PriMera Scientific Engineering
Volume 8 Issue 4 April 2026
ISSN: 2834-2550

NFTs as Instruments of Investigation and Sources of Novel Cybercrimes

Type: Comprehensive Review
Received: November 17, 2025
Published: April 02, 2026

Citation:
Shuq Hussein. "NFTs as Instruments of Investigation and Sources of Novel Cybercrimes". PriMera Scientific Engineering 8.4 (2026): 38-47.

Shuq Hussein*

Department of Law, Edinburgh Law School, UAE

***Corresponding Author:** Shuq Hussein, Department of Law, Edinburgh Law School, UAE.

Introduction

In March 2021, a digital artwork titled Every day: The First 5000 Days sold for $.9 million on Christie's auction site. The question is, what made it special? Spicailly, it was not a physical canvas, but it is a Non-Fungible Token (NFT), a unique digital asset recorded on the blockchain platform. Just 2 years prior, the NFT trade volume was around $ 90 million. In 2022, that number had grown to $17 billion, according to one report by NFT marketplace OpenSea [1].

This meteoric expansion was fuelled by cultural mania, digital scarcity, and speculation. Yet as NFTs amazed the art community and crypto investors, they also caught the interest of another crowd—cybercriminals.

As with any powerful technology, NFTs can be used for better or worse. On the positive side, their open, traceable environment gives law enforcement a new tool to trace illicit money flows. On the negative side, their decentralized, pseudonymous environment creates new channels for fraud, laundering, and evasion.

Can NFTs be employed as a weapon against cybercrime, or are they another clever way for criminals to exploit? While courts and investigators try to keep up with this cyber frontier, they have to wrestle with the implications of gathering evidence, jurisdiction, and the valuation and proprietorship of the things in cyberspace itself.

NFTs as a new type of crime on the blockchain

In recent years, NFTs (non-fungible tokens) have seen a wave of popularity, making digital art and collectibles assets to the tune of billions of dollars. But while there has been this gold rush, NFTs have also made it easy to commit cybercrime, and therefore now, aside from criminals betting on them, they are also being used as tools for money laundering and concealing ill-gotten funds [2].

NFTs can be used by criminals to cover up and launder the origin of stolen money or funds through apparently innocuous transactions, with the help of decentralized and anonymity blockchain technology features. The criminal application of NFTs is of interest to regulators, who now view them as a financial offense in a different perspective compared to merely digital assets [3].

Money laundering by using the NFTs

NFTs have proven to be a valuable new tool in the money launderer's toolkit due to how they replicate the traditional art market, especially in terms of value subjectivity, security, and lack of regulation [4]. The explosive growth in the value of the NFT market and the wildly volatile price of frequently not-good digital art are warning signs. However, it is hard to battle on a legal front due to the subjective and speculative nature of digital art value. NFTs are appealing because they offer anonymity, so individuals can move vast sums of money without anyone raising attention. Also, the NFTs are easily justified to have artistic value by criminals so that the true motive behind the trade is unknown, and dirty money is laundered into seemingly clean profit [5].

One of the most common money laundering methods with NFTs is wash trading, where a launderer creates multiple crypto wallets to buy and sell an NFT they own to themselves. This manipulatively inflates the price of the NFTs, giving the impression of market value, and the criminal money is successfully laundered once the NFT is sold again at the manipulated price to either a clean wallet or a third party. In one study published in 2022, over 260 individuals engaged in some of this monopolistic activity were found to have collected $8.2 million in suspicious profits. This strategy makes it very difficult to trace the real sources of money, as the financial transaction history is clear as legal on public blockchain ledgers. At the same time, it's a self-orchestrated cycle to launder dirty money as clean income [6].

Using the NFTs in Money laundering by some Strategies of hiding the transaction

The NFTs can be applied to each of the money laundering strategies as follows:

Decentralized finance strategies

This strategy allows the users to transact without asked them to identify verification, in NFTs allowed the criminal can mint abasic pieas of digital art as an NFTs then purchase it using illicit money from an anonymous wallet, after that the criminals they resell the NFT to themselves through another wallet, as aresult cerating the appearance of legal digital transaction, so this alloweas the criminal to clean the sources of money by converting it in to profit from the NFT sales [7].

Peel chain strategy

This strategy involves breaking large crypto transactions into many smaller ones to avoid detection. In the money laundries, the NFT mints many low-value NFTs and trades them frequently across multiple wallets in small amounts, so this micro-transaction blends into regular NFT trading activity. Regular NFT trading activity, as a result, makes it hard to detect. For example, 100 ETH can be laundered through 200 NFT trades, each for 0.5 ETH [8].

Chain Hopping Strategy

The chain-hopping strategy aims to switch between two different blockchains to obscure the transaction trail. For example, a criminal can mint an NFT on Ethereum, bridge it to Binance Smart Chain, and then sell it there. Moving the NFT across multiple chains makes it more difficult to trace the source of money [9].

Mixer's strategies

The mixers' strategy works on a scrambled transaction history, breaking the on-chain link between sender and receiver. The launderer uses the mixed crypto to purchase an NFT, and after that, they resell it to a clean wallet or on a different platform. While the purchase originated from mixed money and was transferred through anonymized wallets, the origin of the money becomes obscured [10].

NFT as a new tool to trace illicit money flows

NFT is one of the cryptocurrencies held and traded on the blockchain, and all transactions are recorded and available to the public. This makes it easy to trace the history of who bought or sold the NFT, the price, the owner's name, and so forth. However, this can also

help the investigator trace the trail of stolen NFTs and trace the movement of funds used to buy or sell suspicious NFTs [11].

There are some tools to investigate and monitor NFT activities, such as Etherscan tools, which view wallet activity on the Ethereum blockchain, and Nansen tools for a deeper analysis of NFT trades and wallet connections [12].

And suppose the NFT marketplaces like Open Sea require knowing your customer, meaning users must verify their identity. In that case, it becomes easier to link wallet addresses to real people and catch someone using stolen crypto to buy NFTs. Applying anti-money laundering systems to NFT platforms can automatically flag suspicious behavior and help investigators catch the act faster [13].

Moreover, some NFT platforms or smart contracts can freeze or recover stolen NFTs or reverse a transaction if it was part of the, but only if acted upon quickly [14].

The blockchain investigation used state-of-the-art tools to track criminals, the money, and where it came from and went. We can describe the steps as follows:

Tracing the money

Every crypto transaction on the blockchain shows who sent what to whom. However, using wallet addresses instead of names, the investigators look at:

A. Where the money originated (the initial wallet or address that initiated the transaction).
B. The path it took (through different wallets, exchanges, or blockchains).
C. Where it arrived (the final wallet where the money is kept or withdrawn) [15].

Some techniques used in Blockchain investigation

The expert and the investigator can use some tools to make sense of the complicated trail.

The ownership analysis

This technique is used to know and find who owns the wallet, so based on that, the investigator looks at the patterns in transactions and links to know exchanges of KYC-verified accounts and other online behaviour that might connect the wallet to the real person [16].

Clustering

When people use many wallet addresses to hide their activity, clustering techniques use software to detect common behaviour or shared patterns, which helps reduce confusion caused by seeing thousands of wallet addresses [17].

E-Discovery

E-discovery is a technique used to collect useful digital information from open online sources and personal devices. This tool collected and connected all this data to help create a big-history digital map showing all the transaction details, how the money moved, who was involved, and which devices or people were connected. Collecting these details gives a clearer picture of the whole crime situation [18].

Software investigation tools

This type of criminal needs specialized software tools that analyze thousands of transactions quickly, showing the money moved and possible wallet connections. This approach is called Bilic.

Bilic is a comprehensive, blockchain-based Anti-Money Laundering investigation framework. By adopting this approach, the software helps investigators track crypto transactions in detail by generating charts, tracking money movement, and uncovering patterns [19].

This approach makes it easier and faster for the investigator to solve complex money laundering cases. Based on the BILIC approach, the investigator can use some advanced software to investigate on the blockchain some of these:

FTM dashboard

(Follow The Money) (FTM) tools are used to research crypto assets then designed as a figure to present the transaction and track wallet activity. This tool can support around 47 blockchain networks and allow the users to analyse transactions through several chains, so the user can see all the transaction history details, including the incoming and outgoing transfers and the interaction with smart contracts, with highlights on the activities involving known wallet addresses [20].

This feature of the FTM tool enables investigators to spot suspicious wallet activity, follow digital currency flows, and detect illicit financial activity. The FTM system visually represents how funds move into and out of wallets, making investigations easier, as shown in Figure 1.

Figure 1: Displaying the 'Follow the Money' wallet investigation dashboard featuring a network graph of user transactions and wallet interactions [21].

The Data structure in FTM is as follows [22]:

- ***Entities:*** We aim to present real-time objects like people or companies. Each of these objects has a unique ID, a type (like Person or Company), and associated properties (like name or nationality), as shown in picture (1).

```
{
  "id": "1b38214f88d139897bbd13eabde464043d84bbf9",
  "schema": "Person",
  "properties": {
    "name": ["John Doe"],
    "nationality": ["us", "au"],
    "birthDate": ["1982"]
  }
}
```

Picture 1: Entities.

- ***Reference:*** The reference part links the entity to another entity. For example, a passport entity may reference a Person entity using the holder property.

Picture 2: Reference [23].

As shown in Picture (2), the data must handle references in two directions. For example, they may need to look up a person using a unique ID to track the holder link and a reverse index to find all passports connected to the individual.

- ***Interstitial Entities:*** This is used to present the relationships between two entities, as the person owning the company can be represented by an ownership entity containing both reference and metadata.
- Streams are JSON-based serialized forms of entities. They help transfer large entity data sets and are widely used across FTM tools.

The investigator can use the FTM framework to track the NFT in money laundering crimes by modelling wallets, fund transactions, and the interaction of the entities.

A pattern Recognition engine

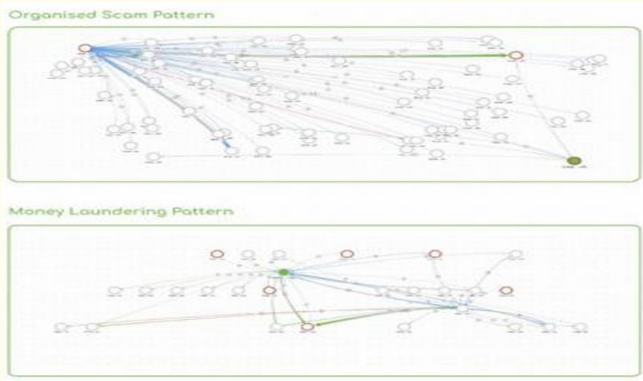
The pattern recognition engine is a program of algorithms that determines the data's regularities and patterns. Additionally, the engine is designed to help users quickly identify key behavioural patterns, streamlining the investigative and fact-finding process. It can automatically detect various activity types, including [24]:

1. Activity of money laundering, such as tracing money through linked wallets or detecting circular patterns of transactions (e.g., carousel scams);
2. KYC behaviour patterns, which exhibit activity at a high level with Know Your Customer sites, to help identify wallet owners;
3. Mixer usage patterns, where connections to mixing or tumbling services are evident;
4. Structured scam cues, where an asset is shifted from a source wallet to an active wallet using a series of small-denominated transactions. As shown in the picture (3).

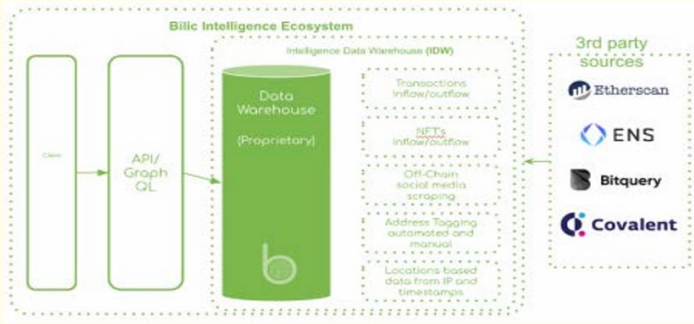
IDW [26]

The IDW is a big data centre that gathers data that law enforcement institutions can use to enhance investigations.

As the diagram shows, the IDW collects, processes, and analyzes blockchain-related data, especially for anti-money laundering crime investigations.



Picture 3: A pattern Recognition engine [25].



Picture 4: Bilic Intelligence Ecosystem [27].

The key components for the process are: First, Clint or the users interact with the system through a client interface as the platform; second, the API/ GraghQL Layer, which allows data querying and communication between the client and the backend; third, the GraphQL API, which is known for efficient, flexible querying; and lastly, the Data Warehouse (proprietary), which is the core piece of the system where all data is stored and processed.

Different types of data were collected in the warehouse. As we see in the second half of the diagram, the data flows from multiple sources: 1- transactions, which track the incoming and outgoing and all the historical movement of cryptocurrency and NFT transactions. 2- collecting the data from the social media platform to enrich the investigation, 3- Address Tagging (automated and manual) by named and labels the blockchain addresses and link it them with the individuals, 4- collecting the location data from the IPs and timestamps, this by using the meta data to infer user locations.

Additionally, as appears from the diagram (4), there are external platforms Bilic integrates with to collect blockchain data, such as Etherscan, [28] An Ethereum blockchain explorer, ENS (Ethereum Name Service), which helps link blockchain addresses to human-readable names, Bitquery, [29] a powerful blockchain data provider, and Covalent, [30] Which offers granular blockchain data and APIs for many chains.

Legal Challenges for the NFTs are rising for the court and investigators

NFTs have become popular digital assets, and their use has grown, but at the same time, several legal challenges are rising for the court and investigators in financial crime. Many countries around the world still don't have clear regulations and classifications to regulate the use and challenges of NFTs, making it harm to decide how they should be treated under the law.

On of the challenges of the NFTs is help the users to stay anonymous, as operate through decentralized blockchain systems, this usually avoid the traditional oversight from banks or the law enforcement or any other government agencies, and help the criminals talk advantage of to hide money or avoid detection, and hard for the law enforcement to track these transaction.

In addition, NFTs are often concluded by the smart contract on blockchain, and these contracts are coded instead of normal legal language, as a result, the court may find this type of contract hard to understand or enforce. And the mistakes in code or other technical issues can also lead to major legal problems. These factors make it hard for judges to apply traditional legal principles and many limit their ability to step in and correct unfair outcomes.

Not regulated until now in many countries

Not all countries regulate NFTs, so the NFT didn't have a specific description in all countries. However, after 2021, when the countries saw the high value of NFTs, they started to regulate their use, as the EU commission proposed Markets crypto assets regulation, which came into effect in 2023. This law includes previous information about all cryptocurrency assets, supports integrity, and protects the consumer from risk. However, paragraphs 10 and 11 exclude NFTs from the law's scope. This included digital art, collectibles, and NFTs that present unique physical assets as real state. As explained in paragraph 11, these assets are non-fungible, and their value is based on distinctive characteristics. They don't pose a financial risk as fungible tokens [32].

However, in some cases, if the functionality of the NFT or actual use makes them fungible, this case may fall under the regulation. Additionally, paragraph 11 adopts the substance-over-form approach, which means that we should look at what the token does, not what it is called, to apply the legal rules of this law to the cryptocurrency asset (fungible or non-fungible).

In the UK, in recent years, its building rules have taken one step at a time by updating existing financial laws to include crypto businesses, as: 1- adding the crypto businesses to anti-money laundering rules, 2- Applying rules to stop misleading crypto advertisement. 3- Creating tools for police to seize crypto used in crimes. On the other hand, the UK hasn't written laws just to regulate the NFTs, and they are not always treated the same way as regular cryptocurrencies, regardless if the NFT is part of a big collection like a regular token. So, while some NFTs might fall outside the rules, others (especially ones that can be used or traded like money) could still be regulated.

In 2025, the UK plans to regulate stablecoins and other crypto assets simultaneously, moving away from its previous step-by-step approach. The FCA's new Crypto Roadmap outlines upcoming rules for stablecoins, crypto service providers, and better user protections, with final regulations expected by 2026 [33].

In the USA, the government is writing new rules to regulate NFTs (unique digital objects like art or music put on a blockchain) more tightly. A proposed bill called the NFT Act says most NFTs used for personal use like art, music, or games will not be regulated as investments or as securities. However, if an NFT is offered to sell for the primary purpose of generating income, it may be regulated as a stock. The regulations are yet to be hammered out, and things are cloudy for the moment. Legislators aim to make it clearer shortly [34].

The classification of NFTs as assets, property, or collectibles is unclear, so the court may struggle to classify them, especially in financial crime cases. Determining which laws apply in money laundering or theft cases involving NFTs is also hard. As we explained above, in countries like the UK and the USA, where NFT-specific laws are either developing or fragmented, criminals can exploit regulatory loopholes to hide illicit funds through NFT trades, and the Investigators may find it difficult to trace transactions, especially when NFTs are moved between unregulated platforms or exchanged for cryptocurrencies.

As mentioned in the EU (*MiCA* law's paragraph 11, NFTs may be regulated not by what they are called but by how they're used (substance-over-form). This creates gray areas—an NFT used as a currency could suddenly be regulated as a financial asset, but only after investigation and legal interpretation.

Decentralized transaction

Blockchain transactions, such as cryptocurrencies and NFTs, happen on a decentralized system, so no company or individual controls the entire system. Due to that, it's difficult for police or law enforcement officials to know who is actually making a transaction [35].

For example, on decentralized exchanges such as the Venus platform, individuals are able to exchange crypto without needing to show their identification or go through frequent checks like banks [36]. The website enables individuals to connect to unhosted wallets, which are crypto wallets with publicly known company names or associated names. That is, the person using the wallet is still anonymous. This makes it extremely hard to track things such as money laundering, since investigators cant always figure out who actually owns the money or where it came from. While blockchain is supposed to be secure and transparent, this anonymous feature can also be exploited by criminals, making it more difficult for law enforcement to carry out their duties.

The anonymity of the NFTs

The lack of regulation for NFTs and anonymity makes them easier tools for money laundering than other financial transactions, which demand identification verification before any transaction.

As trading in NFTs grows, it is increasingly likely that money launderers will use them to do dirty work, moving illicit funds without ease of tracking. They can hack into NFT platform accounts, move NFTs to their digital wallets, and hide the source of the funds. Since blockchain transactions, in most instances, do not require identity verification, it is even easier for people to move funds anonymously [37]. Criminals like this feature on the NFTs because it's hard for the police to tell who is behind the screen.

The Evidentiary and Technical Complexities of Smart Contracts in NFT

Smart contracts used to encode non-fungible tokens (NFTs) raise critical legal issues in modern digital transactions. The contracts are written in computer languages such as Solidity rather than traditional legal terminology, and thus, they are difficult for judges and attorneys to decipher. Such ambiguity negates the judiciary's ability to review or interpret the agreement suitably [38]. Moreover, smart contracts lack conventional evidentiary elements, such as an evident expression of will or written negotiations between parties. Generally, consent is implied by participation in the code, and the question arises whether contractual intent existed. The absence of written or verbal words of will complicates the proof of mutual consent. This subject was brought up in the Hermès v. Mason Rothschild case, which concerned the court deciding whether NFTs that invoked the "Birkin" trademark were a trademark infringement or a protected artistic work.

Second, smart contracts are also susceptible to technical vulnerabilities that can lead to unforeseen legal consequences. Coding errors, for instance, may lead to faulty implementation, and external data sources (oracles) risk being given false or compromised information. A good example is the DAO hack in 2016, in which a coding error was utilized to steal approximately $60 million in Ether, prompting a disputed hard fork of the Ethereum blockchain to reverse the transaction [39]. This phenomenon caused severe legal and ethical problems regarding such one-sided remedial measures. Joined to these challenges is the autonomous and self-executing nature of smart contracts, which largely shortens the judiciary's ability to prevent or alter performance on invocation—against traditional contracts that have greater flexibility for courts to act with discretion in the name of justice. Therefore, the immutable character of smart contracts and NFTs' lack of clarity require a reformulation of present legal and regulatory frameworks, particularly in those places where regulation of digital assets remains in its embryonic stages [40].

Conclusion

Finally, the non-fungible tokens rise as digital assets and potential tools for illicit financial activities, which shows the double-edged sword nature of emerging technologies. Consequently, NFTs are a novel concept of the digital economy impacting ownership, creativity, and value in the internet. But the very technological characteristics that make NFTs appealing — decentralization, pseudonymity and global accessibility — mean they can also be abused by criminals, especially regarding money laundering.

Labelling all the criminals who exploit NFTs by using advanced laundering methods, such as wash trading, decentralized finance (DeFi) transactions, peel chains, chain hopping, and mixers. Both of these methods hide the origin of illicit funds through the design of the underlying technical architecture of blockchain systems, posing substantial legal and investigatory challenges. Digital art has a speculative and subjective value that, paired with no government oversight, complicates the detection and prosecution of these crimes.

Indeed, a powerful countervailing force is on hand: the transparency and immutability of blockchain itself. If you search a little, you will find simple tools similar to Etherscan and Nansen or even more complex software like BILIC and FTM dashboards that help you do digital forensic investigations. Using data clustering methods, ownership analysis, e-discovery, and pattern recognition engines, investigators can map transaction histories, detect nefarious wallet behaviours, and establish connections between pseudonymous actors across the Blockchain.

References

1. Yan Zheng. "The Research of NFT Money Laundering Risks and Regulatory Measures". Frontiers in Business, Economics and Management 6.3 (2022): 78-80.
2. Aadarsh Mani. "A Comprehensive Study of NFTs". International Journal for Research in Applied Science and Engineering Technology 9.4 (2021): 1656-60.
3. Saminu Salisu and Velitchko Filipov. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation". International Conference on Cyber Warfare and Security 18.1 (2023): 338-47.
4. Muddasar Ali and Sikha Bagui. "Introduction to NFTs: The Future of Digital Collectibles". International Journal of Advanced Computer Science and Applications 12.10 (2021): 50-56.
5. Phil Gonserkewitz, Erik Karger and Marvin Jagals. "Non-Fungible Tokens: Use Cases of NFTs and Future Research Agenda". Risk Governance and Control: Financial Markets and Institutions 12.3 (2022): 8-18.
6. Gonserkewitz, Karger, and Jagals.
7. Jelena Ceranic Perisic. "Metaverse, Non-Fungible Tokens, Trademarks - Legal Aspects". Law and Economy 60.4 (2022).
8. Fraud Investigation Network. Peel chain tracing in cryptocurrency investigations (2023). https://www.fraudinvestigation.net/cryptocurrency/tracing/peel-chain
9. Looking out for Whales and Dolphins ORCA. "The State of F The State of F… …". 7 (2024).
10. IDnow. Crypto mixer: A risky game of money laundering and rewards (2022). https://www.idnow.io/blog/crypto-mixer-money-laundering-risk-reward/
11. Brian Elzweig and Lawrence J Trautman. "When Does a Nonfungible Token (NFT) Become a Security?". SSRN Electronic Journal (2022).
12. Moez Krichen. "Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence". Computers 12.5 (2023).
13. Lucas Rohlik. "User Perspective Urban Air Mobility Acceptance Model (UAMAM) Master Thesis in General Management" (2019).
14. Zhanwen Chen and Kazumasa Omote. "Toward Achieving Anonymous NFT Trading". IEEE Access 10 (2022): 130166-76.
15. Salisu and Filipov. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation".
16. Salisu and Filipov.
17. Salisu and Filipov.
18. Salisu and Filipov.

19. Sarah Taylor., et al. "A Comprehensive Forensic Preservation Methodology for Crypto Wallets". Forensic Science International: Digital Investigation (2022).
20. Salisu and Filipov. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation".
21. Jakub Wyczik. "The Rise of the Metaverse: Tethering Effect and Intellectual Property of Crypto Tokens". Journal of Intellectual Property Law and Practice 19.4 (2024).
22. Organized Crime and Corruption Reporting Project. Follow the Money documentation. Follow the Money. https://followthemoney.tech/docs/
23. Organized Crime and Corruption Reporting Project. Follow the Money documentation. Follow the Money. https://followthemoney.tech/docs/
24. Romil Rawat., et al. Dark Web Pattern Recognition and Crime Analysis Using Machine Intelligence (IGI Global) (2022).
25. Salisu and Filipov. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation".
26. Technologies (2023).
27. Salisu and Filipov. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation".
28. Etherscan. Ethereum blockchain explorer. https://etherscan.io/
29. Bitquery. Blockchain API and crypto data products. https://bitquery.io/
30. Shuttleworth D. Covalent: A decentralized blockchain database and API. ConsenSys (2022). https://consensys.io/blog/covalent-a-decentralized-blockchain-database-and-api
31. European Securities and Markets Authority. Markets in Crypto-Assets Regulation (MiCA). ESMA (2023). https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
32. The European Parliament. "European Parliament 2019-2024". no. 2023 (2024): 2-4.
33. Rahman Ravelli. "NFT's (Non-Fungible Tokens) - Risks, Regulation and The Law. Rahman Ravelli Solicitors (2025). https://www.rahmanravelli.co.uk/expertise/nft-s-no.
34. (Fintechnically Speaking. The Challenge of Digital Asset Regulation of NFTs (2025).
35. Ceranic Perisic. "Metaverse, Non-Fungible Tokens, Trademarks - Legal Aspects".
36. Nir Kshetri. "Scams, Frauds, and Crimes in the Nonfungible Token Market". Computer 55.4 (2022).
37. Christie's. 10 things to know about CryptoPunks (2022).
38. Packin NG, ed. Other Legal Issues with NFTs. In: The Cambridge Handbook of Law and Policy for NFTs. Cambridge Law Handbooks. Cambridge University Press (2024): 349-394.
39. Paula Ungureanu, Francesca Bellesia and Carlotta Cochis. "Dealing with Blame in Digital Ecosystems: The DAO Failure in the Ethereum Blockchain". Technological Forecasting and Social Change 215 (2025): 124096.
40. Packin NG, ed. Other Legal Issues with NFTs. In: The Cambridge Handbook of Law and Policy for NFTs. Cambridge Law Handbooks. Cambridge University Press (2024): 349-394.