lavery Lawyers

Crypto asset works of art and non-fungible token (NFT) investments: Be careful!

June 28, 2021

Author

Gabrielle Mathieu

Senior Associate

With the collaboration of

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Jean-Sébastien Desroches

Partner, Lawyer

On March 11, 2021, Christie's auction house made a landmark sale by auctioning off an entirely digital artwork by the artist Beeple, a $69 million transaction in Ether, a cryptocurrency.[1] In doing so, the famous auction house put non-fungible tokens ("NFT"), the product of a decentralized blockchain, in the spotlight. While many extol the benefits of such crypto asset technology, there are also significant risks associated with it,[2] requiring greater vigilance when dealing with any investment or transaction involving NFTs.

What is an NFT?

The distinction between fungible and non-fungible assets is not new. Prior to the invention of blockchain, the distinction was used to differentiate assets based on their availability, fungible assets being highly available and non-fungible assets, scarce. Thus, a fungible asset can easily be replaced by an equivalent asset with the same market value. The best example is money, whether it be coins, notes, deposit money or digital money, such as Bitcoin. On the contrary, a non-fungible asset is unique and irreplaceable. As such, works of art are non-fungible assets in that they are either unique or very few copies of them exist. Their value is a result of their authenticity and provenance, among other things.

NFTs are crypto assets associated with blockchain technology that replicate the phenomenon of scarcity. Each NFT is associated with a unique identifier to ensure traceability. In addition to the art market, online, NFTs have been associated with the collection of virtual items, such as sports cards and other memorabilia and collectibles, including the first tweet ever written.[3] NFTs can also be associated with tangible goods, in which case they can be used to track exchanges and transactions related to such goods. In 2019, Ernst & Young developed a system of unique digital identifiers for a client to track and manage its collection of fine wines.[4] Many projects rely on cryptocurrencies, such as Ether, to create NFTs. This type of cryptocurrency is programmable and allows for metadata to be embedded through a code that becomes the key to tracking assets, such as works of art or other valuables.

What are the risks associated with NFTs?

Although many praise the benefits of NFTs, in particular the increased traceability of the origin of goods exchanged through digital transactions, it has become clear that the speculative bubble of the past few weeks has, contrary to expectations, resulted in new opportunities for fraud and abuse of the rights associated with works exchanged online.

An unregulated market?

While there is currently no legislative framework that specifically regulates crypto asset transactions, NFT buyers and sellers are still subject to the laws and regulations currently governing the distribution of financial products and services[5], the securities laws[6], the *Money-Services Business Act*[7] and the tax laws[8].

Is an NFT a security?

In January 2020, the Canadian Securities Administrators (CSA) identified crypto asset “commodities” as assets that may be subject to securities laws and regulations. Thus, platforms that manage and host NFTs on behalf of their users engage in activities that are governed by the laws that apply to securities trading, as long as they retain possession or control of NFTs.

On the contrary, a platform will not be subject to regulatory oversight if:

1. “the underlying crypto asset itself is not a security or derivative; and
2. the contract or instrument for the purchase, sale or delivery of a crypto asset
    results in an obligation to make immediate delivery of the crypto asset, and
    is settled by the immediate delivery of the crypto asset to the Platform’s
    user according to the Platform’s typical commercial practice.”[9]

Fraud[10]

NFTs don’t protect collectors and investors from fraud and theft. Among the documented risks, there are fake websites robbing investors of their cryptocurrencies, thefts and/or disappearances of NFTs hosted on platforms, and copyright and trademark infringement.

Theft and disappearance of NFT assets

As some Nifty Gateway users unfortunately learned the hard way in late March, crypto asset platforms are not inherently immune to the hacking and theft of personal data associated with accounts, including credit card information. With the hacking of many Nifty Gateway accounts, some users have been robbed of their entire NFT collection.[11] NFTs are designed to prevent a transaction that has been concluded between two parties from being reversed. Once the transfer of the NFT to another account has been initiated, the user, or a third party such as a bank, cannot reverse the transaction. Cybercrime targeting crypto assets is not in its infancy—similar schemes have been seen in thefts of the cryptocurrency Ether.

Copyright infringement and theft of artwork images

The use of NFTs makes it possible to identify three types of problems that could lead to property right and copyright infringement:

> It is possible to create more than one NFT for the same work of art or collectible, thus generating separate chains of ownership.
> NFTs can be created for works that already exist and are not owned by the person marketing them. There are no mechanisms to verify copyrights and property rights associated with transacted NFTs. This creates false chains of ownership.
> The authenticity of the original depends too heavily on URLs that are vulnerable and could eventually disappear.[12]

For the time being, these problems have yet to be addressed by both the various platforms and the other parties involved in NFT transactions, including art galleries. Thus, the risks are borne solely by the buyer. This situation calls for increased accountability for platforms and others involved in transactions. The authenticity of the NFTs traded must be verified, as should the identity of the parties involved in a transaction.

Money laundering and proceeds of crime

In September 2020, the Financial Action Task Force (FATF)[13] published a report regarding the main risks associated with virtual assets and with platforms offering services relating to such virtual assets. In particular, FATF pointed out that money laundering and other types of illicit activity financing are facilitated by virtual assets, which are more conducive to rapid cross-border transactions in decentralized markets that are not regulated by national authorities;[14] that is, the online marketplaces where cryptocurrencies and decentralized assets are traded on blockchains.

Among other things, FATF pointed to the anonymity of the parties to transactions as a factor that increases risk.

Considering all the risks associated with NFTs, we recommend taking the utmost precaution before investing in this category of crypto assets. In fact, on April 23, 2021, the Autorité des marchés financiers reiterated its warning about the "inordinately high risks" associated with investments involving cryptocurrencies and crypto assets.[15]

The best practices to implement prior to any transactions are: obtaining evidence identifying the party you are transacting with, if possible, safeguarding your crypto assets yourself, and checking with regulatory bodies to ensure that the platform on which the exchange will take place is compliant with applicable laws and regulations regarding the issuance of securities and derivatives.

---

1. https://onlineonly.christies.com/s/beeple-first-5000-days/lots/2020
2. On April 23, 2021, the Autorité des marchés financiers reiterated its warnings about issuing tokens and investing in crypto assets. https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/amf-warns-about-the-risks-associated-with-crypto-assets
3. https://www.reuters.com/article/us-twitter-dorsey-nft-idUSKBN2BE2KJ

4. https://www.ey.com/en_gl/news/2019/08/ey-helps-wiv-technology-accelerate-fine-wine-investing-with-blockchain
5. *Act respecting the regulation of the financial sector*, CQLR, c. E-6.1; *Act respecting the distribution of financial products and services*, CQLR, c. D-9.2.
6. *Securities Act*, CQLR., c. V-1.1; see also the regulatory sandbox produced by the CSA: https://www.securities-administrators.ca/industry_resources.aspx?ID=1715&LangType=1033
7. CQLR, c. E-12.000001
8. https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html; https://www.revenuquebec.ca/en/fair-for-all/helping-you-meet-your-obligations/virtual-currency/reporting-virtual-currency-income/
9. https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2020/2020janv16-21-327-avis-acvm-en.pdf
10. https://www.telegraph.co.uk/technology/2021/03/15/crypto-art-market-infiltrated-fakes-thieves-scammers/
11. https://www.coindesk.com/nifty-gateway-nft-hack-lessons; https://news.artnet.com/opinion/nifty-gateway-nft-hack-gray-market-1953549
12. https://blog.malwarebytes.com/explained/2021/03/nfts-explained-daylight-robbery-on-the-blockchain/
13. FATF is an independent international body that assesses the risks associated with money laundering and the financing of both terrorist activities and the proliferation of weapons of mass destruction.
14. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf, p. 1.
15. https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/amf-warns-about-the-risks-associated-with-crypto-assets