

# A Global Guide to a Crypto Exchange Regulatory Framework

Gbolahan Badmus

Legal Associate, Paul Usoro & Co, 1668B, Plot 1668B, Oyin Jolayemi Street, Victoria Island, Lagos, Nigeria

## Abstract

The emergence of bitcoin in 2008 led to the growth and widespread use of cryptos and crypto exchanges. Unfortunately, crypto exchanges have been subject to hacks among other problems causing investors to lose billions of dollars. These problems are attributed to a lack of comprehensive regulatory framework for crypto exchanges. To address them, the paper seeks to provide guidelines on core issues that a comprehensive regulatory framework should address such as licences, minimum capital requirements, regulatory security standards, among others, by drawing experiences across various jurisdictions. The paper thereafter concludes by suggesting ways through which such regulation could be properly implemented and implores co-operation from both the exchanges and regulators to ensure regulatory efficiency.

**Keywords:** crypto, regulation, crypto exchange, initial coin offerings.

**DOI:** 10.7176/JLPG/90-02

**Publication date:** October 31<sup>st</sup> 2019

## 1. Exordium: The Rise of Cryptos

Since the publication of the Bitcoin Whitepaper in 2008<sup>1</sup>, cryptos have taken the financial services system by storm. As of 2019, we have about 2,171 cryptos with a market capitalization of about \$173 Billion.<sup>2</sup> This is unsurprising as the birth of cryptos solved the double spending system that characterized the traditional payment system, while improving the speed and ease of payment.<sup>3</sup> Although, cryptos may have been developed as a form of currency, the use of cryptos as an investment tool has also gained popularity. Furthermore, businesses use cryptos as a means of raising funds for project development and realisation through Initial Coin Offerings (“ICO”). In 2017 and 2018, about \$13 Billion was raised using ICOs.<sup>4</sup>

Notwithstanding their adoption, cryptos have also recorded hurdles. The popularity of cryptos birthed numerous platforms where cryptos are exchanged for other cryptos or fiat currencies. A number of these exchanges have been subject to hacks, costing investors billions of dollars. In the ICO space, it has been stated that about 81 percent of ICOs were shams and half of all ICO projects do not last beyond four months. More recently, due to a poor governance structure of a crypto exchange in Canada, about \$150 Million were inaccessible to investors as the password to access them, which was known only to the CEO, became lost upon his death. It is believed that majority of these problems may be solved by providing a comprehensive framework to regulate crypto activities. Therefore, this article seeks to propose a framework towards achieving a comprehensive regulation for crypto exchanges. Additionally, rather than being tied to a particular jurisdiction, this article tends to serve as a global regulatory guide.

## 2. Towards A Comprehensive Regulatory Framework

### 2.1. What are Crypto Exchanges and What Do They Actually Exchange?

In determining the regulatory scope, regulators should be keen on what is classified as a crypto exchange. Crypto exchanges have been defined as a digital marketplace where users can trade and sell cryptos.<sup>5</sup> Some jurisdictions extend the definition to go beyond mere sale and trade. For example, in South Korea, it is defined as 'any person or entity who engages in the business of storage, management, exchange, sale, purchase or brokerage of the virtual currencies (or cryptocurrencies)'.<sup>6</sup> Once an exchange has been properly defined, then the regulations will be automatically applicable. A comprehensive definition will seek to define both the exchange and type of assets being transacted thereon. Generally, crypto exchanges usually trade crypto-to-crypto (e.g. bitcoin to litecoin) or fiat currency-to-crypto or vice versa (e.g. bitcoin to Nigerian Naira); and may also be centralized (exchange control funds) or decentralised (peer-to-peer control funds).

An examination of the South Korean definition above indicates that there may be a limitation on the type of assets a crypto exchange could deal with by restricting them to only “virtual currencies or cryptocurrencies”.

<sup>1</sup> Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008).

<sup>2</sup> Coinmarket Cap, “All Cryptocurrencies” <https://coinmarketcap.com/all/views/all>.

<sup>3</sup> Flamur Bunjaku, Olivera Gjorgieva-Trajkovska, Emilija Miteva Kacarski “Cryptocurrencies – Advantages and Disadvantages” (2017) *Journal of Economics*, 2 (1). ISSN 1857-9973 pp 37-38

<sup>4</sup> Icodata.io, “Funds Raised in 2018” <https://www.icodata.io/stats/2018>; Icodata.io, “Funds Raised in 2017” <https://www.icodata.io/stats/2017>

<sup>5</sup> Olly Jackson “PRIMER: regulating cryptocurrency exchanges”(February 28, 2019) <https://www.iflr.com/Article/3860956/PRIMER-regulating-cryptocurrency-exchanges.html?ArticleId=3860956>

<sup>6</sup> Revised "Anti-Money Laundering Guidelines for Virtual Currency" <http://www.fsc.go.kr/downManager?bbsid=BBS0030&no=127331> (Emphasis mine).

Since a currency is defined to be widely accepted as a medium of exchange, one may wonder what happens where a crypto exchange deals with a crypto that is issued as a security or as a utility token. For a proper understanding, it is important to shed more light on this. During ICOs, issuers may either issue a security (i.e. tokens that represent an underlying financial asset, for example a right to receive dividend or interest payment); payment (i.e. tokens used as a means of payment); or utility token (i.e. tokens designed not as an investment, rather as a tool to access a particular service). These tokens may thereafter be traded on an exchange, depending on its liquidity. A possible effect of this is that where non-cryptocurrencies are traded, the exchange may be regarded as a regulatory free zone. Foreseeing this problem, the South Korean law assigned a broad definition for virtual currencies to include “token or information stored on said token perceived as a means of exchange or of storage of value by a contracting party, and that is transferrable by electronic means.”<sup>1</sup> This definition seems broad enough to extend to all types of cryptos currently in existence. However, regulators are recommended to consistently be on the lookout for new types of cryptos that may seek to wriggle free from any known definition and update such definitions accordingly.

## 2.2. Qualitative Barrier(s) to Entry

Once a crypto exchange has been appropriately defined, a screening process should be put in place before such exchange can begin operation. Therefore, once an exchange seeks to deal in cryptos, it should be required to apply for a licence granting it the powers to trade. Before granting this licence, minimum requirements<sup>2</sup> will have to be fulfilled and maintained throughout the life of the exchange. For example, to operate a crypto exchange in New York or to cater for New York residents, applicants will require a Bitlicence.<sup>3</sup>

While noting the importance of a qualitative barrier, it is recommended that conditions prior to issuing the licence should be firm enough to curtail risks but not onerous to stifle innovation. This is the bane of Bitlicence. It has been critiqued as intrusive and expensive for exchanges to comply with, particularly start-ups.<sup>4</sup> As a result, numerous crypto exchanges have exited New York and ceased activities with New York residents.<sup>5</sup> Responsively, exchanges seemed to have learned to take advantage of legislative arbitrage by moving to more crypto-friendly countries such as Estonia.<sup>6</sup>

## 2.3. Who are those behind the Screen?

In the financial services industry, anonymity is regarded as a villain principally because it could serve as a cover for nefarious activities such as money laundering, terrorism financing, and could even be a catalyst for hacking exchanges etc. Generally, cryptos run on blockchain technology, which favours anonymity. Although, in the real sense, what they mostly offer is pseudonymity, as parties can be traced to their wallet address.<sup>7</sup> However, the use of mixer services and cryptos such as Monero, Zcash, etc. have been able to better achieve anonymity. To reduce regulatory costs in having to trace every wallet address, and to prevent crypto transactions from being a haven for criminal activities, anti-money laundering (“AML”) measures and Know Your Customer (“KYC”) checks are pertinent.

The first challenge might then be – should old laws be interpreted to apply to crypto exchanges, or should new laws be drafted. For instance, in the United States of America (“USA”), the AML regulation that will govern a crypto exchange will be dependent on whether it is a security, commodity, or currency. If it is a security, it will be governed by the Securities and Exchange Commission (“SEC”);<sup>8</sup> a commodity, Commodity Futures and Trading Commission (“CFTC”)<sup>9</sup>; and a currency, U.S. Bank Secrecy Act (“BSA”)<sup>10</sup>. Based on this classification, existing USA AML regulations should cover most traded cryptos.

The problem may arise where a crypto exchange trades in utility tokens. Utility tokens do not readily fit into the above-stated categories and crypto exchanges dealing in them may be exempt from AML regulations. However, utility tokens could be used to launder money. For example, a criminal could use “dirty money” to purchase utility tokens<sup>11</sup> during an ICO or any other means, sell it on an exchange to purchase bitcoin, and

<sup>1</sup> Chan Sik Ahn, “South Korea AML/KYC regulations on cryptocurrency exchanges” (December 11, 2018) <http://www.iflr.com/Article/3848710/South-Korea-AMKCYC-regulations-on-cryptocurrency-exchanges.html>

<sup>2</sup> Some of these minimum requirements will be dealt with under subsequent headings.

<sup>3</sup> Countries like Malta, Cambodia, Estonia etc. also require a license to set up a crypto exchange.

<sup>4</sup> David Adler, “The BitLicense: Regulatory Overreach or Prudent Response?” (March 26, 2019) [https://news.law.fordham.edu/jcfl/2018/03/26/the-bitlicense-regulatory-overreach-or-prudent-response/#\\_edn9](https://news.law.fordham.edu/jcfl/2018/03/26/the-bitlicense-regulatory-overreach-or-prudent-response/#_edn9)

<sup>5</sup> Daniel Roberts, “Behind the “exodus” of bitcoin start-ups from New York” (August 14, 2015) <http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/>

<sup>6</sup> For example, since the introduction of the licensing requirement in 2017, Estonia has issued about 900 licences; while New York’s four year history of the Bitlicence has only recorded 19 licensees.

<sup>7</sup> However, the use of mixer services and cryptos such as Monero, Zcash, etc. have been able to better achieve anonymity.

<sup>8</sup> 15 U.S.C. §§ 78c (a) (4)–(a) (5).

<sup>9</sup> 7 U.S.C. § 1a (31).

<sup>10</sup> Bank Secrecy Act of 1970, as amended by the USA Patriot Act, 31 U.S.C. §§ 5311 et seq.

<sup>11</sup> Although, the amount of tokens purchased will be dependent on its liquidity in the secondary market.

thereafter exchange for fiat money. To compound issues, the CFTC recently tagged cryptos as commodities.<sup>1</sup> Meanwhile, a financial law professor at the University of Edinburgh emphatically stated that cryptos are not commodities.<sup>2</sup> Without being left behind, the SEC has stated that majority of tokens issued during an ICO are securities.<sup>3</sup> What then happens when these tokens are traded on exchanges; will they automatically morph into commodities?

In certain jurisdictions, regulators have simply updated their rules to include AML provisions for cryptos. For example, the Fifth Anti-Money Laundering Directives in the European Union<sup>4</sup>, and the AML Guidelines in South Korea.<sup>5</sup> However, this may not be easily applicable in the US, as there are different AML regimes. To deal with this classification problem, it is advisable that regulators classify cryptos as a new asset class, and develop regulations to cater specifically for its attendant risks. Walking in this direction is Wyoming, a state in the USA, which recently enacted five legislations categorizing cryptos as a new asset class.<sup>6</sup>

In addition, exchanges can take the lead to self-regulate and enforce the performance of KYC checks to achieve transparency.<sup>7</sup> Exchanges could also ban cryptos that guarantee a certain level of anonymity on its platforms, where KYC provisions do not turn out effective.<sup>8</sup> Furthermore, since traditional financial institutions (“FI”)<sup>9</sup> are relevant parties particularly for crypto-to-fiat exchanges, additional AML requirements could be imposed on FIs to report suspicious transactions. Some of these transactions may include:<sup>10</sup>

- recurrent international wire transfers to digital currency exchanges;
- overall inbound and outbound transactional activity that appears excessive for the customer, given their known source(s) of funds;
- businesses transacting through digital currency exchanges in a manner expected of individuals, (this could indicate front, shell, and/or shelf companies);
- non-profit organizations transacting through digital currency exchanges in a manner expected of individuals. This could indicate misappropriation of funds etc.

While enforcing AML regulations for centralised exchanges could be straightforward, as there is a central authority to hold responsible, a big problem for enforcing AML regulations for crypto exchanges is that some are decentralized, making KYC extremely difficult, as there is no central authority to hold responsible. A way to bypass this difficulty is for regulators to tap into the blockchain technology underlying decentralized exchanges to mine data about the transactions continuously, instead of having to ask a centralized exchange. Although, this may be at the risk of a higher transaction cost.

#### 2.4. (Cyber)securing Exchanges

It is important that regulators impose security standards on each platform in order to reduce hacks and protect investors from loss of funds. For example, exchanges could provide a two-factor authentication method for users to log in. Exchanges could also store a major percentage of users’ cryptos in a cold (offline) storage and spread them in different vaults around the world and maintain a certain percentage in hot (online) storage to provide for customers’ liquidity needs. A problem with cold storage manifested earlier this year, when access to the storage was lost after the death of its CEO<sup>11</sup>. A way to fix this problem is that beyond mandating a percentage of users’ cryptos to be held in cold storage, a specific number of high-level staff should have knowledge or access to the password(s). Regulators could also mandate exchanges to place limits on daily withdrawals. However, in situations where a party needs to withdraw above the limit, a higher level of KYC could be further introduced.

Most importantly, apart from setting technical security standards, exchanges and regulators alike should sensitise investors and staff on inculcating best security practices to protect investors’ funds.

As a backup plan, insurance may come in handy. This could take the form of regulators collaborating with insurance companies to create insurance plans, where investors’ funds could be insured up to a particular amount

<sup>1</sup> ETF.com, “Bitcoin Ruled Commodity; Palladium ETF Shines” (October 01, 2018) <https://www.nasdaq.com/article/bitcoin-ruled-commodity-palladium-etf-shines-cm1030552>

<sup>2</sup> Paddy Baker “Bitcoin Is Not A Commodity, Says Expert In Financial Law” (December 24, 2018) <https://cryptobriefing.com/bitcoin-legal-status>

<sup>3</sup> Securities and Exchange Commission Release No. 81207/July 25, 2017: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934.

<sup>4</sup> Directive (EU) 2018/843. See Article 3

<sup>5</sup> Revised “Anti-Money Laundering Guidelines for Virtual Currency” <http://www.fsc.go.kr/downManager?bbsid=BBS0030&no=127331>

<sup>6</sup> Legiscan, “Wyoming House Bill 70 (Prior Session Legislation)” <https://legiscan.com/WY/bill/HB0070/2018>

<sup>7</sup> An example of this is the Japan’s Virtual Currency Exchange Association, which received approval from the Financial Services Authority. Also, Binance, one of the world’s largest crypto exchanges, have announced a partnership IdentityMind to enhance AML/KYC measures

<sup>8</sup> Coincheck recently kicked out Monero, Zcash, Dash and Augur due to the level of anonymity the cryptos confer.

<sup>9</sup> For the purpose of this section, the regulator could expand the definition of FIs to also include third party payment processors to ensure such funds are traced to its intended (crypto) destination.

<sup>10</sup> Joshua Fruth “Crypto-cleansing: strategies to fight digital currency money laundering and sanctions evasion” (February 13, 2018) <https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I>

<sup>11</sup> This has been mentioned earlier in this article.

in cases of unauthorised access due to an act or omission of the exchange. For example, Coinbase maintains an insurance policy that protects users' digital funds from losses that result from a security breach or hack, employee theft or fraudulent transfer.<sup>1</sup>

### 2.5. Minimum Capital Requirement

A minimum capital requirement is relevant for the buoyancy of any business. For example, to ensure the sustainability of commercial banks in Nigeria, the Central Bank of Nigeria set a minimum capital requirement, among others, and this helped in reducing insolvency rate. In the crypto exchange space, a minimum capital requirement would aid exchanges in withstanding insolvency risks, and also attract 'serious' investors, who would seek to ensure that best practices are adhered with in order to, at least, protect their investments.

In Indonesia, the minimum capital requirement is set at an equivalent of \$106 Million; while in countries such as Japan, Malaysia and Philippines, it ranges from \$100 Thousand to \$2 Million.<sup>2</sup> Exchanges in Indonesia, have however, complained that since the industry is still in its infancy, such high requirements may cripple its growth. Hence, in setting capital requirement, regulators should study the industry and provide a requirement that will not only promote investment but also guarantee its sustainability.

### 2.6. Initial Coin Offerings

Generally, ICOs are issued on the issuer's website. Its intersection with crypto exchanges usually occurs when the issued tokens are subsequently listed. In order to regulate the activities of crypto exchanges as it relates to ICOs, regulators should mandate that the information contained in the white paper issued before conducting an ICO is properly verified by independent experts and relevant disclosures should be made. Once this has been done, the tokens may be approved for listing. This step could also be followed even where the tokens will be issued on the exchange as a primary market (i.e. Initial Exchange Offering).

An alternative to the above method will be to provide a "cool-off" period before the tokens are listed on the exchange. The rationale is to provide a period within which the underlying project (requiring the ICO) will start to blossom, thereby revealing its genuineness, and curbing fraudulent ICOs.

### 2.7. Data Privacy

The importance of data privacy as the world becomes more digital goes to underscore the importance of data privacy. On a crypto exchange, there is continuous traffic of personally identifying information and the need to protect same. In this vein, exchanges should take utmost care in safeguarding personal identifiable information that are retained as part of KYC checks and those resulting from customers' transactional activities.

A new regulation may not be required, at least for Europe, as the GDPR<sup>3</sup> seems to have covered this field. However, jurisdictions without data privacy regulations should take steps to enact same, as this would give confidence to customers that their personal data would remain personal.

### 2.8. Fund Managers

Crypto fund managers are licensed persons who invest all or a percentage of their total portfolio in crypto assets. For a fund manager to require a license to operate, s/he must have invested or intend to invest all or part of his or her portfolio in cryptos. Where the manager seeks to invest all portfolio in cryptos, it is clear that a licence will be required; but where it is in part, regulators should set a minimum percentage of crypto investment that a fund manager must hold before being required to apply for a license. In setting this minimum percentage, regulators should also put market fluctuations into consideration, as this may push non-licensees beyond the minimum-crypto investment threshold. Hence, regulators should provide a "grace period" for non-licensees to appropriately liquidate their excess holding.

Fund Managers, as responsible officers, should also be tasked with implementing KYC checks on their clients, and be made to comply with cybersecurity policies, data privacy, and other key areas as stated in previous paragraphs.

## 3. Conclusion: On a Quest for New Beginnings

It is clear that due to the rise and popularity of cryptos in the financial services sector, a comprehensive regulatory framework is vital to govern this space. Although, not exhaustive,<sup>4</sup> the article has sought to list key areas which regulators should put into consideration while drafting a comprehensive crypto regulation. While

<sup>1</sup> Coinbase, "Digital Currency Balances" <https://www.coinbase.com/legal/insurance>

<sup>2</sup> Karry Lai, "Indonesian crypto firms struggle with new capital requirements" (March 20, 2019) <https://www.iflr.com/Article/3864875/Indonesian-crypto-firms-struggle-with-new-capital-requirements.html?ArticleId=3864875>

<sup>3</sup> The General Data Protection Regulation 2016/679

<sup>4</sup> Other areas regulators should also pay attention to will be setting corporate governance standards and prohibiting general market abusive practices (e.g. pump-and-dump schemes, price manipulation etc.).

existing laws may, to an extent, cater for certain areas such as AML and data privacy, it is important to draft new laws, as existing laws do not appropriately accommodate new technology. For example, new areas such as authentication, cold or hot storage, minimum capital requirements, amongst others, will require new laws.

When it comes to technology, regulators are generally reactive, as technology tends to move at a faster pace. In order to catch up, regulators may run the risk of overregulating as they may have failed to fully understand this new technology, thus crippling innovation. Under-regulating or non-regulating is also not an option as it could create regulatory uncertainties and loopholes; while an outright ban will effectively curtail risks at the altar of sacrificing innovation. Therefore, it is advisable that before issuing laws, regulators should create a regulatory sandbox, whereby they can understand how these exchanges operate and how their underlying technology functions. Furthermore, regulators should also seek input from stakeholders so that all necessary steps will be taken to achieve a beneficial and comprehensive regulation. Another approach for regulators would be to consider co-regulation whereby they issue general guidelines for exchanges to implement. An advantage of this would be the flexibility in implementing these guidelines. However, pending the issuance of a comprehensive regulation or guidelines, exchanges on their own part could create internal policies that will prescribe best practices.

Finally, in drafting this regulation, regulators should ensure that they effectively curb risks (such as protecting investors' funds) and create a platform for the growth and constructive use of new technologies.

## References

- Chan Sik Ahn, (2018) "South Korea AML/KYC regulations on cryptocurrency exchanges" (December 11, 2018) <http://www.iflr.com/Article/3848710/South-Korea-AMKCYC-regulations-on-cryptocurrency-exchanges.html>
- David Adler, (2019) "The BitLicense: Regulatory Overreach or Prudent Response?" (March 26, 2019) [https://news.law.fordham.edu/jcfl/2018/03/26/the-bitlicense-regulatory-overreach-or-prudent-response/#\\_edn9](https://news.law.fordham.edu/jcfl/2018/03/26/the-bitlicense-regulatory-overreach-or-prudent-response/#_edn9)
- Doug Alexander, (2019) "Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins" (February 4, 2019) <https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem>
- Flamur Bunjaku et. al. (2017) "Cryptocurrencies – Advantages and Disadvantages" (2017) *Journal of Economics*, 2 (1). ISSN 1857-9973.
- Hugo Benedetti and Leonard Kostovetsky, (2018) "Digital Tulips? Returns to Investors in Initial Coin Offerings" (2018) <https://ssrn.com/abstract=3182169>
- Joshua Fruth (2018) "Crypto-cleansing: strategies to fight digital currency money laundering and sanctions evasion" (February 13, 2018) <https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I>
- Karry Lai (2019), "Indonesian crypto firms struggle with new capital requirements" (March 20, 2019) <https://www.iflr.com/Article/3864875/Indonesian-crypto-firms-struggle-with-new-capital-requirements.html?ArticleId=3864875>
- Olly Jackson (2019), "PRIMER: regulating cryptocurrency exchanges"(February 28, 2019) <https://www.iflr.com/Article/3860956/PRIMER-regulating-cryptocurrency-exchanges.html?ArticleId=3860956>
- Revised "Anti-Money Laundering Guidelines for Virtual Currency" <http://www.fsc.go.kr/downManager?bbsid=BBS0030&no=127331>.
- Satoshi Nakamoto (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008).
- Sherwin Dowlatabadi (2018), "ICO Quality: Development & Trading" <https://medium.com/satis-group/ico-quality-development-trading-e4fef28df04f> (March 21, 2018).