

# **LAWS428 Research and Writing:**

## **Regulatory Approaches to Crime in the Digital Art Trade**

**Word Count: 3006**

## **Introduction**

The development of blockchain technologies and the subsequent creation of Non-Fungible Tokens (NFTs) over the last decade pose some of the most important legal challenges for regulators in the digital age. One specific area in which legal challenges have become immediately apparent is in the digital art industry, within which NFTs are bought and sold at eye watering prices on the blockchain. Commentators have already identified the capacity for digital art to facilitate and conceal criminal activity. Regulation of the industry is impeded by the anonymity and decentralised nature of the digital art world which could open the doors for crime and money laundering on an unprecedented scale. In this paper I will discuss some specific challenges for regulators, some of the responses emerging globally, and potential regulatory approaches in this area.

## **What is an NFT?**

NFTs, or non-fungible tokens, are unique cryptoassets which are unable to be exchanged or substituted. The tokens constitute a digital signature backed by blockchain technology which proves ownership of something, like a piece of digital art. The concept of purchasing artwork which can never be touched or hung on a wall is strange, yet earlier this year Beeple sold an NFT for \$69 million US dollars in the first digital art sale to be backed by a major auction house. Cartoon cats and memes have similarly amassed prices in the millions. The allure of digital art is a puzzling phenomenon as demand continues to drive their value upwards. NFTs trading occurs on blockchain platforms such as Ethereum, and is governed by ‘smart contracts’. Smart contracts are automated pieces of code which self-execute upon the satisfaction of terms and conditions, removing the need for an intermediary party in transactions. As is the case for any blockchain, data about the transactions is stored publicly on nodes (or computers operated by users), however it is impossible to link the signatures appearing on the ledger with an individual user. While this makes NFT transactions secure from hackers, it also enables purchasers to obscure their transaction histories and makes tracing funds incredibly difficult. Laundering illegitimate funds thus becomes easier and more difficult to detect. Because of the growth of the digital art world via NFTs, digital art has been the focus in conversations surrounding fraud, money laundering, and the financing of crime.

## **Challenges**

The challenges for regulators of NFT technology are extensive and diverse. In terms of the potential for digital art NFTs to become mechanisms for financing crime and laundering money, the key concerns are the consequences of decentralisation and anonymity.

### *1. Decentralisation*

One of the main revolutionary features of blockchain technology is the fact it is a decentralised peer-to-peer system. Rather than empowering an authority with the control of the system, the users drive the market, each transaction occurs between users alone and is automated by a smart contract. The most obvious legal consequence of decentralisation is the lack of jurisdictional boundaries which significantly reduces governments’ regulatory capacity. Cryptocurrencies are alternatives to government-backed currencies and operate independently of banks. The system cannot easily be regulated by our existing law as it is underpinned by a financial system operating on national currency.

Globally, cryptocurrency has had diverse treatment. Countries have taken varied stances in terms of the perceived legitimacy of the system and the use of cryptocurrencies as legal tender. In some countries such

as China, banks and other institutions are prohibited from dealing in Bitcoin and it is not accepted as currency.<sup>1</sup> Conversely, El Salvador recently became the first country to make Bitcoin an official national currency.<sup>2</sup> With this in mind, the likelihood of any form of homogenous international approach or global regulatory body to overcome the challenges posed by decentralisation is slim at best. Regulation will need to occur on a national level and will need to function in response to the unique features of cryptocurrency and NFT exchange. The challenge from the perspective of crime prevention and prosecution is attempting to bring NFT exchanges within the scope of the existing criminal law. Jurisdictional pinpoints are necessary along the chain of each transaction, so that prosecution of criminal activity could occur in the locations where the NFT issuers, investors, or purchasers involved performed the transaction. Holding users liable is also predicated upon being able to identify them.

## 2. *Anonymity*

Money laundering and the financing of crime has long been a concern in the law, and in recent years the legislation surrounding Anti Money Laundering (AML) requirements for businesses and financial institutions has been given considerable attention. An obvious solution to the problem of identifying parties or nodes involved in NFT transactions is to apply AML requirements to transactions on blockchains. While transaction histories using cryptocurrency are stored on a public ledger, connecting the signature on the ledger with an individual is impossible and it is included rather for the purpose of proving the validity of each transaction. Tracing the IP addresses of the computers used is also very difficult.<sup>3</sup> As an alternative to identifying individual users, some countries have adopted an AML-style approach which imposes requirements upon the private companies providing platforms for cryptocurrency exchange. These requirements generally include ‘Know Your Client’ (KYC) protocols and make ongoing monitoring of users mandatory. These approaches are not without their flaws. A central pillar of cryptocurrency and where it derives much of its allure is that it is decentralised and anonymous in the name of protecting customers. Users have pushed back against compliance with regulations which will remove their anonymity, particularly given that many exchanges do not have secure systems of data storage adequate to safeguard users’ information.<sup>4</sup> The KYC approach, in focussing on regulating companies and holding them liable, creates a system where liability bypasses the parties actually conducting illegal activity.

## **Responses**

Some countries have established guidelines and programs to deal with the continued popularity of cryptocurrency exchanges and cryptoasset markets, yet regulations for the use and trade of NFTs are yet to be established. Despite this, an overview of the current global regulatory responses is useful in order to identify strengths and potential flaws, and may provide insight into how these regulations could be extended to encompass NFTs and digital art in the future. Most regulators so far have accepted the benefits

---

<sup>1</sup> Allison M. Lovell “Avoiding Liability: Changing the Regulatory Structure of Cryptocurrencies to Better Ensure Legal Use” (2019) 104 ILR 927 at 944.

<sup>2</sup> Nelson Renteria and Anthony Esposito “El Salvador's world-first adoption of bitcoin endures bumpy first day” (September 8 2021) Reuters <<https://www.reuters.com/business/finance/el-salvador-leads-world-into-cryptocurrency-bitcoin-legal-tender-2021-09-07>>

<sup>3</sup> Above n 1 at 934.

<sup>4</sup> “What is KYC, and How Is it Increasingly Important for Crypto?” (June 18 2021) Binance <<https://www.binance.com/en/blog/421499824684902130/%E2%80%8Bwhat-is-kyc-and-how-is-it-increasingly-important-for-crypto>>

of allowing technological innovation to continue, therefore the responses particularly of Western nations have generally been moderate.

### 1. EU

In response to cryptocurrencies generally, the European Union has taken the approach of extending existing legal frameworks to encompass cryptocurrency. In 2018 Europe included “virtual currency exchanges” in its AML regulations in an attempt to increase the obligations upon operators of exchanges to undertake due diligence on users and record users’ personal information.<sup>5</sup> This was a tentative first step, and in 2020 the European Commission adopted the Markets in Cryptoassets Regulation proposal (MiCA) which is designed as a complete regulatory package to automatically apply in all EU member states.<sup>6</sup> MiCA is stated to “ensure that the EU embraces the digital revolution”<sup>7</sup> and provide certainty about the regulatory treatment of cryptocurrencies and derivative technologies in the European Union.<sup>8</sup> MiCA focusses on regulating the offering of cryptoassets to the public and their admission onto trading platforms, creating a licensing system for Cryptoasset Service Providers (CASPs) based on the kind of asset they are trading in. The proposal differentiates between asset- referenced tokens, e-money tokens, and ‘other’ cryptoassets, and establishes different rules applicable to each. Assets defined as ‘other cryptoassets’ are exempt from specific licensing obligations, and those which are ‘unique and not fungible with other cryptoassets’ are also exempt from the requirement to report on public offerings. NFTs seem likely to be exempt as types of ‘other cryptoassets’ under these proposed regulations, although further guidance from the EU Blockchain Forum states “MiCAR is not intended to apply to crypto assets that are unique and not fungible with other crypto assets, including digital art and collectibles whose value is attributable to the unique characteristics of each crypto asset.”<sup>9</sup> The main practical effect of the MiCA proposal is the requirement that CASPs be authorised to operate and have a registered office within an EU member state before they are entitled to provide cryptoasset services, however the lack of provisions for NFTs would create a significant regulatory gap for companies exclusively dealing in NFTs.<sup>10</sup>

### 2. UK

The UK Financial Conduct Authority (FCA) has adopted a similar approach, requiring authorisation for certain activities. The FCA guidance establishes three categories of cryptoasset; e-money tokens, security tokens, and unregulated tokens. Security tokens are analogous to specific investments (as provided for in existing financial legislation), whereas unregulated tokens are those used for purchasing services or primarily for the purpose of exchange.<sup>11</sup> NFTs are likely to fall within the latter category, but depending on its nature an NFT would have the ability to belong to anyone of the three categories. Regulating them would therefore need to happen on an individual basis, looking at the particular circumstances and nature

---

<sup>5</sup> Pascal Bine, Elizabeth Robertson, Simon Toms, Sidne Koenigsberg, Nadine Kari, Abigail B. Reeves, and Gregory Vianesi “Regulatory Approaches to Nonfungible Tokens in the EU and UK” (15 June 2021) Skadden <[https://www.skadden.com/en/insights/publications/2021/06/regulatory-approaches-to-nonfungible-tokens?fbclid=IwAR03\\_9Zson3a\\_eRhCZiwAn8ySZMZJ-5qE2KIGCWauUsNxDPZmiZleqGnQno](https://www.skadden.com/en/insights/publications/2021/06/regulatory-approaches-to-nonfungible-tokens?fbclid=IwAR03_9Zson3a_eRhCZiwAn8ySZMZJ-5qE2KIGCWauUsNxDPZmiZleqGnQno)>.

<sup>6</sup> Above n 5.

<sup>7</sup> EU Blockchain Observatory Forum *NFT – Legal Token Classification* (EUBOF 2021).

<sup>8</sup> Proposed Council Regulation of 24 September 2020 For a Regulation of the European Parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.

<sup>9</sup> Above n 7 at 4.

<sup>10</sup> Above n 5.

<sup>11</sup> Above n 5.

of the token in each case. In terms of AML provisions, the FCA will undergo a qualitative assessment of managers of cryptoasset businesses to ensure they are ‘fit and proper’ to be operating, and unlike the MiCA Proposal, this system could apply to businesses dealing exclusively with NFTs.<sup>12</sup>

### 3. USA

In the U.S, the main regulatory advance has been to impose mandatory Know Your Client (KYC) requirements for most cryptocurrency exchanges, backed by the threat of liability for companies failing to perform their due diligence under the Patriot Act.<sup>13</sup> The U.S. Financial Crimes Enforcement Network (FinCEN) has also proposed a system whereby banks and financial institutions verify the identities of those holding digital asset wallets. The banks would be responsible for monitoring users and reporting on transactions worth over US\$3,000.<sup>14</sup> This approach demonstrates treatment of cryptocurrency as money, whereas other regulatory bodies within the US have elected to define virtual currency as a ‘commodity’ (CFTC) or as ‘property’ (IRS).<sup>15</sup> On the whole, however, the federal government and financial institutions have taken a neutral approach to blockchain technology and have focused resources on taskforces and study teams to receive and formulate advice on appropriate regulatory responses.<sup>16</sup>

### 4. Other

Other countries have taken more extreme approaches; in China the government has been hostile towards allowing cryptocurrency exchanges to develop and have brought in increasingly stringent regulations making it difficult and unprofitable to engage in virtual currency markets. On the other end of the spectrum, El Salvador has embraced Bitcoin in an effort to rebuild a struggling economy. The global anti-money laundering organisation FATF (Financial Action Task Force) released guidance in March to deal with decentralised finance (DeFi) platforms. The guidance essentially proposes classifying any DeFi entities running their programs for profit as ‘virtual asset service providers’ (VASPs), which are made subject to potentially onerous AML responsibilities. The proposal has met resistance. Many feel it is an example of regulatory overreach and is out of touch with the realities of the DeFi market.<sup>17</sup> In New Zealand, IRD treats cryptoassets as property and AML requirements apply to those operating cryptocurrency services. Aside from these, regulations in New Zealand are scarce.<sup>18</sup> Around the globe, regulations thus far have been tentative and vague as concerns about limiting positive technological advances are thought to outweigh the perceived risks. Unfortunately this may not be the case for much longer- the perks of cryptocurrency and NFT exchanges for criminals are conspicuous and examples of

---

<sup>12</sup> Above n 5.

<sup>13</sup> Above n 4.

<sup>14</sup> Jon Southurst “FinCEN proposes new KYC rules for ‘non-hosted’ wallets” (December 21 2020) Coingeek <<https://coingeek.com/fincen-proposes-new-kyc-rules-for-non-hosted-wallets>>.

<sup>15</sup> Luke Parker “Bitcoin is Officially a Currency, Property, Money, and Now a Commodity” (September 18 2015) Brave New Coin <<https://bravenewcoin.com/insights/bitcoin-is-officially-a-commodity-first-cftc-ruling-against-a-bitcoin-options-trading-platform>>.

<sup>16</sup> Javier Sebastian “Blockchain in financial services: Regulatory landscape and future challenges for its commercial application” *BBVA Research* (online ed, Madrid, December 13 2016) at 9.

<sup>17</sup> Erin Genç “Anti-Money Laundering Rules Targeting DeFi, NFTs Could Be Fatal, Analysts Warn” (March 24 2021) Decrypt <<https://decrypt.co/62600/fatf-money-laundering-rules-defi-nfts>>.

<sup>18</sup> Emma Lindblom “Is Cryptocurrency Legal In New Zealand?” (February 10 2021) Legalvision <<https://legalvision.co.nz/e-commerce/cryptocurrency-legal>>.

petty fraud in the digital art scene have already begun to emerge.<sup>19</sup> The need for effective regulation particularly of NFTs is becoming readily apparent.

### **Potential Regulatory Approaches**

There are endless possibilities for regulatory approaches to NFTs and digital art, all of them inevitably requiring an element of compromise. Here I will discuss the potential for combining bespoke and pre-existing legal frameworks to limit the need for ongoing amendments and legislative overhaul on behalf of regulatory bodies.

#### *1. Crypto-Exceptionalism*

An overarching consideration for regulators is whether or not to bring virtual currency and NFT exchanges within the boundaries of existing domestic law. The alternative is to draft a bespoke system which operates parallel to existing legislative frameworks. A certain level of what Shane Greenstein calls “internet exceptionalism” must be accepted in relation to crypto-assets and the law. Where Greenstein argues that overly emphasising the Internet’s unique features in a regulatory setting is wrong, David Harvey contends that “in some cases the technologies of the digital paradigm are so different from those preceding that the validity of those rules in the context of the new technologies must be re-examined.”<sup>20</sup> The fact the marketplace on which NFTs are bought and sold is embedded within an entirely separate network, and assets are paid for and exchanged using cryptocurrency means our existing laws which cater to a jurisdictional, gold standard system are no longer entirely ‘valid’.

Applying existing AML provisions to deal with digital art NFTs is possible under UK and EU law, and might seem like a simpler method of flagging suspicious transactions than creating an entirely new system. Transactions involving artwork worth 10,000 euros or more are already subject to specific AML measures, and while NFTs are not specifically referenced, the term ‘works of art’ could feasibly extend to NFTs.<sup>21</sup> This simple solution does not deal with the fact that enforceability of AML compliance against anonymous financial service providers is difficult. For example, SushiSwap is a DeFi platform operating anonymously. The developer is unknown as is the jurisdiction where they operate.<sup>22</sup> Against this company the threat of liability is essentially empty.

On the other hand, creating some form of novel system to regulate cryptocurrency and crimes is challenging. The industry experiences continual modification, as new uses for blockchain technology and applications of the NFT concept emerge daily. A system which targets the current risks in a specific way faces the inevitable problem of quickly becoming outdated, whereas broad and vague parameters may fail to properly address concerns. Defining NFTs is a difficult task of itself, as there is potential for the technology to be developed in a way that avoids restrictions. Moreover, imposing liability on exchange platforms (by using AML provisions) misses the true objective of identifying and holding criminals to account, however the anonymity

---

<sup>19</sup> Jacklin Kwan “An artist died. Then thieves made NFTs of her work” (July 28 2021) Wired <<https://www.wired.co.uk/article/nft-fraud-qinni-art>>.

<sup>20</sup> David Harvey *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (1<sup>st</sup> ed, Hart Publishing, Portland OR, 2017) at 1.

<sup>21</sup> Above n 5.

<sup>22</sup> Above n 17.

problem is an important one impeding their identification. Regulations will need to weigh all these concerns against one another in formulating appropriate measures.

## 2. *A Potential Hybrid System of Regulation*

While the law might not be capable of removing layers of anonymity in blockchains, or directly regulating the network, it is capable of regulating people and the market upon which NFT exchanges rely. An ideal regulatory system will be one that requires minimal amendment to existing law, imposes minimal restrictions on development, and does not overly burden law enforcement. Regulators should focus on the points at which they have access or influence. For example, De Filippi and Wright suggest applying legal or financial pressure upon users in order to incentivise interaction with cryptocurrency exchanges and NFT traders who are cooperative with AML obligations and law enforcement. Such pressure could also be used to penalise conscious efforts to engage with illegal platforms.<sup>23</sup>

Regulators could also capitalise on the peer-to-peer system. Historically, money laundering involves the process of filtering funds through a line of intermediaries, goods, and banks. While these transactions are more traceable through the existing technology and regulatory frameworks, doing so is time consuming and laborious. Where NFTs are more reticent, they are also simpler in nature. No banks or middle men are involved; the exchange is a direct transfer between vendor and purchaser, governed and instigated by a smart contract. If that exchange were able to be registered in some way and the parties identifiable, the allure of the NFT art market for criminals would be significantly diminished. One potential method of doing so would be to engage with the Internet's existing IP protocol which supports blockchains. Internet service providers (ISPs) are capable of identifying IP addresses linked to blockchains, which are themselves transparent records of transactions. This could be used as a measure to block or penalise activity with non-compliant platforms.<sup>24</sup> We have seen from its use in China that ISP monitoring is effective, however there are moral and political objections to empowering the state to take on an invasive 'watchdog' role.

Despite this concern, utilising coercive methods might be a necessary approach to deal with money laundering and financing of crime, and it could be argued stringent measures are necessary given the importance of this object. Once the initial problems of anonymity and traceability are dealt with, a simple licensing system could be put in place which registers NFT transactions and changes of ownership just like we do with vehicles. By registering transactions, the existing financial law framework can be applied to the NFT art trade and suspicious transactions can be dealt with alongside financial crimes involving national currency. The benefit of this system is that it focuses on the core of the issue, being AML compliance, and simply seeks to block usage of hostile platforms. It does not require extensive legislative overhaul, and there is considerable room within the framework for technological development to continue.

## **Conclusion**

Approaching regulation of a technology such as NFTs is a complex task. A large obstacle for regulators is the desire to maintain the discretion and decentralised nature of blockchain technology itself, as these

---

<sup>23</sup> Primavera De Filippi and Aaron Wright *Blockchain and the Law: The rule of code* (1<sup>st</sup> ed, Harvard University Press, Cambridge, Massachusetts; London, England, 2018) at 176.

<sup>24</sup> Above n 23 at 177.

factors are considered its primary benefits. The capacity for the digital art NFT trade to become a hotbed of criminal activity cannot be ignored, however, therefore certain features must be compromised for the greater purpose of protecting consumers and preventing crime. A moderate regulatory tilt is preferable in the early stages of NFT development as this will leave room for the yet unknown consequences of the trade to come to light, however this approach might soon change as we learn more about the technology. Early attempts at regulation around the world show a positive trend towards cryptocurrency and NFTs, and a desire to allow the market to grow organically. Time will tell whether governments continue to be willing to accept both the risks and the rewards which come with such a passive approach.