understanding what audit or other mechanisms are in place to ensure that the assets and/or other mechanisms supporting the stablecoin in fact exist; and
- taking reasonable steps to ensure that customers are not confused as to the asset;
- considering the impact on the overall operations of the exchange, including settlement and business continuity.

III. Addressing market manipulation, pricing and liquidity

Digital asset markets and exchanges are only recently coming under the scrutiny of international regulators, lawmakers and financial industry advisory bodies. From 2011 through 2017, market behaviour on exchanges has largely been self-policed and governed by the feedback and influence of their respective communities, many of whom are not confined to one jurisdiction when participating in the market. Initial regulatory inroads have largely focused on AML compliance and targeted exchanges offering fiat onboarding. Exchange regulation entered the spotlight in 2017 with Japan's Financial Services Agency[6] being the first to officially regulate 11 exchange operators in September 2017, and Australia passing legislation requiring exchange registration with AUSTRAC[7] in December 2017. There are wildly varying levels of maturity across exchanges, both in terms of trading technology, broader market infrastructure linkages and embedded preventative controls to protect markets from bad actors.

Three key areas which demand focus from digital asset exchanges to advance the industry forward: (1) market manipulation, (2) pricing and liquidity and (3) trading measures.

1. Market manipulation

As global regulators begin to weigh in on the evolving digital asset markets[8], it is highly likely that basic international anti-manipulation and market abuse standards may soon apply to digital asset exchanges. Common schemes which are illegal in securities and commodities markets are not yet adequately prevented or policed in digital asset markets today.

Within digital asset markets, one highly common and typically fraudulent practice today is the 'pump and dump' scheme[9] where a group is gathered to coordinate investors to hype a thinly traded asset on social channels, then bid up the price ('pump') at a specified time, only to rapidly sell ('dump') with the hope of cashing out at the peak trading price. The CFTC has already recognized pump and dump schemes as fraud, issued a customer advisory memo[10] and offered a bounty of 10-30% for Good Samaritan whistle-blowers providing information which leads to a successful enforcement action. Digital asset exchanges can influence higher standards of conduct, monitoring and enforcement of suspected fraud and price manipulation by:

- setting clear trading rules and terms of use (see GDAX[11]);
- performing periodic reviews of suspicious price spikes; and
- applying terms of use controls (temporary account freeze, etc.) where strong evidence suggests that a fraud was committed.

Another more opaque but common challenge for today's digital asset markets is preventing insider dealing, front-running and spoofing schemes. Exchanges have a bigger role to play and can directly influence or prevent these schemes with innovative technical solutions and market surveillance. Centralized exchanges can directly implement order-book transparency standards to shine light on dark pools and take action via strict internal policies and controls over trades made by the exchange and its employees. Periodic independent review and audit can help to

6 Japan's FSA gives official endorsement to 11 cryptocurrency exchanges.
7 AUSTRAC: Are you a digital currency exchange provider?
8 Relevant moves by selected regulators: JFSA CFTC EBA FINMA AUSTRAC SFC MAS PBOC (普通话).
9 Inside the group chats where people pump and dump cryptocurrency.
10 Customer Advisory: Beware Virtual Currency Pump-and-Dump Schemes.
11 GDAX: Trading Rules - See 2.13-2.15 Market Manipulation Prohibited.

provide public trust and assurance that rules are followed. Appropriate controls can help prevent insider dealing. Alternately, distributed exchanges have the technical advantage of a fully decentralized order book (recorded on chain), which has the potential to provide full transparency and auditability.

Lastly, wash trading schemes on exchanges can more readily be prevented by direct action from exchanges. Clear trading rules[12] and simple technical upgrades to trade matching algos to prevent orders which result in self-execution can prevent manipulation. Exchanges which do not provide this basic standard of protection (or appear to flout it entirely, as alleged of certain exchanges) may soon see their customers seeking a more trustworthy exchange.

2. Pricing and liquidity

The global market for trading digital assets is highly fragmented today and has experienced notable pricing differences across global exchanges, readily able to be reviewed on an asset-by-asset basis through sites such as CoinMarketCap[13]. Pricing variations for the same asset on global exchanges are primarily due to differences in liquidity, jurisdictional onboarding restrictions, and exchanges' bank limits on wire transfers and capital controls, which tend to limit arbitrage opportunities to parties actively trading on multiple exchanges. Standards that can be applied to promote accurate pricing are similar to dual listed companies, where prices should move in lock-step across jurisdiction barring any major differences in liquidity, governance, taxation and base currency prices (whether fiat or digital assets).

The definition of liquidity is whether an asset can be readily sold and converted into a base asset, typically 'cash', without materially impacting the price of the asset. To assess the liquidity of a digital asset, a base currency or asset must be selected against which to measure relative liquidity. For example, while Bitcoin may be readily convertible into US Dollars, many ERC20 tokens require conversion to BTC/ETH before converting to USD. Exchanges can support asset liquidity monitoring and promotion of enhanced liquidity by measuring digital asset liquidity (e.g. how readily a digital asset can be converted into BTC/ETH without materially impacting the price) and putting in place policies and procedures for review and assessing whether they can continue to adequately support trading assets which have fallen below baseline liquidity thresholds via OTC services or other methods.

Broader market liquidity can be measured using a variety of indicators[14] including pre/post trade price transparency, volumes, open interest, breadth of investors, number of active market makers, relationship of price relative to volume, bid/ask spreads, etc. Liquidity is typically a symptom of both asset quality and market structure. Exchanges can play a role in supporting collaborative market-structure enhancements that can be made to broadly promote liquidity. These include the following:

- Consolidation, connectivity or linkage across fragmented exchanges (to improve price discrepancies
- Encouraging price transparency standards
- Promoting a more diverse set of investors, including institutional investors
- Encouraging more market-makers

12 See 2.9-2.11 Self-trade prevention.
13 CoinMarketCap.
14 Guidance for supervisors on market-based indicators of liquidity.

- Supporting robust associated markets (securities lending, securities financing, derivatives, ETFs/funds)
- Dissemination of real-time and historical trade, pricing and reference data
- Experimentation with things like maker/taker pricing and tick sizes.

3. Trading measures

Standard exchange safety measures such as market-wide trading halts, Limit Up-Limit Down (LULD) [15] rules or volatility interruptions ('circuit breakers') are not yet widely used across digital asset exchanges. In comparison, a 2016 study of international trading venues indicated usage of various types of circuit breakers at 86%, up from 60% in 2008.[16] Exchange usage of circuit breakers prevents the market and/or single assets from trading outside specific price bands by setting static or dynamic price ceilings and floors above and below certain reference prices.

Those in support of circuit breaker usage advocate that the use of the technology allows for a market pause to reassess order book and strategy during times of panic or extraordinarily high volatility such as the May 2006 Dow-Jones 'flash crash', the January 2015 end of the CHF-EUR peg, or the ETH crash to $0.10 on GDAX in mid-2017.[17] However, while usage of circuit breakers is widely accepted in mature trading venues, there are a number of challenges to implementation of similar measures on new and emerging trading venues, including digital asset exchanges, due to the highly volatile and fragmented landscape of trading venues that exists today. As a result, circuit breakers must be carefully considered before implementation.

The China CSI 300 provides an example with a similarly volatile and young market with a predominantly new retail-investor base. In January 2016, brand new circuit breaker thresholds were released by the China Securities Regulatory Commission ('**CSRC**'), and were subsequently triggered twice in the first day of market usage, prompting a market shut down. Following another trigger and shutdown a few days later, the circuit breaker thresholds were cancelled by the CSRC amid worries that the mechanism was "deepening the sell-off" and "the current negative impact outweighs the positive impact."[18]

In FX markets, use (or lack thereof) of circuit breakers following the Swiss National Bank removing the CHF-EUR peg has prompted heated debate and a relevant example from a more mature global market. Two broad criticisms of the use of circuit breakers in FX markets are (1) the lack of a central global regulatory framework to define and enforce thresholds and (2) the varied needs of market participants (retail vs. institutional) and impacts of trading halts on each, suggesting that centralized and official price transparency is a pre-requisite to implementation of circuit breakers.[19]

At this stage in the evolution of digital asset exchanges, challenges to implementation of circuit breakers abound. As local regulations solidify, global standards are agreed, and market participants diversify, this may be an area of future consideration. However, implementation of circuit breakers currently appears to be impractical and detrimental to proper market functioning at this early point on the maturity curve.

15 http://www.luldplan.com/index.html.
16 World Federation of Exchanges: Survey on Circuit Breakers (2016).
17 Why Wall Street Trading Tech Needs to Enter the Crypto Market.
18 Circuit Breakers and New Market Structure Realities.
19 EuroMoney: Circuit breakers are not the simple answer to extreme FX volatility.

IV. Regulatory considerations: licensing and authorization

Digital asset exchanges are internet-based platforms designed to facilitate the trading of digital assets and accordingly they can access customers across the world with a relatively limited physical footprint in any single jurisdiction.

Traditional exchanges and trading platforms are subject to laws and regulations (usually in the form of a licensing or authorization regime) in the jurisdiction(s) in which they operate and/or market and the intermediaries (brokers/trading and clearing participants) who can access the platform also usually need to have some form of license or authorization.

Digital asset exchanges are direct-to-customer platforms and typically operate without the need for intermediaries to place orders on behalf of their users or hold users' assets in custody. As such, a digital asset exchange can function as a broker, custodian and trading venue at the same time.

Recent events[20] have shown that regulators are increasingly scrutinizing exchanges on two fronts; firstly, they want to ensure that digital asset exchanges are not facilitating trading in regulated financial products (e.g., tokens which have the characteristics of securities) without holding the appropriate license or authorization and, secondly, they want to understand how exchanges market their services to potential customers and whether such marketing activity itself constitutes some form of regulated financial activity for which a license or authorization is required. Other features, such as the provision of leverage, may also trigger regulatory scrutiny.

These issues are exacerbated by the absence of any internationally harmonized view of token characterization, meaning that a token which is not classified as a 'security' (or other regulated product) in one jurisdiction might be classified as a 'security' (or other regulated product) in another jurisdiction. Additional features and services, such as leverage, derivatives, futures etc., are also subject to jurisdictional differences.

How should digital asset exchanges deal with the challenges presented by the patchwork of varying international approaches to regulation in order to establish compliant but also commercially efficient, scalable platforms?[21]

One approach, which currently seems to be the most widely adopted approach in the market, is that the website for the exchange is accessible globally, but certain jurisdictions and categories of customer are 'switched off' pursuant to the exchange's terms and conditions and its client onboarding procedures.

Under the terms and conditions of the exchange, customers from certain prescribed jurisdictions are expressly prohibited from using the services of the exchange. Customers are required to submit detailed 'know your customer' information to the exchange and, based on a review of that information, the exchange can verify that the customer is not from a restricted jurisdiction and is

[20] For example, Binance being warned by the Japanese Financial Services Authority for doing business in Japan without a license, the U.S. SEC taking action against Bitfunder for facilitating the trading of security tokens without holding the appropriate licenses.

[21] As discussed in the Introduction, this document focuses on centralized digital asset exchanges. For completeness, we note that there will be a host of other considerations for decentralized exchanges. For example, where the listing of a token is purely based on user voting, certain tokens which may be characterized as 'securities' (or other regulated products) could be listed and traded on the decentralized exchange, which may then trigger licensing and authorization issues for the exchange. In addition, if there are regulatory developments in the future which result in a listed non-security token becoming a security, there will be further considerations as to how these tokens should be dealt with.

not otherwise prohibited from accessing the exchange's services (e.g., because the individual is subject to sanctions).

The same 'switching off' approach could be taken with respect to specific digital assets. For example, a digital asset which is not classified as a 'security' in Switzerland but would be classified as a 'security' in Hong Kong could be made available for trading for Swiss persons but 'switched off' for Hong Kong persons. This approach would reduce the risk of the exchange facilitating trading of 'securities' without a license in a particular jurisdiction but, as a commercial matter, may result in limiting the range of digital assets that are available to trade in some jurisdictions.

This approach allows the flexibility to 'switch off' an entire jurisdiction, where it is clear that this is required by applicable laws and regulations, and to fine tune the exchange's offering in other jurisdictions by only 'switching off' the ability trade specific tokens.

Marketing of exchange services should be in compliance with applicable laws and regulations of the target jurisdiction (e.g. marketing activities should not be conducted in 'switched off' jurisdictions). Where marketing is conducted through a website, measures should as those discussed below should be adopted. In conjunction with these 'switching off' safeguards, it also would be prudent for exchanges to limit active/concerted marketing campaigns to permitted jurisdictions (i.e., jurisdictions which have not been 'switched off') and in which there are not a significant number of tokens on the exchange which are 'switched off'.

In addition, exchanges also may need to implement further measures including, but not limited to, the following:

- include a generic catch-all clause in the terms and conditions of the exchange stating that services will not be provided to persons where the use of such services would be contrary to applicable laws and regulations;
- notify customers about tokens which are 'switched off' in the relevant jurisdictions;
- implement systems and controls so that such persons cannot actually trade the 'switched off' digital assets, including geoblocking and IP address checks; and
- to avoid inadvertently triggering any marketing restrictions, the website and marketing materials of the exchange should list the jurisdictions which are not 'switched off' (i.e. are 'switched on').

The 'switching off' approach for jurisdictions is only a partial solution, given the pervasive use of Virtual Private Networks in the industry. The above outlined approach therefore needs to be coupled with necessary sanctions screening using a reliable provider for sanctioned persons and entities.

For completeness, another approach is to only permit the trading of tokens in certain jurisdictions as prescribed by the exchanges and block all other jurisdictions (i.e. the 'switching on' approach). Customers will therefore be unable to access the exchange's website or trade tokens in jurisdictions which have not been 'switched on'. The advantage of the 'switching on' approach is that operational risk of providing services in a jurisdiction where such services are prohibited should be lower. This also provides a more comprehensive mechanism for dealing with legal and regulatory risk. From an

efficiency standpoint, it also narrows the jurisdictions that need to be monitored on an ongoing basis.

Irrespective of whether a 'switching on' or 'switching off' approach is adopted, the key will for exchanges will be to carry on thorough jurisdictional analysis and have effective customer screening and robust controls.

One further consideration is that exchanges should have appropriate procedures in place to react to abrupt changes to regulations or regulatory expectations in a particular jurisdiction. For example, if a regulatory change in a certain jurisdiction results in the trading of digital assets becoming unlawful or a certain token is recharacterized as a security, exchanges will need to immediately 'switch off' the relevant jurisdiction or the trading of the relevant token. To address this, exchanges should consider implementing the following best practices:

- monitor regulatory developments in jurisdictions where the exchange's tokens are traded and on an ongoing basis. If there is a potentially adverse change, the exchange should assess whether this merits 'switching off' the jurisdiction as a whole or certain tokens from being traded in the jurisdiction. Where there is some ambiguity, the exchange may wish to obtain an updated legal opinion from the issuer or from the exchange's own legal counsel to confirm the legal and regulatory status of the relevant tokens;
- require issuers to disclose to the exchange, among other things, (i) any material issues with the status or condition of the project, financial condition, management team of the issuer; and (ii) any other material changes to information submitted in the original listing application by the issuer, pursuant to the continuing obligations requirements under the listing rules;
- prohibit users in affected jurisdictions from 'buying' the relevant tokens but (subject to the bullet point below) permitting them to sell such tokens; and
- engage in discussions with the local regulator to resolve how the affected token holders can exit their positions (e.g. whether it is permissible for the token holders to make a final trade within a prescribed timeframe). Otherwise, such token holders may have to hold on to tokens which they cannot dispose of, which may therefore be valueless. In any event, this risk should be clearly identified to exchange users.

V. AML/KYC issues and recommendations

1. Importance of AML/CTF controls

As noted in a June 2014 report[22] issued by FATF, convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to ML/TF abuse for the following reasons:

- they may allow greater anonymity than traditional non-cash payment methods;
- the global reach of virtual currency means that responsibility for anti-money laundering and counter-terrorist financing ('**AML/CTF'**) compliance and supervision /enforcement may be unclear; and
- components of a virtual currency system may also be located in jurisdictions that do not have adequate AML/CTF controls.

As such, there is a greater impetus for digital asset exchanges to develop and maintain a strong AML/CTF program, so as to enable them to meet their compliance obligations in the relevant jurisdictions where they provide services.

Several jurisdictions globally, including the United States, Japan and Australia have also introduced mandatory registration and compliance obligations for digital asset exchanges, which include detailed AML/CTF obligations which reflect best practices in the market.

Even in countries which have not moved to ban digital asset exchanges or introduce specific legislation to regulate the exchanges, financial services, tax and data privacy regulators and law enforcement agencies have sought to access and review customer and transaction records to carry out their regulatory functions.

General de-risking trends by banks globally are also challenging digital asset exchanges to improve their AML/CTF practices so as to avoid their bank accounts from being frozen or shut down due to breaches of AML/CTF policies. There are also concerns that a closure of bank accounts of digital asset exchanges in regulated jurisdictions may lead to a poorer competition environment for digital asset services, and leave them outside the effective control and oversight of regulators in the major jurisdictions in which they operate.

By following best practices in KYC, exchanges can enhance their reputation with users, regulators and ancillary service providers (including banks), and build a credible and sustainable brand in the market.

2. Market observations

According to Cryptocoincharts,[23] as at May 2018, there are 193 digital asset exchanges with a daily volume of about USD6.95 billion. However, there are significant variations in how these exchanges carry out KYC due diligence.

---

22 FATF Report, *"Virtual Currencies – Key Definitions and Potential AML/CTF Risks"* (June 2014).

23 See https://cryptocoincharts.info/markets/info, as extracted on 4 May 2018.

At one end of the spectrum, there are centralised 'anonymous Bitcoin exchanges'[24], whereby users are permitted to use the services of the exchange without identity verification. This means that in most cases, only an email and a password need to be provided before users undertake trading in the exchange. As noted by FATF in a 2015 report, the anonymity of these exchanges and the challenges to conduct a proper identification of the participant mean that such exchanges have higher ML/TF risk.[25]

On the other end of the spectrum, there are centralised digital asset exchanges which carry out full KYC due diligence processes before carrying out users for services, and verify the identity of users and beneficial owners.

There are also decentralised exchanges which enable peer-to-peer exchanges of digital assets, whereby users keep their own private keys and trade directly with one another. These exchanges usually do not hold any user assets, and there is direct matching between traders with an atomic swap protocol or some other mechanism utilised. Dark pools for digital assets are also currently under testing by some start-ups.

Although many decentralised exchanges have taken the view that no due diligence processes are required since they do not have access to any funds, FATF has viewed decentralised exchanges as posing the highest risk, which would necessitate enhanced due diligence being conducted on individuals. It may not be clear which entity is deemed the operator and hence responsible for AML/CTF and there is also currently a lack of clear practical solution for such due diligence to be conducted in the industry, which also presents serious challenges for effective AML/CTF compliance and supervision.

What is clear is that a balance needs to be struck between ensuring that ML/TF risks are identified and mitigated, and ensuring that users are not overly encumbered by the verification requirements of any specific exchange, to avoid the scenario of a 'race to the bottom' in terms of KYC standards. It is with this objective in mind that we have proposed the best practices below.

3. Risk assessment

In designing and implementing an AML/CTF program, the digital asset exchange should conduct its own risk assessment to understand its vulnerabilities and determine the level of resources necessary to mitigate risks. In doing so, it may wish to consider the following:

- **Type of exchange.**
- **Jurisdictions serviced** – Where services are provided in higher risk jurisdictions, the digital asset exchange should also ensure that it has robust AML/CTF systems.
- **Customer base and target market** – Generally, the information and documentation required for institutional customers is likely to be more intensive, given that more

[24] See list on Bestbitcoinexchange: http://www.bestbitcoinexchange.net/anonymous/.
[25] FATF report dated June 2015, *"Guidance for a Risk-based Approach: Virtual Currencies"*.

information is usually needed to understand the entity's profile, business and account activity, in order to identify any relevant adverse information and risks.

- **Scope of business** – Where smaller volumes are traded, and where the tokens and types of products offered are limited, a simpler risk assessment may suffice. Conversely, where the exchange's products and services are more complex (e.g. cryptofutures or other derivatives products are offered), a more sophisticated risk assessment process may be required.

The risk assessment should also be reviewed and approved by senior management, and can form the basis of the development of policies and procedures to mitigate ML/TF risk. It should be properly documented, maintained and communicated to relevant personnel. It should also be reviewed periodically and in any event when business activities change or relevant new threats emerge.

4. AML/CTF program

Once the digital asset exchange has conducted the risk assessment, it should use it to develop an AML/CTF program which should include:

- a system of written policies and procedures around customer on-boarding, KYC, customer due diligence and ongoing due diligence;
- an enhanced due diligence program for additional customer identification and verification; measures in certain circumstances deemed as high risk;
- policies on management oversight and control, including in relation to the inclusion of a Money Laundering Reporting Officer, compliance and audit function, and staff screening and training;
- a system of policies and procedures to maintain and execute an effective sanctions screening program, and transaction monitoring and alert investigation process;
- periodic independent testing to ensure the effectiveness of AML/CTF systems; and
- policies and procedures on record keeping which adhere to any regulatory, tax and data privacy requirements. As far as possible, digital asset exchanges should maintain records in relation to the purchase, conversion and sale of virtual currency.

Governments may impose higher or lower requirements than what is set out above. In such cases, the digital asset exchange should aim to follow the higher standards applicable.

Where third-party regtech providers are used to assist with sanctions screening, document authentication and verification processes or otherwise, the digital asset exchange should also develop a system of policies and procedures in relation to the selection and oversight of the third-party provider.

5. Specific observations in relation to KYC

- Digital asset exchanges should aim to conduct verification of users as early as possible in the account signup process, and in any event before the deposit of monies or the commencement of trading.
- Screening sources and lists should be regularly reviewed to ensure that they are up to date. The Office of Foreign Assets Control has also indicated that they may include digital currency addresses on its Specially Designated list of blocked persons, companies and entities.[26] There will likely be vendor services developed to offer screening services for digital currency addresses.
- Multiple accounts should be discouraged as there is a heightened risk of structuring (split transactions or wash trades) to evade tax enforcement or regulatory recordkeeping and movement restriction thresholds, and avoid scrutiny generally.
- We are aware of regulatory technology solutions/products which are being developed or which are already available in the market, such as Polymath, which screens for accredited investors that have gone through KYC checks. While such technology may be helpful, exchanges should note that the definition of accredited investors and KYC standards varies in different jurisdictions and that limiting users to accredited investors may not necessarily address all regulatory issues (e.g. licensing and authorisation issues).
- There may be certain requirements applicable on exchanges with regard to maintenance of tax information and records.
- Cooperation between exchanges and law enforcement officers is encouraged to blacklist compromised addresses/accounts.

[26] See OFAC FAQs at : https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

VI. Custody issues and recommendations

1. Selecting an appropriate model

As mentioned earlier, a digital asset exchange can function as a broker, custodian and trading venue at the same time. The term 'custody' is used here generally (i.e. holding assets on behalf of the end user/client).

To date, digital asset custody models have primarily been based around co-mingled omnibus-like accounts, where similar users' assets are pooled in one account. The identification and ring-fencing of users' digital assets is arguably far preferable, to ensure that the assets will not form part of the estate available to the liquidator in the event of the insolvency of the custodian. It also helps assure users of the protection of their assets despite the custodian's liabilities incurred through operational losses, particularly where regulatory capital requirements do not apply. Segregated accounts do come with their challenges and costs however. Set out below is an overview of some of the key advantages and challenges of omnibus accounts versus segregated user accounts:

Omnibus accounts		Segregated user accounts	
Advantages	**Challenges**	**Advantages**	**Challenges**
Operationally straightforward, reducing operational risk	Insolvency risk for users - not recorded on chain as the owner	Relies on strong record-keeping mechanics at the exchange level	Higher operational risk
Cost effective for the exchange and therefore also for the user	Becomes a centralized 'honey pot' that may attract internal or external theft and cybersecurity attacks	Cybersecurity attacks and theft in relation to other accounts should not taint the user account, unless directly hit	Higher costs, slower settlement
Can facilitate fast settlement - user generally does not need to wait for assets to be shifted from cold storage (i.e. usually not affected by % of assets stored in hot vs. cold wallets)	Relies on strong record-keeping mechanics at the exchange level		Unless users' interest recorded on chain (or via trust arrangements - see below), arguably offers no higher protection than omnibus accounts

It is not the intention of this paper to favor one model over another. This is an area under development and which has idiosyncratic technological and operational aspects that are different to traditional custody models for cash and securities. We expect market practice to develop over time.

Set out below are important factors to consider:

- **Third parties** – The use of reputable professional third parties to act as independent custody service providers should be considered. However, we recognise that there remains a paucity of such providers at this stage with the right track record and expertise.

- **User options** – A combination of models, with variable pricing, should be considered where feasible, to enable users to choose the level of protection they wish for their assets.

- **Disclosure** – Adequate risk disclosure is essential. At minimum, users should be advised prominently about the way in which assets are held on the exchange, and whether moving assets to their own personal digital wallets is a safer option.

- **Own assets** – Extreme care is required in relation to proprietary digital assets. These should be segregated altogether and not commingled with user assets.

- **Trust arrangements** – Trust arrangements can strengthen custody models from a user standpoint in markets that recognise trust structures. That is, a declaration of trust over assets in an omnibus account and/in segregated user accounts can help ensure that in an insolvency event, the assets are appropriately treated as those to which users (and not other creditors) are beneficially entitled. However, licensing requirements should be carefully considered and the arrangements must be documented properly.

2. General principles for custody

Custody and safety of digital assets temporarily held on exchanges are matters of priority for the industry, given the large number and scale of exchange hacks. The list below represents only some of the digital asset custody best practices and recommendations. It should not be construed to be an exhaustive list of all required controls and appropriate safeguard measures[27].

- Digital asset exchanges should screen all employees appropriately and ensure adequate training and supervision at all times. An appropriate internal function should be assigned to the safekeeping of assets, such as a security officer.

- Digital asset exchanges should establish and maintain internal procedures that ensure the maintenance of appropriate standards of recording and management with respect to user digital assets and fiat currencies.

- Digital asset exchanges that store, hold, or maintain custody or control of digital assets and fiat currencies on behalf of a person must hold that same type and amount of digital assets and fiat currencies owed to the person.

- Digital asset exchanges should not create a right of lien, offset or encumbrance or any other right with respect to user digital assets or fiat currencies, excluding (i) custodian fees and (ii) transaction fees.

- Customer terms and conditions should not only cover the products and services available, but also make clear the respective rights, obligations, responsibilities and risk allocation of the parties, plus appropriate dispute resolution mechanisms. Procedures should also be clear on the exchange, with frequently asked questions posted and updated from time to time.

- Digital asset exchanges should have a clear fee structure that is readily accessible to customers. Where fees involve calculations, illustrative examples should be considered.

- Digital asset exchanges should keep the following books and records for at least 7 years from the date of creation, or such longer period as is required by applicable law:

[27] Similar principles could be applied to custody services providers.

  - Amount, date, time, payment instructions and fees for each digital assets and fiat currencies transaction
  - Non-completed, outstanding, or inactive digital assets and fiat transactions
  - Bank statements and bank reconciliation records
  - Any statements or valuations sent or provided to customers
  - Records of all customer complaints and investigations

- When applicable, a digital asset exchange should conduct reconciliations between its internal accounts and those of any third party by whom custody assets are held.

- Real-time controls should be implemented for matching and reconciliation to confirm the validity of all digital asset transactions executed using private keys which belong to the exchange.

- Cold storage refers to digital assets kept offline as opposed to hot wallets which are being used to cope with withdrawal request. Exchanges should develop a custody plan in line with liquidity management principles; e.g. assess technical options for cold storage custody services to enhance the security of assets left on the exchange. Amounts kept in hot wallet should be kept to a minimum (ideally more than 97% of customer assets should be stored offline). Customers should be educated and encouraged to utilize cold storage wallet custody solutions. In addition to liquidity management principles, limits and triggers on the percentage of assets held in hot storage should be set, with monitoring measures put in place to ensure limits are adhered to, whilst the exchange is liquid and operating effectively.

- For both cold storage and hot wallet, measures shall be put in place by digital asset exchanges to safeguard customer and proprietary assets from fraud, negligence and mishandling:
  - Digital asset exchanges should use hardware security modules ('**HSM**') which are physical computing devices that safeguard and manage cryptographic keys, and provide secure execution of critical code. HSMs come with a certain level of regulatory assurance, such as the Federal Information Processing Standard certification and Common Criteria (an international standard).
  - Digital asset exchanges should use a multi-signature storage vault set up (ideally requiring at least three keys out of five or more to initiate a transaction).
  - Security protocols surrounding management of private keys for both hot and cold storage should be audited.

- Digital asset exchanges should proactively communicate their strategy for newly created digital assets in case of hard fork or airdrop.

- For each account, digital asset exchanges should provide periodic personalised reports detailing the holdings both in digital assets and fiat currencies.

- Digital asset exchanges should publish on their website risk assessment indicators outlining the level of risk of the digital asset to (potential) users.

- Digital asset exchanges should monitor customer accounts to check for any inactive/ dormant accounts and set out the procedure by which those accounts may be closed and claims may be made for relevant assets.

- Customers should have a clear understanding as to how they can have access to and withdraw their digital assets, particularly in times of stress.

- Digital asset exchanges should implement a business continuity and recovery plan with clear policies and procedures in the case of a catastrophic event. Relevant information should be made available to users of the exchange.

VII. Cybersecurity issues and recommendations

Fundamentally, digital assets are fully digital and decentralized. Yet, today's digital asset exchanges are mostly centralized and have proven to be vulnerable to hacks. Similarly, while the blockchain itself is considered secure as a concept, the framework, implementation or Application Program Interfaces ('**APIs**') around digital assets often contain vulnerabilities that can be exploited, as happened in the case of Ethereum for example. The safety of user assets should be the primary objective.

There are many international standards which set out in significant detail the best practices that should be adopted, often based in turn around the cybersecurity lifecycle. Among the most comprehensive of these is the U.S. National Institute of Standards and Technology ('**NIST**') Cybersecurity Framework[28], first published in 2014 and most recently updated in April 2018 with contributions from stakeholders across sectors from the U.S. and around the world. The NIST Framework's core outlines measures to identify and protect against risks, and to detect, respond to and recover from incidents.

Many of these international best practices are applicable equally to digital exchanges as they are to any other type of organization. There are also cyber risks that are specific to digital assets and exchanges, which we set out in the second part of this section. The list below represents only some of the cybersecurity best practices and recommendations. It should not be construed to be an exhaustive list of all required controls and appropriate safeguard measures.

Some of these best practices are to be implemented by the digital asset exchanges whilst others are driven by the users.

- Have a dedicated specialized team in charge of cybersecurity, led by a security officer.
- Perform staff background checks and ensure staff are educated on cyber-attacks (e.g. phishing).
- The time between the discovery of an operating system or application vulnerability and the emergence of an exploit is getting shorter, sometimes only a matter of hours. Digital asset exchanges should develop a process to promptly install security patches and not break existing systems in the process. More specifically, Internet facing devices should be fully patched in a timely manner.
- That said, information system stability changes rely heavily on software and hardware changes being tested prior to deployment, and the decision on whether to allow deployment into the live environment must be based on test results. Digital asset exchanges should adopt formalized governance and policies for sound operational change and release management. An increasing cyber risk is the compromise of the supply chain of legitimate software, such as the patches supplied by a Ukrainian accounting software provider used as a vehicle to deploy the NotPetya worm.
- Digital asset exchanges should promote the practice of penetration testing to proactively discover potential vulnerabilities. Penetration testing vendors should be rotated every two years.

[28] NIST Cybersecurity Framework, 16 April 2018, https://www.nist.gov/cyberframework.

- Digital asset exchanges should adopt measures and establish processes to increase security and resistance of the IP networks administered by them.

- Digital asset exchanges should apply Distributed Denial of Service (DDoS) protection and mitigation tools.

- Digital asset exchanges should install firewalls which deny all connections by default and allow only explicitly defined connections.

- Digital asset exchanges should implement intrusion detection/prevention system to detect and prevent malicious communications.

- Attacks on digital asset exchanges are often advanced persistent threat type attacks. Therefore, suitable network monitoring technologies should be employed through the network to benchmark 'normal' traffic and spot anomalous behaviours or access.

- Appropriate network segregation should be adopted to isolate critical networks from non-critical ones.

- Various cases have been reported of user IDs and passwords being stolen by fraudsters through phishing emails, fraudulent websites and malwares. Digital asset exchanges should systematically require the usage of multi-factor authentication to verify a user's identity. This should also apply to the usage of any APIs made available by the digital assets custodians and exchanges.

- Authentication credentials such as passwords should be salted and hashed (not encrypted) on the back-end systems, to protect them if they are compromised, and to prevent leakage via an inside job.

- For digital asset withdrawals, digital asset exchanges should use a security feature that requires users to click a link sent to an email prior to release the transaction. If the link is not clicked within a short time period, the withdrawal should be cancelled.

- Digital asset exchanges should make login notifications an opt-out security feature, allow users to temporarily lock and suspend their account in case of emergency and offer IP Whitelisting options. (Login notifications are an extra security feature that can help alert users if someone accesses their account. IP Whitelisting allows to create lists of trusted IP addresses or IP ranges from which users can access a specific domain).

- Where proprietary software or APIs are in use, suitable peer review and testing of code is necessary to ensure that any vulnerabilities are identified and remedied promptly. A separate development environment should be maintained to allow testing of code in a way that does not risk compromising the stability of live systems. Similarly, testing of the software should be undertaken on an offline copy of the relevant blockchain, not in the live environment to avoid inadvertent or unintended actions being applied to the live blockchain (as was the case on the Ethereum platform).

- Specifically for digital asset exchanges, digital asset transactions are secured using a combination of a private and public key. Funds held by exchanges on behalf of their users

are secured by the exchange's private key. Avoiding malicious transactions depends upon keeping that private key secure:

- Steps should be taken to require multiple employees within the exchange to approve/authenticate transactions over certain limits, to mitigate the insider threat. This can be done technically (using multi-signature wallets), rather than just relying on operational procedures.
- Large balances of digital assets should not be held in 'hot' wallets since, if they are hacked, the entire balance is susceptible to being transferred out by a malicious actor. Instead, only the minimum balance necessary for the immediate transactions necessary for the exchange should be maintained in hot wallets.
- Hardware secured cold wallets should be used for any other balances. Physical security should also be placed around them.

VIII. Risk mapping

The objective of risk mapping for the digital asset exchanges is to identify, measure, manage and/or control the relevant risk that may have an impact on the exchange, including legal risks, credit risks, market risks, operational risks, etc. The process of risk mapping is fundamental as this will help to set the strategic risk objectives for the exchange.

The following are examples of relevant considerations that should be taken into account:

- **Risk culture** – This helps to determine the manner in which the exchange manages risks on a day-to-day basis. The risk culture should embed risk awareness, accountability and transparency, with a strong emphasis on the timely identification and reporting of risk exposures.

- **Risk objectives** – This should align with the business and strategic objectives of the exchange and be reviewed on an annual basis.

- **Risk appetite** – It is also important to ensure that the risk management framework is underpinned by an effective risk appetite framework, which refers to the policies, processes, controls and systems, with clearly defined responsibilities, through which risk appetite is established, communicated and monitored.

- **3 Lines of Defence:** The exchange should adopt a '3 Lines of Defence' model. The first line of defence would be responsible and accountable for identifying, assessing and managing risk. Second line of defence is responsible for defining the risk management framework, while the third line of defence would often be Internal Audit, who would provide independent assurance to the Board and other key stakeholders over the effectiveness of the system of controls.

- **Risk management cycle:** A typical risk management cycle would start with business strategy where the risk management activities would actively support, followed by the establishment of risk appetite which set out the level of risk that the exchange is willing to accept in pursuit of the business objectives. Risk policies and procedures would then be put in place that stipulates the relevant standards and controls, which would help the day-to-day risk management function to identify all of the key risk exposures, and these risks should be monitored on an ongoing basis and be reported as needed.

IX. Engagement with external stakeholders

Digital asset exchanges are likely to interact with a wide variety of external stakeholders that are important to its business. These external stakeholders could include, but are not limited to, the following:

Exchange participants	Banks and other institutions	Service providers	Regulators and other authorities
• Customers • Product issuers • Market makers • Algorithmic traders	• Banks • Lenders • FX providers • Insurers and brokers • Custodians	• Technology / data • AML/KYC services • Legal and company secretarial • Tax, accounting, audit • Other advisors and vendors	• Company registrations • Licences and approvals • Enquiries and investigations • Production orders • Periodic filings • Reports • Law enforcement

The requirements of each stakeholder differ. However, they generally require the following:

- ***Knowing your stakeholders*** – Mapping which stakeholders are relevant to the exchange, what their needs are and how they will be met through internal controls, contracts and systems.

- ***Engaging well*** – Designating specific personnel for each relationship or group of relationships. Engaging in a well-considered manner, including providing responses within agreed or mandatory timeframes and obtaining advice when needed.

- ***Resolving issues*** – Clear internal escalation procedures and a defined process to resolving enquiries, complaints and investigations.

- ***Self-reporting when you need to*** – Understanding the legal, regulatory and contractual obligations that require you to report issues proactively to certain stakeholders. Significant consequences such as criminal liability, breach of contract, financial penalties and/or loss of insurance can result from a failure to do so, depending on the facts.

Covering the fundamentals

At a higher level, critical to the success of stakeholder relationships and the confidence of customers and the broader market is a robust business and governance structure.

These will typically be of particular interest to banks and regulators, who may ask for copies of relevant materials and ask the exchange significant details about your business.

The key elements include, but are not limited to, the following:

- ***Governance*** – A strong overall governance framework led by the Board. This should clearly articulate the roles and responsibilities of officers, senior management and personnel, together with clear reporting lines and management information systems.

- ***Business plan*** – A clear business plan that is kept up-to-date. This should include the objectives, products and services of the exchange, together with an assessment of the market, risks and

opportunities, plus a detailed description of the execution strategy, a company and management summary and financial plan.

- ***Risk management framework*** – A robust risk management framework with oversight from a designated Risk Committee. This should include the risk policy and standards, monitoring and reporting procedures, as well as the relevant information security and business continuity strategy.

- ***Internal controls*** (including compliance controls) – Comprehensive written policies, procedures and other controls approved by the Board to ensure effectiveness and efficiency of operations as well as compliance with the Exchange's legal and regulatory obligations, and to address the areas of risk to which the exchange is exposed. These should be supported by internal or external compliance and audit services, and supplemented with legal and tax/accounting advice as needed.

- ***Documentation with stakeholders*** (including customer terms and privacy policies) – Legally binding agreements with counterparties, including customers and service providers, together with appropriate privacy and confidentiality policies. The documentation should also include AML/KYC materials and other due diligence materials, externally published policies, together with relevant legal opinions and other advice obtained in connection with the business.

- ***Adequate resources*** – All necessary personnel, technology, financial and other resources to execute the exchange's business plan, implement its controls, meet stakeholder requirements and comply with applicable law. Personnel should include designated senior managers at least covering exchange oversight, technology, finance, compliance, marketing and operations.

- ***Training and guidance*** – Adequate initial and periodic formal and on-the-job training for staff and relevant service providers (where applicable) to ensure business objectives are met and compliance controls are met. Regular updates and support should be provided.

- ***Regulatory engagement*** – Proactively engage with local and overseas regulators and law enforcement agencies, albeit subject to the applicable data restrictions.

In response to the regulatory uncertainty and perceived high-risk profile of the digital asset exchanges, there are reports that a large number of banks in Asia have closed down the existing bank accounts of digital asset exchanges and are reluctant to open new bank accounts for digital asset exchanges. When adopting these ASIFMA best practices, banks might get more comfortable with servicing the digital asset exchanges.

ANNEX: Issuance of tokens

This Annex briefly describes the process through which many tokens are commonly issued publicly, for context only. It is not exhaustive. As noted in paragraph 1 of the Introduction, there are multiple ways in which tokens can be offered, and in which digital asset exchanges may become involved. Other terminology may also be used.

Overview

During token sales, companies issue 'tokens' ('coins' or similar), which are essentially digital coupons,[29] recorded on an indelible distributed ledger of the kind that underpins many digital assets. Most token sales operate by having purchasers make payment in other assets (usually Bitcoin or Ether) to a smart contract that records payment and distributes a prescribed value in the new token or coin, either immediately or at a later point in time.

The tokens issued pursuant to a token sale event can serve a wide variety of different functions, from granting holders present or future access to a service or product (these tokens are usually referred to as 'utility tokens'), entitling them to profit participation in the issuing company (these tokens are usually referred to as 'security tokens') or simply providing a medium of exchange, like Bitcoin.

Certain tokens may also be sold privately or otherwise distributed outside of a public token sale (e.g. as a fee for service). In such cases, additional steps, materials and considerations are likely to apply.

Pre-token sale

Planning and concept development

During the planning stage, the management team establishes the terms of the token sale. Key decisions include the structure of the sale, pricing, funding goals, target purchasers, use of proceeds and the terms and conditions of the tokens. These considerations are closely linked to the commercial objectives of the project and, consequently, terms and conditions of different token sale events vary significantly.

Most frequently, token sale events are capped and issued on a first come, first served basis. This means that there is a fixed amount of tokens that purchasers can buy on a first come basis and at a fixed price (or a price ratchet, i.e. early buyers can purchase tokens more cheaply than later buyers). Alternatively, a token sale event can be structured as an auction, which can be capped or uncapped. During an auction, purchasers bid and specify the amount they wish to pay for tokens. Care is required to ensure that regulatory implications are appropriately considered.

Whitepaper and other materials

Before launching a token sale, the management team would usually make an initial announcement of its intention to issue tokens in order to gauge market appetite. Such initial reactions may have important consequences for the pricing and scale of token sale events. A token issuer may also hire the services of 'promoters' to promote the token through online marketing, such as through the use of Twitter, Reddit, Medium, Facebook and Instagram.

[29] That is, actual or contingent rights to something.

The management team will also typically create a whitepaper and issue it to potential purchasers and/or make it publicly available on their website. The whitepaper is the main marketing document of a token sale event and sets out key information about the project and tokens. Among other matters, a whitepaper customarily outlines the market size, the business model, the project development roadmap and provides specific details of the terms of the token sale, as well as rights which may attach to the tokens.

Numerous other documents and strategies may be used as part of marketing, including pitch decks, flyers, promotional articles, bounty programs and videos. The terms and conditions of the sale are also of critical importance.

Legal and compliance

Because of growing regulatory scrutiny and a better understanding of the nature and scale of laws that apply, the legal aspects of token sales are becoming increasingly important. This is especially true in relation to the nature of the rights which attach to tokens, as well as AML/KYC and corporate governance matters. In order to ensure credibility of a token sale event and its AML/CTF compliance, issuers increasingly put in place mechanisms to comply with securities and other laws, verify purchaser's identities and/or exclude investors from certain jurisdictions.

Token sale event

Process

As noted above, purchasers usually purchase tokens using other established digital assets, such as Bitcoin or Ether. In certain cases, fiat may also be accepted. Participation in a token sale also requires a wallet which is compatible with the protocol and the platform used for the token sale event. The wallet stores the owner's private key which is used to send and receive coins/tokens.

During the token sale, purchasers send their payment to the public address of the developers and receive tokens in return. Importantly, the specific process and conditions of the issue will vary in each case. The tokens may sometimes be issued or activated after payment – for example, following completion of AML/KYC procedures.

An example of a token creation is by way of creating an Ethereum smart contract. Investors register on the platform used for the token sale event, are informed of a special Ethereum wallet address and send ETH to this address. After the end of the token sale event, the tokens will be automatically distributed to the right owners. Most token sale events involve tokens that are based on the ERC-20 protocol and don't own their own blockchain. The ERC-20 is a token standard that follows specific rules on the Ethereum blockchain.[30]

Phases

The management team decides pricing and the number of stages for each token sale event, but generally there are multiple stages and prices increase with time. Unlike initial public offerings (IPOs) where investment bankers determine the value of the company at a particular share price, in the case of token sale events, the value of the token is typically decided by issuing company at a price they determine.

[30] The ERC-20 standard has been finalised and is also referred to as EIP-20.

As foreshadowed above, before offering tokens to investors, the management team often sets aside a percentage of tokens for the founders, development team, promoters etc.

Numerous token sale events begin with a pre-sale, taking place before the official public sale. The aim of the pre-sale is to attract sizeable investors in order to give the project momentum and positive publicity. These early investors are often offered a discount – often ranging from 10 to 50 percent.

Post-token sale

Following issuance, purchasers are generally free to use and/or transfer their tokens. For example, to participate in the project ecosystem, they can use the token to buy products or services of the issuing company, once the project is in operation. Conversely, if they no longer have a need for tokens, only need fewer tokens or wish to monetise a gain / crystallise a loss in the value of the tokens, they may wish to sell them.

If the project fails or the company pivots their service offering resulting in no/limited token utility, token holders may be left holding valueless tokens with little to no ability to influence the company that issued the tokens in the first place, particularly, where the tokens do not represent equity.

Authors

Mark Austen
CEO
Laurence Van der Loo
Senior Manager

Rebecca Carvatt
Director, Financial Services Advisory

William Hallatt
Partner
Grace Chong
Registered Foreign Lawyer (Singapore)

Zennon Kapron
Director

Urszula McCormack
Partner

Simon Hawkins
Counsel
Kenneth Hui
Associate

Etelka Bogardi
Partner
Emma De Ronde
Partner

Henri Arslanian
Fintech & Crypto Lead, Asia
Lei Wang
Senior Manager

ASIFMA would like to extend its gratitude to all the individuals and member firms who contributed to the development of this report. We also appreciate the contributions of the digital asset exchanges consulted as part of this project.

asifma
Growing Asia's Markets

asifma
Growing Asia's Markets

UNIT 3603, TOWER 2
LIPPO CENTRE
89 QUEENSWAY
ADMIRALTY
HONG KONG
TEL +852 2531 6500

WWW.ASIFMA.ORG