ISSN 2764-6068

International Journal of Law in Changing World

NFTs and the Legal Landscape
SPECIAL ISSUE

INSIDE THIS ISSUE

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Special Edition Editor's Note

NFTs and the Legal Landscape - A New Frontier in Intellectual Property, Digital Ownership, Financial Crime, Collective Organisations and Consumer Protection

In the ever-evolving digital landscape, Non-Fungible Tokens (NFTs) have emerged as a disruptive force, challenging the traditional paradigms of digital asset ownership and control. As Fortnow and Terry aptly highlight, NFTs seek to redefine the relationship between creatives, users, and digital artwork, a relationship historically dominated by powerful online intermediaries operating under the access model [1].

The prevailing access model, underpinned by a blend of technological, legal, and market dynamics, has largely curtailed the ability of creators and individual internet users to exert meaningful control over digital assets. Instead, these assets are predominantly governed by centralized intermediaries, offering seemingly unlimited access. While this model boasts advantages, such as a robust rights management system ensuring IP security and user convenience [4], it is not without its criticisms. The most glaring concern for creators is the 'value gap' - the disparity between the value generated by intermediaries and the compensation received by content creators [3]. This concern was so profound that it catalysed significant reforms in the EU's digital platform regulations in the form of the DSM Directive and, most recently, the DSA Act [2].

Centralized intermediaries, with their overarching influence, have not only skewed the value distribution but have also left users vulnerable. The tentative nature of access rights means users can be deprived of their digital assets without warning, rendering them powerless against potential misuse by these intermediaries [5].

This special issue of the journal underscores the profound impact of NFTs on Intellectual Property law. We are privileged to feature contributions that delve deep into this relationship from diverse legal perspectives. Dr. Ioanna Lapatoura offers a compelling analysis of the intricate relationship between NFTs and trademark law, using the MetaBirkins case as a focal point. Daniel Becker and Aylton Gonçalves, on the other hand, explore the implications of NFTs within the Brazilian legal framework.

Published November 2023

However, the legal ramifications of NFTs extend beyond IP law. In that context, Matteo Alessandro challenges traditional notions of property in light of NFTs, while Marica Ciantar examines the transformative potential of NFTs and Decentralized Autonomous Organizations (DAOs) in reshaping collective organizational governance. Prof. Dr. Yulia S. Kharitonova explored legal issues of decentralized services in the context of utility NFTs. J.-G. A. Hanneman researched DAOs and AI-based Smart Contracts. The darker aspects of NFT transactions are also addressed, with Ass Prof. Dr. Dimitrios Kafteranis, Dr. Huseyin Unozkan and Prof. Dr. Umut Turksen elucidating their alignment with financial crime regulations. Moreover, the discourse on NFTs in private law is expanded upon by Dr. Elena Tzoulia, who highlights their intersection with the secondary digital consumer protection acquis in the EU.

This issue serves as a testament to the multifaceted legal challenges and opportunities presented by NFTs. Through the insightful contributions of our esteemed authors, we hope to foster a deeper understanding and stimulate further discourse on this pivotal topic.

[1] Fortnow, M., Terry, Q. (2021) "The NFT Handbook: How to Create, Sell and Buy Non-fungible Tokens" (John Wiley & Sons, Incorporated), 47-57.

[2] Frosio, G. (2021) "Reforming intermediary liability in the Platform Economy: A European Digital Single Market Strategy'", Northwestern University Law Review Online, 251, 112-119

[3] Perzanowski, A., Schultz, J. (2018) "The end of ownership: Personal property in the Digital Economy" (The MIT Press).

[4] Rifkin, J. (2002) "The age of access: How the shift from ownership to access is Transforming Modern Life" (Penguin).

[5] Rosati, E. (2021) 'The DSM directive Two Years on: Do things ever get easier?', IIC - International Review of Intellectual Property and Competition Law, 52 (9), 23-33.

ABOUT THE EDITOR

Ioannis Revolidis – PhD, Resident Academic Lecturer, Department of Media, Communications & Technology Law, Centre for Distributed Ledger Technologies, University of Malta
e-mail: ioannis.revolidis@um.edu.mt
Scopus Author Profile:
https://www.scopus.com/authid/detail.uri?authorId=57194702661
Google Scholar ID:
https://scholar.google.com/citations?user=ITGuRhcAAAAJ&hl=en
ResearchGate Profile: https://www.researchgate.net/profile/Ioannis-Revolidis

Published November 2023

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.60

UTILITY NFT: LEGAL ISSUES OF DECENTRALIZED SERVICES

Yulia Kharitonova
Lomonosov Moscow State University, Moscow, Russia

Article Information:

Received
July 31, 2023
Approved
July 31, 2023
Accepted
October 3, 2023
Published
November 30, 2023

Keywords:

Non-fungible tokens,
utility tokens,
tokenization of economies,
digital assets

ABSTRACT

With the popularity of metaverse, the number of questions about the legal framework of utility tokens has also grown. In this area, the application of blockchain allows us to generalize the experience of tokenization of services. A countertrend is the evolution of NFTs from digital image right authentication to a utility solution that allows consumers to benefit from the possession of rights in the community. A legal analysis of utility NFTs in the metaverse leads to the need to apply the provisions of securities law to tokenization services. However, possessing the features of digital rights, utility NFTs cannot always be the investment, which requires the exclusion of such tokens from the scope of regulation of the law on crowdfunding.

FOR CITATION:

Kharitonova, Y. (2023). Utility NFT: Legal Issues of Decentralized Services. International Journal of Law in Changing World, Special Issue NFTs, 3-17. DOI: https://doi.org/10.54934/ijlcw.v2i3.60

1. INTRODUCTION

The mega-popularity of non-fungible tokens (NFTs) is now waning[1], leaving only the most optimistic investors in the industry with a general confidence that the market will not only survive but expand. At the same time, the law and legal order are still looking at the possibility of full legalization of investments in this type of entity. It seems that this discussion is still relevant in the legal community because the stability of the trend has just reached a plateau and it is possible to discuss what legal mechanisms are applicable to the formalization of relations regarding the issuance of tokens, and in particular, utility NFTs.

Residents of the metaverse can trade assets or goods with each other. We proceed from the concept of NFTs in the metaverse as the best digital asset to ensure the originality of goods and services in metaverse [3].

Metaverse NFTs are unique digital assets that can be bought and sold within the shared virtual space of the metaverse. The metaverse is a virtual shared space where users can interact with each other and digital objects in a seemingly real way. Its most basic definition refers to "the concept of a fully immersive virtual world where people gather to socialize play and work." It is a simulated digital environment that combines augmented reality (AR), virtual reality (VR), blockchain, and social media principles to create areas for rich user interaction that imitate the real world [11].

NFTs play a significant role in the metaverse by providing a way to represent unique digital assets such as virtual real estate, in-game items, and collectibles on a blockchain. The use of NFTs and digital assets in the metaverse helps create a more dynamic and engaging virtual world by allowing users to own and interact with digital assets in a meaningful way [5].

[1] According to a report by DappRadar, a resource that analyzes the market for decentralized applications (dApps) in March 2023, NFT trading volume increased to $2 billion for the first time since last May, up 117% from the previous month, with 6.3 million sales./ https://dappradar.com/blog/category/dapp-industry-reports.

https://doi.org/10.54934/ijlcw.v2i3.60

2. THE EVOLUTION OF NFTS

According to popular perceptions, NFTs are just collectible pictures that are sold unnecessarily expensive on all sorts of dubious platforms, and yet in the vast majority of cases do not give collectors any rights beyond the possession of a virtual asset[2] [9].

Indeed, NFTs are often associated with digital assets of various types including video, text, animated GIFs, and audio and are the most popular, with NFTs - images - holding the palm [13]. Until recently, this sort of token has been emphasized. For example, museums, tokenizing works of art in their possession, followed the path of creating a digital copy of the picture with the possibility of transferring ownership of the token - the picture to the buyer at auction. In this case, the material object in which the work of art is expressed as well as the rights to the result of intellectual activity belonging to the museum were not transferred to anyone and had nothing to do with the token [8].

However, technological experiments and the involvement of more and more participants in the tokenization process have led to a significant expansion of the range of popular NFTs on well-known marketplaces and exchanges. Trading platforms have consistently identified five major segments of the NFT market, namely collectibles, metaverses, games, art, and utilities. Meanwhile, the 2021-2022 market studies show that utility NFTs are the main source of secondary effects and collectible NFTs are the main source of secondary effects for both yield and volatility [14]. It is also noted that in some jurisdictions, utility tokens have sometimes become the predominant form of tokens offered in ICOs [3].

The market is now developing towards “strengthening” the tendency of tokening objects by providing the media file contained in the token with additional capabilities in the form of access rights to the service or content, subscription, or usage in a certain way. That is, in the context of issuing NFTs, a new social relation appears that requires a specific regulation.

[2] Sothebys. $17 Million Realized in Sotheby's First NFT Sale with Digital Creator Pak. URL: https://www.sothebys.com/en/articles/17-million-realized-in-sothebys-first-nft-sale-with-digital-creator-pak (дата обращения: 17.07.2023).

[3] International Law Practicum Includes Chapter News. A publication of the International Section of the New York State Bar Association. 2018 | VOL. 31 | NO. 1// https://www.maldonadoleon.com/web/publicaciones/2018IPV1.pdf

https://doi.org/10.54934/ijlcw.v2i3.60

Utility NFTs (sometimes also call consumer tokens) «bring real value to the owner. The creator of such an NFT provides consumers with special privileges»[4]. For example, it could be a token that provides membership to a club, access to cloud storage, or a loyalty token that can be redeemed for a physical good such as a cup of coffee, or perhaps access to a specific content in a multiplayer online game. Services eticket4, Poniminalu, for instance, created utility tokens to sell tickets to concerts[5]. Chiliz Chain with brands introduces the benefits of blockchain technology to the sports and entertainment industry by minting fan tokens, NFTs, and other digital assets[6]. Utility tokens have been successfully used in the music industry[7].

Utility tokens finance the development of their product or service, reward and incentivize early adopters and network promoters, align economic incentives between supply, demand, and the marketplace, and enhance network effects among all participants [2].

In the legal sphere, the qualification of such relations becomes very «painful». For example, when it comes to issuing tokens for a digital image, from a legal point of view, it is not the work that comes first but the corresponding rights protected in the token. The transfer of rights within a token is now the most bottleneck of legal regulation in different legal orders. The emergence of a serious market segment of utility NFTs raises the question of legalization of their circulation in Russia and abroad.

3. TOKEN VS DIGITAL RIGHTS

An NFT is essentially an immutable electronic file that verifies the ownership of a digital good and provides a statement of the origin, terms of ownership, and history of its transfer from the moment of issuance. In Russia, the legal analysis of token issuance is usually based on the notion of digital rights enshrined in Article 141.1. of the Civil Code of the Russian Federation: “As digital rights shall recognize obligation rights and other rights named as such in law whose content and terms of exercising are defined

[4] What is Utility NFT: everything a crypto-enthusiast needs to know // https://gq--blog-ru.turbopages.org/gq-blog.ru/s/bitcoin-invest/utility-nft/.

[5] https://www.forbes.ru/tehnologii/341989-kontramarka-soseda-rossiyskie-startapy-hotyat-otkryt-vtorichnyy-rynok-biletov-na?ysclid=lk8bmq9cop602613323 (дата обращения: 17.07.2023).

[6] The first Chiliz project served as a kind of bridge between sports teams and fans, primarily providing token holders access to information about players and events, souvenirs with team symbols, as well as selling NFT tickets to sporting events// https://www.chiliz.com/company/

[7] Kings of Leon have pioneered the world of musical NFTs: they have release the album 'When You See Yourself' as an NFT series, which gives the holder access to the artwork, a super album cover and a 'Golden Ticket' that guarantees the holder four front row seats to one show of every major Kings Of Leon tour for the rest of life// https://www.nme.com/news/music/kings-of-leon-have-generated-2million-from-nft-sales-of-their-new-album-2899349 (дата обращения: 17.07.2023).

https://doi.org/10.54934/ijlcw.v2i3.60

in compliance with the rules of an information system having the features established by law. The exercise, disposal of a digital right, in particular the transfer, putting in pledge, encumbrance of a digital right in other ways, or the restriction of the disposal of a digital right, are only possible in an information system without addressing a third party.”.

This provision of the law has drawn criticism from lawyers and the industry.

How are tokens and digital law related? Is it possible to separate digital law from a token? A token exists as a mathematical algorithm that is used to verify the validity of ownership of an asset in a digital format. Creating digital rights requires some format for key information storage. A token is used for this purpose. The authentication function of a token in a distributed ledger network, such as a blockchain, is as important legally as the assignment of an asset to the corresponding token as a notional unit. Thus, the proactive offering of NFTs may not be at all the same as how the basic asset transfer relationship is regulated.

Utility NFTs provide opportunities for participation in the community of an ecosystem. For instance, by providing benefits to community members within projects, revenue sharing or pre-selling tokens. Also, examples with concert and match ticket sales demonstrate the prospects of integrating the NFT market with real world events. It is also important to remember that the items exchanged in the NFT market are organized into collections, certain sets of NFTs that in most cases have common features. Collections can range in nature from sets of trading cards, collections of artistic masterpieces, virtual spaces in online games, and of course collections of utility tokens are also in demand.

Consequently, the digital rights that accompany the transfer of a token must be capable of being measured against the beneficial effect of the token, be legally enforceable as an obligation, and be covered by specific digital rights legislation. Otherwise, the issuance and circulation of such rights fall outside the scope of direct legal regulation, often depriving the holders of adequate protection.

4. THE LEGAL REGIME OF NFTS

The Swiss Financial Market Supervisory Authority's (FINMA) defines utility tokens as tokens that are designed to provide digital access to an application or service. Utility tokens are contrasted with payment tokens, which are synonymous with cryptocurrency and have no additional functions, and asset

https://doi.org/10.54934/ijlcw.v2i3.60

tokens, which represent assets such as participation in real physical assets, companies, or earnings streams, or an entitlement to dividends or interest payments.

Russia has also created regulation of utility digital rights. Under Article 8 of the Crowdfunding Law[8] (also known as Capital Raising Act), the utility rights named as such in the law relate to digital rights and may indirectly transfer of:

1) the right to demand the transfer of thing(s);

2) the right to demand the transfer of exclusive rights to the results of intellectual activity and (or) the right to use the results of intellectual activity;

3) the right to demand execution of work and (or) provision of services.

Russian law thus stipulates that utility digital rights include only claims, which in the framework of obligatory relations correlate with the debtor's obligation to transfer tokenized property or execute works/provide services.

Comparing the Russian approach with the foreign one allows some researchers to argue that the definition of utility digital assets in the legislation of European states and the United States is simpler by design. For example, “in Switzerland, utility tokens are defined as a unit based on distributed computing technology that provides the owner with digital access to an application or service. Here utility tokens are not a claim as in Russia» [9]. However, a reference to the Swiss Federal Council Report «Legal framework for distributed ledger technology and blockchain in Switzerland. An overview with a focus on the financial sector” shows that this is not entirely true. According to the Report, “utility tokens can frequently also be assumed to constitute claims. Even if a token is intended to provide access to a service, for example, it may still be regarded as the representation of a claim similar to a contract for work and services or an agency contract”[9].

The Russian structure of token transfer through the sale of digital rights gives rise to two-level relations: first, a digital right “to the right to demand the transfer/execution of...” is acquired and then this right of demand itself is enforced. At the same time, the utility digital right is qualified under Article 128

[8] The Federal Law "On the investment promotion using investment platforms" 02.08.2019 N 259-FZ
[9] Legal framework for distributed ledger technology and blockchain in Switzerland An overview with a focus on the financial sector. Federal Council report. Bern, 14 December 2018// https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf

https://doi.org/10.54934/ijlcw.v2i3.60

of the Civil Code of the Russian Federation as a special type of civil rights object, while the law on crowdfunding defines its turnover on the basis of digital right sale and purchase transactions. The specifics of Russian legal regulation are that the statement of the law is understood to mean that "a utility digital right may become an object of civil turnover only if it provides a certain tangible or intangible good" [1] (Article 8 of the Crowdfunding Law).

Currently, in the vast majority of cases, Russian crowdfunding platforms are used to place applications for borrowing money for executing government procurement contracts. It seems to be true that the construct of utility digital rights is not suitable for the transfer of collectible NFTs. It in this sense that the statement that "NFT cannot be considered utility digital rights" [6] was correct. However, Russian law may still be relevant with respect to utility tokens.

As in Russia, foreign researchers support the idea of two steps to the transfer of a digital asset: first we sell the token and then we get the execution of the claim contained in the token.

It is argued that it is necessary to extend the rules of personal ownership and possession to NFTs, and since transactions with NFTs are made in the form of sale and purchase, the law on the sale and purchase of personal property should be applied.

Investigators agree on the need to extend personal property and ownership rules to NFTs. If transactions with NFTs are made in the form of sale and purchase, the law on sale and purchase of personal property should apply to them. "NFTs are expressly sold on the basis of narratives of ownership" [7]. For Russian law, the idea of «digital personal property» is very revolutionary and is not yet applicable. However, we can support the argument that applying the model of sale and purchase of things to token transfers will protect those who acquire scarce and valuable digital assets as true owners, not just users of platforms. It is also possible to minimally change the law. According to Article 8 of the Crowdfunding Law, the content and conditions for utility digital rights realization are determined in the investment platform. At the same time, participants of investment engagement are users of the platform. The platform dictates the terms of user agreements. Therefore, the interests of utility token holders become secondary to the business interests of platform operators.

https://doi.org/10.54934/ijlcw.v2i3.60

5. LEGAL UNDERSTANDING OF NONFUNGIBILITY

The non fungibility of a token as one of its key characteristics implies the representation of a unique digital asset that cannot be equally exchanged or traded for another NFT of the same type. Nonfungibility means that their perceptive value depends on their individual characteristics. The concept of nonfungibility creates a digital certificate of authenticity that cannot be reproduced.

In distributed ledger technology, a record of a token's ownership is always available, immutable, and ensures that it can have only one owner at any given time. From the legal perspective, the non fungibility of a token raises the question of extending to it the rules on an individually defined thing. Russian arbitration practice has long established the position that individually defined things may include those "that can be identified and distinguished among other things" (Ruling of the Arbitration Court of the Volgo-Vyatsky District of 17.04.2019 N F01-918/2019 in case N A79-5617/2018). Can this approach be extended to utilitarian NFTs?

Tokens, as digital units existing in a registry, are always identified and in that sense unique.

In the general division of the High Court of the Republic of Singapore [2022] sghc 264 is specified: «tokens, as digital units existing in a registry, are always identified and in that sense unique. In a case involving an injunction against NFT Bored Ape, the Supreme Court of the Republic of Singapore explained: "With respect to the technical aspects of such NFTs, each NFT in the BAYC collection was minted on the Ethereum blockchain with an individual and unique hash number recorded on the blockchain along with a unique token identifier that served as publicly verifiable proof of origin. NFT Bored Ape had the following hash number recorded in the blockchain: 11c6ce8133ae11a9008557dd1c0bdd4b81 d88b9d1609ab4dac2716a4b3f14465." [10]

However, it seems that the nonfungibility of tokens is primarily due to the uniqueness of the object of tokenization. The term "fungible" comes from the economics and accounting literature. In the context

[10] BAYC is a collection of 10,000 NFT Bored Ape - unique digital collectibles that live on the Ethereum blockchain. Bored Ape doubles as your Yacht Club membership card and grants access to members-only benefits, the first of which is access to THE BATHROOM, a collaborative graffiti board." The Bathroom "contains a canvas accessible only to wallets containing at least one ape. Like any good dive bar bathroom, this is the place to draw, scrawl, or write expletives. Each ape-holder will be able to paint a pixel on the bathroom wall every fifteen minutes. A members-only canvas for the discerning minds of crypto Twitter// https://nfts.wtf/bored-ape-yacht-club-goes-boom/

https://doi.org/10.54934/ijlcw.v2i3.60

of economics, the term “fungibility” refers to the ability of a good or asset to be exchanged with other individual goods or assets of the same type. Fungible assets simplify the processes of exchange and trade because fungibility implies equal value of the assets. An NFT is an individually defined item.

NFTs are essentially a certificate of uniqueness of a digital object - a digital cryptographic certificate (digital asset). Thus, in Nike v. StockX, which pointed out that according to StockX, its NFTs are merely «claim tickets» to access physical shoes stored in a “vault” after a buyer purchases them and provide proof of ownership and authenticity [11].

The qualification of a token depends on the purpose of its issuance and the functions it should fulfil in circulation. At the same time, the emergence of tokens is expressed in the possibility of changing their characteristics. We can make the standard NFT usable by simply adding some "utility" to it.

You don't even need to create separate NFT to do this. It is possible to add a set of utilities to a particular NFT or collection in various ways. Formally, Russia allows the issuance of digital rights that simultaneously meet the attributes of digital utilitarian right and a digital financial asset. Given the insufficient experience of Russian business in implementing projects of this sort, the legislator considered applying the relevant rules even into tax legislation:

“Property-Related Tax Deductions for amounts received by the taxpayer in the tax period from the sale of other property (except for securities and property obtained as a result of the redemption of digital financial assets and (or) digital rights, including simultaneously digital financial assets and utilitarian digital rights)” (subparagraph 1, paragraph 1, Article 220 of the Tax Code of the Russian Federation).

6. UTILITY NFTs ON THE INVESTMENT MARKET

Under the Crowdfunding Law, utility NFTs may be put out only if the digital rights they embody are mentioned in the law and are traded on one of the platforms in Russian jurisdiction. The Crowdfunding Law sets out the conditions under which utility digital rights become an object of civil turnover. The person attracting investments must, in accordance with the rules of the investment platform, establish the

[11] Online reseller StockX LLC said in a court filing Thursday that images of Nike sneakers it sells as non-fungible tokens do not violate Nike Inc trademarks, arguing that Nike had shown a "fundamental misunderstanding" of NFTs by suing StockX last month// https://www.reuters.com/legal/litigation/stockx-strikes-back-nike-nft-lawsuit-2022-03-31/. In July 2023, the case is still unsettled and an examination is underway (https://storage.courtlistener.com/recap/gov.uscourts.nysd.574411/gov.uscourts.nysd.574411.153.0.pdf). The prospects for the suit are controversial.

https://doi.org/10.54934/ijlcw.v2i3.60

content and conditions for exercising utility digital rights (the substance of the right (claim); the procedure for exercising the utility digital rights; the number of utility digital rights offered).

The primary purpose of the adoption of this law was to regulate relations arising in connection with investing and attracting investments using investment platforms. Article 5 of the Crowdfunding Law establishes that the purchase of utility digital rights is one of the options for investment.

The question arises, in all cases, should NFT be issued within the framework of digital platforms controlled by the Central Bank of Russia? That is, the sale of NFT - concert tickets [12] formally falls under the law on crowdfunding as a method of investment.

As noted above, not all tokens are initially conceived as investment assets. Since tokens may change their purpose, acquire utility as they become more widely circulated, and due to possible hybridity, NFTs issued in the Russian jurisdiction are potentially subject to the legal regime established by the Crowdfunding Law.

All companies offering NFTs in jurisdictions where regulation in this area has been applied have faced a similar problem. It is known that crypto companies in the U.S. planning to put out tokens are afraid of getting under the control of the U.S. Securities and Exchange Commission (SEC) often considers tokens as securities. The entire crypto industry is now watching the dispute between the largest NFT marketplace Coinbase and the SEC.

According to the SEC lawsuit, Coinbase made available for trading assets that are offered and sold as securities formalized as investment contracts. In particular, they included crypto assets with trading symbols of SOL (Solana), ADA (Cardano), MATIC (Polygon), FIL (Filcoin), SAND (Sandbox), AXS (Axie Infinity), CHZ (Chiliz), FLOW (Flow), ICP (Internet Computer), NEAR (NEAR Protocol), VGX (Voyager VGX), DASH (Dash), NEXO (NEXO) [13]. Coinbase's objections are based on the fact that the mentioned tokens are not investment securities. The marketplace emphasizes that “Coinbase does not list securities or offer products to our customers that are securities”[14]. For example, as mentioned above, CHZ tokens from Chiliz are not designed to generate passive income.

[12] https://teamring.org/en/cashback/stores/view/id/69.
[13] https://storage.courtlistener.com/recap/gov.uscourts.nysd.599908/gov.uscourts.nysd.599908.1.0.pdf
[14] https://www.coinbase.com/blog/we-asked-the-sec-for-reasonable-crypto-rules-for-americans-we-got-legal.

https://doi.org/10.54934/ijlcw.v2i3.60

In general, the distinction of tokens into cryptocurrencies, tokens-commodities, and tokens-securities is still very controversial. Coinbase's position in the above dispute also relies heavily on the evolving (still possible appeal) process of Ripple Labs. On July 13, 2023, Ripple Labs obtained a judgement in the United States District Court for the Southern District of New York, ruling partially in favor of the company.

According to the SEC complaint, Ripple; Christian Larsen, the company's co-founder, executive chairman of its board, and former CEO; and Bradley Garlinghouse, the company's current CEO, raised capital to finance the company's business. The complaint alleges that Ripple raised funds beginning in 2013 through the sale of digital assets known as XRP in an unregistered securities offering to investors in the U.S. and worldwide. Ripple also allegedly distributed billions of XRP in exchange for noncash considerations, such as labor and market-making services [15]. Since 2021, Ripple has insisted in objections to the case that the XRP token has currency value and utility. The XRP token is traded as a Ripple cryptocurrency token that is used to transfer funds across borders at a low cost - securely and instantly. It is used as an intermediate currency to offer financial institutions a more economical way to exchange both cryptocurrency and fiat currency[16]. Ripple argues that assets of this nature should be considered commodities rather than securities, on par with commodities and their derivatives.

On July 13, Judge Analisa Torres handed down a long-awaited decision in SEC v. Ripple. Ripple. The judge, after analyzing the term “investment contract”, a term recognized as a security under the Howey doctrine. The opinion answered the first question by analyzing the term “investment contract” found throughout the securities laws under the Howey doctrine because investment contracts are definitionally a security. Investment contracts do not require a literal contract, and instead apply to transactions or schemes where there is an «investment of money» in a «common enterprise» with the «expectation of profits», «solely through the efforts of another». The opinion does this by attempting to draw a distinction between sales of XRP through literal investment contracts and sales not involving actual contracts. For example, the opinion held that the “efforts of another” part of the test was missing because some programmatic buyers, as opposed to the institutional buyers, could not have known whether their funds would go directly to fund Ripple’s efforts. The judge issued a verdict that neither sales nor other forms of

[15] https://www.sec.gov/news/press-release/2020-338
[16] https://ripple.com/xrp/

https://doi.org/10.54934/ijlcw.v2i3.60

offering of XRP tokens issued by the company nor sales of those tokens to private investors amounted to investment contract transactions, meaning that XRP tokens were not actually recognized as securities.

The Ripple case reminds us of other cases where crypto assets have been tried to be equated with securities. Telegram's story issuing Gram tokens also raised the question of the coins' utility. Since Telegram created a scheme to maximize profits by allowing the original investors to resell the tokens on the secondary market and to receive profits from the investment, the SEC and then the court recognized as securities transactions the sale of tokens in which investors were promised a return on their investment. The SEC has previously made it clear that Ethereum also started out as a security, as the Ethereum Foundation used it to raise money. But even now, the coins can earn the equivalent of interest, which again raises the question of applying securities laws to the circulation of this type of asset. At the same time, when excluding Ethereum from the circle of securities, the SEC pointed to the decentralized distribution of crypto-assets. Thus, decentralized crypto assets that are not intended to generate income from investing in them may eventually be exempted from securities regulations.

In European countries, the same debates develop. In 2022, the Malta Financial Services Authority (MFSA) justified in its Guidelines on Virtual Financial Assets[17] that the European Markets in Crypto Assets Regulation (MiCA) may not be extended to NFTs. MFSA proposes to remove NFTs from the virtual financial asset framework because they are unique and nonfungible and therefore cannot be used as payments for goods and services or for investment purposes. A utility token does not fall under the MiCA regulations. However, a crypto-asset may be recognized as an investment asset if it is intended to be used in part for investment.

The researchers also insist that NFTs cannot qualify as securities and do not fall under securities legislation as long as their sole purpose is to provide digital rights to access [4]. Utility tokens, which constitute access to a blockchain application or service, are not inherently securities, but the way they are marketed, sold, or even transferred may look like a securities offering. Of course, some tokens cannot be categorized in any one way. However, financial market regulation should not be imposed on tokens that are in fact utility tokens, i.e., tokens only for consumers and not available as financial instruments [12].

[17] The Virtual Financial Assets Framework: Non-Fungible Tokens. GUIDELINES// https://www.mfsa.mt/wp-content/uploads/2023/06/The-Virtual-Financial-Assets-Framework-Non-Fungible-Tokens-Guidelines.pdf

https://doi.org/10.54934/ijlcw.v2i3.60

The Russian law does not take into account that trading in utility tokens can be conducted both at Russian digital financial asset exchange operators and on foreign platforms that are not subject to Russian law. In this regard, against the background of the emerging trend in Russia, it is necessary to consider the fact that separate independent rules for regulating the turnover of utility tokens, different from the legislation on attracting investments, are required. A possible step, in our opinion, would be to distinguish between utilitarian digital rights issued and traded under the rules of the Crowdfunding Law and other utilitarian tokens not related to tokenization of claims for investment purposes. In general, the purchase of utility tokens giving the right to service or participation in a concert does not pursue investment purposes as the main goal, and therefore it is not logical to require from the person issuing them, for example, the preparation of an investment proposal, disclosure of information in the prescribed amount, etc. As a first step, we propose to specify in the law on crowdfunding itself that tokens issued not for the purpose of attracting investment but for tokenization of the service are not subject to this law.

7. CONCLUSIONS

Experience in implementing NFT technology in various business areas shows that distributed ledger technology offers a standardized infrastructure for tokenizing physical objects and services, creating digital versions of them so that such tokens (“fungible or non fungible”) can be owned, exchanged and shared digitally. Many companies have already realized the opportunities for development and customer acquisition through the issuance of NFTs. The Russian jurisdiction is following the general trend, but in order to attract new issuers to Russian platforms, work will need to be done to improve the mechanisms for regulating the circulation of NFTs.

https://doi.org/10.54934/ijlcw.v2i3.60

REFERENCES

[1] Alekseeva D.G., Arzumanova L.L., Batrova T.A., Peshkova (Belogortseva) H.V., Rotko S.V., Chernyus N.Y., Shpinev Y.S., Timoshenko D.A. (2021). Commentary to the Federal Law of August 2, 2019 N 259-FZ "The Federal Law «On the investment promotion using investment platforms» and on amendments to certain legislative acts of the Russian Federation" (article-by-article). *SPS ConsultantPlus.*

[2] Benedetti, H., Caceres, C., & Abarzúa, L. Á. (2023). Utility Tokens. In: *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges* (pp. 79-92). Emerald Publishing Limited.

[3] Brown Sr, R., Shin, S. I., & Kim, J. B. (2022). Will NFTs be the best digital asset for the Metaverse? *SAIS 2022 Proceedings*, 16.

[4] Caytas, J. (2018). Regulation of Cryptocurrencies and Initial Coin Offerings in Switzerland: Declared Vision of a 'Crypto Nation'. *Incl. Chapter News*, 31, 53.

[5] Cheng, S. (2023). Metaverse and Digital Asset. In: *Metaverse: Concept, Content and Context* (pp. 123-144). Cham: Springer Nature Switzerland.

[6] Churilov A.Yu. (2022). Legal regulation of the turnover of non-interchangeable tokens: problems and prospects. *Khozyaistvo i parvo*, 1, 64 - 75.

[7] Fairfield, J. A. (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Ind. LJ*, 97, 1261.

[8] Gubaeva E.A. (2022). NFT-art and the activities of museums: points of contact. *Law and Business*, 4, 10 - 16.

[9] Jones, J. (2021). Brian Eno shares his critical take on art & NFTs. *Open Culture*, December, 30.

[10] Kondova, G., & Simonella, G. (2019). Blockchain in startup financing: ICOs and STOs in Switzerland. *Journal of Strategic Innovation and Sustainability*, 14(6), 43-48.

[11] Laeeq, K. (2022). Metaverse: why, how and what. *How and What*. Available at: https://www.researchgate.net/profile/Kashif-Laeeq/publication/358505001_Metaverse_Why_How_and_What/links/62053bb0afa8884cabd70210/Metaverse-Why-How-and-What.pdf

[12] Massad, T. G. (2019). It's time to strengthen the regulation of crypto-assets. *Economic Studies at Brookings*, 69.

https://doi.org/10.54934/ijlcw.v2i3.60

[13] Makori, J. (2023). *10 most expensive NFTs ever sold (2023).* CoinGecko. Available at: https://www.coingecko.com/research/publications/10-most-expensive-nfts-ever-sold

[14] Umar, Z., Alwahedi, W., Zaremba, A., & Vo, X. V. (2022). Return and volatility connectedness of the non-fungible tokens segments. *Journal of Behavioral and Experimental Finance*, 35, 100692.

ABOUT THE AUTHOR

Yuliya S. Kharitonova– Doctor of Law, Professor, Head of the Center for Legal Research of Artificial Intelligence and Digital Economy, Professor of the Department of Entrepreneurial Law, Lomonosov Moscow State University, Moscow, Russian Federation.
e-mail: sovet2009@rambler.ru

ABOUT THIS ARTICLE

Conflict of interests: Author declares no conflicting interests

https://doi.org/10.54934/ijlcw.v2i3.60

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.57

KNOW YOUR NFTS:

COMPLIANCE AND ENFORCEMENT CHALLENGES IN TRADING OF NON-FUNGIBLE TOKENS

Dimitris Kafteranis
Centre for Financial and Corporate Integrity, Coventry University, UK

Huseyin Unozkan
Haliç University, Istanbul, Turkey

Umut Turksen
Centre for Financial and Corporate Integrity, Coventry University, UK

Article Information:
Received
December x, 2023
Approved
December x, 2023
Accepted
October x, 2023
Published
November x, 2023

Keywords:

NFT,
illicit financial flows,
cryptocurrency,
money laundering

ABSTRACT

Non-Fungible Tokens (NFTs) is a new virtual asset phenomenon the trade of which has spread quickly without any regulation as no legislation has been adopted in the EU, USA or the UK where the majority of NFT trading takes place. Concerns have been raised about NFTs and their relation to fraud and money laundering as anonymity and price volatility of NFTs create a unique and profitable asset for criminals. This paper addresses two main issues: (1) trading statistics on NFTs, their analysis, and if and to what extent NFTs are used for financial crimes purposes; and (2) the legal challenges posed by the misuse of NFTs for fraud and other economic crimes. The final section of this paper provides feasible regulatory and business solutions that can help businesses to mitigate risks emanating from NFTs. It is argued that legal scholars, businesses and/or regulators cannot solve the challenges and risks posed by NFTs on their own, requiring multidisciplinary research from academia and knowledge exchange between private and public stakeholders to close this gap.

FOR CITATION:

Kafteranis, D., Unozkan, H., & Turksen, U. (2023). Know Your NFTs: Compliance and Enforcement Challenges in Trading of Non-Fungible Tokens. International Journal of Law in Changing World, Special Issue NFTs, 18-51. DOI: https://doi.org/10.54934/ijlcw.v2i3.57

1. BRIEF OVERVIEW OF NFTS AND THEIR GROWING POPULARITY

Non-Fungible tokens (NFTS) refer to cryptographic assets that represent ownership of unique digital items such as art pieces, music files, and other forms of media. Unlike cryptocurrencies such as Bitcoin and Ethereum, which are fungible and interchangeable with one another based on their value equivalence, NFTs are non-interchangeable owing to their uniqueness. NFTs employ blockchain technology that certifies the authenticity and provenance of a specific virtual asset by recording it in an immutable ledger. This means that once an NFT is created on a particular blockchain network such as Ethereum or Binance Smart Chain, it cannot be altered or replicated due to its unforgeability. The demand for NFTs has increased significantly in recent years owing to the unique attributes they possess and the profits they have yielded. They can serve as proof of ownership over rare virtual property; moreover, artists can use them as new models for monetising their work [5]. Notwithstanding these benefits offered by NFTs, there remain significant concerns surrounding their potential misuse for financial crimes such as money laundering and fraud schemes because they operate outside regulated markets.[1] In other words, NFTs are a product of decentralised financial sector. The anonymity afforded by some decentralised marketplaces makes it challenging for auditors and regulators to monitor such trading effectively. It remains crucial for both buyers and sellers involved in NFT transactions to understand the associated risks.

NFTs made their first appearance in 2017 with the launch of a video game, CryptoKitties on the Ethereum blockchain. This game allowed for the ownership and trading of unique digital cats, each with its own distinct attributes stored on the blockchain. CryptoKitties allowed users to buy, sell, and breed unique digital cats represented as NFTs, which could not be replicated or exchanged for identical tokens. This concept of unique virtual assets represented on a blockchain caught on quickly and has since expanded to various other types of virtual assets, including art, music, and collectibles.

Arguably, the most significant expansion of NFTs' has happened in the art market whereby NFTs have been presented as a new form of digital art. Traditionally, we think of art - or high art – as a painting by Picasso, Dali or Modigliani. The times are changing so does art. NFTs are a new trend and, maybe, the

[1] On 14 April 2023, the Virtual Assets Contact Group of the FATF raised concerns again about the misuse of virtual assets for money laundering and other illegal activities. The group is concerned that many countries have failed to implement legal measures. Available at: https://www.fatf-gafi.org/en/publications/Virtualassets/Press-Release-FATF-VACG-2023.html (accessed, 20.05.2023)

https://doi.org/10.54934/ijlcw.v2i3.57

future of art. They became particularly "famous" in 2021 when Beeple's collage, 'Everydays - The First 5000 Days' was sold by Christie's for USD 69 million (Reyburn, 2021).[2] During the COVID-19 pandemic, art found new ways to expand or, from a more critical perspective, the rise of NFTs has coincided with the traditional art market being subjected to stricter anti-money laundering (AML) rules in the European Union (EU).[3] For instance, the EU AML Directive designates "persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more" as obliged entities. These persons have a duty conduct 'know your customer' (KYC) practices, due diligence in trading of art and report suspicious activity transactions to the financial intelligence units.[4] Putting the traditional art market on the radar of AML rules, Financial Intelligence Units (FIUs) and law enforcement agencies (LEAs) may have driven criminals to search for alternative methods of laundering their proceeds of crime.

Apart from the art market, NFTs have expanded to other sectors. For example, NFTs have become very popular in the online gaming industry. Numerous online video games allow players to own and trade unique-in-game items, such as weapons and armour, represented as NFTs. Others allow players to own and trade unique characters, represented as NFTs, that can be used in multiple games. For instance, Sandbox is an Ethereum-based decentralised NFT gaming metaverse which enables non-tech savvy users to create, sell, use and monetize their own virtual reality NFTs (www.sandbox, accessed 25.05.2023).

NFTs can also be found in the music, audio and video industry. For instance, in March 2021, the rock band "Kings of Leon" offered an NFT-limited edition of their latest album (www.nme.com, accessed 25.05.2023). NFTs are used in charity as well. In March 2021, Jack Dorsey raised USD 2.9 million for charity by selling the first ever tweet. He donated the money to an African charity (Harper, 2021). An increasing number of charitable organisations use NFTs to raise funds. In the USA, Taco Bell sold 25 taco-themed NFT GIFS (NFTacoBells) to support the Taco Bell Foundation's Live Más Scholarship (Clark, 2021). These NFTs sold out within 30 minutes, with one selling for USD 3,646 (3,368 euros

[2] This has been the highest amount of money paid for an NFT so far.
[3] European Parliament and European Council Directive 2018/843 of 30 May 2018 amending Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.
[4] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU; available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843 (accessed, 29.06.2022)

https://doi.org/10.54934/ijlcw.v2i3.57

approx). The foundation will also receive 0.1% of every subsequent sale, meaning the foundation will continue to benefit long after the initial auction as NFTs can contain smart contracts whereby royalties can be built into them [6]. Newly established Covid:aid is the first UK charity wholly dedicated to supporting people affected by the pandemic. Covid: aid auctioned off its logo as an NFT, offering the winning bidder the chance to be the world's first founding charity crypto-philanthropist (https://covidaidcharity.org, accessed 25.05.2023).

In recent years, the fashion industry has also shown tremendous effort to digitally transform and adapt fashion in the digital era. Brands are using NFTs to attract, verify and connect with consumers from all over the world (https://zipmex.com, accessed 18.05.2023). For fashion brands, digital fashion opens up a completely new field of activity. They can sell their fashion not only in the real world, but also in the virtual world via NFTs - especially in the gaming world. There, too, clothing plays an increasingly important role. The RTFKT brand was, as an example, established in 2019 and became a specialist in selling virtual sneakers (https://rtfkt.com, accessed 18.05.2023).

Last but not least, NFTs are becoming popular in the sports industry. For example, the National Basketball Association (NBA) launched a new NFT initiative, the Association NFT, where NBA's highlight moments become collectibles (https://nbatopshot.com, accessed 18.05.2023). The appearance of the NFTs will evolve based on players' performance. The more accomplished a player is throughout the season, the more their NFT will visually change. Top Shot is about video moments whereas the latest NBA initiative is closer to collectible cards, with a dynamic twist. In regard to the football industry, Sorare comes to mind in the realm of fantasy sports leveraging gamified NFTs (https://sorare.com, accessed 18.05.2023). It is currently the biggest platform for trading football NFTs. Players can purchase player card NFTs and each week, they can create line-ups and earn points based on players' real-life performances.

These examples of the expansion and use of NFTs as part of virtual asset trading demonstrate that NFTs have become well established business activity and it is clear that they will continue to grow. What is also clear is that authorities have not responded swiftly to regulate this decentralised financial sector.

This paper aims to analyse the legal status of NFTs in relation to money laundering and other financial crime risks. The focus of this legal analysis is to identify the legal status of NFTs under EU law, and examples from other jurisdictions are provided, when appropriate. In the first part, the analysis focuses

https://doi.org/10.54934/ijlcw.v2i3.57

on the potential use of NFTs for money laundering and other financial crimes with reference to a number of examples of the use of NFTs for illegal activities. In the second part, the challenges posed by NFTs for detecting and preventing illegal activities are scrutinised. This is followed by statistics on the transactions of NFTs in order to highlight the growing demand of NFTs, the growing value of NFTs trade and the lack of official NFT statistics. Following the analysis of the statistics, the EU legal landscape pertaining to NFTs is explored which demonstrates that NFTs are in a grey legal zone for the time being. In the final part, proposals for further regulatory responses, research and training are offered.

This article uses doctrinal and analytical methods to review the current legal literature on the issue of NFTs and money laundering. Apart from the legal analysis, the article explores statistics which give a unique and inter-disciplinary perspective to this study. The originality of this article lies on the combination of legal analysis and statistics as well as the proposals made which will enhance the safe use of NFTs and limit the criminal use of NFTs. In addition, this study is timely following the recent adoption of relevant EU legislation on crypto-assets which excludes NFTs. This article recommends that the EU consults relevant business stakeholders, adopts specific rules on NFTs in relation to anti-money laundering rules and invests in more research and training to be conducted.

2. EXPLANATION OF THE POTENTIAL FOR NFTS TO BE USED FOR MONEY LAUNDERING

NFTs have recently gained significant popularity and value in the art and virtual asset world. At the same time, the rise of NFTs has also brought concerns about their misuse as part of financial crimes and money laundering schemes (Department of the Treasure, 2022). This is because NFTs provide a convenient and practical means for illicit transactions with minimal physical interaction, thereby avoiding detection by law enforcement agencies (Kafteranis and Turksen, 2022).

The anonymity provided by NFTs, coupled with the lack of regulation in the industry, makes it difficult for authorities to trace or prevent illicit transactions involved in NFT trade. Furthermore, NFTs can be used as a tool to facilitate money laundering since they offer a high degree of flexibility in moving value across borders without oversight, taxation or detection (Kafteranis and Turksen, 2022). One of the main challenges with NFTs is the ability to verify the identity and legitimacy of both parties involved in a transaction.

https://doi.org/10.54934/ijlcw.v2i3.57

This lack of transparency and accountability in transactions may encourage criminals to utilise NFTs for fraudulent purposes, such as using fake identities, transferring proceeds of crime, or manipulating the value of NFTs for personal gain. Given the decentralised nature of the NFT industry, their susceptibility to being exploited for financial crimes is a growing concern among financial regulators worldwide (Department of the Treasure, 2022), (FCA, 2022). To address these concerns, some NFT marketplaces such as OpenSea and Quantus have voluntarily implemented their anti-money laundering (AML) protocols and KYC requirements for NFT transactions (https://opensea.io, accessed 18.05.2023), (www.quantusgallery.com, accessed 18.05.2023). These self-imposed rules require NFT marketplaces to conduct due diligence on their customers, including identity verification and transaction monitoring, to ensure compliance with relevant anti-fraud and AML laws. While, self-regulation could provide a degree of deterrence for criminal use of NFTs, given the major fraud, corruption and money laundering scandals in the regulated financial services markets such as banking and investment, we argue that voluntary self-regulation would not suffice to safeguard the public against malfeasant use of NFTs. Similar concerns were raised when crypto currencies first emerged as a decentralised virtual asset[5] which then led to the inclusion of cryptocurrency market to be included in the relevant legal regimes for countering financial crime and AML. Authorities have had a chance to be proactive about regulating NFTs yet we have not seen any legal developments to date.

The anonymity and lack of regulation make NFT trading susceptible to money laundering. Unlike traditional banking systems, which require identity verification and compliance with AML laws, NFTs can be bought and sold anonymously on blockchain platforms, making it difficult to trace the origin of the transactions.[6] This makes it easier for criminals to transfer and convert their illegally acquired funds into NFTs, which can then be sold on exchanges or marketplaces without leaving a paper trail. Another way in which NFTs can be used for money laundering is through their high value and volatility.

[5] The same characteristics make crypto currencies attractive to criminals. See: Congressional Research Service. (2019) Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals. available at: https://sgp.fas.org/crs/misc/R45664.pdf (accessed 29.06.2022)

[6] Anonymity is a major issue in relation to NFTs. From the trading perspective, there is a risk that users will trade with themselves (wash trading) and, thus, will be able to launder their money themselves. Criminals, by abusing anonymity, can create their own NFT, register it on a marketplace and then purchase it themselves.

https://doi.org/10.54934/ijlcw.v2i3.57

Because NFTs can be bought and sold for millions of euros, criminals can use them to obscure the source of their illicit funds.[7] They can purchase high-value NFTs using their illegally obtained money and then sell them for cash, appearing as though they obtained the funds through legal means. This process enables criminals to evade detection by law enforcement agencies and financial regulators. Furthermore, the lack of regulation in the NFT market allows criminals to inflate the price of a particular NFT artificially (Chainalysis, 2022). This can be achieved through 'wash trading', where an individual or group of individuals would artificially inflate the price of NFTs by continuously buying and selling them among each other, creating false demand and driving up the price. Criminals can then sell their NFTs for a profit, even though the true value of the asset does not align with its original sale price.

While not all NFTs are used for illicit activities, and many legitimate buyers and sellers use them in a transparent and legitimate manner, the potential for NFTs to be used as a tool for money laundering highlights the need for increased regulation and oversight in this emerging market to prevent misuse and criminal activities.

3. EXAMPLES OF NFTs BEING USED FOR ILLICIT ACTIVITIES

As the NFT trade increase, it is inevitable that they will be increasingly used for money laundering, allowing individuals to transfer illicit funds anonymously. Criminals can hack into user accounts on NFT marketplaces and transfer NFTs to their own accounts, making it difficult to trace the origins of the funds (Owen and Chase, 2021). The lack of KYC checks on blockchain transactions also makes it easier for individuals to transfer funds without oversight or detection.

In tandem with the warning from the U.S. Treasury Department that "the ability to transfer some NFTs via the blockchain without a centralized intermediary may make them attractive to those seeking to launder illicit proceeds" (Department of the Treasure, 2022). Indeed, we have identified some of the emerging criminal schemes involving NFTs.

[7] The sale of an NFT for USD 69 million and the rise in prices of CryptoPunks demonstrate a volatile market where exorbitant amounts of money are involved. Christies. (2008). 10 things to know about CryptoPunks, the original NFTs; available at: https://www.christies.com/features/10-things-to-know-about-CryptoPunks-11569-1.aspx (accessed 29.06.2022).

https://doi.org/10.54934/ijlcw.v2i3.57

In one case, a trader on the online marketplace OpenSea was charged with wire fraud and money laundering for insider trading in NFTs (U.S. Attorney's Office, 2022-a). In another case, in March 2022, the US Department of Justice arrested two people for NFT fraud and money laundering (U.S. Attorney's Office, 2022-b). The defendants executed a one million-dollar NFT fraud scheme in January 2022 and were preparing to execute a second one prior to their arrests. In the UK, the HM Revenue and Customs Authority (HMRC) arrested three people who were hiding drug money of 1,4 million pounds using NFT purchases (www.bbc.co.uk, accessed 12.04.2023). It was later revealed by the police that the suspects were using sophisticated methods like stolen identities, false addresses, unregistered mobile phones, and fake invoices to disguise their original identities. HMRC stated that it had seized three digital NFTs which were being used for illegal investments (www.bbc.co.uk, accessed 12.04.2023).

4. CHALLENGES POSED BY NFTs FOR DETECTING AND PREVENTING ILLICIT ACTIVITIES

The emergence of non-fungible tokens (NFTs) has created a new avenue for the purchase and sale of unique virtual assets, such as artwork or music. However, it has also introduced challenges in detecting and preventing money laundering. On one hand, NFTs can potentially make it easier to identify the origin and ownership of virtual assets. This is because each NFT is a unique and identifiable virtual asset which can be traced on the blockchain back to its owner. On the other hand, NFTs can also facilitate money laundering by allowing criminals to convert their illicit funds into virtual assets through online payments.

The decentralised and anonymous nature of blockchain transactions can make it difficult for law enforcement agencies to identify money laundering activities. Decentralised exchanges such as Venus allow users with unhosted wallets to exchange crypto assets without a centralised party that would be obliged to conduct KYC, Customer Due Diligence (CDD), and AML checks (Department of the Treasure, 2020). Unhosted wallets facilitate anonymity in the blockchain and it is very difficult to establish who the beneficial owner is and that puts into question the benefits offered by blockchain technology.

https://doi.org/10.54934/ijlcw.v2i3.57

Additionally, the lack of clear regulatory guidance and industry standards for NFTs adds to the complexity of detecting and preventing money laundering through this avenue. As the placement stage is seen as the most critical for money launderers, NFTs provide an avenue to launder proceeds of crime successfully. The current legal frameworks in the EU, the US and the UK (leading jurisdictions in the Financial Action Task Force) do not address the challenges posed by NFTs nor do they provide a legal definition of NFTs (www.fatf-gafi.org, accessed 12.04.2023). This point will be discussed later in more detail, but it is certainly a basic and urgent issue that needs to be addressed by legislators. Apart from the regulatory gap on NFTs, it seems that government agencies do not fully understand the concept of NFTs and their functioning and they may not be able to differentiate them from fungible crypto-assets [7]. The fact that authorities have not actively engaged with the regulation of NFTs creates another barrier to the detection and prevention of financial crimes involving NFTs.

Furthermore, wash trading is a serious issue which hampers the detection and investigation of illegal activities involving NFTs. Wash trading can be defined as when the buyer and seller in a transaction are the same person or two persons colluding [9]. The wash trading activity is done to inflate the value of a specific asset with the hope that it will attract new buyers to support that false pricing level. In these cases, the seller will plan the pricing and different wallets involved and make the market look very profitable when, in reality, the action is being entirely orchestrated behind the scenes. According to the Commodity Futures Trading Commission in the USA, wash trading involves entering into or pretending to enter into transactions in order to create the appearance of purchases and sales, without incurring market risk or changing the trader's market position (www.cftc.gov, accessed 25.05.2023). The Financial Conduct Authority (FCA) in the UK has also assessed wash trading and its relation to money laundering. The FCA considers certain market-abuse practices, including wash trading, as potential indicators of money laundering activities. The FCA has highlighted wash trading incidents in connection with money laundering and has referred to the Financial Action Task Force's (FATF) reports on trade-based money laundering risks (FCA, 2019).

The FATF identified various techniques of trade-based money laundering some of which include over- and under-invoicing of goods and services, over- and under-shipment of goods and services, multiple invoicing of goods and services, and falsely described goods and services (FATF, 2020). In conventional financial markets, this is banned as it misleads the rest of the market about the true level of demand, distorts the prices and entices others to trade based on fake information and misleading value. Coordinated

https://doi.org/10.54934/ijlcw.v2i3.57

wash trades can be effective in artificially pumping price floors. Wash trades may also be a tactic used by money launderers to wash money into a more verifiable asset. These types of trades are typically characterised by NFTs selling at a price that is much higher than their market price (Grossman, 2023).

Finally, sleep-minting is a new form of fraud that may occur in NFT trading when an individual exploits a vulnerability in a smart contract or creates a limited-edition NFT contract to mint NFTs in the representation of other users and later claim ownership of those NFTs [1]. This type of fraud is particularly advantageous for individuals seeking to profit in the NFT industry by obtaining an endorsement from a well-known NFT user.

All the aforementioned elements pertaining to NFTs illustrate the urgent need for regulatory authorities to establish clear and specific rules for NFT trading. Before discussing the regulatory response to NFTs, some statistics will be presented in relation to NFTs and money laundering which will help to understand the extent of the transactions and funds involved in NFT trading.

5. STATISTICS ON MONEY LAUNDERING AND NFTS

5.1. Overview of recent money laundering statistics in the EU

Basel Anti Money Laundering Index evaluates the risk of money laundering and terrorist financing in 203 countries.[8] This calculation depends on reports released by international organisations such as; Financial Action Task Force (FATF), Transparency International, the World Bank, and the World Economic Forum. According to the latest report in 2022, in the European Union and Western Europe zone, "Belgium, Cyprus, the Netherlands, Spain, and the UK are listed by the US as major money laundering

[8] Basel AML Index 2022, Public Edition Ranking money laundering and terrorist financing risks around the world; available at: https://index.baselgovernance.org. (accessed, 25.05.2023)

https://doi.org/10.54934/ijlcw.v2i3.57

destinations. Malta is grey-listed by the FATF as a jurisdiction with strategic deficiencies in its AML /CFT framework".[9]

The mutual evaluation report (MER) conducted by FATF represents an assessment of the measures a country takes to fight money laundering (ML) and terrorism finance (TF) as well as the proliferation of weapons of mass destruction.[10] A MER entails a detailed 'description and analysis of a country's system for preventing criminal abuse of the financial system [and] focused recommendations to the country to further strengthen its system'.[11] When FATF conducts a MER, it uses the 40+ AML Recommendations as its benchmarks to measure the effectiveness and compliance of a country's AML framework with the recommendations.[12] One of the recommendations is on suspicious transactions reporting, which states, in part, that: 'The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether because of possible prosecution for a [ML] or TF offence or otherwise (so-called "indirect reporting"), is not acceptable' (FATF, 2012-2022, p.87).[13]

The endeavours of countries in the fight against ML depict the seriousness of the countries' willingness to fight against illicit events in cryptocurrencies. The wish of countries in fighting ML shows important clues for future regulations which may include NFT trades.

The analysis of the MER here is focused on the compliance component involving some EU Member States whose reports were released in recent years of 2022 and 2023, as well as bordering countries of Norway, Turkey and the UK whose reports were released in 2022 and 2023 respectively. In these MERs, there is a section on compliance with the FATF standards, whereby the categorised outputs of each recommendation are divided into the following elements: non-compliant with the recommendations, partly compliant with the recommendations, largely compliant with the recommendations, and compliant with the recommendations. In this regard, Table 1 is composed of an analysis of these compliance levels from the MERs for 2021 and 2022.

Table 1. *FATF Mutual Evaluation Reports Recommendation Results*

[9] https://www.fatf-gafi.org/
[10] https://www.fatf-gafi.org/en/publications/Mutualevaluations/More-about-mutual-evaluations.html.
[11] https://www.fatf-gafi.org/en/publications/Mutualevaluations/More-about-mutual-evaluations.html.
[12] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html;
[13] FATF (2012-2022), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, www.fatf-gafi.org/recommendations.html.

https://doi.org/10.54934/ijlcw.v2i3.57

	Non Compliance	Partly Compliance	Largely Compliance	Compliance	Non Compliance Rate	Partly Compliance Rate	Largely Compliance Rate	Compliance Rate
Bulgaria-2022	0	23	15	2	0.0%	57.5%	37.5%	5.0%
Croatia-2022	0	19	17	4	0.0%	47.5%	42.5%	10.0%
Estonia-2022	0	15	18	7	0.0%	37.5%	45.0%	17.5%
Finland-2022	0	7	24	9	0.0%	17.5%	60.0%	22.5%
France-2022	0	3	18	19	0.0%	7.5%	45.0%	47.5%
Germany-2022	0	5	18	17	0.0%	12.5%	45.0%	42.5%
Ireland-2022	0	6	17	17	0.0%	15.0%	42.5%	42.5%
Poland-2022	0	17	21	2	0.0%	42.5%	52.5%	5.0%
Norway-2023	0	3	18	19	0.0%	7.5%	45.0%	47.5%
Turkey-2022	2	4	22	12	5.0%	10.0%	55.0%	30.0%
UK-2022	0	1	15	24	0.0%	2.5%	37.5%	60.0%
EU-Average	0	12	19	10	0.0%	29.7%	46.3%	24.1%

According to Table 1, the UK has the biggest compliance rate with 60%, and France follows with 47.5%. When the EU average of the compliant rates in the MERs is considered, according to Table 5, the compliant rate is 24.1%, the largely compliant rate is 55.6%, and the partly compliant rate is 19.8%. To notice the differences more clearly, the analysis in Table 1 has been converted to Figures 1 and 2, which can be found below.

https://doi.org/10.54934/ijlcw.v2i3.57

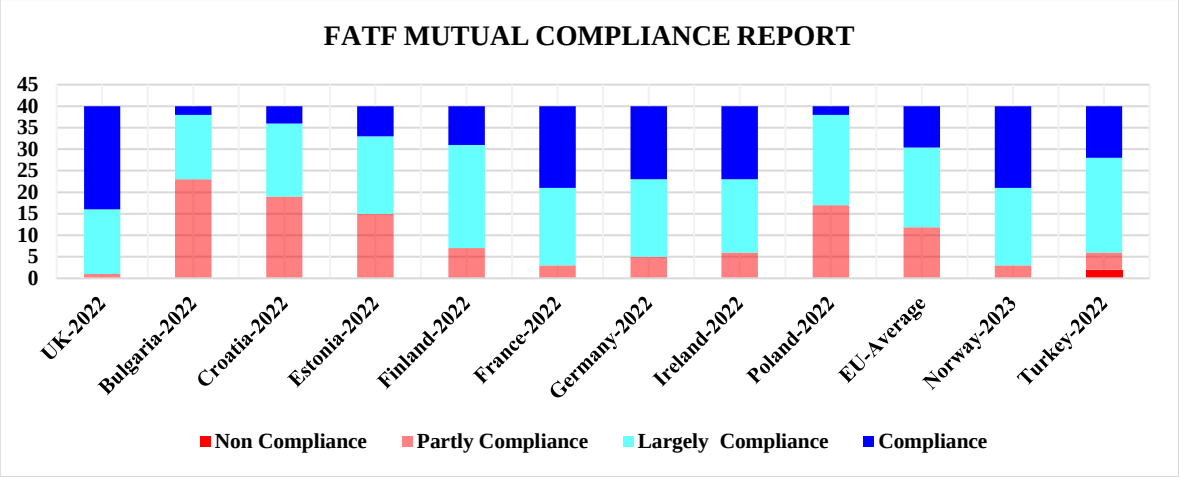


Figure 1. *FATF Recommendations Results of States in 2021 and 2022*

In Figure 2, blue bars compose of compliance and largely compliant fields, while red bars compose of partly compliant and non-compliance fields.

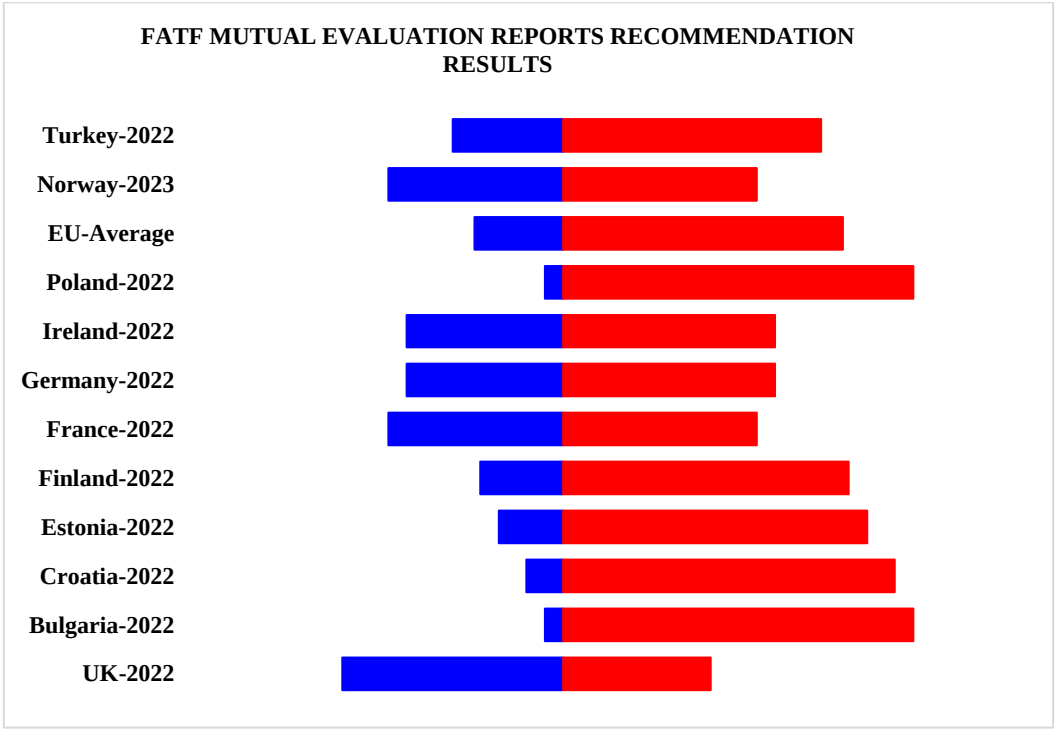


Figure 2. *FATF Recommendations Results of States in 2021 and 2022 with two categorized perspectives*

https://doi.org/10.54934/ijlcw.v2i3.57

Based on the results from these jurisdictions, the average compliance levels of each EU Member State can be seen. According to Figure 3, the average compliance rate in EU Member States is 24.1%, and the largely compliant rate in EU Member States is 46.3%. On the other hand, the average partly compliant rate in the EU Member States is 29.7%.

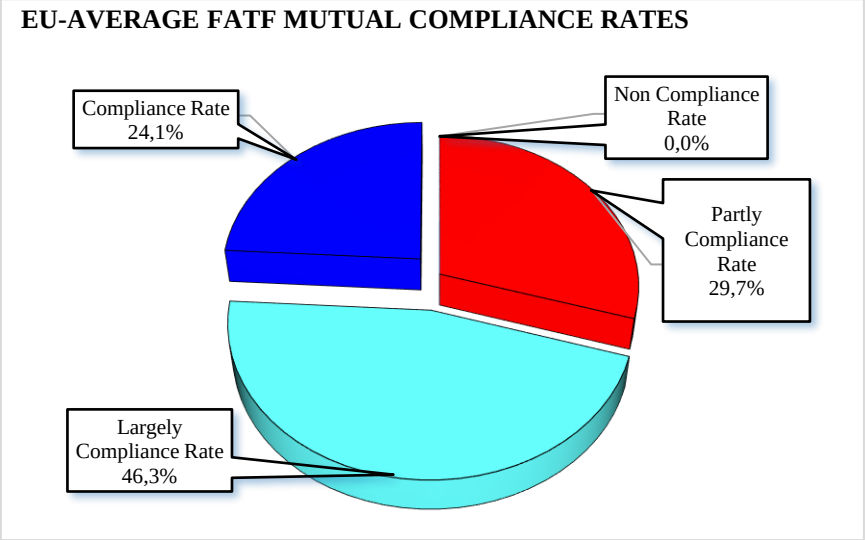
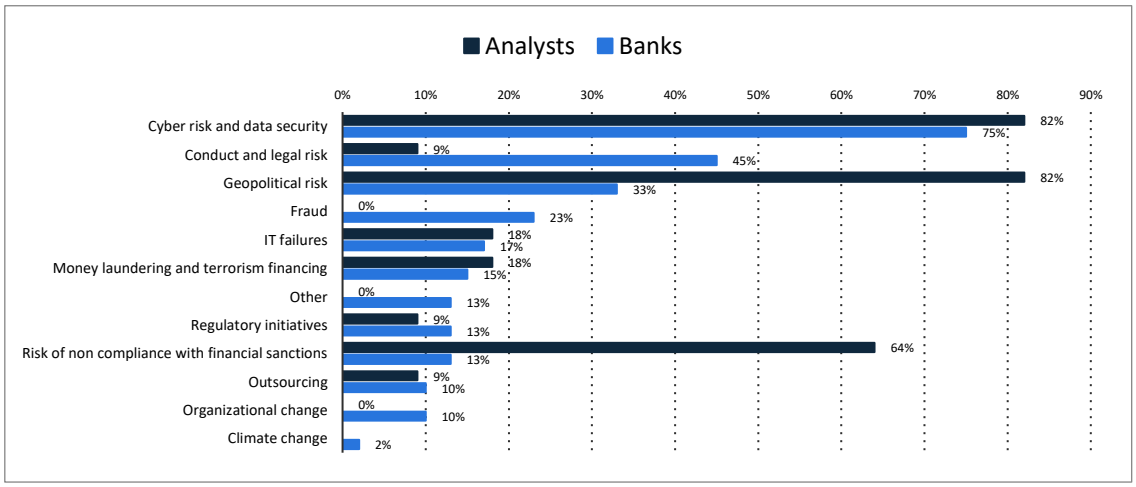


Figure 3. *EU Member States' Average in Compliance with FATF Recommendations*

For the European banking system in 2022, among the operational risk factors, money laundering and terrorist financing composed 18% of total risk according to analysts, whereas banks evaluated this risk rate by 15%. Money laundering activities not only relate to banking sector transactions but also includes other financial actors and trades in which proceeds of crime can be laundered. Figure 4 depicts the main drivers of operational risk for the banking sector in Europe (Statista, 2022-a).



https://doi.org/10.54934/ijlcw.v2i3.57

Figure 4. *Main drivers of operational risk for the banking sector in Europe according to European banks and analysts in 2022.*

The United Nations Office on Drugs and Crime (UNODC) predicts that the amount of money laundering worldwide may be up to 1.87 trillion euros (www.unodc.org, accessed 25.05.2023). Eurojust's statistics indicate that money laundering cases made up almost 15% of cases notified to the Agency between 2016 and 2021. These findings underpin the scale and seriousness of ML and the likelihood that NFTs can be utilised for ML.

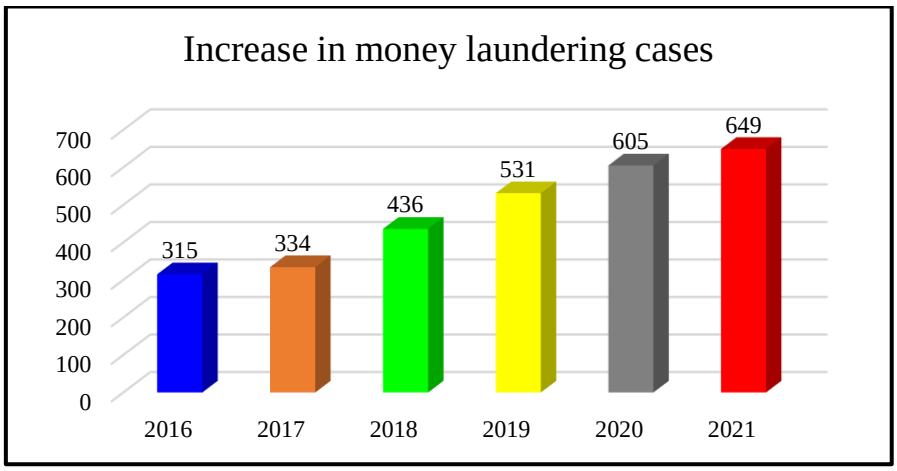


Figure 5. *Money laundering cases registered at European Union Agency for Criminal Justice Cooperation, Source: www.eurojust.europa.eu*

The number of cases related to money laundering events notified to Eurojust has constantly increased since 2016, making up 12–14 % of all notified cases. [14] In the same report, Eurojust shares the money laundering events in which EU Member States are involved. In Table 2, this is presented.

In Table 2, it can be seen that in some EU member states ML events are higher than others. When we order the countries in descending order, the first five countries are; Italy (723), France (637), Spain (578), Germany (569), and the Netherlands (398).

[14] European Union Agency for Criminal Justice Cooperation. "Eurojust Report on Money Laundering", 2022. available at: https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering (accessed, 25.05.2023)
Eurojust assessed that, virtual assets were still outside the scope of EU legislation and this situation increase the risks related with crypto assets. Although virtual asset service providers (VASPs) have to provide information and send transaction details in suspicious situations, virtual asset transactions need additional regulations.

https://doi.org/10.54934/ijlcw.v2i3.57

The analysis of the descriptive statistics on money laundering demonstrates that the phenomenon is ongoing and large amounts of money are involved even in strictly regulated jurisdictions such as the EU, the UK and the US. The involvement of NFTs in money laundering and other financial crime activities makes the picture more complex as it will be analysed below.

Table 2. *EU Member State Involvement in money laundering cases*

EU Member State Involvement in Money Laundering Cases			
State	As owner	As requested participant	Total
BE	60	219	279
BG	87	185	272
CZ	90	116	206
DK	20	70	90
DE	133	436	569
EE	37	68	105
IE	13	78	91
EL	133	73	206
ES	167	411	578
FR	267	370	637
HR	24	88	112
IT	380	343	723
CY	59	155	214
LV	147	105	252
LT	31	103	134
LU	22	145	167
HU	113	172	285
MT	16	110	126
NL	154	244	398
AT	47	160	207

https://doi.org/10.54934/ijlcw.v2i3.57

PL	70	217	287
PT	107	120	227
RO	128	202	330
SI	96	72	168
SK	74	110	184
FI	49	49	98
SE	92	80	172

5.2. Digital structure, transaction details and statistics related to popularity of NFTs

NFTs consist of two different components in their digital structure. The first component is smart contracts, which are stored on ERC721-Etherchain. The second component is the content and metadata, which is too large to be stored on Etherchain. As a result, the smart contract addresses the metadata on Etherchain permanently, but the user/owner can only access the metadata until it is deleted (Benson, 2021). If the data storage field no longer supports the NFT, the owner will no longer be able to access his/her NFT (Ravenscraft, 2022).

This temporary situation makes NFTs vulnerable, and additional regulations are required to protect individuals, especially against risks stemming from structural weaknesses.

Moreover, data mining activities on NFT transactions to collect transaction details are limited due to the privacy-based structure of smart contracts. In the case of NFTs, each NFT is assigned a unique code group generated as a distinct identifier. This code, obtained through computer science abilities, serves as the Application Binary Interface (ABI), enabling communication between two program modules, typically between the metadata for NFTs (operating systems) and the smart contracts for NFTs (user programs) (Quicknode, 2023).

In data mining processes for transaction details, researchers and quantitative analysts in finance commonly focus on capturing the total value of the transferred products. However, in the case of NFT transfer transactions on ERC721 and ERC1155, extracting the value of the product is not straightforward without the use of ABI. While researchers and quantitative analysts can gather transaction details for ERC721 and ERC1155, the value of the product cannot be obtained without ABI.

https://doi.org/10.54934/ijlcw.v2i3.57

Furthermore, another challenge in the data purification process for NFT transactions arises from dependent transactions. Some transactions on ERC721 and ERC1155 involve activities such as airdrops or non-transfer/non-mint processes, which need to be taken into consideration during the data cleansing process.[15]

In the minting, transfer, or safe transfer method IDs within transactions, a new ownership is acquired through the transaction. However, in other types of transactions, there is no transfer of ownership for any NFT. Due to this distinction, when analysing new ownership of NFTs, the data purification process needs to specifically collect, mint or transfer details from transactions. It is important to note that although there are designated code groups for each of these transaction types, users have the flexibility to utilise other codes in their mint or transfer transactions.

To visualise these transfers and examine the transaction methods, a screenshot of the transfers on Etherscan is provided in the figure below.

Transaction Info	Method	Age	From	To	Type
0x08c3b69f31b13a581...	Borrow	23 secs ago	*深大高财生.eth	0x294693...8D98a20B	ERC-721
0x79e832223e5d05ae...	0x00000000	23 secs ago	fastrabbit.eth	0xbbFEa9...35688Cf7	ERC-721
0x07f34171fbb8668ffe...	Mint Batch	23 secs ago	Null: 0x000...000	0xD52b58...C9a8161E	ERC-1155 x2
0xdc8a69a70e279ac6...	0x00000000	23 secs ago	sladdict.eth	0x700b8B...e03CF33b	ERC-721
0x2e0de4d6e813d081...	Mint	35 secs ago	Null: 0x000...000	bookiedew.eth	ERC-1155
0x5060b19e19c7f4a0f...	Claim And Burn	35 secs ago	0x23916B...0779f323	0x0fE959...867aEa3B	ERC-721
0x9525fabe745836925...	Safe Transfer ...	35 secs ago	0x988351...9A358477	0x81cB16...044a68eB	ERC-721
0x812e2639e35b1fea5...	Bulk Transfer	47 secs ago	0x1f588d...1Bc42caA	0x9a201E...7F57E92e	ERC-721
0x812e2639e35b1fea5...	Bulk Transfer	47 secs ago	0x1f588d...1Bc42caA	0x9a201E...7F57E92e	ERC-721
0x8c8fb58c31ad3ab5f...	Match Advanc...	47 secs ago	0xee5A43...Aa221Bb4	0x17F081...18330Cd0	ERC-1155
0xb4e26cea053d0b62...	Mint	47 secs ago	Null: 0x000...000	141344.eth	ERC-721

Figure 6. *Transaction samples on ERC721 and ERC1155.*[16]

[15] Available at: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/ (accessed 11.05.2023)
[16] Available at: https://etherscan.io/nft-transfers (accessed 11.05.2023, time 11.00 am in GMT+1)

https://doi.org/10.54934/ijlcw.v2i3.57

In the specified transaction procedures on ERC721 and ERC1155, each of these methods has a designated code group, and transactions must begin with these method IDs. As a result, individuals can easily trace the movements of these products on the blockchain, enabling market evaluation and token analysis. However, users may not always adhere to the transaction code rules defined in smart contracts. Consequently, the data purification processes require additional improvements to accurately identify ownership transactions.

Due to these challenges, data and statistical report providers often resort to utilising all transaction numbers, total wallet numbers, or total payment amounts for transfers. These alternative measures are employed to compensate for the difficulties in precisely tracking and categorising ownership transactions. [17]

Moreover, at the time of writing this paper, there has been no statistical output or analytical reports related to NFTs by state or public authorities. All the available datasets and statistical information on NFTs have been released by private entities. The statistics provided by crypto research companies are limited because of the reasons related to the smart contracts, ABI and transaction method IDs difficulties which were explained above.

Because of the difficulties in tracking transaction details of NFTs, NFTs are seen as vulnerable products for illicit financial activities. Fraudsters do not want to be tracked and NFT based illicit activities provide a field in which fraudsters could not be tracked easily.

Although the popularity of NFTs has increased in general, there are variations in terms of their use or popularity in different segments of the NFT market. In the calculation of the amount of total sales, the transaction details of wallet movements are taken into account. Therefore, the in-game transfers of NFTs are not considered in NFT game sales values. As explained in Table 3, it is clear that sales in game and art segments have consistently increased and these two segments were not affected by the decrease in 2019. The general NFT sales amount increased enormously in 2021 (Statista, 2022-b).

Table 3. *Value of sales involving a non-fungible token (NFT) in different segments from 2018 to 2021 (in million U.S. dollars only recordings on ETH transactions)*

[17] Available at: https://api.a16zcrypto.com/wp-content/uploads/2023/04/State-of-Crypto.pdf (accessed, 25.05.2023)

https://doi.org/10.54934/ijlcw.v2i3.57

	2018	2019	2020	2021
All	36.77	24.02	66.78	13981.9
Collectible	13.86	2.71	16.45	7130.05
Game	5.19	11.59	15.26	2153.82
Art	0.05	0.45	17.11	2107.57
Metaverse	16.35	5.38	15.97	630.99
Utility	1.29	4.11	2.41	75.5
DeFi	0	0	0	19.75
Undefined	0.03	0	0	1864.22

The increased rate and amounts of NFTs in various segments in 2021 were different from each other. Accordingly, each segment analysis may give specific and unique information about NFT trading.

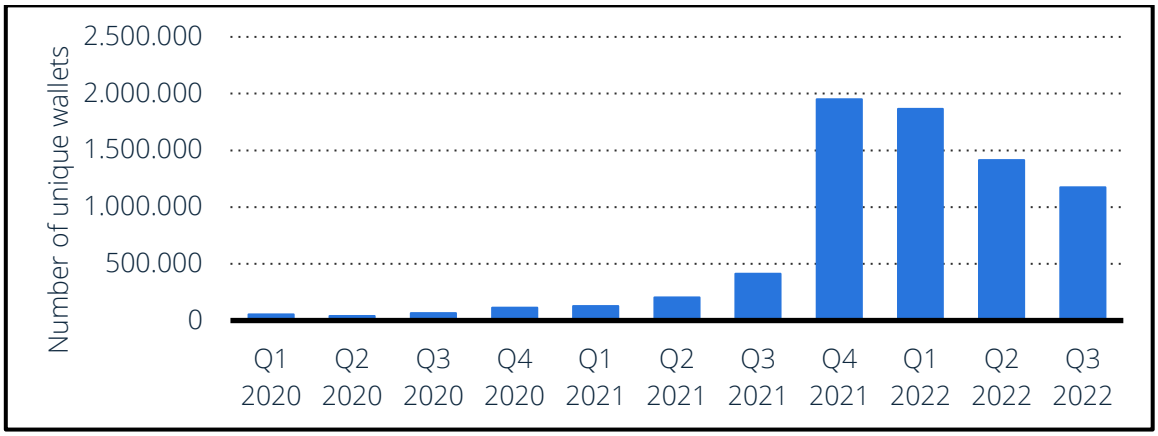


Figure 7. *Number of unique wallets that either bought or sold an NFT asset worldwide from 1st quarter of 2020 to 3rd quarter of 2022*

Figure 7 shows that NFT usage and popularity in the crypto world reached the top level in the third quarter of 2021 and the first quarter of 2022 (Statista, 2022-c). This indicates that NFT popularity was still very high in 2022.

Table 4. *Search interest of consumers in the search term "NFT" in 206 different countries and territories worldwide from December 2021 to November 2022*

https://doi.org/10.54934/ijlcw.v2i3.57

World General		European Union		Population on 1 January 2022
Rank	**Country**	**Rank**	**Country**	
1	China	12	Cyprus	**904,705**
2	Hong Kong SAR	27	Malta	**520,971**
3	Singapore	46	Estonia	**1,331,796**
4	Gibraltar	49	Netherlands	17,590,672
5	Macao	50	Slovenia	2,107,180
6	Cayman Islands	55	Romania	19,038,098
7	Nigeria	56	Portugal	10,352,042
8	Andorra	57	Latvia	1,875,757
9	Taiwan	75	Belgium	11,631,136
10	Mongolia	76	Lithuania	2,805,998
11	Philippines	77	Ireland	5,060,005
12	Cyprus	86	France	67,842,582
13	Bermuda	90	Sweden	10,452,326
14	Lebanon	94	Austria	8,978,929
15	South Korea	97	Croatia	3,879,074
16	Guam	102	Spain	47,432,805
17	Venezuela	106	Bulgaria	6,838,937
18	French Polynesia	107	Denmark	5,873,420
19	Sint Maarten	112	Italy	58,983,122
20	Canada	124	Germany	83,237,124
29	United States	127	Hungary	9,689,010
53	United Kingdom	131	Greece	10,603,810
58	Albania	132	Slovakia	5,434,712
85	Turkey	160	Poland	37,654,247

https://doi.org/10.54934/ijlcw.v2i3.57

According to search results on Google, the crypto interest of customers can be gained state by state (Statista, 2022-d).[18] In Table 4, the Worldwide rankings of the countries are presented.

In Table 4, it is clear that among EU member states, Cyprus and Malta have a bigger interest in NFTs than other EU Member States. Besides, Asian countries' interest in NFTs is higher than EU Member States. According to Table 4, between EU countries, the total populations of the countries lesser than 1.5 million have a bigger interest in NFTs than higher than 1.5 million total populations.

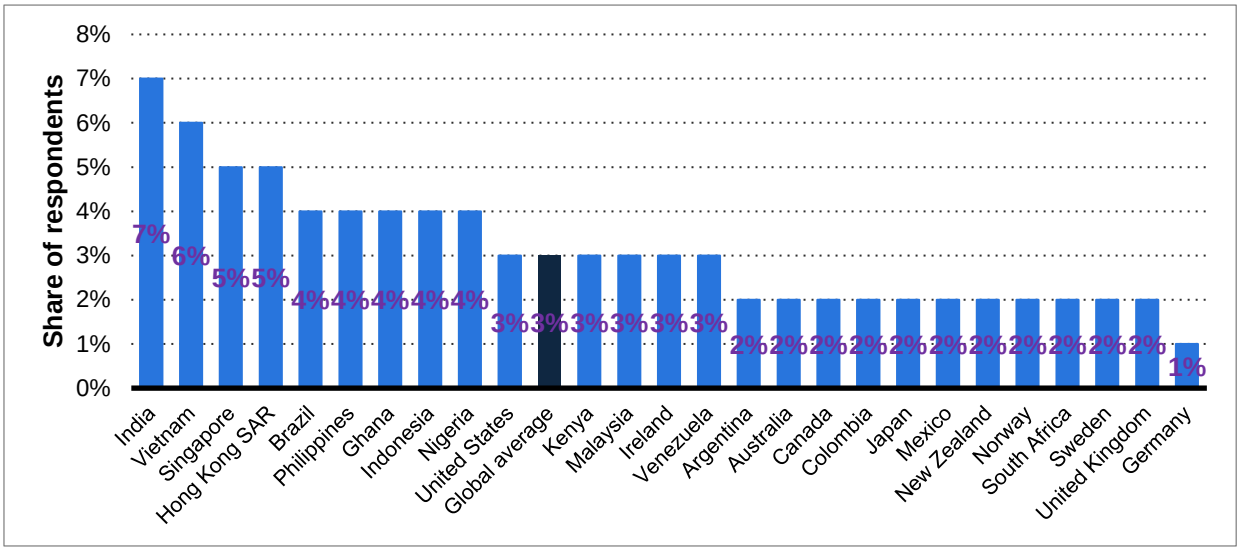


Figure 8. *Percentage of adults who own an NFT in selected countries worldwide as of September 2022*

In Figure 8, NFT adoption in 26 countries is presented (Statista, 2022-e). In Figure 8, the share of adults who own NFTs is given. The data used in this chart is composed of observations from July 2022 to September 2022. The owning rate assessed the individuals who are 18 years or older. The results are the average rates of these three months. As seen in Figure 8, there is no European Union Member State in the first 10 countries in the adoption of NFTs. The rate of NFT ownership in the EU is lower than the global average.

[18] Available at: https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en (accessed 21.05.2023)

https://doi.org/10.54934/ijlcw.v2i3.57

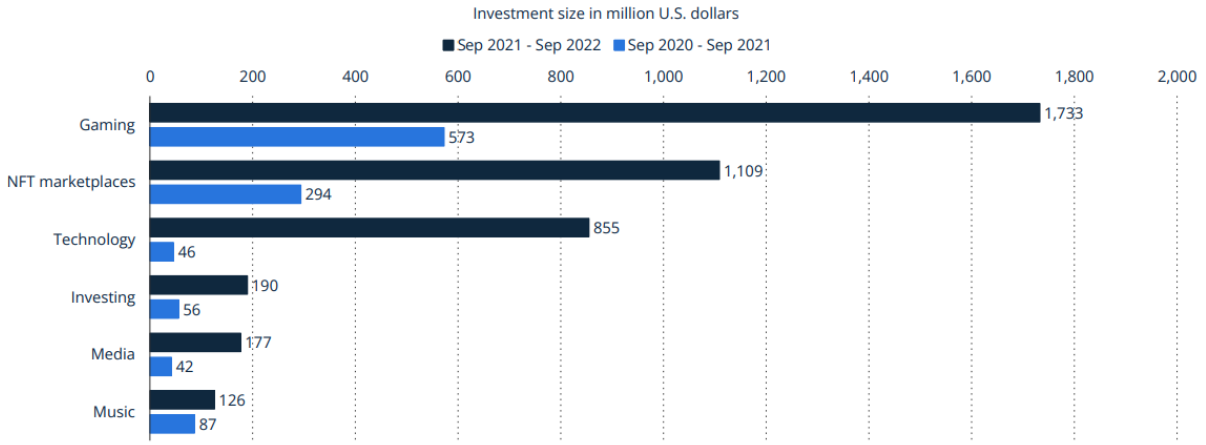


Figure 9. *NFT categories with the highest value of investments from September 2020 to September 2021, and September 2021 to September 2022 (in million U.S. dollars)*

According to Figure 9, it is clear that the investments in NFTs in each segment were higher in 2022 than in 2021 (Statista, 2022-f). Thus, it can be concluded that the returns from NFTs in the markets of these segments will increase in 2023.

The biggest investment in NFTs was in the game segment in 2022. This can be another important issue for suspicious transactions because in-game transaction detection is not as easy as EtherScan transactions. Because in-game transactions happen in a private database and the database is managed by the game company, each game company has the ability to share suspicious transactions because in trade-based regulations customers' privacy is under protection. This means that, under the current legal framework, the game companies can assess if transactions are suspicious or not but they have no legal duty to report these.

Besides, many new companies declared their interest in NFTs and allocate a budget to invest in NFTs in the near future.[19] One of the biggest investors in NFTs in the near future may be Amazon (Basulto, 2023). The company declared its interest in NFTs and this may help formal and informal actors to understand the complicated structure in detail and construct regulations more efficiently because Amazon

[19] https://www.nftculture.com/sponsored/latest-nft-projects-to-invest-in-2023/
https://wellfound.com/startups/industry/nft-5
https://www.analyticsinsight.net/top-ten-nft-development-companies-in-2023/
https://www.nftme.tv/

https://doi.org/10.54934/ijlcw.v2i3.57

declared the new initiative as "NFTMe", which explores NFT culture and disruption worldwide (Bhardwaj, 2023), (Iddenden, 2023).

Some of the crimes on NFTs are; money laundering (Zeljko B and Momcilo), fraud [10], theft (Elliptic, 2022), wash trading (Gilbert, 2022) and sleep minting [1].

In the "Global Financial Stability Report" from International Monetary Fund (IMF), cryptocurrencies' reliability in terms of an investment tool was assessed as weak and evaluated as a regulation need field. In this report, IMF offered a large and urgent regulation for virtual assets and virtual asset service providers (VASPs). [20]

5.3. Analysis of the limitations of current data on NFT-related financial crime

Table 1 presented some of the different segments in which NFT sales are involved. These include; Collectibles, Games, Art, Metaverse, Utility, DeFi and Music.

Especially NFT-based game industry should be seen as different from other segments because transaction details of users therein cannot be traced on-chain transactions. The money paid for game creatures in the NFT world happens in a private platform in which only the game company has the transaction details. As per the user terms and conditions, especially customer privacy, game companies in the NFT-based game industry do not wish to share the transaction details some of which may include ML.

NFT marketplace transactions are another important issue to focus on. When the transactions happen in a cryptocurrency marketplace the details can be gained via chain transactions because these kinds of transactions put traces on chains. Whereas the transactions in private companies such as game-based NFT marketplaces like Aixie Infinity, do not place any trace in any public field. Thus, tracking in-game transactions is not easy because they are not recorded in a publicly open area like Etherchain

[20] International Monetary Fund (IMF). "Global Financial Stability Report", 2022, available at: https://www.imf.org/en/Publications/GFSR (accessed, 20.05.2023)
According to classical investment methods such as equities, there is an increasing trend with investment methods and market volatility, and in crypto markets volatility is higher. In 2022, bitcoin price decreased by more than 50 percent, and some crypto funds were unwound. In this period, stable coins, which are expected to have a stable value close to dollar, such as Terra, collapsed.
Other stable coins such as Tether, the largest collateralized stable coin, decreased significantly too. On the other hand, some other stable coins received some additional money inputs and gained capability to maintain parity during this high volatile period.

https://doi.org/10.54934/ijlcw.v2i3.57

transactions. The transaction details are obtained only by the game companies in which these transactions happen.

On 28 March 2023, a suspicious in-game money laundering event was submitted to the San Francisco federal court in the USA. In Roblox which is one of the biggest children's gaming platforms, over 300 users were confronted with ML by buying fake in-game items with in-game currency.[21]

In another event involving Roblox, the company was charged with fraud and arbitrarily deleting trading records. During the court proceedings, it was stated that: "The trick is simple: Roblox encourages users to purchase in-game content on the platform which it has made available—and from which Roblox earns real money—without performing any meaningful oversight to ensure that the content coming into its marketplace complies with the platform's policies. After its users have paid for their purchases, Roblox then performs sham 'content moderation' by deleting content which it has determined violates its policies. Roblox then refuses to refund anything to its users for their deleted content. When users report that their content has disappeared in error and demand refunds, Roblox cleverly deflects its irresponsible profit-seeking behavior by alleging that the content violated the platform's policies, without any actual detail, offering Roblox cover to engage in a fraudulent content deleting scheme" (Neale, 2023).

The charges were upheld and Roblox agreed to pay $7.5 million to affected users (Neale, 2023).

These kinds of illicit activities could not be detected without complaints from game users because in-game transactions are not publicly open like Etherchain transactions.

Another important factor for illicit financial activities with NFT is the definition of these structures (McDowell, 2023). In a case in the Southern District of New York on the 8th of February 2023, an artist Mason Rothschild was found to have violated the brand protections of Hermès, and the First Amendment of the US Constitution did not protect his 100 "Metabirkins" NFTs due to not being artistic creatures.[22]

Moreover, as stated earlier, collecting the transaction details on Etherchain is not easy. The transaction procedures implemented by Etherchain must be carried out under the whitepaper procedures

[21] United States District Court Northern District of California San Francisco Division Case 3:21-cv-03943-WHO

[22] U.S. District Court for the Southern District of New York, No. 1:22-cv-00384.
The court decision is: "The nine-person jury found Rothschild liable for trademark infringement, trademark dilution and 'cybersquatting' (the practice of using a name in bad faith with the intent of making a profit) and awarded Hermès $133,000 in total damages (an estimation that at least includes the amount he is thought to have earned from the works) on 8 February, the third day of deliberations."

https://doi.org/10.54934/ijlcw.v2i3.57

declared by Ether. However, not all of the NFT transactions have been constructed according to the procedures correctly. This is why the codes for transfers and mints (in which transaction hash starts with defined codes) have not been created according to the whitepaper correctly in each transaction. Because of this reason, attention to the data purifying process is needed to prepare datasets to analyse illicit flows. In this purifying process, researchers have to focus on the metadata (other than NFT structural component) from the transactions which includes mint and transfer details.

6. REGULATORY RESPONSES TO NFTs AND MONEY LAUNDERING

6.1. Overview of current EU regulatory responses to NFTs and money laundering

Given the complexity and vulnerabilities inherent in NFTs, it is imperative to establish a regulatory framework that ensures the safety, transparency, accountability and stability of markets in crypto assets and NFTs. The EU's proposed Markets in Crypto Assets Regulation (MiCAR) is a step towards an innovation-friendly regulatory framework for crypto assets. The MiCAR proposal aims to provide rules on the public offering of crypto-assets, the admission of crypto-assets on a trading platform, the licencing of crypto-asset service providers and the implementation of market abuse rules for crypto-assets businesses.[23] On 20 April 2023, the European Parliament approved with 529 votes in favour the adoption of MiCAR.[24] The text should now be formally endorsed by the Council, before it is published in the EU Official Journal.

MiCAR provides a definition for crypto-assets, the first EU legal instrument to do so. MiCAR thus defines crypto-assets as "digital representation of value and rights which may be transferred electronically, using distributed ledger technology or similar technology".[25] However, the MiCAR may not address all challenges posed by NFTs specifically. The worth of NFTs can be attributed to their distinct features and the usefulness they offer to token holders. While these tokens are traded, they are not easily exchangeable, and their relative value cannot be determined by comparing them to existing markets or similar assets because they are unique. Consequently, MiCAR appears to exclude NFTs from its scope due to their limited financial utility. However, fractionalised NFTs, which are fractions of an NFT, or NFTs released

[23] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final, p. 2.
[24] Available at: https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu (accessed, 20.05.2023)
[25] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final, Article 3(1)(2).

https://doi.org/10.54934/ijlcw.v2i3.57

in large series or collections, are not unique or non-fungible in and of themselves and, as such, are not exempted by MiCAR.

There are three main categories of token in the proposed MiCAR. These are asset-referenced token, e-money token and other crypto-assets with different requirements for each in relation to licencing and issues. NFTs may fall under the last category, "other crypto-assets". In this last category, issuers of crypto-assets do not have any specific licensing obligations but are required to be a legal entity (even if they are established outside the EU) and to comply with certain business and governance conduct requirements.[26]

While this category of "other crypto-assets" will be subject to specific rules on *inter alia* admission to trading on a trading platform, the authorisation of related service providers and market abuse rules, the proposal **exempts** issuers of crypto-assets which are unique and non-fungible from the requirement to publish a white paper for public offerings. Consequently, NFT providers and traders will be exempted from the obligation to publish such a white paper but they will be subject to anti-money laundering and counter-terrorist financing rules. In the recitals of the MiCAR, special reference is made to "virtual assets" as defined by the Financial Action Task Force (FATF). According to this definition, a virtual asset 'is a digital representation of value that can be traded, or transferred, and can be used for payment or investment purposes' (FATF, 2020). In its latest draft guidance on March 2021, FATF replaced a previous reference to "assets that are fungible" with "assets that are convertible and interchangeable" (FATF, 2021). This definition from FATF may involve NFTs but this is not clear, yet.

The latest development on MiCAR indicates that the European Parliament proposed changes to the upcoming anti-money laundering proposal for reform and insisted that NFT platforms and companies providing NFT-related services are within the scope of the regulation (Field, 2023). The changes proposed by the European Parliament will fill the gap created by MiCAR which leaves NFTs out of its scope. This new information seems to confirm unofficial reports from September last year that the European Parliament was pressing for the inclusion of decentralised finance (DeFi),[27] decentralised autonomous organisations (DAOs), and NFTs into the proposed AML/CFT legislative reform which is currently under

[26] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final, Article 13.
[27] "DEFI is a kind of distributed ledger-based finance and applications contemplated to alter the present financial means-centralized finance."

https://doi.org/10.54934/ijlcw.v2i3.57

discussion. Unfortunately, this information is based on leaked documents from the European Parliament therefore, they should be treated with caution until an official announcement is made.

Overall, it is evident that regulations for markets in crypto assets and NFTs are necessary to promote stability, transparency, and sustainability. As the market continues to evolve and grow, regulators must remain vigilant and adaptable to ensure that regulations keep pace with developments in these markets while promoting innovation and protecting investors and consumers. The proposals below highlight the importance of establishing a regulatory framework for markets in crypto assets and NFTs.

6.2. Proposals for future regulatory action

With the emergence and growing popularity of NFTs, there has been a call for regulation to address potential legal, financial, and ethical issues. The lack of clear regulatory oversight for NFTs has led to concerns within the art world, particularly regarding issues of intellectual property, ownership rights, taxation, and financial crime. Therefore, it is important to consider potential proposals for future regulatory action on NFTs [8].

One possible proposal is to require NFT creators and platforms to provide clear disclosures regarding ownership rights, including any potential limitations or restrictions. This would help to mitigate disputes over ownership and prevent fraudulent or unauthorised sales. NFTs serve the purpose of establishing undeniable digital ownership over various types of assets, including but not limited to digital collectibles, crypto art, intellectual property rights, online games, real estate, jewellery, vehicles, licenses, and financial documents. When classifying a particular NFT, it is essential to consider the type of asset it represents. For example, the definition put forward by MiCAR would apply only to NFTs that do not represent financial instruments under other financial laws of the EU, such as Directive 2014/65/EU (known as MiFID II). If MiFID II is enacted and provides a clarification of the current definition of financial instruments to include crypto assets within its scope, then NFTs that represent financial instruments may be considered as financial assets.

Given the diverse nature of assets that NFTs can represent, one could argue that their classification should align with the underlying nature of the goods they represent. For instance, if an NFT represents a financial asset, it should be classified accordingly, while if it represents digital art or crypto collectibles,

https://doi.org/10.54934/ijlcw.v2i3.57

it should have the same status as traditional art or collectibles. As such, the classification of NFTs should be based on the underlying asset type, which can vary from financial instruments to virtual assets. It can be suggested that national supervisory authorities outlined in MiCA should be responsible for classifying NFTs. Relying solely on legal opinions drafted by the private sector to classify crypto assets may result in a "race to the bottom" among EU jurisdictions,[28] as crypto asset service providers (CASPs) and token issuers may relocate their businesses to countries where lawyers are more likely to draft favourable legal opinions. Therefore, placing the responsibility of NFT classification under the jurisdiction of national supervisory authorities could mitigate this issue and create a standardised framework for NFT classification across the EU.

According to the analysis by the UK Jurisdiction Taskforce in its Legal Statement on Cryptoassets and Smart Contracts,[29] it is suggested that NFTs can be classified as intangible property known as "things in action" and consequently qualify as property [4]. This perspective has been supported in various court cases in England,[30] New Zealand,[31] and Singapore.[32] By treating NFTs as property, these legal decisions enable the assignment of property rights to NFTs and contribute to providing legal certainty to both NFT holders and CASPs involved in NFT transactions. This marks a crucial step forward in establishing a solid legal framework for NFTs.

If an NFT is a property that is traded then just like any other tangible and intangible asset, it should be subject to a degree of oversight and due diligence. Accordingly, there should be a requirement for NFT platforms to implement Know Your Customer (KYC) and AML procedures to verify users' identities and prevent illegal activities such as money laundering, terrorism financing or tax evasion. A further proposal is for regulators to work with industry stakeholders to develop standards and best practices for NFT creation, distribution, and sales. This could involve developing guidelines for identifying and addressing potential legal issues, ethical considerations such as artist compensation and attribution, and consumer protection concerns. Overall, proposals for future regulatory action on NFTs should involve a combination of measures to promote transparency, accountability, and ethical behaviour. Furthermore, efforts should

[28] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593, Article 81.
[29] UK Jurisdiction Taskforce. 2019. Legal statement on cryptoassets and smart contracts. Pp. 09-12. available at: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf, (accessed, 27.11.2022)
[30] AA v Persons Unknown [2020] 4 WLR 35; Fetch.AI Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm).
[31] Ruscoe v Cryptopia Ltd [2020] NZHC 728; Jonathan Dixon v R - [2015] NZSC 147.
[32] [2022] SGHC 264. Originating Claim No 41 of 2022 (Summons No 1800 of 2022).

https://doi.org/10.54934/ijlcw.v2i3.57

be made to balance regulation with innovation to ensure that NFTs can continue to thrive and evolve as an important element of the digital economy.

One additional proposal for future regulatory action on NFTs could be the establishment of a dispute resolution mechanism to handle disputes related to ownership, provenance, and authenticity of not only NFTs but also other types of virtual assets. This would provide a way for parties to resolve their disputes without resorting to expensive litigation or arbitration. This proposal aligns with the regulatory standards promulgated for mandatory dispute resolution mechanisms within governance frameworks, as it can help to ensure that any disputes related to NFTs are addressed efficiently and in a transparent manner. Furthermore, the establishment of a dispute resolution mechanism for NFTs could potentially increase confidence among buyers and sellers, thereby promoting greater participation in NFT market activities. This proposal would also address the current lack of clarity and consistency in resolving disputes related to NFTs, as there is currently no established legal framework or mechanism for resolving such disputes. Additionally, the establishment of a dispute resolution mechanism for NFTs would enable parties to obtain legal and impartial solutions in a cost-effective and time-efficient manner, which would be beneficial for all stakeholders involved in the NFT market.

Another potential proposal for future regulatory action on NFTs is to require the use of Distributed Ledger Technology (DLT) to track and manage the ownership and transfer of NFTs.[33] This would provide greater transparency and accountability for NFT ownership, as well as help prevent fraudulent activity. In addition, regulations should also address the potential environmental impact of NFTs, particularly in terms of energy consumption. It is important to strike a balance between regulation and innovation so that NFTs can continue to evolve as an integral component of the digital economy while also ensuring that they adhere to ethical standards and do not harm the environment. Moreover, the usage of Blockchain-enabled solutions has been proposed for asset identification by binding tokens to physical properties.

[33] 'Distributed Ledger Technology' or 'DLT' means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, whether the same is certified under that Act or otherwise; 'DLT asset' means – (a) a virtual token; (b) a virtual financial asset; (c) electronic money; or (d) a financial instrument, that is intrinsically dependent on, or utilises, Distributed Ledger Technology;"
available at: https://www.mfsa.mt/wp-content/uploads/2018/12/fintech-main-legislation.pdf (accessed 25.05.2023)

https://doi.org/10.54934/ijlcw.v2i3.57

6.3. Training and research

The domain of NFTs is a rapidly developing area that merges technology and art and lacks a well-defined regulatory framework. The surge in sales of NFTs and their increasing production and distribution have created a growing demand for training among the entities responsible for governance, law enforcement, and suspicious transaction reporting in this sphere. Law enforcement agencies (LEAs) need to remain current and well-informed regarding the workings of NFTs and the associated risks. The US Department of the Treasury's report on "Money Laundering and Terror Finance Through the Trade in Works of Art" published in February 2022 highlights the need to regulate and oversee NFTs as a developing domain of digital art (Department of the Treasure, 2022). The report emphasizes the necessity of updating guidance and providing training to LEAs, as well as customs and asset recovery agencies, to identify the risks and opportunities available to launderers (Department of the Treasure, 2022). However, the question of the most efficient way to organise this training remains unresolved, given the scarcity of specialised academic training programs on NFTs and the limited expertise in this domain.[34]

On an academic level, the teaching of art law, NFTs, and money laundering is minimal. Higher education institutions do not provide courses on NFTs, limiting the ability of LEAs to benefit from these courses individually (www.qmul.ac.uk, accessed 29.06.2022), [2].[35] While private organisations such as Christie's and the Blockchain Council provide courses on NFTs that offer a good understanding of NFTs,[36] they do not concentrate on the nexus of NFTs, money laundering, and other crime risks and anti-money laundering (AML) policies. In addition, some initiatives for training in the crypto world, such as Crypteya, are not compatible with the traditional academic approach to professional training and development.[37]

To resolve this scarcity of specialised training, LEAs must establish Public-Private Partnerships (PPPs) with experts in the field by combining expertise from academia, industry, and independent actors [3].[38] The ideal solution for LEA training would be to bring all stakeholders together in PPPs to provide

[34] At the time of writing this article, several LEAs around Europe indicated that they have not received any specific training on NFTs.
[35] The first one is an LLM about art, business and law where, this year, certain classes are introduced for NFTs. The second is the recent announcement of Miami Law School introduction of its innovative NFTs course.
[36] Christie's Education. (2022) Virtual Course Understanding Crypto Art and NFTs. available at: https://education.christies.com/courses/continuing-education/short-courses/understanding-crypto-art-nfts (accessed 29.06.2022) and Blockchain Council. available at: https://www.blockchain-council.org (accessed 29.06.2022).
[37] Crypteya Academy. available at: https://crypteya.academy (accessed 29.06.2022).
[38] The authors propose the introduction of public-private partnerships with law enforcement practitioners, lawyers, computer science experts and cyber-forensics specialists in the framework of crypto currency regulation and enforcement.

https://doi.org/10.54934/ijlcw.v2i3.57

valuable insights that will aid in the rapid emergence of NFTs. If PPPs are not feasible, a particular NFT training program should be established within the police academies. It is well-known that police academies have their own training programs to educate and prepare their personnel. The course should include NFTs from legal and technological perspectives, designed by legal scholars, technology experts, and other related professionals. LEAs should understand the technological structure of NFTs, their position in the art market, and the combination of technology and art. An analysis of the business risks of NFTs should also be included in the training. NFTs represent a new "asset," and it is not typical to have a new "asset" in the market, let alone one that combines art and technology.

The training should also cover the legal aspects of NFTs, including the definition of NFTs from a legal standpoint, the legal uncertainties surrounding NFTs in the art market, and the application of AML policies to NFTs. Finally, the quality of training may be affected by the lack of financial resources and the absence of personnel, equipment, and facilities. Thus, it is essential to demand better financial resources to reorganize and modernize LEA training. Given the global expansion of technology, NFTs and the crypto world, in general, should receive special attention.

7. CONCLUSIONS

NFTs have traits that make them attractive to money launderers, such as anonymity, volatility, and a lack of regulatory rules (Congressional Research Service, 2019).[39] One solution to the challenges posed by NFTs is legal and regulatory certainty. Regulators should define NFTs and provide AML rules that should apply to those trading in NFTs. Legal uncertainty surrounding NFTs creates challenges not only for LEAs and regulators but also affects legitimate traders of NFTs who respect AML rules. By regulating NFTs, legal clarity and consistency would be provided to legitimate traders of NFTs and to NFTs holders, which in turn could boost the functioning of this new asset and optimize its benefits for society (Congressional Research Service, 2019). A legislative framework governing NFTs can be achieved via the EU and national laws of the Member States and other legal systems. Whilst a new EU legislation may take several years, regulators and LEAs or international organisations such as the FATF can issue guidelines as a soft law instrument. Guidelines should be issued for NFTs in which more information on how to handle suspicious NFTs transactions and on how to apply AML rules and policies are articulated. Compliance professionals will most likely follow these guidelines to keep their businesses "clean," and

[39] The same characteristics make crypto currencies attractive to criminals.

https://doi.org/10.54934/ijlcw.v2i3.57

FIUs and LEAs will benefit from more information on NFTs to investigate suspicions of money laundering. Such guidelines should be carefully drafted in consultation with key stakeholders.

In summary, the rapid growth of NFTs raises important regulatory considerations within the art world and beyond. Therefore, policymakers must carefully consider potential proposals for future regulatory action on NFTs to ensure that this new asset class is subject to appropriate transparency, accountability, and ethical standards.

REFERENCES

[1] Guidi, B., & Michienzi, A. (2022). Sleepminting, the brand new frontier of Non Fungible Tokens fraud. GoodIT '22: *Proceedings of the 2022 ACM Conference on Information Technology for Social Good*, pp: 75-81

[2] Skipp, C. (2022). Innovation and Tech at Miami Law – First Law School in U.S. with NFTs Course. Miami School of Law. Available at: https://www.law.miami.edu/news/2022/january/innovation-and-tech-miami-law-first-law-school-us-nfts-course (last visited 29.06.2022)

[3] Courtois, N.T., Gradon, K. T. & Schmeh, K. (2021) Crypto Currency Regulation and Law Enforcement Perspectives. *arXiv preprint arXiv*:2019.01047. Section 11.1. available at: https://arxiv.org/abs/2109.01047 (last visited 29.06.2022)

[4] Cooper, G. (2022). Personalty+, (2022) *Trusts & Trustees*, 28(5), pp. 447–450, available at: https://doi.org/10.1093/tandt/ttac029 (last visited 05.04.2023)

[5] Cooper, G. (2021). Virtual Property: Trusts of Cryptocurrencies and Other Digital Assets. *Trusts & Trustees*, vol 27(7), pp. 622-624. available at: https://doi.org/10.1093/tandt/ttab027 (last visited 25.05.2023)

[6] Ellul, J., & Revolidis, I. (2023). Non-Fungible Tokens (NFTs), Smart Contracts and Contracts: The need for Legal and Technology Assurances. *SSRN*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4325415 (last visited 20.05.2023)

[7] Houser, K., & Holden, J. T. (2022). Navigating the Non-Fungible Token. *Utah Law Review*, 2022(5), p.891-939. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4055535 (last visited 5.04.2022)

[8] Aksoy, P. Ç. (2023). The applicability of property law rules for crypto assets: considerations from civil law and common law perspectives. *Law, Innovation and Technology*, 15(1), 185-221. Available at: https://doi.org/10.1080/17579961.2023.2184140 (last visited 05.04.2023)

[9] Serneels, S. (2023). Detecting wash trading for nonfungible tokens. *Finance Research Letters*, 52:103374. Available at: https://doi.org/10.1016/j.frl.2022.103374 (last visited 5.05.2023)

[10] Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, D. S. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11, 1-35.

ABOUT THE AUTHORS

Dimitris Kafteranis – PhD, Assistant Professor in Law at Centre for Financial and Corporate Integrity, Coventry University, Coventry, UK
e-mail: ad8164@coventry.ac.uk
ORCID ID: https://orcid.org/0000-0001-9895-6112
Google Scholar ID:
https://scholar.google.com/citations?user=kf0vXVIAAAAJ&hl=el

Huseyin Unozkan – PhD, Assistant Professor at Haliç University Industrial Engineering, Istanbul, Turkey
e-mail: ae1008@coventry.ac.uk
ORCID ID: https://orcid.org/0000-0001-9659-287X
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/ABF-8486-2021
Google Scholar ID:
https://scholar.google.com/citations?user=fhRlGj8AAAAJ&hl=tr
Scopus ID:
https://www.scopus.com/authid/detail.uri?authorId=57969037100

Umut Turksen – PhD, Professor in Law at Centre for Financial and Corporate Integrity, Coventry University, Coventry, UK
e-mail: aa8628@coventry.ac.uk
ORCID ID: https://orcid.org/0000-0002-3143-6072
Google Scholar ID:
https://scholar.google.com/citations?user=NSP_sx0AAAAJ&hl=en

ABOUT THIS ARTICLE

Conflict of interests: Authors declare no conflicting interests.

Funding: The research for this paper is funded by the Scientific and Technological Research Council of Turkey (TUBITAK) and the TRACE project which is supported by the European Union.

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.58

NFTs, DAOs AND SMART CONTRACTS, WHERE IS THE DECENTRALISATION?

Marica Ciantar
Centre for Distributed Ledger technologies, University of Malta, Malta

Article Information:

Received
July 20, 2023
Approved
July 29, 2023
Accepted
October 3, 2023
Published
November 30, 2023

Keywords:

NFTs,
DAOs,
smart contracts,
law,
decentralisation

ABSTRACT

DAOs, decentralised autonomous organisations, you have the power, right? Well, like most other matters now-a-days, it depends.
Oftentimes, the relationship between NFTs and DAOs is intertwined as a DAO may be set up with the purpose of creating NFTs or else, one may buy an NFT to become a DAO member. Both DAOs and NFTs make use of smart contracts on a blockchain. The purpose of this paper is to answer the following questions: How decentralised is a DAO? What is the role of NFTs within a DAO? How can NFTs enhance the workings of a truly decentralised autonomous organisation?
The author believes that decentralisation should stop being used as a hype word in the blockchain sphere and discusses about certain problems regarding centralised and decentralised points in a DAO, whether they realised or not. Both the Maltese Innovative Technology Arrangement and Services Act and the Wyoming Decentralized Autonomous Organizations Supplement will serve as focus as these laws directly regulate DAOs and in turn serve as a means to protect the member and the client of the DAO, and their NFTs.

FOR CITATION:

Ciantar, M. (2023). NFTs, DAOs and Smart Contracts, Where is the Decentralisation? International Journal of Law in Changing World, Special Issue NFTs, 52-79. DOI: https://doi.org/10.54934/ijlcw.v2i3.58

1. INTRODUCTION

This paper will discuss the novelties just some of the novelties brought about by Web3, these being, non-fungible tokens (NFTs), decentralised autonomous organisations (DAOs) and smart contracts. A discussion on these is important as they are on the route to change companies and organisations as we know it, to a degree at least. Focus will be on the tri-partite relationship between NFTs, DAOs and smart contracts and the role of NFTS within DAOs. Hence, there will be an exploration of how NFTs can operate within a DAO, enhance its workings, and potentially fix any shortcomings of the DAO. Furthermore, an important conversation will be held as regards the decentralisation of DAOs and how NFTs may be a potential solution for such.

A company willing to dip its toes into such innovations are more likely to stay relevant and may also create a buzz around it for some time which has the potential of increasing sales and clients. An example of such company is Budweiser. During the 2022 Super Bowl commercial titled "Zero in the Way of Possibility" showed a man in an art museum staring at a painting of a woman with an animated pair of blue glasses. This establishing the relationship between the Nouns DAO and Budweiser.

This decision to collaborate was passed by the Nounders who decided to buy back a Noun and gift it to Budweiser which changed its Twitter profile picture to the image of the pixelated beer mug and feature the Nouns glasses during the Super Bowl. This deal was done entirely on Ethereum with cryptocurrency hence, the transaction can be viewed and verified by all. In addition to this, Budweiser is now part of the Nouns DAO and as a Nounder has all rights pertaining thereto [18].

This example is perfect as it incorporates DAOs, NFTs and smart contracts which are the focus of this paper. It also shows that DAOs and companies may work together with collaborations potentially improving the image of both.

2. SOME DEFINITIONS

Before moving forward, it is important to give some definitions to the terms being used as some carry different meanings to different persons.

DAOs, smart contracts and NFTs promise transparency, however it is important to distinguish between actual transparency and technical transparency. Seeing the code is one thing however being able

https://doi.org/10.54934/ijlcw.v2i3.58

to read and understanding its nuances and capabilities is entirely another. It may be argued that only seasoned developers can claim to fully comprehend the code and its functionalities hence, for non-experts understanding the code can be challenging. Nonetheless, technical transparency allows a better degree of understanding than no transparency and offers a unique level of openness and accountability which more traditional organisations or companies may not always have.

2.1 Non-Fungible Tokens (NFTs)

An NFT may be described as a digital certificate on the blockchain associating a user with an image with each differing from the other according to its metadata and unique identifiers, hence each NFT is distinct from the other [25].

Gayton and Murray describe a fundamental difference between tokens and NFTs which, albeit sometimes used interchangeably, tokens are fungible and interchangeable whilst NFTs are unique and non-interchangeable. With regards DAOs, the NFTs uniqueness lies in the fact that it can be used to vote in one DAO but not another [9].

2.2 Smart Contracts

Nick Szabo is the father of smart contracts describing them as, "computerised transaction protocols that execute the terms of a contract" which work in an accelerated way to verify or execute digital negotiations and enable peer-to-peer transactions between individuals [25]. Smart contracts "enhance security, increase transparency and reduce the ability for individuals or small groups to break policies or rules via automation…(hence they) allows DAPs to automate a host of actions of certain conditions are satisfied." [17]

Smart contracts and NFTs are fundamental in the operations of a DAO as tokens may be in the form of NFTs which may be brought via smart contracts from the DAO itself or any other point allowed by it. NFTs have multiple uses within a DAO ranging from being used as currency, voting tokens and so on. Smart contracts and NFTs enable transparency, security and efficiency within the DAO.

2.3 Decentralised Autonomous Organisations (DAOs)

More contradictions lie when it comes to giving a definition to DAOs however each definition gives a different shade to what a DAO is.

https://doi.org/10.54934/ijlcw.v2i3.58

In their purest form, DAOs are an organisation, hence a group of people with a common mindset or goal. They are autonomous meaning that the organisation uses automated means such as smart contracts and hence, operate on the blockchain via smart contracts thus ensuring transparency and trust without the need to trust a third party. Lastly, DAOs are decentralised hence there is no centralised authority making the decisions hence, the failure of one member will not lead to the organisation's collapse [31], unlike what happens to companies upon the failure of its director. However, this perfect theory is, by far, further than the practical reality for a number of reasons which will be described hereunder.

According to Murray et al, DAOS are organisations "managed entirely through protocols that are encoded and enforced via smart contracts rather than human beings". They continue that DAOs "create opportunities for individuals to quickly and securely organise, raise funds and govern themselves while maintaining anonymity or pseudonymity." [17]

Jack du Rose (2016) gives a further definition to a DAO, describing such as "a type of decentralised application which incentivises its users to engage in activity which furthers its agreed business objectives by enabling them to work together without requiring them to trust one another." [31]

Chohan focuses on the more technological side of the DAO thus describes it as an "organization that is run through rules encoded as computer programs called smart contracts" governed by "pre-programmed algorithms that are executed by computers based on code." [4]

A similar approach is adopted by De Fillippi and Wright which describe a DAO as a "particular kind of decentralised organisation that is neither run nor controlled by any person but entirely by code. As opposed to other decentralised organisations – which are operated by individuals who had the ultimate decision-making power – DAOs are designed to run autonomously on a blockchain." [5] They emphasis how a DAOs activities are determined by the blockchain's protocol with the smart contracts dictating how the organisation makes the decisions and how the DAOs interact with the outside world. They continue that the nature of the blockchain network further ensures that all codified clauses perform as planned [5].

DAO enthusiasts define DAOs as a "dynamic set of working relationships that continuously and dynamically self-organize around projects and outcomes" hence, creating an environment wherein members are incentivised to engage in activities without the requirement of trust. Since they assume that members are there to contribute to the community, "the purpose of the business is to undertake economic

https://doi.org/10.54934/ijlcw.v2i3.58

activities in the interest of its worker-members, rather than to make a profit for the cooperative itself or external investors." [31]

In this author's opinion, a DAO may be defined as a blockchain-based organisation which operates via the use of smart contracts. The organisation's autonomy and decentralisation are subject to the preferences of its members and founders and can benefit as either a non-profit or a profitable entity. Hence, albeit ideally a DAO is a decentralised and autonomous organisation, in practical scenarios, a spectrum exists which ranges from complete centralisation to complete decentralisation and an entity will position itself on this spectrum based on its preferences and requirements. This in turn will dictate the level of atomisation and the type of organisation appropriate for that entity's particular mission.

3. INFLUENCES WITHIN A DAO

Lawrence Lessig identified four ways of regulating behaviour and these include law, social norms, market forces and architecture with each mode being interdependent and effecting the other. Laws are typically enforced by governments and courts, market forces include economic incentives and gaps in the market, social norms are the unwritten rules of behaviour and architecture refers to the physical spaces, which on the internet/blockchain is more commonly referred to as the code [12].

These four factors of regulating behaviour also influence the behaviour of DAO members and how a DAO is programmed to act. Hence, they are present before the birth of the DAO, during its life and at the end thereof. Furthermore, they are ingrained within the workings of the DAO, including the human element which is ever present and may also possibly lead to a point of centralisation within the DAO, as will be discussed below.

It is a misconception that blockchain is unregulated. The law will punish those who do not comply with the laws apply to blockchain which include, but are not limited to, consumer protection laws, employment laws, copyright laws and so on. Regulation deters persons from engaging in mischievous behaviour on the blockchain and such deterrent is quite important especially in light of the recent scandals, such as the FTX saga. Nevertheless, the law should strike a balance as not to halt innovation whilst still protecting blockchain users, including DAO members.

Social norms are enforced by the DAO community which dictates what is deemed acceptable within the group and what is not. The social norms of the DAO's members can be a reflect of its ethos,

https://doi.org/10.54934/ijlcw.v2i3.58

for example when a DAO is set up for charitable purpose as opposed to a DAO set up to defraud persons. In either case, there is a community of persons who stick together to achieve a common goal. There are instances wherein, within the community, regardless of pseudonymity, influential members may hold sway over others' votes, making the community dynamic crucial to the DAO's success. Furthermore, as will be discussed later, such will prove to be a centralised point within the DAO.

A significant role is also played by the market which may be the reason for the DAOs formation. For example, a DAO may be set up to address a gap in the market, to make a profit by providing a particular service or product which is in high demand or due to there being some other favourable market condition. The market may also determine whether a DAO is a success or else a failure. The DAO must be able to, via governance or code, pivot in response to certain changes in the market and be agile in response to economic fluctuations.

The code, which Lessig terms the architecture, is very important in the workings of the DAO since the DAO is built entirely out of code, from the blockchain it is built on and the smart contracts coded to determine how the DAO will work and enable the transactions and voting mechanisms, amongst other things. Hence, code is central to the operations of a DAO. Nevertheless, there are many limitations and risks and some even argue that code is bound to fail. since code cannot be changed such is a double-edged sword as it guarantees that things will work as intended however any potential bugs cannot be addressed unless specifically provided for and allowed in the code. Furthermore, in a proper DAO any changes to the code requires an overwhelming majority hence, there is no central authority which unilaterally changes the foundation on which the DAO is based.

4. DECENTRALISATION OF DAOS – A HOAX?

As help by Gayton and Murray, “most DAOs are decentralized in name only.” [9] As stated earlier the perfect and purest way of a DAO to operate is via automated means, through an organisation and with no centralised actor calling the shots. Hence, DAOs offer the promise of a democratic utopia however this is not always the case due to various issues, such as liability in the case of lawsuits or for legal compliance.

Tying back with Lessig’s modes of regulating behaviour, certain factors may have an overwhelming amount influence on others. A particular example of this is certain DAOs wherein a particular member has an overwhelming amount of influence with the organisation due to being regarded

https://doi.org/10.54934/ijlcw.v2i3.58

highly. Another example is having the code allowing the DAO to veto certain decisions. These can all skew with the decentralisation of the DAO showing that the reality of decision-making is more nuanced than simple democracy due to the various factors which influence the outcome [31].

Speaking about decentralisation in the blockchain space is crucial as, especially with DAOs, similar to what happened to the internet and ISPs, "[n]o matter how decentralized a service is to start with, left to itself, things eventually tend towards centralization" [15]. This may be due to a number of reasons including that, "centralisation is the best means to wealth and power [23]. Tse confirms the probability of DAOs acting in a centralised manner, "DAOs will likely witness increasingly centralised token holder bases, and moreover, increased power in the hands of controlling token holders." [31]

In this author's opinion, a degree of centralisation is inevitable however hope remains that it will be limited to adhere to the philosophy behind the idea of the blockchain. Certain centralised actors may be realised, such as some exchanges or mining pools whilst others are not as recognised, such as the developer's role in writing the code on which the blockchain, smart contracts and DAOs run upon, as will be described hereunder.

4.1 The Development Team

For any project, a development team is important to create the initial framework. In the blockchain sphere, developers are even more crucial as they are the ones who write the code, the rules and architecture so to say. Hence, even in fully decentralised autonomous organisations, there is always the initial human element at a point in time. As Tse points out, centralisation during the birth of the DAO is the most efficient way forward as initiators are in the best position to achieve their goals, he holds that "All of these DAOs were established by a centralized development team or person, including Bitcoin's Satoshi Nakamoto." [31] Hence, developers have the potential to be able to hold a significant amount of power, the effects of which are long lasting and determine the decisions which can be taken and how such decisions may be taken. Developers may determine also the immutability of the code hence they may also determine whether the community may bring about any changes to it or whether it absolutely cannot be changed. Hence, the development team determines the parameters within which the community acts, giving them a direct way of effectively restricting the actions of members. This puts the development team in a critical role when determining the power dynamics within the DAO.

https://doi.org/10.54934/ijlcw.v2i3.58

Upon deployment on the blockchain, members of a DAO place their trust in the developers who wrote the code and also in the code of the underlying blockchain. Such trust can be fragile if the developers misuse their power or act in ways which harm the DAO. This factor is often overlooked, and persons blindly trust that the code would perform as intended or perceived by them. Members trust that the code is bug-free, contains sufficient decentralised governance mechanisms and is safe for them to use. Hence, maliciousness is not automatically presumed when one interacts with a DAO [31].

There are those who argue centralization issues can be mitigated once the DAO is launched, however, studies show that individuals tend to have a strong status quo bias. Therefore, it ultimately depends on the development team's decision to retain their decision-making power, despite any economic or psychological factors at play [31]. Furthermore, the degree of centralisation or decentralisation may reflect the development team's integrity and intentions since it is in their total control, and they are in a position wherein they can potentially exploit any code weaknesses or loopholes to scam the token holders.

However, there are other, more reasonable, and justifiable reasons why developers may wish to retain a degree of centralisation. Some of the reasons may be that they wish to control how the DAO is operating and ensure that it is following the intended path, try to ensure its success and also to protect against malicious behaviour.

4.2 The One-Token-One-Vote System

The one-token-one-vote system may be exploited by someone who holds a majority amount of tokens. If one person holds most of the tokens, they may influence the outcome of the vote in a negative manner and for ignoble purposes such as to benefit themselves at the expense of other members or at the expense of the DAO itself. According to Kaal, this problem may be circumvented by more mature voting systems such as, quadratic voting, futarchy, liquid democracy, conviction voting, and reputation-based voting. These aim to balance the risks and rewards of voting and prevent exploitation by majority token holders [10].

The problem presented by the one-token-one-vote system is also presented in traditional limited liability companies wherein majority shareholders act at the expense of others. The law provides safeguards for the prejudiced minority shareholders. A classic case is that of Ebrahimi vs Westbourne Galleries Ltd [1973] AC 360 (HL) wherein a partnership was formed by Ebrahimi and another who were

https://doi.org/10.54934/ijlcw.v2i3.58

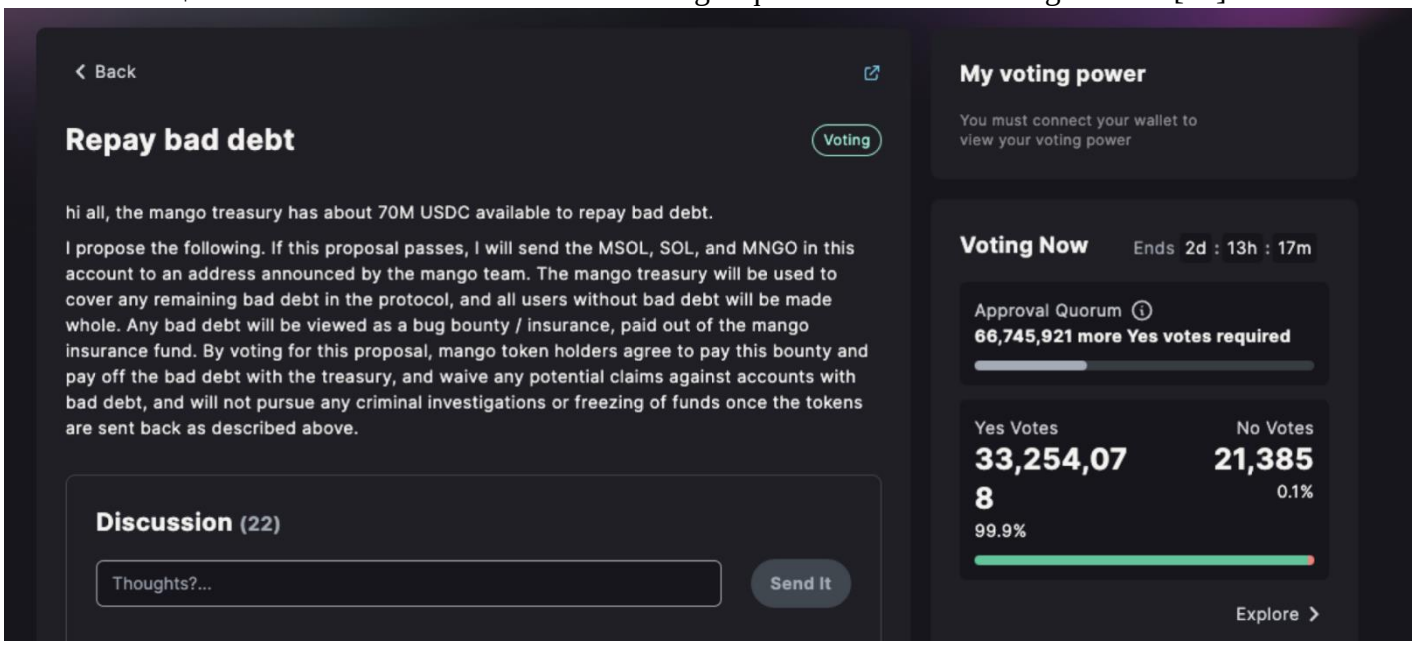
directors. Afterwards, the son of the other director also became a director resulting in them holding the majority of the shares. They used their powerful position to vote Ebrahimi out of office who therefore requested for a winding-up order before the House of Lords which held that the typical requirements of a quasi-partnership were breached. Hence, the House held that there was a violation of the mutual trust and confidence which shareholders should have, hence the House of Lords ordered the winding up of the business. Lord Wilberforce held that this remedy can be given when there are small private companies described as quasi-partnerships and situations such as the following,

"(i) an association formed or continued on the basis of a personal relationship, involving mutual confidence – this element will often be found where a pre-existing partnership has been converted into a limited company;

(ii) an agreement, or understanding, that all, or some (for there may be "sleeping members") of the shareholders shall participate in the conduct of the business;

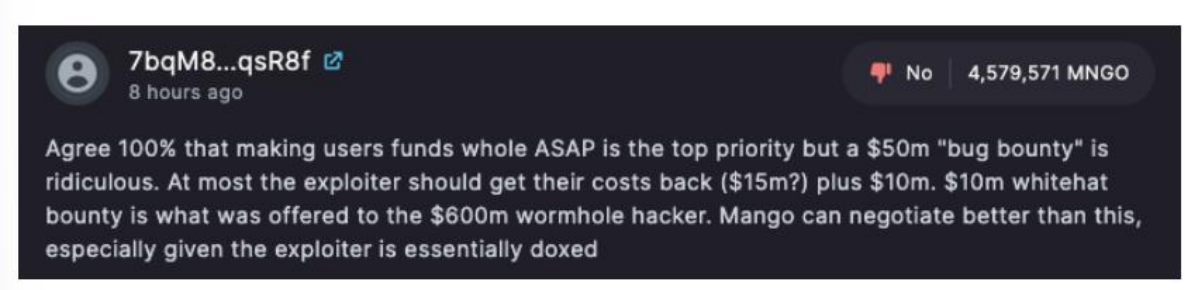
(iii) restriction upon the transfer of the members' interest in the company – so that if confidence is lost, or one member is removed from management, he cannot take out his stake and go elsewhere" [28].

A blockchain related incident which shows the danger of the one-token-one-vote system is the recent episode surrounding the Solana-based Mango Market's DAO. In October 2022, an exploit in the protocol of the DAO allowed hackers to steal over $100 million from the DAO leaving the treasury with a deficit of $116.7 million and with the hacker having acquired 438 million Mango tokens [14]. The hacker



https://doi.org/10.54934/ijlcw.v2i3.58

proposed his own solution by demanding a settlement in the DAO's governance forum which read that "Within 12 hours of the proposal opening, you shall send back the assets other than USDC, MSOL, MNGO, and SOL as a show of good faith," and continues that "The remaining assets shall be sent within 12 hours once the vote is complete and passes" [20] [24].



Following the proposal, the vote passed, and the hacker agreed to return the stolen funds, a move that investors such as Tyler Reynolds considered to be "monoric" [7] [29].

However, the hacker, found out to be Avraham Eisenberg is currently facing the possibility of being held liable under both criminal and civil law for his actions. The representatives for the DAO held that the proposal which passed violated contract law due to the duress/violence experienced by those who voted in the affirmative. Under criminal law he has been accused of having, "wilfully and knowingly, directly and indirectly, used and employed, and attempted to use and employ, in connection with a swap, a contract of sale of a commodity in interstate commerce, and for future delivery on and subject to the rules of a registered entity, a manipulative and deceptive device and contrivance", commodities manipulation and wire fraud [29].

This continues to show that, as held perfectly by the McMillan lawyers, "In their isolated system the votes undoubtedly seem powerful, and they are in a business sense as they operate as a cooperative of sorts aggregating purchasing power…But that doesn't mean that a DAO proposal and vote can cure all ills: like it or not, that's what the courts are for" [19].

5. GOVERNANCE WITHIN A DAO

NFTs and DAOs share a symbiotic relationship as each may benefit the other. NFTs allow DAO members access to make meaningful changes within the DAO whilst the DAO may provide the

https://doi.org/10.54934/ijlcw.v2i3.58

governance needed to support the NFT communities. Sometimes NFTs may also have their own DAOs. Hence, there is a dynamic relationship where NFTs and DAOs co-operate to promote the objective sought in an interdependent relationship between them which reveals a complex web of interaction and dependencies that shape the digital landscape [25].

Thus, this is why it is important to have a conversation on how NFTs may help in the governance of a DAO.

A DAO proposal is a suggestion put forward by a member of the community so that the other members of the DAO see whether it is something they want to pursue as a DAO or not. Proposals may be various and of different importance and can range from changes to the DAO's code to suggestions for community events.

The way a proposal is voted on depends on the specific DAO. In certain DAOs, all token holders have the right to vote on proposals whilst in other DAOs there is threshold which the number of votes must reach. The way that proposals and voting are put forth is determined by the development team, initially, but the DAO may put up a proposal to change the way proposing and voting can be done. Due to the possibility of an overwhelming number of proposals, certain DAOs may require payment or the use of NFTs to make a proposal, which helps to discourage superficial proposals, such system has been taken up by Dash [26].

Depending on the underlying code, proposals may be brought forward depending on the type of NFTs one has and the same applies for voting. Tokens may be bought or else acquired in other ways, such as being awarded as a 'reputation award' for the work the holder has performed within the DAO. Tokens, which may be in the form of NFTs, allow members to steer the DAO in the direction they wish for it to be steered, save for any limitations present within the code [26]. For example, in Tezos, there are rounds of voting to determine which, if any, are adopted.

Voting allows the members to have a say in which the DAO is steered. However, reference here is made again to Lessig's ways of regulating behaviour. It cannot be said with absolute certainty that decisions are taken freely as there are a number of psychological, social and environmental factors come which come into play.

https://doi.org/10.54934/ijlcw.v2i3.58

In addition to the one vote per token system described above there are various other problems in a DAO which concern voting, such as voter apathy. To encourage participation in a DAO, there may be certain incentives for voting however these may lead to careless or irrational voting which may lead to the DAO not operating well and being negatively affected [31]. Therefore, there is a fine line to thread when it comes to deciding the best way forward to ensuring that voting is done in a proper and educated manner allowing the DAO to prosper.

According to Kaham and Rock, a voter with no economic interest to vote may either, not vote, cast a less informed vote, look at how one with an economic interest voted and vote in a similar way or be influenced by extrinsic factors [2].

A way of ensuring more educated votes is via liquid democracy which allows members to delegate their vote to another member. A DAO making use of such type of democracy includes Tezos wherein bakers (delegates) vote on behalf of participants. However, Tse holds that this may make it difficult for the member to know whether the vote was correctly used or not.

Buying votes is another potential issue within a DAO but DAOs can impose voting restrictions for tokens which have been recently traded, however this can be circumvented through malicious off-chain deals. Some DAOs address this issue by giving royalty funds to the community through the DAO, thus helping to align incentives and discourage buying of votes [31].

According to Tse, the transparency offered by the blockchain provides safeguards against malicious activities by majority token holders, however challenges are present due to the anonymity or pseudonymity of identities. To address this issue, the DAO could implement voting ceilings hardwired into the smart contract's code. Nevertheless, this approach may lead to issues of disproportionate control and potential manipulation through the use of multiple addresses [31].

6. THE LAWS

We clear have a limitation regarding the use of colours, particularly if we consider our logo colors. We could apply darker versions of the journal colours and give it a modern look. We also will need to spend money if we want to create a QR Code for our journal.

https://doi.org/10.54934/ijlcw.v2i3.58

As this paper suggests, regulation play a key role in ensuring protection against fraudulent activities or unintentional errors. The law is important in preventing both fraudulent and unintentional acts and help in reducing the risks faced by members whilst also providing a remedy when members are being prejudiced. Hence, the law can protect members by providing both remedies and preventative measures to safeguard them against possible prejudices.

The law may unfortunately be viewed as an obstacle to the project's success and hype however, on the contrary, it should serve as an essential tool to facilitate the project's success, compliance and smooth operation in the real world where blockchain activities are being regulated.

In this context we will explore two jurisdictions, namely Malta and Wyoming, where regulations have been implemented to govern the operations of blockchain based projects which include DAOs.

6.1 The Maltese Innovative Technology Arrangements and Services Act

Malta has regulated DAOs through the Innovative Technology Arrangements and Services Act (ITASA), by regulating technology arrangements which DAOs are categorised under. The Malta Digital Innovation Authority (MDIA) is responsible for overseeing these arrangements and ensuring compliance with regulations. While all DAOs are considered technology arrangements under Maltese law, not all technology arrangements are categorised as DAOs hence there may be similar innovative technology arrangements regulated the same as DAOs. For the purpose of this article, the terms 'DAOs' and 'innovative technology arrangements' will be used interchangeably [11].[1] To get certification under ITASA, DAOs and other technological arrangements must adhere to certain general requirements such as compliance with the standards of legality, integrity, transparency, compliance, and accountability and the MDIA must confirm that there are no grounds for refusal of authorization and assess all documentation and software accessible to users of the arrangement. If requirements are met certification is granted thus establishing a high level of trust and credibility among users and stakeholders [11].[2]

To ensure that the innovative technology arrangement is appropriate for its intended purpose, the MDIA must also ensure its fitness and suitability based on the information provided in the application. Hence, this includes verifying that the technology has the qualities, attributes, features, behaviours, or

[1] First Schedule (Articles 2 and 8)
[2] article 8.

https://doi.org/10.54934/ijlcw.v2i3.58

aspects as declared. Should the technology be owned or controlled by a legal organisation, the MDIA will assess the fitness and propriety of the administrator and shareholders with over 25% shares or ownership interests or rights allocating effective control. Additionally, the software must undergo an independent review by a registered systems auditor approved by the MDIA. This would ensure that the code is thoroughly assessed by a party who is free from any involvement or interests in the DAO. These strict standards allow the MDIA to uphold a high standard of quality and maintain the trust of all stakeholders.

The independent systems auditor must perform a comprehensive review of the DAO to ensure that it meets the reasonable standards required for its purposes, qualities, features, attributes, behaviours, or aspects and ensure that it is working as intended. The DAO must also maintain a registered technical administrator and provide evidence to the MDIA that it meets all prerequisites for certification, adheres to standards, and can address critical matters. The DAO must be capable of modifying parameters or functionalities in response to future legal requirements and must have measures in place ensuring correct operations. The MDIA or a designated person should be allowed to intervene in the workings of the DAO or technological arrangement when this is considered necessary.

Furthermore, it is essential that the DAO complies with all applicable laws and guidelines, is capable of carrying out its legal obligations and has in-built technology features which allow the technical administrator to intervene transparently and effectively should there be a material cause of loss to a user or a material breach of the law. Thus ensuring that any loss or breach of law is addressed immediately, and measures are implemented to prevent future occurrences.

The MDIA requires that all purposes, qualities, features, attributes, limitations, conditions, terms of service, and behaviours or aspects of the DAO be communicated in English and in an easily accessible and comprehensible format. This would help ensure clarity and transparency for users and puts them in a position to make an educated choice. In the case of any discrepancy between the English language and the code or other languages used, the English language shall prevail, once again ensuring protection of the members of the DAO.[3]

An important aspect of having a DAO registered in Malta is that it can conduct business in all Member States of the EU due to the EU's obligation to acknowledge the existence of legal entities or

https://doi.org/10.54934/ijlcw.v2i3.58

persons from other Member States. By operating under Maltese law, DAOs can benefit from legal certainty in a grey area while also operating within the EU framework, providing a favourable environment for their operations.

6.2 The Wyoming Decentralised Autonomous Organisations Supplement

The Decentralised Autonomous Organisation Supplement holds that the Wyoming Limited Liability Company Act applies to DAOs, which are defined as, "a limited liability company whose articles of organization contain a statement that the company is a decentralized autonomous organization".[4]

The law in Wyoming allows the conversion of a limited liability company (LLC) into a DAO by amending its articles of organization which should thereafter include a statement indicating that the rights of members in a DAO may differ from those in other LLCs, and that the law may define, reduce, or eliminate fiduciary duties and restrict transfer of ownership interests, withdrawal or resignation from the DAO, return of capital, and dissolution. The name of the DAO should clearly show its status hence, included must be the abbreviation "DAO" or "DAO LLC". [5]

Anybody may form a DAO but such requires the signing and delivering of the articles of organization to the Secretary of State for filing and maintaining a registered agent in Wyoming. A DAO can operate for any lawful purpose, regardless of whether it is for profit or not.[6] The articles of organization and any smart contracts used to manage or operate the DAO govern all aspects of the DAO thus include, transferability of membership interests, withdrawal of membership, distributions to members before dissolution, and procedures for amending or changing the articles of organization and smart contracts.[7]

A DAO can be either member or algorithmically managed, with management vested in members if member-managed, or the smart contract if algorithmically managed, unless otherwise specified in the

[4] State of Wyoming. DAO Supplement. 17-31-104.
[5] ibid
[6] State of Wyoming. (n.d.). DAO Supplement. 17-31-105.
[7] State of Wyoming. (n.d.). DAO Supplement. 17-31-106.

https://doi.org/10.54934/ijlcw.v2i3.58

articles of organization or operating agreement.[8] A DAO may only be algorithmically managed if the underlying smart contracts are able to be updated, modified, or otherwise upgraded.[9]

Members can withdraw according to the articles of organization, smart contracts, or operating agreement. Upon withdrawal, the member shall forfeit of all membership interests in the DAO, including governance or economic rights, unless otherwise provided.[10]

Similar to an LLC, a DAO may also dissolve upon the expiration of a fixed duration, by a vote of the majority of members of a member-managed DAO, or upon the occurrence of events specified in the underlying smart contracts, articles of organization, or operating agreement. A DAO may also dissolve if it does not approve any proposals or take any actions for a year or by order of the Secretary of State if the DAO is no longer performing for a lawful purpose.[11]

The articles of organization and operating agreement of a DAO are effective as statements of authority. If there is a conflict between the articles of organization and operating agreement, the articles of organization take precedence. However, if there is a conflict between the articles of organization and the smart contract, the smart contract takes precedence.[12]

7. FUTURE RESEARCH AND LIMITATIONS

This section will be tackled by making reference to the various DAO projects currently operating as to see whether they are being practical and effective in ensuring the proper running of the DAO and also that decentralisation is maintained. NFTs may enhance the workings of a DAO in a number of different ways, such as through governance or through voting. However, NFTs do not do this alone as the code of the smart contracts, DAO and underlying blockchain must establish an ecosystem where the NFTs work as intended.

[8] State of Wyoming. (n.d.). DAO Supplement. 17-31-109.
[9] ibid
[10] State of Wyoming. (n.d.). DAO Supplement. 17-31-113.
[11] State of Wyoming. (n.d.). DAO Supplement. 17-31-114.
[12] State of Wyoming. (n.d.). DAO Supplement. 17-31-115.

https://doi.org/10.54934/ijlcw.v2i3.58

Shilina's (2021) perspective highlights the potential of NFTs, she holds that "NFTs are the best way of producing and maintaining membership proof for clubs, events, or communities. Since they are blockchain-backed, they can be used as digital tickets to various events as well as exclusive clubs. They may even be used to access limited edition articles and items that are out of reach for many."

There are various types of DAOs, all of which may benefit from the unique properties of NFTs, but the ones most relevant for this paper are collector DAOs which focus on the NFT landscape [25]. In collector DAOs, members contribute to the DAI in exchange for governance rights or ownership of assets thus creating a mutually beneficial relationship between the DAO and its members, who are able to pool their resources and expertise to invest in NFTs and grow the DAO's assets [3].

Explored in this section are various projects making use of NFTs in the governance of DAOs.

7.1 Lunar Society DAO

The Lunar Society DAO, previously known as Moonbirds, is a vehicle to support the PROOF team initiatives. As held by PROOF, "the Lunar Society is being set up as an additional route for funding and licensing, rather than the only route to partnership for brands who want to work with us."[13]

Like other DAOs, the Lunar Society accepts proposals and votes thereon. An innovative way of limiting proposals made is by requiring such proposals to be sponsored by five other NFT holders who are not members of the proposal team thus ensuring that proposals have the backing of other DAO members from the community to stay relevant to be voted upon.[14] Proposals can be made on the following crucial matters which effect the organisation and encompass issues such as grant funding to support the DAO's growth, trademark usage to utilise Moonbirds, Mythics or Oddities names or logo and the key of approval which grants the holder access to the Lunar Society Seal and signposting. Further proposal types should be available in the near futures as to ensure that members have a say in more decisions effecting the organisation.[15]

[13] PROOF of Documentation <https://docs.proof.xyz/society/what-role-does-the-lunar-society-play>
[14] PROOF of Documentation <https://docs.proof.xyz/society/membership-and-voting>
[15] PROOF of Documentation <https://docs.proof.xyz/society/what-role-does-the-lunar-society-play>

https://doi.org/10.54934/ijlcw.v2i3.58

Voting can be done by those who hold Mythics or Moonbirds NFTs. One Moonbirds NFT provides three votes, whilst one Mythic NFT provides one vote thus ensuring that Moonbirds lead the DAO similarly to majority shareholders, and Mythics lead it similarly to minority shareholders in a company.[16]

The Lunar Society DAO promotes open innovation thus allows individuals outside the organization to collaborate with members of the DAO on proposals for projects. However, a community member must be part of the team to represent the proposal in the DAO and join in Discord discussions, however the project's leader need not have an NFT.[17] This approach is beneficial as it allows more opportunities for the DAO to grow and better its operations. Furthermore, open innovation may help the DAO become more popular and thus may encourage more members to join and participate more fully in the organisation.

The Lunar Society DAO has tackled influential voting by keeping voting records private, allowing one to see only his own voting record. This would help in reducing the pressure for individuals to vote in a certain way and may also reduce vote buying.[18] In this author's opinion, albeit this takes away from transparency, the Lunar Society has potentially taken away an influential point within a DAO which may lead to possible centralisation.

Furthermore, the Lunar Society DAO will also start allowing members to delegate their vote to another Society member and albeit such may be done for any reason PROOF "recommend delegation to subject matter experts as well as those sufficiently engaged in the process so as to actively take part in votes." Hence, PROOF allows the members to delegate their votes whilst also issuing a warning that it is important for delegation to be educated and not be abused of. Another safeguard is that there will be a cap on delegation concentration protecting against malicious activity. In addition to this, there will be delegate overrides hence, if by default individuals delegate their voting power, they may then personally vote and upon the happening of this, the delegated vote (which would be the first vote in this case) would be diregarded. This ensures that individuals retain ultimate autonomy over their votes, allowing them to make informed decisions that align with their personal beliefs and preferences. This feature represents a

[16] PROOF of Documentation <https://docs.proof.xyz/society/membership-and-voting>
[17] ibid
[18] Ibid

https://doi.org/10.54934/ijlcw.v2i3.58

significant step towards democratizing decision-making processes within DAOs and fostering a more equitable and inclusive governance system.[19]

7.2 Space Knight Club[20]

Another DAO is the Space Knight Club which "is a 2-layer platform that is both public and private, that aims at giving back 100% of the royalty funds earned by the project back to the community through a DAO process". There are two types of club members, the more privileged private ones (Knights) and the public members (Spacewalkers). Private club members are those with the ultimate control of the project royalties and this is done through multisig (multiple signatures) safe.

NFTs are a big part of the Space Knight project, using them to prove membership, control funds and submit proposals. Spacewalker NFT holders are called spacewalkers and may submit proposals and vote on which proposals should go forwards. They vote via snapshot.org to "avoid manipulation" and is a way the DAO attempts to guarantee community members control of funds. If a proposal gets more than 30 spacewalkers it would be discussed by the Knights (private club members). The Knights are exclusive private club members and if more than half of them agree on a proposal it is executed immediately via the Gnosis multisig safe.

Each Spacewalker NFT has a holding period ranging from 30 to 300 days and Spacewalkers who hold the NFT for such determined period would qualify as a Knight after standing trial or being vouched by existing members. This rigorous way of progressing to the Knight status shows the exclusivity of the Club wherein members are having more of a say on who gets to be in a privileged position, and it is not solely the code and a simple purchase of an NFT which would allow one to start determining the faith of the DAO.

Knights either become owners of the Gnosis multisig safe or else receive their proof of Knighthood via the exclusive Knight NFT which cannot be sold or transferred due to holding certain exclusive privileges. Not having an economic incentive from the sale or transfer of this prestigious NFT would help

[19] PROOF of Documentation <https://docs.proof.xyz/society/membership-and-voting>
[20] Watts, A. (2021). CoinCodex: Mixing DAO and NFTs, the Space Knight Club [SKC] Vision. Newstex.

https://doi.org/10.54934/ijlcw.v2i3.58

curb against those who may wish to attain such Knight status to sell it at a profit thus ultimately helps protect the DAO and its members.

Hence, there are two gatekeepers in this DAO, the Spacewalkers and the Knights, for a proposal to go to the Knights it must be passed through the Spacewalkers and for it to be executed it must be passed through the Knights. This is an effective way of to ensure that meaningful proposals which are likely to have a positive impact on the DAO are passed whilst not overwhelming members with the number of proposals. It also creates a hierarchy in the DAO wherein those who are the most loyal to it are to consider the ultimate fate thereof. This may prove to also be an effective way of ensuring that members are protected from those with ill intentions as to infiltrate the DAO one would need to first go through the required 30 Spacewalkers and then garner half of the Knights support.

7.3 The Nouns DAO[21]

What makes the Nouns DAO particularly innovative is that each Noun is considered an "irrevocable member of the DAO," creating a dynamic system of governance where members are incentivized to remain active and engaged. Furthermore, it is marketed as a platform which will operate in perpetuity with a Noun being once “every day, forever”.

Once one acquires a Noun, such immediately becomes a member of the DAO with rights which are non-transferable but delegable. Nounders, who are Noun holders, may be rewarded with Nouns hence the system work to encourage more participation in the process and thus potentially more loyalty towards the DAO.

The Nouns DAO is not entirely decentralised with a point of centralisation being the Foundation’s "emergency power" veto however such will only operate until the DAO is ready to implement an alternative. Such veto power may prove essential to the workings of a DAO particularly when a proposal poses "non-trivial legal or existential risks" to it or the Foundation.

Although this approach may not be fully automated or perfectly decentralized, it can help safeguard the interests of the DAO and its members. By considering proposals on a case-by-case basis, a human element is retained, ensuring that certain decisions are not solely driven by the code. However, it also

[21] Nouns DAO, <https://nouns.wtf/>

https://doi.org/10.54934/ijlcw.v2i3.58

shows that there are not enough incentives to ensure that a person works in favour of the DAO as there will always the possibility that someone would try to sabotage the DAO.

7.4 Flamingo DAO[22]

The flamingo DAO describes the potential of NFTs perfectly by holding that, "NFTs evolve and ascribe value in the hands of artists, game makers, metaverse creators or dwellers, and DeFi at large. FLAMINGO aims to support, purchase, archive, collect, and potentially tokenize important pieces of this ecosystem." They continue that, "NFTs represent the digitization and financialization of digital property and intellectual property."

The Flamingo DAO prioritises NFTs and shows how they can help in the governance of a DAO by holding that investment strategies are NFT-focused and members may also fractionalise NFT holdings with any NFT purchased having the potential to be "lent, held, displayed in a digital art gallery, or used as collateral in other DeFi platforms" depending on the choice of the members.

Despite relying on member management and decentralized applications, Flamingo has opted to form as a Delaware limited liability company, hence, giving its members more secure protection from liability and minimising fiduciary obligations.[23] In its documents, Flamingo holds that it "is entirely member-directed and managed by the Members through democratic voting." Moreover, there is no general partner and there will not be unless members vote for such however Flamingo holds clearly, that it "wouldn't be in the spirit of things".[24]

The DAO holds clearly that joining it should be an educated choice potentially also including advice from a lawyer and tax advisor. Albeit it is actually a company, Flamingo operates as a DAO by holding that the operating agreement may be amended if half of the members or more thereof vote to approve such amendment. Members may also, by majority vote, wind down Flamingo and members would be responsible for expenses of liquidation.[25]

[22] Flamingo DAO <https://docs.flamingodao.xyz//>
[23] Flamingo DAO <https://docs.flamingodao.xyz/Organization.html#how-is-flamingo-structured>
[24] Flamingo DAO <https://docs.flamingodao.xyz/Investments.html#how-do-members-of-flamingo-make-purchase-decisions>
[25] Flamingo DAO <https://docs.flamingodao.xyz/Dissolution.html>

https://doi.org/10.54934/ijlcw.v2i3.58

Being a member of this DAO is also a privilege with members having to be 'accredited investors' and there being a cap of 100 members. This cap is a precaution taken by the DAO to ensure that, should Flamingo Units be considered securities there would already be compliance. Furthermore, there must be certain checks to ensure the lawful operation of the DAO such as anti-money laundering, Know Your Customer, and Office of Foreign Assets Control checks. [26] Additionally, there is a service provider to take care of the administrative functions hence the developers of the DAOs seem to have structured it in a way which ensures, as much as possible, legal compliance and although this may take away from the perfectly decentralised DAO it provides, in this author's opinion, appropriate safeguards to its members.

Voting rights may be bought and each Flamingo Unit may be sold in blocks of 100,000 and for the price of 60 ETH. Each block would give the member 1% voting rights and 1% pro rata rights to the proceeds. A member will not be able to purchase multiple flamingo units thus creating a centralised point in the DAO as each member can only buy up to 9% Flamingo Units.[27] Members may vote via the Flamingo DApp on decisions related to Flamingo and such is done through smart contracts on the Ethereum blockchain. Similarly, to other DAOs, the member may not be required to vote on all matters and anyone may delegate his vote to another with the member being able to cancel or re-delegate their vote any time.[28]

The documents of Flamingo make it clear that purchases are speculative, involve risk and are made by the members or their delegates. Flamingo will be the holder of all rights secured and members determine how proceeds are distributed and such will be received on a pro-rata basis. Members "reserve the right to fractionalize the NFT for the benefit of each Member, lend the collection to other gaming platforms, or show any purchased NFTs at digital galleries, etc. The Members have full discretion on how the NFTs will be used once acquired."[29]

Should there be the decision to purchase an NFT such will be purchased by the Service Provider or a member on behalf of the members with each purchase being held by Flamingo itself or fractionalised into tokens.

[26] Flamingo DAO <https://docs.flamingodao.xyz/Membership.html>
[27] ibid
[28] Flamingo DAO <https://docs.flamingodao.xyz/VotingRights.html>
[29] Flamingo DAO <https://docs.flamingodao.xyz/Proceeds.html>

https://doi.org/10.54934/ijlcw.v2i3.58

Rage quitting is described as members who withdraw their capital from the Flamingo and such is a right afforded to the members written even in the code of the DApp and smart contracts. Any pro rata portion of unallocated capital will be returned to the member upon rage quitting and the member will not be able to participate further albeit he may sell his interest if other members approve.[30]

Flamingo works with smart contracts to administer activities and help with funding investments, distributing proceeds, voting and so on. The smart contracts have been audited by a number of companies including, ConsenSys Diligence, MolochDAO, and MetaCartel. This would help improve trust in the DAO by the members as there is more assurance that the code would work as intended. furthermore, the code is publicly available hence, members may either employ their own auditors or else be able to make a decision on it themselves.[31]

7.5 Lobster DAO[32]

Lobster DAO started out in an informal manner with persons on the lobsterchat receiving an NFT. They later started using snapshot to become a DAO. Lobster NFTs (10b57e6da0 NFT) were not all allocated in the traditional manner of acquisition, hence, through buying them however most were given to those who contributed to research and known NFT collectors, with the remaining went to governance. For one to acquire a Lobster NFT today, they must either participate in the Lobster Chat or NFT Avenue or else hold a top-tier NFT such as CryptoPunks.

Royalties received by the DAO are split with 30% going to the artists and the remaining going to Governance. The 10b57e6da0 NFT gives holders preferential treatments both off-chain and on-chain as it would allow them to go to conferences and split the collector into metadata as to sponsor or support other projects. Moreover, holders may be able to utilise the extracted metadata and do things such as build games and so on.[33]

Similar to the Lunar Society DAO, the Lobster DAO also requires a minimum of 3 NFT holders' support to create a proposal which may be made by creating an issue to discuss a topic on github and snapshot the proposal.

[30] Flamingo DAO <https://docs.flamingodao.xyz/RageQuitting.html>
[31] Flamingo DAO <https://docs.flamingodao.xyz/SmartContracts.html>
[32] Lobster DAO <https://github.com/lobster-dao/overview>
[33] ibid

https://doi.org/10.54934/ijlcw.v2i3.58

7.6 Planet DAO[34]

Planet DAO is another example of an innovative DAO. It allows members to play and connect in Alien Worlds Metarverse with other NFT holders via Trilium (TLM). NFTs play a central role as players may utilise them to play games on the Binance Smart Chain and WAC. Planet DAO also encourages participation in weekly council elections and proposal submissions, this may ensure that proposals and discussions are done regularly, and that the DAO would continue to generate activity.

Players have an incentive to acquire TLM by mining NFTs as it allows them to control other Planet DAOs and unlock more gameplay. These examples demonstrate the innovative ways in which NFTs and DAOs can come together to create unique and rewarding experiences for digital communities.

7.7 Ape DAO[35]

Ape DAO is "an Innovation focused Protocol focused on expanding the Aurora Blockchain with Unique Projects in Gaming, De-Fi & NFT that rewards, distributes profits of the ecosystem back to all the holders of The Ape Club NFT & our native token $GBA (Golden Banana)."

NFTs are used in order to obtain $APE tokens. A product of the DAO is Ape Mania, a P2E NFT game that uses Golden Banana as its primary currency. This DAO is also quite ingenious in that it offers a rebate program that encourages users to explore and invest in more Aurora projects, hence Aurora projects are being marketed in this way and they may also have a larger following. Furthermore, it may also be characterised as a marketing tactic as users who receive funds may be more incentivised to continue investing in the projects.

7.8 Other DAOs

There are various other DAO projects we can include in this paper such as Rarible [25] which is a "non-financial-transaction NFT marketplace that is solely focused on creators, also has the required procedures for regulation under the aegis of a Decentralized Autonomous Organization (DAO), which is represented by the governance token known as RARI (DAO)." Holders of Rarible tokens include producers and collectors who may vote on platform enhancements and participate in moderating the

[34] Alien Worlds <https://alienworlds.io/>
[35] The Ape DAO <https://www.theapedao.finance/>

https://doi.org/10.54934/ijlcw.v2i3.58

marketplace. Collectors may see artworks and select which are those they think are best for investment [25].

Similarly, Meebits DAO[36] aims at creating "a vehicle for funding innovative projects that will develop the ecosystem around Meebits", with members gaining access to governance and ecosystem building through a general membership NFT [25].

8. CONCLUSION

One may argue that DAOs work on a spectrum ranging from complete decentralisation (after deployment) to complete centralisation. This author believes that transparency and honest with community members are essential to determine the success of a DAO, as demonstrated by PROOF and the Nouns DAO in the instances mentioned above. In such cases, when there is a parting from the perfectly decentralised autonomous organisation, it is crucial to have this be communicated to the community members so that they make informed decisions and truly understand what they are signing up for.

This is something which regulation is allowing since a lot of emphasis is put on transparency, as discussed during the discussion on the Innovative Technology Arrangements and Services Act of Malta and the Wyoming Decentralised Autonomous Organisation Supplement. Transparency is urgently needed in the blockchain sphere to ensure that DAOs remain a credible type of organisation and ensure that they stay sustainable.

The answer to some of the problems of DAOs is through NFTs. NFTs may be present from the birth of the DAO to their end. The development team may determine different classes of NFTs giving members different rights and may form a hierarchy within the DAO. During the running of the DAO, NFTs may be useful as both membership and governance tokens hence allowing members to steer the DAO in the direction they wish, should it be allowed by the code, hence the development team and also serve as a stamp of one's perceived loyalty to the DAO. Furthermore, they may help generate revenue for the DAO and their metadata may make it possible for members to split them up and build projects thereon, as seen from the projects analysed above.

[36] Meebits DAO <https://www.meebitsdao.com/>

https://doi.org/10.54934/ijlcw.v2i3.58

REFERENCES

[1] Alien Worlds <https://alienworlds.io/>

[2] Baniak, A. (2020). Blockchain and Corporate Law: Revolutionary Change or Solutions in Search of Problems?. Indiana Law Journal, 96(4), 1199-1244. <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1162&context=ilj>

[3] Brummer, C. J., & Seira, R. (2022). Legal Wrappers and DAOs. <https://ssrn.com/abstract=4123737 or http://dx.doi.org/10.2139/ssrn.4123737.>

[4] Chohan, U. W. (2017, December). The Decentralized Autonomous Organization And Governance Issues (University Of New South Wales, Discussion Paper) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055>

[5] Du Rose, J. (2016, May 4). Clearmatics, Ethercasts & Colony [Speech to the London Ethereum Monthly Meetup].

[6] Du Rose, J., De Filippi, P., & Wright, A. (2018). Blockchain and the law: Decentralised Autonomous Organisations. In A. Wright, P. De Filippi, & I. Brown (Eds.), Research Handbook on Electronic Commerce Law (pp. 148-176). Edward Elgar Publishing.

[7] Fernau, O. (2022) Mango DAO Votes to Let Hacker Keep Nearly $50M Of Stolen Funds. The Defiant. <https://thedefiant.io/mango-caves-to-hacker>

[8] Flamingo DAO <https://docs.flamingodao.xyz//>

[9] Gayton, C., & Murray, A. (2022, May). DAOs, NFTs, Web 3.0, and the metaverse: What does it all mean? KM World, 31, 3-3,5. <https://ejournals.um.edu.mt/login?url=https://www.proquest.com/magazines/daos-nfts-web-3-0-metaverse-what-does-all-mean/docview/2672769877/se-2 >

[10] Kaal, W. A. (2021, March 6). A Decentralized Autonomous Organization (DAO) of DAOs. Social Science Research Network. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3799320>

[11] Laws of Malta. (2018). Innovative Technology Arrangements and Services. Chapter 592. Available at: https://legislation.mt/eli/cap/592/eng/pdf

[12] Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.

[13] Lobster DAO <https://github.com/lobster-dao/overview>

[14] Lodge, M. (2022, March 14). DeFi Trading Platform Mango Markets Loses $117 Million in Hack. Investopedia. <https://www.investopedia.com/mango-markets-got-hacked-6750070>

[15] Matthan, R. (2017, December 20). Bitcoin and the law of centralization. LiveMint. Retrieved from <www.livemint.com>.

[16] Meebits DAO <https://www.meebitsdao.com/>

[17] Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? Business Horizons, 66(2), 191-202. https://www.sciencedirect.com/science/article/abs/pii/S0007681322000714#:~:text=Web3%3A%20Decentralizing%20the%20internet,et%20al.%2C%202022)

[18] Murray, K., Schiller, B., & Snyder, J. (2021). The promise of a decentralised internet: What is Web3 and how can firms prepare? Journal of Business Research, 134, 633-640. <https://www.sciencedirect.com/science/article/abs/pii/S0007681322000714#:~:text=Web3%3A%20Decentralizing%20the%20internet,et%20al.%2C%202022)>

[19] Nelson, D. (2023) Mango Markets Exploiter Thought a DAO Protected Him. Then US Courts Showed Up. CoinDesk. <https://www.coindesk.com/business/2023/01/31/mango-markets-exploiter-thought-a-dao-protected-him-then-us-courts-showed-up/>

[20] Nelson, J. (2022). Mango DAO Offers Hacker $47M to Settle Without Pressing Charges. Decrypt. <https://decrypt.co/112016/mango-dao-solana-defi-hacker-47m-offer>

[21] Nouns DAO, <https://nouns.wtf/>

[22] PROOF of Documentation <https://www.proof.xyz/society>

[23] Rachmany, G. (2019, August 13). What Could a DAO Look Like? Hackernoon. Retrieved from <https://hackernoon.com.>

[24] Schroeder, S. (2022) Hacker steals $100 million from crypto project Mango, then things get weird. Mashable. <https://mashable.com/article/hacker-steals-mango-crypto-100-million>

[25] Shilina, S. (2021). A comprehensive study on Non-fungible tokens (NFTs): Use cases, ecosystems, benefits and challenges. Journal of Innovation & Knowledge, 6(3), 114-121 <https://www.researchgate.net/publication/361443799_A_comprehensive_study_on_Non-Fungible_Tokens_NFTs_Use_cases_ecosystem_benefits_challenges >

[26] Sims, A. (2020). Blockchain and Decentralised Autonomous Organisations (DAOs): The Evolution of Companies? Journal of Business Law, 5, 404-423. < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524674>

[27] State of Wyoming. DAO Supplement. <https://sos.wyo.gov/Forms/WyoBiz/DAO_Supplement.pdf>

[28] Trebilcock, M. J. (1973). The Common Law of Restraint of Trade: Recent Trends. McGill Law Journal, 19(1), 30-62. < https://lawjournal.mcgill.ca/wp-content/uploads/pdf/2434601-trebilcock.pdf>

[29] U.S. Department of Justice. (2023, January 20). United States of America v. Avraham Eisenberg. Case 1:23-cr-00010-RMB. <https://www.justice.gov/usao-sdny/press-release/file/1566841/download>

[30] The Ape DAO <https://www.theapedao.finance/>

[31] Tse, N. (2021). DAOs and the corporate form. Stanford Journal of Blockchain Law & Policy, 4(1), 24-44 <https://www.researchgate.net/publication/344604673_Decentralised_Autonomous_Organisations_and_the_Corporate_Form>

[32] Watts, A. (2021). CoinCodex: Mixing DAO and NFTs, the Space Knight Club [SKC] Vision. Newstex. <https://www.proquest.com/docview/2625051720?accountid=27934&parentSessionId=VUrr0D9yEWtgpTZIJnwifwPNuo0DIt66jimZOBPna2A%3D&pq-origsite=primo>

ABOUT THE AUTHOR

Marica Ciantar – Centre for Distributed Ledger Technologies, University of Malta, Malta
e-mail: marica.ciantar.17@um.edu.mt

ABOUT THIS ARTICLE

Conflict of interests: Author declares no conflicting interests

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.59

DECENTRALIZED AUTONOMOUS ORGANIZATIONS:

UNLOCKING THE FULL POTENTIAL OF BLOCKCHAIN TECHNOLOGY FOR THE REAL PHYSICAL WORLD BY EXPLORING SELF-ORGANIZING AND SELF-REGULATING DECENTRALIZED SYSTEMS BY APPLYING SMART CONTRACTS AND FIRST ATTEMPTS OF APPLYING AI

Jan-Gero Alexander Hannemann
University of Nicosia, Nicosia, Cyprus

Article Information:

Received
July 22, 2023
Approved
July 29, 2023
Accepted
October 3, 2023
Published
November 30, 2023

Keywords:
DAO,
blockchain,
NFT,
ICO,
DAG

ABSTRACT

This paper explores the potential of DAOs (Decentralized Autonomous Organizations) built on blockchain technology, which are expected to revolutionize our computing and transaction infrastructures This paper will focus on the legal classification of DAOs, with an emphasis on the mechanisms of raising capital through ICOs and NFTs as alternative financing options for easier access to capital. The potential of linking DAOs and AI is also briefly addressed. Corporate law must keep pace with this rapid change, and the question arises whether it is "sufficiently flexible to make room for the new technical possibilities" and to cover completely "new forms of organization" based on software code that may be inadequately reflected in existing regulations. Overall, this paper highlights the potential of DAOs and their impact on the future of business models, organizational structures, and financing options.

FOR CITATION:

Giovannini, C. J. (2023). DAOs: Unlocking the Full Potential of Blockchain Technology for the Real Physical World by Exploring Self-Organizing and Self-Regulating Decentralized Systems by Applying Smart Contracts and First Attempts of Applying AI. International Journal of Law in Changing World, Special Issue NFTs, 80-117. DOI: https://doi.org/10.54934/ijlcw.v2i3.59

1. INTRODUCTION

The development of blockchain technology or DLT (distributed ledger technology) is being followed with great interest around the world, as it enables major changes in numerous economic fields due to its "revolutionary but also disruptive properties" (Appendix No. 1) [34]. Similar to the Internet in the 1990s, this technology will completely transform society and revolutionize our computing and transaction infrastructures.

What started with the first decentralized cryptocurrency, Nakamoto's Bitcoin protocol, in the midst of the financial crisis in 2008 as a reaction to an unstable international financial and banking system, was only the starting point of a much more massive development. For the real innovation is the data structure underlying this cryptocurrency, namely the blockchain, which on the one hand enables decentralized structures and the hosting of decentralized applications, so-called D-Apps (see Appendix No. 2) [7] and on the other hand drastically reduces the need for middlemen in many sectors of the economy [7].

This has triggered the automation of many business processes in Industry 4.0 [1] while significantly reducing any transaction costs. That’s because blockchain technology is not just a "tamper-proof cashbook for storing transactions or cryptocurrencies" [12], but it is the basis for supercomputer networks such as the IPFS (Inter-Planetary File System) [42] or the Turing-complete/Turing-powerful EVM (Ethereum Virtual Machine) [9]. Alan Turing's thought that a machine might one day be empowered to learn and "in the process become its own independent steward of itself" is becoming a reality by combining Blockchain technology with Artificial Intelligence (AI) and creating self-operating electronic systems from "Cyberdyne Skynet" fiction.

The technical networks created in this way no longer serve only as a substitute for payment, but can autonomously control almost any "process," [17] making them elementary foundations for processing, coordinating, incentivizing, and financing IoT applications and the basis for the next generation of robotics. Blockchain technology is accelerating such developments and may one day be the starting point for a company without employees, as it already enables robotic process automation (RPA) in ways never before possible [31]. The "self-owning company" that is controlled by a "strong" artificial intelligence and buys back all its shares, thus becoming free and ownerless, as already presented in 1986 by Meir Dan-Cohen in his book "Rights, Persons and Organizations", is no longer pure utopia [7].

https://doi.org/10.54934/ijlcw.v2i3.xx

So-called DAOs (Decentralized Autonomous Organizations) play a prominent role in this because they can prepare completely new business models of autonomous AI systems as a basis for AI applications. In the meantime, it is no longer a problem, even for non-experts, to set up their own DAO within a very short time, e.g., using modular systems such as the Aragon project or DAOStack [35]. Thus, with the Aragon Project, up to 5,000 DAOs have been founded to date (cf. Appendix No. 3). Some people would like to talk about a "DO-ocracy" or even a "DAOcracy" [15], focusing on the completely new forms of collaboration that DAOs enable and that give individuals a variety of unprecedented new creative freedoms [25]. DAOs are "profoundly changing the way humanity organizes its work."[25]. The ability to retain control over one's digital identity and emancipate oneself from centralized platforms and surveillance capitalism while co-creating and co-owning one's digital identity is very attractive to millions of users [14].

There is also the possibility of capturing any value digitally using blockchain technology (e.g., in the form of NFTs, ERC 721 tokens, etc.) and exchanging it digitally and in a decentralized manner. Thus, a blockchain can also serve as a central repository for security by "tokenizing" a company's stock, a government bond, a syndicated loan, or other securities and trading the token quickly and transparently in the market like a bitcoin. Corporate law must keep pace with this rapid change, and the question is whether it is "sufficiently flexible to allow room for the new technological possibilities" and to capture entirely "new forms of organization" built on software code that may be inadequately reflected in existing rules [39].

This paper will deal primarily with DAOs. It will attempt to delve into the concept of Decentralized Autonomous Organizations (DAOs). The history of DAOs is presented, tracing the origin of the concept and its development over time. Next, the essay examines the functioning and structuring of DAOs, including general information about their operation and the tokens that comprise them. Additionally, the decision-making process of DAOs and how members can join via NFTs is explored. The crucial role of smart contracts in the functioning of DAOs is also discussed. The essay then moves on to explore oracles and their relationship with the physical world, examining how they enable blockchains to connect with real-world data. Furthermore, the essay analyzes how DAOs can be used as financing instruments through Initial Coin Offerings (ICOs) and Non-Fungible Tokens (NFTs). Blockchain technologies are enabling a new form of crowd- or mass-capitalism that gives the public an immediate stake in the success and emergence of autonomously operating organizations that are self-powered and not only realize entirely

https://doi.org/10.54934/ijlcw.v2i3.xx

new P2P (peer-to-peer) markets that can be collectively owned, but also "drive digital upheaval." Assets coordinated by DAOs have increased tenfold from 2021 to 2022, growing to over $14.5 billion as of August 2022 [25]. It also briefly discusses the potential of combining DAOs and AI to enable not only a purely decentralized organization, but one that will operate completely autonomously for the foreseeable future as well as the possibilities to use DAOs to fight the climate change.

2. HISTORY OF THE DAO

The concept of a DAO is not entirely new. For example, even before DAOs, there were so-called chaordic organizations, such as the VISA company, which can be understood as a precursor to DAOs [4]. Of course, VISA's organizational model has changed over the years, leaving behind the initial structures from the 1970s. The first functionally operating DAO to attract greater attention was "The DAO" project. This project is the most well-known, well-documented, and consequential blockchain hack to date. The fact that the venture behind this project had its starting point in 2016 in Germany, Saxony [39], is at least as surprising as the far-reaching consequences of the hack for the second largest Blockchain network Ethereum, which was split into two different networks (Ethereum and Ethereum Classic) in a hard fork as a consequence (see Appendix No. 4).

In April 2016, programmer Christopher Jentzsch published a whitepaper (*Teichmann*, 2017), which further specified the project "The DAO". "The DAO" makes one think of a venture capital company or a decentralized investment fund [25], which collects funds from its members in exchange for governance tokens. Tokens are a type of token to which a specific right is securitized. A governance token allows the holder to participate in digital voting processes [25]. The governance tokens of "The DAO" were fungible (freely transferable) and could be traded anonymously [25]. The DAO was about deciding collectively, through a simple majority vote, how to invest the money collected in the most profitable way [39]. The ostensible aim was to subsequently profit from agreed repayments.

Although the original goal of the German programmers was to finance their own company (Slock.It UG) by means of a vote of the governance token holders, each governance token holder also had the opportunity to submit their own proposals to the vote, provided these could have been paid for using Ethereum [25]. Upon reaching the required quorum, the underlying smart contract should have orchestrated the governance of the capital flows in an automated manner after a successful vote [37]. In doing so, "The DAO" had taken two security measures. First, there was a kind of curator (reviewer) who

managed a list of potential investment projects and could be voted out by members at any time. Secondly, the invested Ether with a minimum holding period of about 28 days was parked in a Sog. Child-DAO temporarily parked and could not be used immediately [39].

Since the legal situation was not entirely clear even to the programmers, it was agreed that they would simply make the code freely available to the public and the organization could then be activated by third parties on the Ethereum Blockchain [24]. Eventually, the programmers selected one of the DAOs created in this way by third parties, invested in it, and promoted it heavily using their German Slock.it UG [24]. After "The DAO" - which consisted of just 900 lines of programmed code - was initialized, the project quickly collected 11,994,260.98 ETH (which was about 14% of the total cryptocurrency holdings of the Ethereum platform), worth more than $160 million at the time. The "largest crowdfunding project of all time" to the present day had been created [24].

A "digital bank robber" managed to steal about3,689,577 ETH from this already huge amount on June 17, 2016, which was about 30% of the total amount collected. The market value at the time was about $50 million [24]. This would have been more than 14 billion US dollars at the peak of ETH in 2022. The hacker had cleverly exploited a flaw in the source code of "The DAO" and was thus able to fork over the money [17]. The smart contract allowed deposited money to be withdrawn again, which led to the hacker appropriating other users' money as well [39]. This was a so-called replay attack. The hacker could not be identified at times due to the anonymized data structure of the blockchain, although there is increasing evidence that the hacker(s) could be located in Austria (*Shin*, 2022). This hacking had an immense impact on the Ethereum blockchain, as about one seventh (14%) of the total ETH holdings had gone into "The DAO" (see above). However, since the money could only be paid out after a lock-up period of one month, the Ethereum community had time to work out a solution in a lively, transparent discussion that could be tracked by everyone on the Internet [24].

In the process, the developers of Ethereum around Vitalik Buterin worked towards a hard fork, which allowed the affected users to reverse the purchase of their shares (*Willcke*, 2016). A hard fork always occurs when new functions are introduced into a blockchain network that were considered invalid in previous versions. The nodes or miners that do not then upgrade to the current software version can then no longer join the longer, existing blockchain chain, so the ledger splits and there are two cryptocurrencies side by side (see Appendix No. 4). Since the hard fork comprehensively rewrites the protocol, users had to decide whether they wanted to belong to the old now "flawed" blockchain or to the new network [37].

It was a matter of "drying up the bad guy...in a dead corner of the blockchain" by starting a "new fork in the chain." Since the vast majority of node operators (nearly 99%) agreed to a so-called hard fork - by installing a software update [37] - that recorded the preceding creation of "The DAO" and the theft of the money as undone, it was possible to undo the hack.While the money was now temporarily parked on a child DAO, the hard fork could be successfully carried out [37], which in turn led to the fact that a large part of the funds could be secured and returned to the investors [17].

The immutability of the blockchain was removed for this one very specific individual case by the retroactive rewrite, which was seen as an imposition, especially by part of the community, as it undermined the trust of the users [39]. In particular, the principle of "code is law"[39] was invoked, and it was felt that the code would be compromised by a "vigilante justice system supported by a majority of participants"[17]. Furthermore, the opponents of the hard fork argued that there was precisely no attack on the system or criminal act, but that the hackers had merely exploited a vulnerability in the code [17]. Therefore, there were also some node operators (about 1% - including the hackers) who chose to continue the old blockchain under the name "Ethereum Classic", which in turn were excluded from the new Ethereum network for lack of installation of the update [37].

Conversely, the updated clients were no longer compatible with the consensus rules of "Ethereum Classic" and were in turn excluded from this network. Without a doubt, the hack of "The DAO" can be classified as disloyal, as it clearly violated the purpose of the company [37] and the error of the smart contract was not intended in this way. If one were to come to a different conclusion, one could also say - to illustrate the absurdity of this discussion - that it would be legitimate to collect other people's cats in the city and to claim that they were running around freely and could therefore be accessed by anyone and that all social rules would have to be suspended in such a case, even if the majority of society would classify this as theft in the sense of § 242 StGB ivm § 90a BGB. It seems absurd that participants in a DAO would also want to subordinate themselves to the rules in the software in the event of a hack and would also want to accept malfunctions of the software in advance. At least as absurd is the justification of the cat thief that the cat was attracted to him because he discovered that cats have an error programmed into their DNA and like to change owners for a bowl of milk and that this genetic programming and the feelings of the animal triggered by it should therefore be placed above the applicable law.

Of course, participants can deviate from the content of the code if it now seems nonsensical or an existing loophole has been abused as in the case of "The DAO". The case of "The DAO" has once again

impressively shown how important increased security is for trust in blockchain systems, because such systems are particularly at risk of falling victim to hacker attacks and even small security gaps in the smart contract can have a significant impact [37].

Even though the project "The DAO" failed, media attention was drawn to DAOs and the Ethereum Blockchain despite this incident or perhaps because of it. In retrospect, this development has even been quite instrumental in popularizing the idea of independently operating organizations - i.e. DAOs [26]. As a result, there are now a wide variety of DAO projects with a wide variety of focuses. Baur has attempted to classify DAOs according to their basic function and has defined four main DAO types. Thus, he distinguishes between management DAOs (a project as a whole is operated by the DAO and services are offered to third parties), financing/investment DAOs (voting-based investment associations such as "The DAO"), the donation DAOs (charitable purposes are pursued here) and control DAOs (coordination of software - important in the IoT field). While these concepts have overlaps, they are very different in their respective market interactions (see Appendix No. 5). Following this classification, this thesis will largely focus on financing/investment DAOs, management DAOs and control DAOs. This classification makes it possible to take a generalized look at DAOs and not get lost in looking at individual projects (such as the Collector DAO, Flamingo DAO, MakerDAO, Uniswap or building block DAO systems like Aragon) - all of which have specific character traits.

3. FUNCTIONING AND STRUCTURING OF A DAO

The following part explains the general functioning of a DAO. In doing so, the design and structure are highlighted as well as the question of how joining a DAO can be done, what belongs to the participants of a DAO and how they can control the DAO.

3.1. General information on the functioning and structure of a DAO

A DAO is composed of a large number of smart contracts, which - upon the occurrence of certain events - can execute themselves [23]. The DLT (blockchain) is only the basis for the DAO, which is set up on this infrastructure like an app or application. In principle, a DAO can run on any blockchain that provides a suitable infrastructure. Probably the most common infrastructure of the 2020s is currently provided by the Ethereum blockchain, but there are also other blockchains that could be considered just as well and [26], purely theoretically, it would be possible to set up a blockchain of one's own, on which

https://doi.org/10.54934/ijlcw.v2i3.xx

the DAO would then in turn be set up. Nevertheless, a large number of smart contracts are usually programmed, which then make up the DAO, and are subsequently stored on an existing blockchain to initiate the DAO [23].

3.2 The tokens of a DAO - Who owns the DAO, how to join it and how the decision making is done

Those who wish to have a "share" in the DAO can acquire so-called tokens (which can be thought of as value coupons on which certain rights are securitized - see above) in the DAO. This can be done in two ways: Either by the user contributing intangible services (services, creative activities or the like) and being paid for them in tokens, or by exchanging an accepted currency (e.g. ETH or BTC) for a token [16]. For the latter, the user only has to send the accepted currency to the smart contract address of the DAO and in return receives tokens transferred to his wallet [23], which are generated directly during the period of an ICO (Initial Coin Offerings) or come directly from the wallet of the DAO in the later course.

A wallet or wallet address is a "public key" (PuK) to which anyone can send cryptocurrencies or NFTs and which can also be viewed by anyone, but which only the owner can dispose of by means of a private key (PrK). For example, tokens on the Ethereum Blockchain are created using the ERC-20 standard (Ethereum request for comments-20), which defines 6 mandatory functions (total token balance, balance, transfer, transfer from, approve, allowance) and includes three optional functions, such as name, symbol, and the number of decimal places after the decimal point.[1] Since the various token types are very diverse and can be securitized with a wide variety of rights, only the tokens most relevant to DAOs, namely the simple tokens without voting rights (investment tokens) and those with voting rights (governance tokens, more rarely also equity tokens or governance certificates), will be examined in more detail below [7].

Here, too, it must be noted that the dividing lines cannot be drawn so easily and vary from project to project. However, this approach may suffice for a general consideration. An ordinary token (e.g. in the form of an investment token) would, for example, participate in profit distributions and would have an intrinsic value that could be sold later on the market with an increase in value, if necessary [24]. The comparison with different share classes suggests itself (A-shares with voting rights, B-shares with less voting rights, C-shares without voting rights, etc.), which, for example, have different voting rights or

[1] *The Ethereum Foundation*, ERC-20 TOKEN STANDARD, accessible at: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/,[Last time retrieved on March 10th, 2023].

https://doi.org/10.54934/ijlcw.v2i3.xx

profit participation. A governance token is an entitlement certificate and, in addition to the basic properties of an investment token, also gives holders the opportunity to participate in voting processes regarding the direction of a DAO (Cf. Appendix No. 6) [16].

It is by no means an exaggeration to say that the "heart of every DAO" is the "software-driven voting mechanism". It is then the members of the DAO who - depending on the design of the DAO - ideally steer the organization in the desired direction and extend or adapt the underlying self-executing program code of the smart contracts through voting procedures [16]. In doing so, all participants can "interact with the software within the constraints set by the software using their wallet address." The problem here - as with any member-dependent organization - is that participation in voting is idR low, and it is common for less than 10% of those eligible to vote to participate in voting (*Greilich* 2022).

In general, governance tokens are also fungible, i.e. freely transferable, and can be traded anonymously. Problematic for the voting processes is that individuals can acquire multiple governance tokens. Even if this were excluded in the protocol, it would not be possible to control how many wallet addresses with then one governance token each an individual person owns due to the anonymity. As a rule, a small group therefore holds a large proportion of the governance tokens [32]. It can therefore happen that so-called "whales" (designation for investors who hold a particularly large number of governance tokens) can enforce their decisions on the basis of their token majority [15].

The governance token holders can submit proposals within the DAO, whereby an overloading of the system by mass requests or not seriously meant fun proposals is prevented by paying a deposit for each submitted proposal, as well as in some projects by prior review by so-called reviewers (curators). However, the concrete design varies from DAO to DAO. Financing or investment DAOs will be projects into which collected capital is to flow in the form of a shareholding. Governance token holders can then vote on proposals; if a quorum previously set in the code is reached, the DAO's code will independently execute the desired transaction and any subsequent steps (*Mann*, 2022).

In this way, unlike traditional organizations, this form of decision-making is not left to the top management but is stored in the DAO's code. Decision-making and decision-making can be implemented much more cost effectively and quickly with greater transparency and traceability [26]. In addition, governance token holders can form an "association will" and pursue the advancement of a "common purpose" by providing capital and participating in voting.

https://doi.org/10.54934/ijlcw.v2i3.xx

3.3 Smart Contracts as the Basis for DAOs

As we understand smart contracts today, they were already conceived in the 1990s by Nick Szabo [29], although the discussion about automatically executing programs certainly goes much further back in time [29]. Depending on how you look at it - if you also want to understand the first commodity vending machines as "simplified versions" of modern smart contracts [13] - they were "in use long before the German Civil Code came into force."[29]. In this context, the Ethereum blockchain was the first platform to enable smart contracts and D-apps, explaining the dominant position of this blockchain (see Appendix No. 7) [10]. Thanks to the "Turing-completeness of the smart contract architecture", the possibilities of designing a DAO are almost unlimited [4]. This then also ensures that people and machines can be coordinated autonomously by means of a DAO through specifically adapted smart contracts - without the connection to classic business entities [26].

3.3.1 How smart contracts work.

In a sense, the smart contract works like an autonomous agent in that it automatically responds to input it receives from external accounts or other smart contract programs running on the network [7]. Thus, based on an "if" operation or "if...else-statement" known in the programmer's language, an "if-then" logic is programmed in that triggers or omits a certain operation when a certain pre-defined event occurs (e.g., paying out an amount of money to a certain wallet address) [16]. The smart contract also has a wallet address to receive payments in cryptocurrencies [3]. The Smart Contract virtually executes itself based on its set of rules [39].

A Smart Contract can consist of as little as a few hundred lines of code and can therefore be used in any country and by anyone with an internet connection, thanks to the transnational nature of a Blockchain [7]. Smart contracts have many advantages: they offer companies and organizations entirely new ways to protect themselves from misappropriation, misuse of their assets, self-dealing, and opportunistic behavior by enabling much better internal control, automating many mundane processes [7], and coordinating an increasing number of market and non-market activities [7].

In addition, smart contracts can be used over and over again, perform very small-scale operations (especially important in the IoT space where micro payments are involved), and map so-called D-apps through them. Finally, they are also the basis for DAOs, which are composed of a large number of smart

https://doi.org/10.54934/ijlcw.v2i3.xx

contracts [7]. Furthermore, they can be used to map areas without central intermediaries (which slow down processes) even if they are of such small scale that previous structures (e.g., a notary) would not take them on for reasons of time and cost (especially e.g., micro-payments to sensors) [7].

Through smart contracts, many processes can be negotiated in an automated manner, entire production processes can be freely initiated and executed by intermediaries, and finally, payment transactions can be handled automatically [1]. At the same time, the whole thing takes place at such high speed that they are also suitable for "time-sensitive applications" [17]. Smart contracts create trust because the parties know that the code - provided it correctly reflects their intentions and the circumstances underlying them occur - will be executed fully automatically on the blockchain [17]. And because this execution occurs identically and almost simultaneously on all nodes worldwide in a decentralized manner (see Appendix No. 8), there is no need for additional entities to subsequently enforce the execution (e.g., a court) [23].

In this sense, smart contracts are the backbone of DAOs. They are also DeFi applications, which can be understood as small, tamper-proof, highly transparent (the internal logic of the deterministic program code can be understood by anyone) computer programs that are stored and executed on the blockchain [32]. Contractual agreements can also be mapped in these programs, enabling the automatic exchange of services and the immediate enforcement by execution of the contracts. The word "smart" does not stand for "clever" or "smart," but is equated in programming jargon with "uniquely identifiable" and "forgery-proof". The comparison with a vending machine is often used to describe smart contracts: The customer can select a product, is shown a price, deposits the money and then - depending on the filling status of the vending machine - receives either the product or his money back in a fully automated manner, since the contract, which is transparent to the customer, fulfills itself [34].

3.3.2. Smart contract - a contract or just code?

The parties using a smart contract must have negotiated the underlying conditions of the smart contract in advance and agree that they want to have this contract executed automatically by means of a smart contract on the blockchain. The contractual agreements are recorded in software code and then processed and executed in a decentralized manner by all nodes supporting the underlying blockchain network [7]. However, the concept of a contract is misleading, as the smart contract is not a contract but merely a program code that can at most still mirror a contract from the real physical world, but executes

https://doi.org/10.54934/ijlcw.v2i3.xx

it in a fully automated manner [39], which, however, does not lead to the smart contract becoming a contract in the legal sense [29].

According to the prevailing opinion, the concurring declarations of intent [39] and the will to be legally bound (Rechtsbindungswille) are missing. In addition, the initiator of the smart contract also takes a back seat to it and can no longer change it independently [39]. In most cases, smart contracts are used to "fulfill or control already existing debt relationships."[12] Smart contracts are merely to be seen as "automated business processes and legal transactions, which, however, would already have existed longer than the German Civil Code (BGB)" [29]. *Baur* would therefore even like to see the name Smart Contract replaced with the term "controlling software code". Only the supporters of the "code is law" principle see a smart contract as a "new legal institution" that can no longer be interfered with by the legislature [see in this paper: Section 4].

3.3.3. Problem of immutability and reversals of smart contracts

A repeatedly cited disadvantage of smart contracts is that - unlike centralized institutions with intermediaries - an erroneous or unauthorized transaction cannot be reversed after the network of nodes on the blockchain has validated it [7]. And, of course, there is always the risk of a programming error occurring with a smart contract (see "The DAO") [32]. Since no party controls the blockchain on which the smart contract has been placed, and the smart contract executes itself, it cannot be stopped after it has been activated, and the conditions contained in the code are executed. Subsequent correction is then generally no longer possible unless the entire network is reset, as in the case of "The DAO" (see above) [17]. This can only be counteracted if the parties have already programmed the possibility of stopping the program into the smart contract in advance [7]. Thus, one can also integrate withdrawal agreements into a smart contract or the possibility to call an arbitration court to decide the dispute [7].

The concern that smart contracts can no longer be changed is unfounded, however, because there are now enough functionally adequate "workarounds" to counteract the consequences of a smart contract once it has been executed by means of anticipatory behavior. It is therefore possible - something that is often overlooked in the discussion - to limit the executive character of smart contracts without this being particularly difficult. There are various approaches here that do not collide with the basic principles of blockchain technology. Anticipating every conceivable case in advance and storing possible contract violations and their resolution in the code seems unrealistic; but one can at least make regulations on how

to deal with a reversal situation (possibly also in the real physical world) [12]. *Freidank* also correctly recognizes that possible problems "can be solved well with the current law, however, if the possibilities and limits of the technology used are always kept in mind and appropriate contractual provisions are made"[12].

If it is recognized that any undesirable developments cannot be anticipated in the code, a smart contract can be programmed in such a way that part of the code draws on an external source, such as an external library (this is referred to as modifiable libraries). In this way, one can build in a "back door" to adapt the Smart Contract in parts later on, if both sides agree or a judge should order this. A back-reference function (in German: Rückverweisfunktion) is also conceivable, in which an existing smart contract refers to another smart contract that is later initiated in an optimized manner if essential elements of the agreement change.

In other words, smart contracts could of course be modified retrospectively if they were programmed intelligently and with foresight. So-called "reverse transactions" protocols, which either require the cooperation of the repayment debtor or aim to withdraw certain assigned legal positions that are still tied to the blockchain (e.g., computing capacities, usage rights, licenses, etc.), are also being tested [12].

Other possible solutions involve a smart contract only implementing certain transactions after a certain grace period and recording them on the blockchain [12], which is what made reversal possible in the first place in the case of "The DAO" project [12]. Viewed in this way, the smart contract would then retain financial assets or other benefits like a "trustee" until the other party has confirmed receipt of its performance or an objection period has expired or a waiver of revocation has been declared [29]. Recently, so-called "Chameleo Hash Functions" on so-called "Redactable Blockchains" have also been discussed, which make it possible to change the entries on a Blockchain after the fact without immediately triggering a hard fork [12].

Despite all these approaches, there is no question that smart contracts will not be able to take into account all the legal intricacies, at least not in the near future, especially if these are difficult to anticipate and it is therefore not possible to transfer these specifics into the "strict logic of the code" [7]. This may possibly change due to "Strong AI", i.e. "strong artificial intelligence" (which can perform several

https://doi.org/10.54934/ijlcw.v2i3.xx

specialized operations simultaneously) in connection with DAOs, the development of which is expected in the near future [33].

4. ORACLES AND HOW BLOCKCHAINS CONNECT TO THE REAL PHYSICAL WORLD

Smart contracts and DAOs stored on the blockchain can connect and interact with external systems (such as programs, sensors, RFID chips) or with individuals and legal entities through interfaces to the real world - so-called oracles - which allows them to incorporate information from the real physical world (off-chain) into their processes [7]. This allows a DAO to respond to changing conditions in near real-time and verify events from the real world [7]. An example of such a process would be the fully automated matching of the shipping status of an online order by an Oracle that can access the API of the shipping company's website, and automatically pass a confirmation to the smart contract when the package has been shipped. The confirmation then distributes a specific token to the contract partner [17].

A real-world independent person could also function as an Oracle and reflect information back to the blockchain or smart contract or DAO. For example, an arbitration judge/arbitrator previously appointed by the parties who analyzes the facts of the case and communicates his or her decision (see Appendix No. 9) [29]. Or the farmer who detects certain stress factors in the field (e.g. pest infestation) and enters it manually into a database using a suitable input device [1]. Currently, the largest and still fastest growing application field for Oracles is crypto-derivatives. That is, betting on the market performance of specific asset classes (e.g., cryptocurrencies, stocks, commodities, etc.) via blockchain-based derivatives protocols that align smart contract-driven monetary distributions with real external market developments and therefore require real-time information from the real world [32]. Using Oracles, it is also possible to capture performance disruptions in the real world and - if these performance disruptions have been anticipated - address them using smart contract programming (e.g., temporarily shutting down resources or locking a smart lock, etc.) [29].

This definitely also poses dangers because the "exclusion of external data sources typical of blockchain is partially removed" [12] and dependencies on external information arise [32]. This can lead, for example, to data sources connected to the Oracles being manipulated. Examples include a website that is hacked and transmits false data, or a human Oracle that can be corrupted and willingly and knowingly provides false information, which in turn leads to incorrect operation of the connected smart contract or DAO (so-called Oracle Problem) [32]. Such a danger can be reduced if several independent data sources

are used, which is now already practiced in many projects that rely on decentralized Oracle networks with a large variety of data sources [32].

Especially in the area of automation Oracles play an important role, because they connect the digital with the analog world [29]. The importance of Oracles is particularly exciting in view of IoT and robotics. Should a DAO have a "physical existence," such as a robot, it could also use this very directly as an Oracle in the real-physical world and then interact even more directly with the real environment. The prerequisites for this are already in place today. Just take a look at fully automated corporate organizations and the use of merchandise robots [31]. It is possible that the involvement of humans will no longer be necessary in this area and that the intermediary replacement, which currently operates only digitally, will become part of the real physical world [31].

5. THE COMBINATION DAO WITH ARTIFICIAL INTELLIGENCE (AI): THE FULLY AUTOMATED DAO

Humans have been dreaming of creating artificial humans, robots and self-managing companies for a very long time, i.e. a company without humans, the "No Man Society". The concept of Artificial Intelligence and self-governing organizations has accompanied mankind for centuries. For example, the first philosophical attempts to formalize thinking can be found in the 13th century with the Mallorcan philosopher *Ramon Llull*. *Gottfried Wilhelm Leibniz* also dealt with the "algebra of the mind", with the help of which one should arrive at a result "as it were by the action of a machine". And finally, *Alan Turing* developed the decisive thoughts on the functioning of an artificial intelligence and the question of whether machines would one day be able to think for themselves. Although *Schwemmer* already assumes that an "autonomously acting artificial intelligence" will be used at least partially in the DAO [35], this is not the case.

At the present, we do not yet have a "strong AI", i.e. an artificial intelligence that would be largely self-determined and comparable to human intelligence, and that can perform several operations in parallel (see above) [33]. However, some scientists, such as *Kurzweil*, believe that we will soon reach the technological singularity where a strong AI can operate at a human level. In particular, the connection of the DAO with an AI could play a crucial role in this. Strictly speaking, the name "DAO" is not correctly chosen for today's decentralized organizations because, although the DAO can automate certain processes, we are not currently at the point where the Decentralized Autonomous Organization can operate truly

https://doi.org/10.54934/ijlcw.v2i3.xx

autonomously from humans by means of "Strong AI" because this "Strong AI" does not currently exist [17]. Actually, one should therefore correctly speak of a DO (Decentralized Organization) [35].

At this moment, DAOs merely serve as a "virtual framework" which, at best, helps to "structure the activities of the participating members and to channel their will formation" [16]. In any case, no DAO that is completely devoid of human control can be expected in the foreseeable future. Apart from that, an AI cannot be a contracting party due to the lack of appropriate legislation, since it cannot be a natural person, a legal entity or a partnership [17] and cannot be granted any personal rights. Recent developments, such as Google's LaMDA AI, which claims personality rights [17], are promising, and it has already been proven that AI is capable of creating things that exceed the expectations or the knowledge of its programmers provided in the Deep Learning process. It is likely that, much like legislators have given legal personality to companies in the past, these developments will soon require a new legal framework to properly capture the rights and responsibilities of DAOs that will be autonomously controlled by AI in the foreseeable future [7].

For the discussion in this paper, however, actual autonomously operating AI-controlled DAOs can be disregarded for the time being, as no project has yet become known in which a "Strong AI" and a DAO have been combined. Especially interesting might this discussion furthermore become if we think about even more sophisticated developments in the DLT field such as for example but not only limited to DAGs (Directed Acyclic Graphs) and how they might be brought together with AI.

6. THE DAO AS A FINANCING INSTRUMENT VIA ICOs AND NFTs

In addition to its structure-giving function and its function for the proportionally autonomous orchestration of processes, a DAO also has the function of an alternative financing option for easier access to capital. By means of the blockchain, shares in companies can be "tokenized", i.e. converted into virtual shares recorded on the blockchain (see above) [7]. It is not uncommon for DAOs to issue other tokens (often in the form of crypto-coins or as NFTs) in addition to certificates in the form of governance tokens.

Thus, a DAO itself can become a kind of Bitcoin as its tokens become more valuable over time. NFTs in particular have become increasingly popular in this regard in recent years, as they allow for individualization in addition to a granted right, e.g., a voting right (Cf. Appendix No. 10). Investors can also individualize, even personalize these tokens - unlike shares - with very different added values (such

as utility functions, property rights, license fees, participation rights, convertible loans, etc.) and acquire them directly from the DAO, the company or the projects [10].

This issuance of coins is called an Initial Coin Offering (ICO). ICOs are comparable to the issuance of shares, the Initial Public Offering (IPO). In order to be able to offer a classic security (IPO), companies must - for the protection of investors - idR create numerous documents and fulfill verification requirements, which is not only costly and time-consuming, but above all also very complicated, which is why most public markets remain closed to startups and small companies [7]. Unlike IPOs, ICOs hardly have to submit to any regulations - at least at the moment - due to their novelty and decentralization [7]. Even though they are now recorded as securities in the U.S., for example.[2]

Thus, with just a few lines of code, a DAO can conduct an ICO, not only bypassing existing financial regulations, but also launching a global public offering to anyone. This makes it easier for the DAO to collect money from private investors without routing it through government agencies or centralized intermediaries. One is rightly reminded of popular crowdfunding platforms (such as Kickstarter, Betterplace, GoFundMe or IndiGoGo) [7]. The similarities between crowdfunding projects, investment DAOs, ICOs and IPOs are also evident in the communication with potential investors, whom one tries to animate to invest in the project, which is why documentation of the project is made available (in the case of DAOs and ICOs so-called whitepapers, in the case of IPOs a "securities prospectus" in the sense of § 32 III No.2 BörsG).

The whitepapers (mostly published on a website of the project) then contain a description of the technical details of the project, basic biographical information about the project founders and advisors as well as goals and hopes, which are roughly outlined [7]. In most cases, the tokens are implemented on the Ethereum blockchain (using an ERC-20 protocol), but they can also be created on their own blockchain. Many DAO project also issue Non-Fungible Tokens (NFTs) instead of crypto coins (see above). These are also mostly implemented on the Ethereum blockchain (using an ERC-721 protocol).

Such issuance of coins is also very secure due to the verification and validation capabilities, transparent, tamper-proof, and time-based recording of each transaction on the blockchain [7]. This form of raising capital is an interesting alternative to risky venture capital (VC) contracts, convertible loans,

[2] ICOs are classified as securities transactions in the United States, relying on the U.S. Supreme Court case 'SEC v. Howey Co' from 1946 and applying the so-called 'Howey Test'. Further details can be found in: *Burniske/Tatar*, Cryptoassets, p. 258.

https://doi.org/10.54934/ijlcw.v2i3.xx

loans (credit agreement), debentures, etc., especially for startups and small companies, because, on the one hand, they are easy to implement, and the initiators retain control over their companies [22].

This also explains the popularity of ICOs (cf. Appendix No. 11). However, there are still many ambiguities due to the lack of regulation, which has advantages and disadvantages in equal measure [22]. Issues discussed include regulatory issues, related prospectus and permission requirements [22], compatibility with the "strict requirements of the German Civil Code (BGB)", tax issues, and how to deal with international buyers and sellers [22]. The "technology-neutral approach" pursued by BaFin is encouraging, which at least puts any licensing obligations of financial instruments with regard to ICOs and tokens in the background.[3]

7. CONCLUSION

In conclusion, the Decentralized Autonomous Organization (DAO) is a rapidly growing phenomenon that is transforming the way we think about organizational structures and decision-making processes. This essay has explored the history of DAOs, their functioning and structure, the role of smart contracts and oracles in DAOs, and the potential for combining DAOs with artificial intelligence. We have also examined how DAOs can be used as financing instruments through Initial Coin Offerings (ICOs) and Non-Fungible Tokens (NFTs). The emergence of DAOs is part of a broader trend towards decentralized and democratized systems, enabled by blockchain technology. DAOs offer a new way of organizing and managing resources that is transparent, democratic, and more equitable. They allow for a high level of automation, reducing costs and increasing efficiency. While DAOs are still in their early stages, there is no doubt that they hold great promise for the future of organizational structures and decision-making processes. As the technology continues to evolve, we can expect to see even more advanced forms of DAOs that incorporate AI, DAGs and other cutting-edge technologies. However, as with any new technology, there are also risks and challenges associated with DAOs. For example, there are questions around governance, legal forms, regulation ingeneral, and security that need to be addressed. Nevertheless, it is clear that the benefits of DAOs outweigh the risks, and we can expect to see their continued growth and adoption in the years to come.

[3] *BaFin*, Second notification regarding prospectus and permit obligations related to the issuance of so-called crypto tokens (Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token), accessible at: https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_wa_merkblatt_ICOs.html, [Last time retrieved on March 10th, 2023].

REFERENCES

[1] Baumann, J. & Sesing, A. (2020) Smart, Smarter, Smart Contracts – Vertragsagenten, Blockchain und automatisierte Vertragsdurchführung in der Industrie 4.0, in: Jürgen Taeger (Hrsg.), Deutsche Stiftung für Recht und Informatik

[2] Baur, J. (2021) Die gesellschaftsrechtliche Außenhaftung für die Verbindlichkeiten von Decentralized Autonomous Organizations, in: Hoeren, Thomas/ Forgó, Nikolaus (Hrsg.), Schriftenreihe zum IT- und Informationsrecht (Peter Lang Verlag).

[3] Blocher, W. (2016) The next big thing – Blockchain – Bitcoin – Smart Contracts, 8(9), P. 612-618.

[4] Büch, M. (2022) Das ewige Phänomen der DAO: Warum eine revolutionäre Organisationsidee in der Welt der Blockchain gefangen bleibt, REthinking, 4, P. 4-10.

[5] Burniske, Ch., Tatar, J. (2018) Cryptoassets – The Innovative Investor's Guide to Bitcoin and Beyond, (Mc Graw Hill Education Publishing House).

[6] Dan-Cohen, M. (1986) Rights, Persons and Organizations (University of California Press, Berkeley).

[7] De Filippi, P. Wright, A. (2018) Blockchain and the Law – The Rule of Code. (Harvard University Press, Cambridge).

[8] DuPont, Q. Experiments in algorithmic governance: A history and ethnography of "The DAO" a failed decentralized autonomous organization, P. 157 – 177, in: M. Campbell-Verduyn (Hrsg.), Bitcoin and beyond (Routledge).

[9] Fan, L. Cronemberger, F., Gil-Garcia, J. R. (2020) Using Blockchain Technology to Manage IoT Data for Smart City Initiatives: A Conceptual Framework and Initial Experiments Based on Smart Contracts, in: Gil-Garcia, J. Ramon, Gasco-Hernandez, Mila/ Pardo, Theresa A. (Hrsg.), Beyond Smart and Connected Governments – Sensors and the Internet of Things in the Public Sector, (Springer Schweiz).

[10] Fisch, Ch. (2019) Initial coin offerings (ICOs) to finance new ventures, Journal of Business Venturing 2019, 34 (1), P. 1-22.

[11] Fleischer, H., Goette, W. (2022) Münchener Kommentar zum GmbHG, (C.H. Beck Verlag, München).

[12] Freidank, A. (2020) Blockchain in der Digitalisierung – Aufsetzen eines Blockchain-Projekts, in: Jürgen Taeger (Hrsg.), Deutsche Stiftung für Recht und Informatik (Tagesband). P. 583-598.

https://doi.org/10.54934/ijlcw.v2i3.xx

[13] Froitzheim, O. (2018) Code is Law, isn't it?, in: Jürgen Taeger (Hrsg.), Deutsche Stiftung für Recht und Informatik (DSRITB 2018).

[14] Glatz, F.(2022) Building Common Ground – How DAOs unlock the future of Work and Social Media, REthinking: Law, 4, P. 36-40.

[15] Greilich, K. (2022) Interview with KrauseHouse Co-Creator Commodore: How 2.000 strangers are trying to buy a NBA-Team using NFTs and organizing online, REthinking: Law, 4, P. 20-27.

[16] Hahn, Ch.(2022) Die Decentralized Autonomous Association (DAA) – Governance Dezentralisierter Autonomer Organisationen (DAO) qua (Ideal-)Verein?, Neue Zeitschrift für Gesellschaft, 15, P. 684-694.

[17] Heckelmann, M. Zulässigkeit und Handhabung von Smart Contracts, Neue Juristische Wochenschrift, 8, P. 504- 510.

[18] Isaacson, W. (2014) The Innovators – Die Vordenker der digitalen Revolution von Ada Lovelace bis Steve Jobs (Bertelsmann Verlag).

[19] Kurzweil, Ray (2014) Menschheit 2.0.: Die Singularität naht (Lola Books, Berlin).

[20] Lavington, S.(2014) Alan Turing and his Contemporaries: Building the world's first computers, (Princeton University Press).

[21] Lenzen, M. (2020) Künstliche Intelligenz – Fakten, Chancen, Risiken, (C.H. Beck Verlag).

[22] Lupu, R. (2017) Krypto-Token: Lukrative Finanzierung oder juristische Falle für Unternehmen?, in: Jürgen Taeger (Hrsg.), Deutsche Stiftung für Recht und Informatik. P. 637-650.

[23] Mann, M. (2017) Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp?, Neue Zeitschrift für Gesellschaft, 26, P. 1014-1020.

[24] Mann, M. (2020) Komplexe Smart Contracts: Die Decentralized Autonomous Organization, in: Braegelmann, Tom/ Kaulartz, Markus (Hrsg.), Rechtshandbuch Smart Contracts, (C.H. Beck Verlag).

[25] Mienert, B. (2022) Dezentrale Autonome Organisationen (DAOs) als alternative Organisationsstruktur der Zukunft – Die verschiedenen DAO-Typen und die rechtlichen Herausforderungen, REthinking: Law, 4, P. 28-34.

[26] Mienert, B. (2021) Wyomings DAO-Gesetz – Blaupause für die Regulierung Blockchain-basierter dezentraler autonomer Organisationen?, Recht Digital 2021, 8, P. 384-392.

[27] Müller, R. Ethereum und Smart Contracts, Seminararbeit 2018, Fachbereich Informatik Hochschule Bonn-Rhein-Sieg.

https://doi.org/10.54934/ijlcw.v2i3.xx

[28] Paulus, Ch., Matzke, R. (2017) Digitalisierung und private Rechtsdurchsetzung - Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?, Computer und Recht 2017, 33, 12, P. 769-778.

[29] Paulus, Ch., Matzke, R. (2018) Smart Contracts und das BGB – Viel Lärm um nichts?, Zeitschrift für die gesamte Privatrechtswissenschaft, 4, P. 431–465.

[30] Pesch, P. (2019) Blockchain, Smart Contracts und Datenschutz Risiken und Grenzen Blockchain-basierter Smart Contracts, in: Fries, Martin/ Paal, Boris P. (Editors), Smart Contracts (Mohr Siebeck Verlag), P. 13-24.

[31] Reyes, C. (2021) Autonomous Corporate Personhood, Washington Law Review, 96, Nr. 4, P. 1453-1510.

[32] Schär, F.(2021) Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis REVIEW, 103.

[33] Schönberger, D. (2018) Deep Copyright: Up and Downstream Questions Related to Artificial Intelligence (AI) and Machine Learning (ML), Vol. 10, P. 35 - 58.

[34] Schrey, J. (2017) Rechtliche Aspekte der Blockchain (Neue Juristische Wochenschrift) P. 1431 – 1436.

[35] Schwemmer, S. (2021) Dezentrale (autonome) Organisationen, Archiv für die civilistische Praxis, 4, P. 556- 595.

[36] Schulz, Th. Verantwortlichkeit bei autonom agierenden Systemen – Fortentwicklung des Rechts und Gestaltung der Technik (Nomos Verlag).

[37] Spindler, G. (2021) Blockchaintypen und ihre gesellschaftsrechtliche Einordnung, Recht Digital, 7, P. 309-317.

[38] Sundararajan, A.(2016) The sharing economy: The end of employment and the rise of crowd-based capitalism (MIT Press Verlag).

[39] Teichmann, Ch. Digitalisierung und Gesellschaftsrecht, Zeitschrift für die gesamte Privatrechtswissenschaft 2, P. 247- 272.

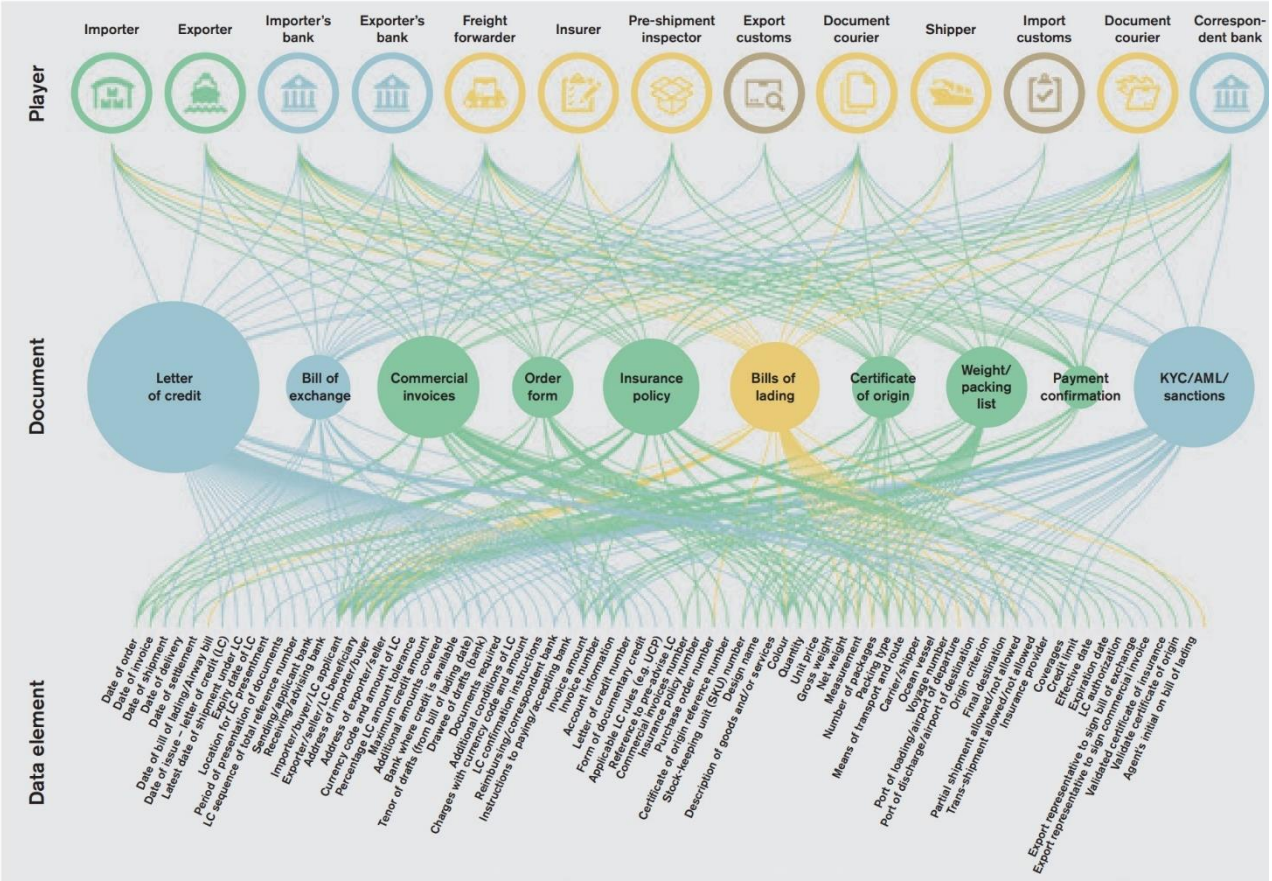
[40] Vigliotti, M. (2020) The Executive Guide to Blockchain – Using Smart Contracts and Digital Currencies in your Business (Palgrave Macmillan)

[41] Wilkens, R. (2019) Was sind Smart Contracts? In: Smart Contracts – Grundlagen, Anwendungsfelder und rechtliche Aspekte (Springer Gabler).

[42] Yano, M., Dai, Ch., Masuda, K., Kishimoto Y. (2020) Blockchain and Crypto Currency – Building a High Quality Marketplace for Crypto Data, 1 (Springer Publishing House).

APPENDIX

Appendix No. 1 - The various transaction partners that blockchain technology makes obsolete



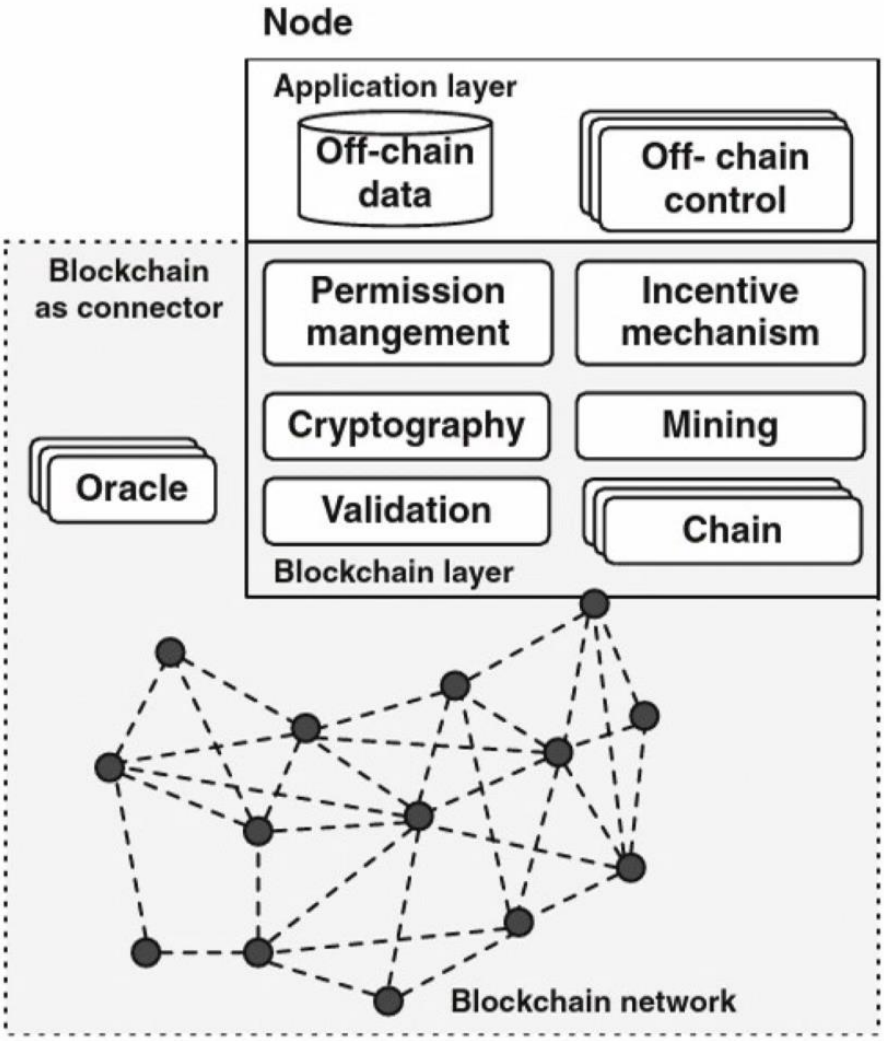
The diagram shows the necessary transaction partners that can be involved in a financial transaction. Many of these transaction partners are made redundant by blockchain technology and protocols such as Bitcoin.

Source: *Ganne*, World Trade Organization – Can Blockchain revolutionize international trade?, p. 22 mwN.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 2 - Overview of the functionality, and the different layers of a blockchain.

Appendix No. 2.1 - Basic Chemical Overview of the Functionality of the Layers of a Blockchain.

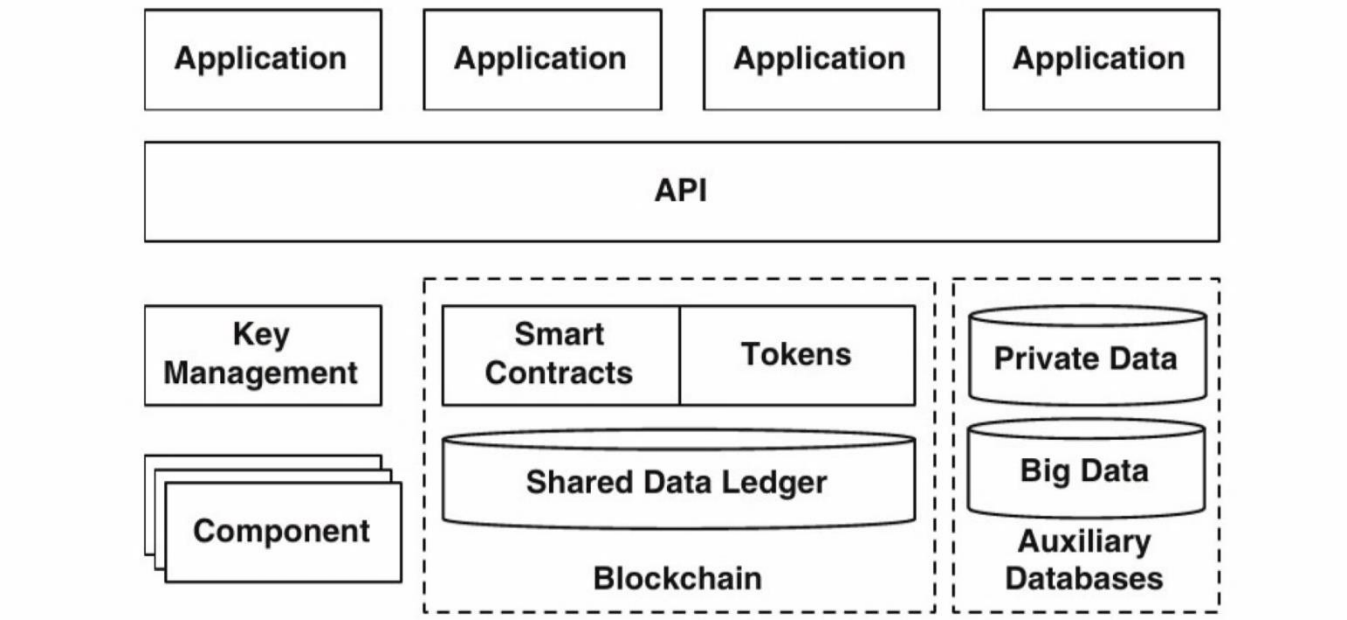


The blockchain first requires a network of nodes (here: blockchain network), which keeps the blockchain decentralized operational. The various layers are then built on top of this network. The whole thing starts with the first layer, which maps the basic functions (here: Chain, Validation, Mining, Cryptography, Incentive mechanism, Permission management). Finally, there is a layer on which certain programs can be executed (here: application layer), oracles can be connected via the API of the blockchain and bridges can be built into the real-physical world.

Source: *Xiwei Xu/ Ingo Weber/ Mark Staples*, Architecture for Blockchain Applications, 1. Auflage 2019 Springer Verlag, Schweiz, P. 14 mwN.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 2.2 - Overview of the "Applications" built on top of the Blockchain in the Layer Model.



In the diagram, you can once again see schematically how the blockchain architecture is structured for the integration of third-party applications and for mapping a DAO. The blockchain and the data ledger form the basis on which everything else (e.g., the smart contracts or tokens) is built. An API can then be used to create interfaces in the real physical world (so-called oracles) or to integrate applications and other programs from third parties. In this way, it is also possible to build a communication channel to a wrapper via the API.

Source: This overview builds on an earlier work: Vgl. *Xiwei Xu/ Ingo Weber/ Mark Staples*, Architecture for Blockchain Applications, 1. Auflage 2019 Springer Verlag, Schweiz, P. 84 mwN.

https://doi.org/10.54934/ijlcw.v2i3.xx

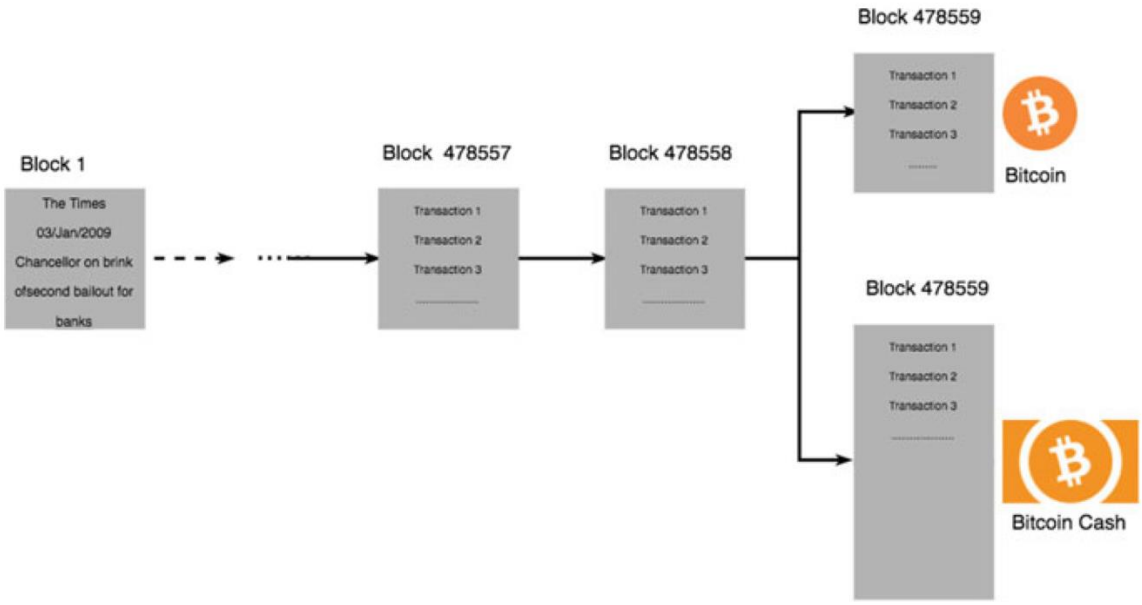
Appendix No. 3 – Development of the Aragon initiative to establish DAOs

Through the Aragon DAO Initiative, close to 5,000 DAOs have already been realized using the building block system provided. At the same time, the market capitalization rate is 16.9 billion US dollars.

Source: *Juliette Chevalier*, The Smart Contracts Behind DAOs, Vortrag auf der EthCC [5], vom 19. - 21. Julie 2022, accessible at: https://www.youtube.com/watch?v=ezhY4DDtCoU&t=5s, [Last time retrieved on March 10th, 2023].

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 4 - Process of a hard fork using the example of the split of Bitcoin into Bitcoin and Bitcoin Cash



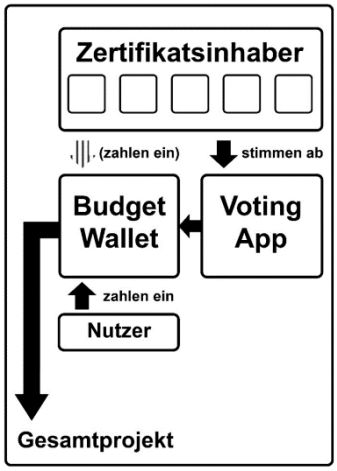
This graphic can be applied to the Ethereum project. It shows how the Bitcoin network split into Bitcoin and Bitcoin Cash in a hard fork on 01 August 2017. The users who carried out the Bitcoin hard fork did so in order to increase the transaction speed of Bitcoin Cash.

Source: Maria Grazia Vigliotti/ Haydn Jones, The Executive Guide to Blockchain – Using *Smart Contracts* and Digital Currencies in your Business, 1. Auflage 2020, Springer Nature Switzerland, P. 59

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 5 - Functioning of different DAOs according to *Baur*

Appendix No. 5.1 - Functioning of the Management DAO

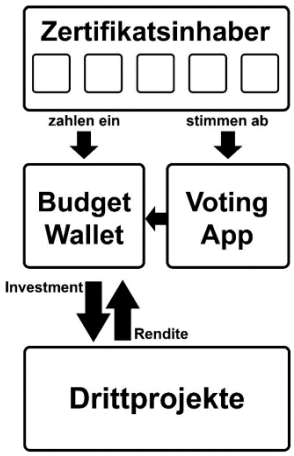


First, interested parties pay money into the DAO's budget wallet. In this way, they become "certificate holders", i.e. governance token holders. Subsequently, the governance token holders can vote on the use of the funds from the Budget Wallet by means of a voting app (which is already a basic element of the DAO). The DAO then organises the disbursement of the funds independently and offers third parties ("users") e.g. services. The "users" then in turn pay money to the DAO's Budget Wallet in order to be able to use certain services.

Source: *Baur*, Die gesellschaftsrechtliche Außenhaftung für die Verbindlichkeiten von Decentralized Autonomous Organizations, P. 57.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 5.2 - Functioning of the Investment DAO

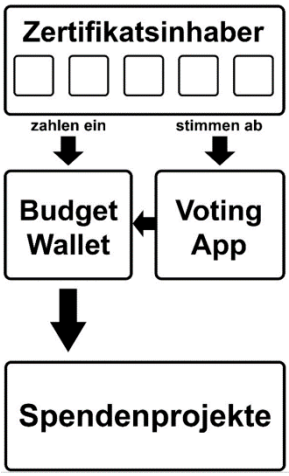


First, interested parties pay money into the DAO's budget wallet. In this way, they become "certificate holders", i.e. governance token holders. Afterwards, the governance token holders can vote on the DAO's investment goal using a voting app (which is already a basic element of the DAO). The DAO then automatically invests the Budget Wallet funds in third-party projects. The third-party projects pay a return to the DAO's Budget Wallet. The governance token holders can then vote whether the third-party funds are retained, reinvested or paid out to the governance token holders.

Source: *Baur*, Die gesellschaftsrechtliche Außenhaftung für die Verbindlichkeiten von Decentralized Autonomous Organizations, P. 60.

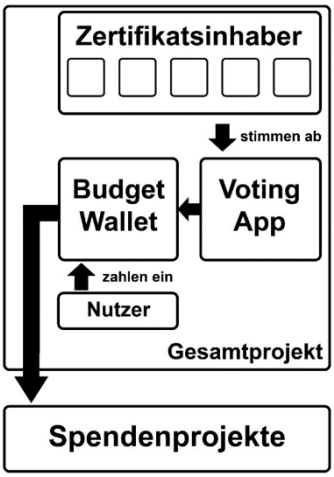
https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 5.3 - Functioning of the Donations DAO



The donation DAO works like the investment DAO (see above), with the only difference that no returns are expected from the donation project and the money only flows in one direction (namely to the donation project).

Source: *Baur*, Die gesellschaftsrechtliche Außenhaftung für die Verbindlichkeiten von Decentralized Autonomous Organizations, P. 63.

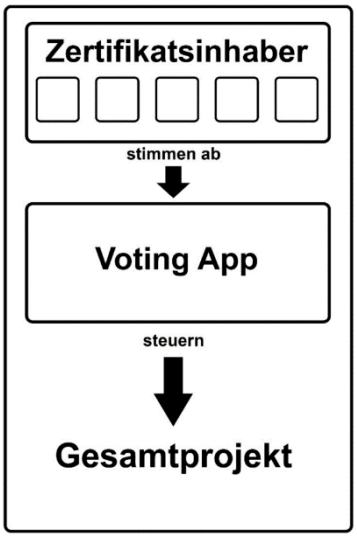


The only exception to this would be a so-called donation-annex DAO, where the DAO offers a service in addition to the funding goal of the donation project and raises money for the donation project through this.

Source: *Baur*, Die gesellschaftsrechtliche Außenhaftung für die Verbindlichkeiten von Decentralized Autonomous Organizations, P. 65.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 5.4 - Functioning of the Control DAO



With the governance DAO, the "certificate holders", i.e. governance token holders, can vote directly on the overall project. Such a DAO could be used, for example, to coordinate software processes in the IoT area.

Source: *Baur*, Die gesellschaftsrechtliche Außenhaftung für die Verbindlichkeiten von Decentralized Autonomous Organizations, P. 67.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 6 - Procedure for voting by means of governance tokens

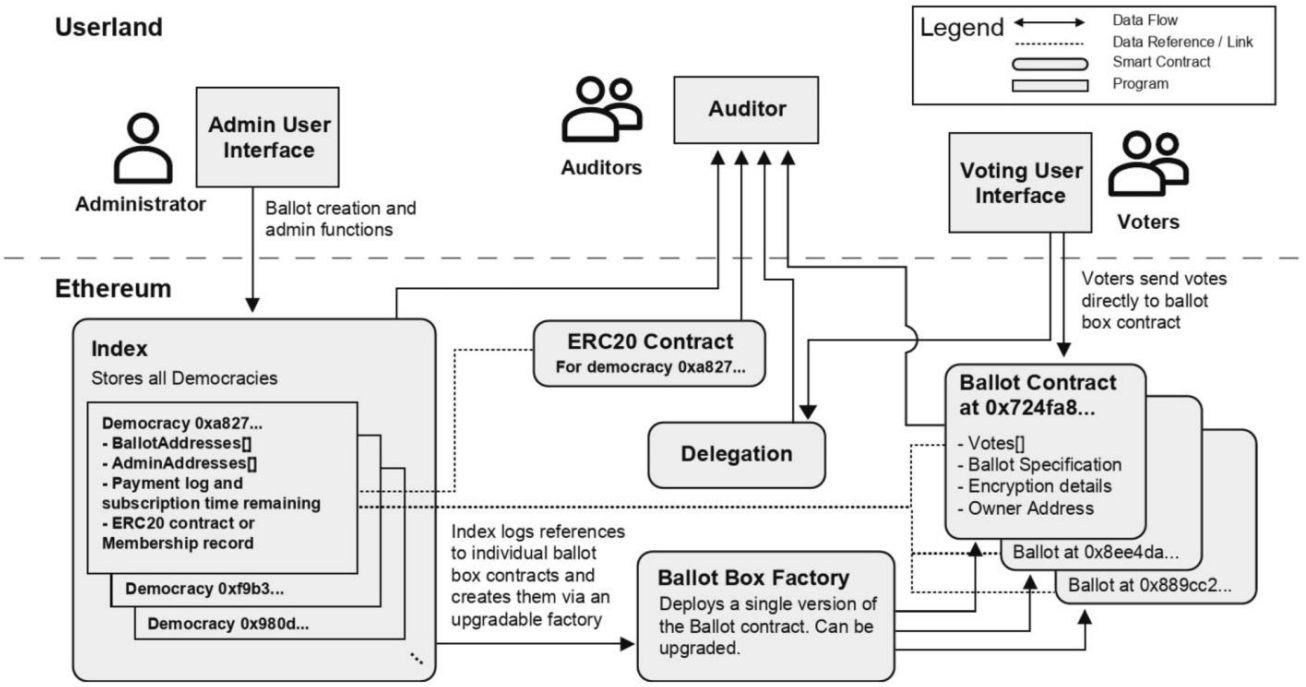


Fig. 13.1 Planned architecture for Tokenvote before development

The graphic shows the voting process with governance tokens. The Ethereum blockchain was taken as the basis here. It should be noted that smart contracts on other blockchain systems are sometimes executed quite differently than on Ethereum. However, since Ethereum currently serves as the benchmark for smart contract operations and most DAOs are currently based on the Ethereum blockchain, this graphic was deliberately chosen for further explanation.

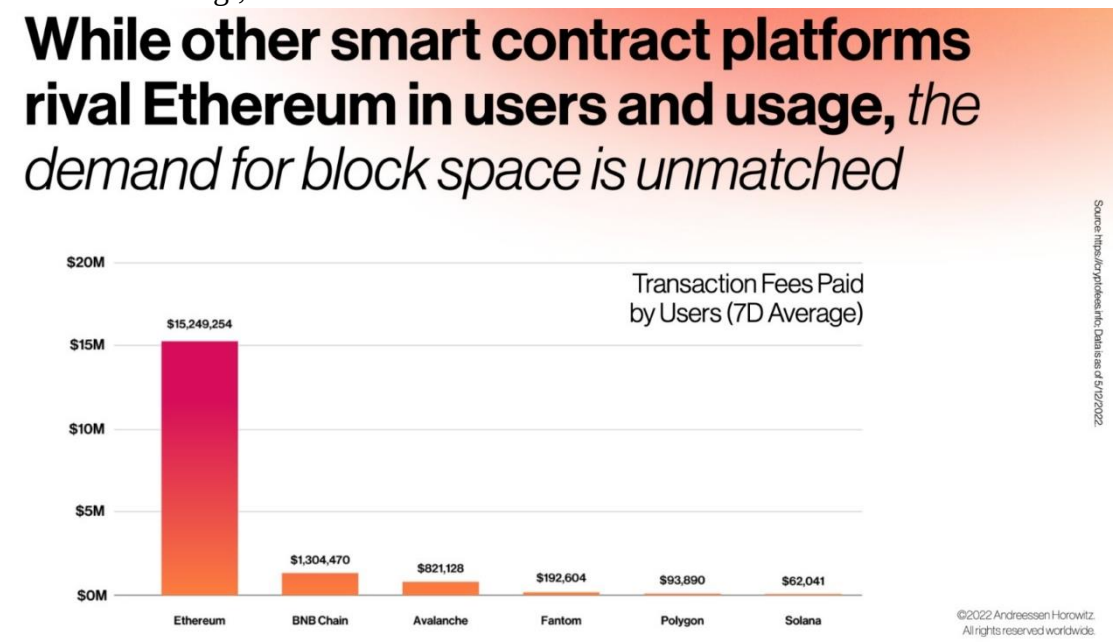
It should also be taken into account that each governance token can have different basic requirements and that the voting processes also vary. In the diagram shown here, however, it becomes clear how the mechanism works in general. For example, certain issues are first made available to the auditors. After they have validated the voting content, the governance token certificate holders can vote on it. No longer visible on the diagram is how a smart contract implements the proposal in the event of a positive vote, which is often done by releasing cryptocurrencies or tokens to one or more wallet addresses.

Source: *Xiwei Xu/ Ingo Weber/ Mark Staples*, Architecture for Blockchain Applications, 1. Auflage 2019 Springer Verlag, Schweiz, P. 263.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 7 - Ethereum Smart Contracts

Diese Grafik zeigt, dass



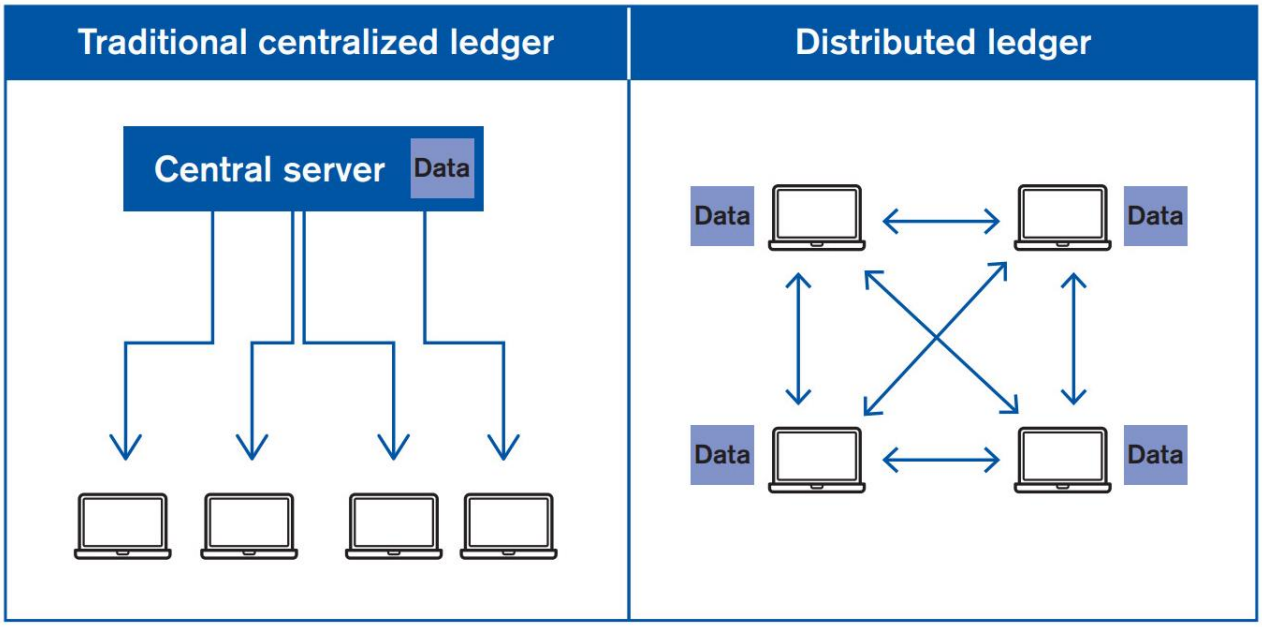
Ethereum in particular continues to dominate the market.

Source: *Andreessen Horowitz*, While other smart contract platforms rival Ethereum in users and usage, the demand for block space is unmatched, vom 12. May 2022, accessible at: Cryptofees.info;dataisasof5/12/2022, [Last time retrieved on March 10th, 2023].

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 8 - Nodes as the basis of decentralized systems

Appendix No. 8.1 - Centralised system compared to decentralised systems with nodes



The graphic shows the difference between centralised systems (left) and decentralised systems (right).

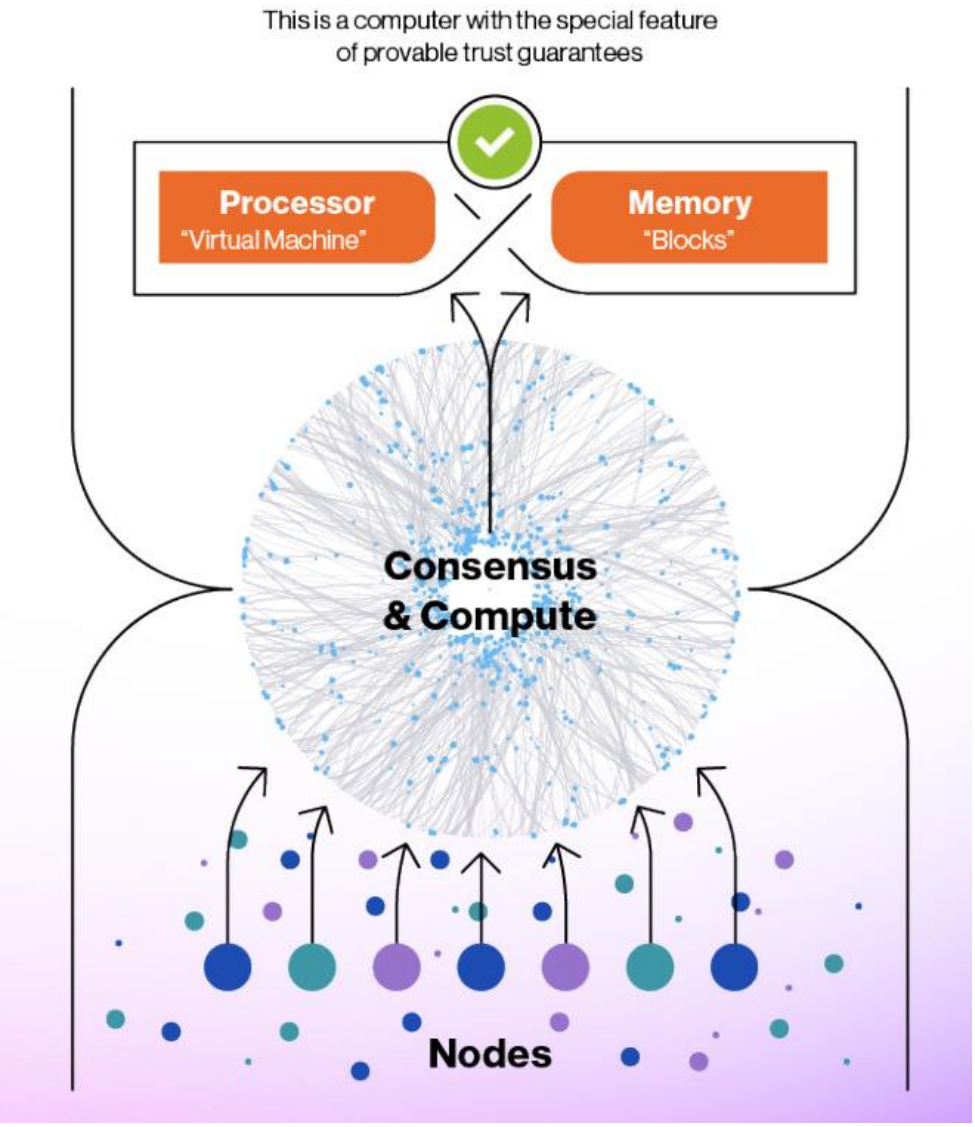
In centralised systems (left), all data is located on a central server. If this server is hacked or damaged, the entire data system is affected. Of course, there are security measures such as server mirroring and backup copies to prevent this.

In the decentralised system (right), all data is on different nodes. Depending on the design, all nodes have all the data or it is split up. In any case, the data is mirrored several times and well protected against loss or hacker attacks.

Source: *Ganne*, World Trade Organization – Can Blockchain revolutionize international trade?, P. 6.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 8.2 - Functioning of nodes in connection with a virtual machine via a blockchain

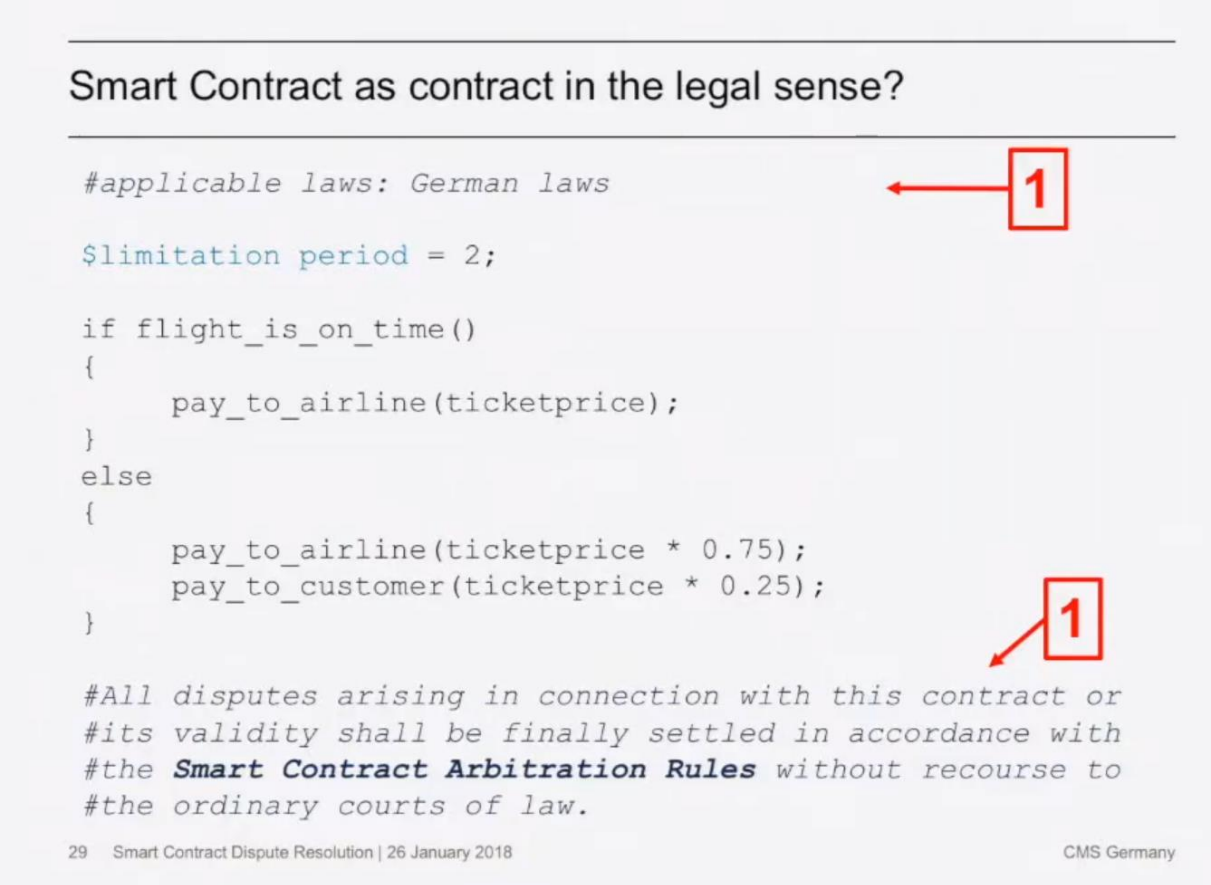


The nodes are physical computers or computing units that are connected to each other and jointly adjust the consensus mechanism. It is obvious to use them later for more intensive computing operations such as AI operations (comparable to the time sharing concept of the 1960s).

Source: *Andreessen Horowitz*, While other smart contract platforms rival Ethereum in users and usage, the demand for block space is unmatched, vom 12. May 2022, accessible at: Cryptofees.info;dataisasof5/12/2022, [Last time retrieved on March 10th, 2023].

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 9 - Example of a smart contract with a dispute resolution clause in the code

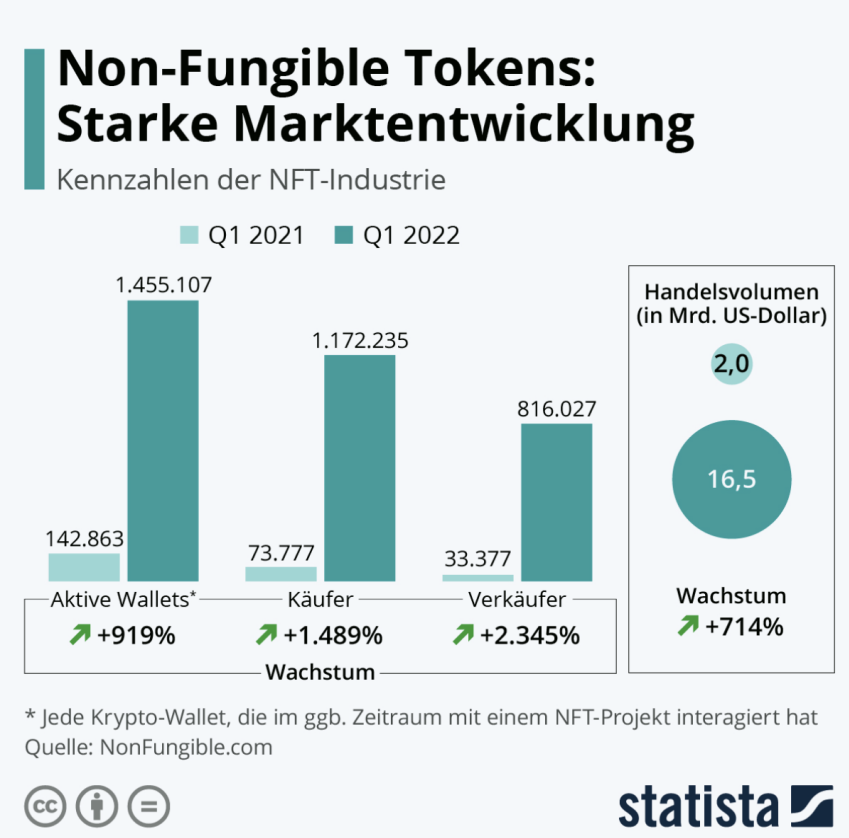


The Smart Contract states that German law is to be applied first and that an arbitration judge is to arbitrate in the event of a dispute.

Source: *Markus Kaulartz (CMS Hasche Sigle)*, on Blockchain Arbitration, Auf der Konferenz "blockchain, law, blockchainlaw?" an der *Humboldt-University* Berlin am 25.02.2018.

https://doi.org/10.54934/ijlcw.v2i3.xx

Appendix No. 10 - Market Development of NFTs



Source: Statista

Appendix No. 11 - ICOs as a financing model

The number of ICOs has grown significantly. Every DAO usually also has an ICO, as the governance tokens are issued in the course of an ICO. This can be used to raise money for the operation of the DAO as well as for the actual operations of the DAO.

The chart shows the capital raised via ICOs and the exponential growth of projects each from 2014 - 2018. What it does not show is the sharp drop in 2018 and the subsequent recovery phase.

Source: Maria Grazia Vigliotti/ Haydn Jones, The Executive Guide to Blockchain – Using *Smart Contracts* and Digital Currencies in your Business, 1. Auflage 2020, Springer Nature Switzerland, P. 20

https://doi.org/10.54934/ijlcw.v2i3.xx

ABOUT THE AUTHOR

Jan-Gero Alexander Hannemann – Master Student at Nicosia University, MSc in Blockchain and Digital Currency
e-mail: jga.hannemann@googlemail.com

ABOUT THIS ARTICLE

Conflict of interests: Author declares no conflicting interests

Acknowledgements: I would like to express my sincere gratitude to several individuals who have provided invaluable support and assistance in the development of this essay.

First and foremost, I would like to thank my wife, *Dr. Maryna Psol, LL.B.* who has been a constant source of encouragement and inspiration throughout this journey. I am also grateful to my two children, *Gerrian Leonardo Lui-Jin* and *Valeria Sophie Le-Yao*, for their unwavering support and understanding during times of intense focus and long hours of work.

I would also like to extend my thanks to my parents, who have always been my rock and my guiding light, providing me with the love and support I needed to pursue my dreams.

My friend *Anton* deserves special recognition for his technical input and guidance whenever I told him about my work, which was instrumental in shaping my ideas and refining my arguments.

I am also grateful to *Professor Tim Dornis*, who facilitated the contact that led me to Malta, and eventually made this essay possible.

Finally, I am appreciative of the guidance and support provided by *Ioannis Revolidis*, who coordinated my contribution to this journal.

Thank you all for your support and encouragement, without which this essay would not have been possible.

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.61

THE US "METABIRKINS" CASE IN THE LIGHT OF EU IP AND CONSUMER PROTECTION LAW

Eleni Tzoulia
Aristotle University, Thessaloniki, Greece

Article Information:

Received
July 31, 2023
Approved
July 31, 2023
Accepted
October 3, 2023
Published
November 30, 2023

Keywords:

crypto art,
trademark infringement,
digital content supply contract,
legal defect,
consumer protection

ABSTRACT

In early 2023 a United States (US) court ruled that a crypto art collection named "Metabirkins", depicting the famous "Birkin" bag of Hermès, infringed trademark rights. This ruling conferred Hermès the power to ban the commercial exploitation of Metabirkins by their designer, through a permanent injunction order. By the time that order was issued, however, several Metabirkins had already been sold to third parties. Taking this case as a point of reference, this paper examines crypto art transactions from the perspective of EU intellectual property (IP) and consumer protection law. First, it clarifies the conditions under which the purchasers and licensees of Non-Fungible Tokens (NFTs) fall under the consumer concept. Then, it examines whether the critical facts would constitute a trademark infringement in the EU, and what would have been the impact of such an infringement on the rightful use of the NFTs by their right-holders. Finally, the paper discusses Directive 2019/770 in protecting consumers and its applicability in the blockchain ecosystem.

FOR CITATION:

Tzoulia, E. (2023). The US "Metabirkins" Case in the Light of EU IP and Consumer Protection Law. International Journal of Law in Changing World, Special Issue NFTs, 118-140. DOI: https://doi.org/10.54934/ijlcw.v2i3.61

1. INTRODUCTION

Roughly, the term blockchain refers to a database formed within a network of peer nodes, i.e., interconnected computers sharing their resources. The data recorded into this network is sorted chronologically into sequential blocks after having been encrypted through asymmetric encryption mechanisms. The cryptogram corresponding to each new blockchain entry is a continuation of the immediately preceding one.

With these technical features, blockchain can ensure that the content it hosts acquires certain registration date, remains confidential, and becomes tamper-proof. This is achieved without the supervision and control of an external authority. Instead, the peer nodes mutually agree to adhere to a specific security protocol being enforced by themselves. In essence, their consensus concerns a certain verification process for the hash values of the blockchain entries [24].

1.1 The concept of crypto art

Due to the above characteristics, blockchain has been used for the last 15 years to simulate legal relationships and acts which in the analog environment would have been performed through the mediation of public authorities. Such are, for example, the issuance and exchange of value titles known as "crypto currencies". The so-called "Non-Fungible Tokens" (NFTs) represent one of the most recent trends in the pertinent ecosystem [9].

The concept of NFTs was first implemented in the “Ethereum” blockchain which was originally developed to host transactions with the cryptocurrency “Ether”. An NFT is the digital fingerprint of a blockchain entry pertaining to an asset, other that money. By entering the blockchain, the asset acquires a unique hash value, which functions as a time-stamped certification of its origin. In this sense, NFTs differ from each other even if they concern assets of the same type and/or of the same beneficiary. They are sold and bought in the blockchain environment in exchange for cryptocurrency or conventional money.

To date, NFTs have been assigned to digital content of various types, from journalistic texts and trademarks to in-game avatars and screenshots. It is argued that even physical assets from the analog environment, such as shares, securities, real estate titles, etc., can be turned into tokens, thus bypassing any legal institutions having supervised until now their issuance and circulation [10]. Primarily, however, NFTs have been used in recent years for the singularization of digital "art" files, such as images, GIFs,

https://doi.org/10.54934/ijlcw.v2i3.61

music, videos, etc. A new category of “works” has thus emerged, which are characterized as "crypto artworks" or "tokenized artworks" because they have an encrypted reflection on the blockchain [11].

In many cases the price of NFT artworks has soared into millions. This is surprising, given their nature as digital files. Customarily, the artistic value of digital artifacts has been considered dubious, which has also kept their economic value low. The reason is that, on the one hand, digital files are susceptible to unlicensed use and replication. On the other hand, advanced technology, in particular artificial intelligence (AI), is deployed for their creation. This is considered to reduce the resources required for their production in terms of human labour and material investments, as well as to disrupt the causal link between human contribution and creative output [4]. Therefore, it is reasonable to wonder what exactly the purchasers of crypto art pay for, and what are their rights when the expected qualities are missing.

1.2 The “Metabirkins” case

These contemplations have been brought under the spotlight on the occasion of a dispute which recently occupied US courts between the luxury fashion house Hermès and the pseudonymous artist “Mason Rothschild”. Rothschild created a series of 100 digital images depicting Hermès' famous “Birkin” bag covered in fancy fur. The images were linked to corresponding NFTs on the blockchain and offered for sale under the name “Metabirkins”.

The above activity instigated opposition from Hermès, which has trademarked both the word "Birkin" and the design of its famous bag. The company brought a case of trademark infringement before the US courts and in February 2023 the Southern District Court of New York ruled in its favour, awarding Hermès $133,000 in damages[1]. Shortly after this ruling, Hermès initiated permanent injunction proceedings before the Federal Court of Manhattan. At the end of June 2023 a permanent injunction order was issued, compelling Rothschild and auxiliary persons to: a) refrain from any further use of the Birkin marks, b) transfer the ‘www.metabirkins.com’ domain to Hermès, c) stop using their social media for the promotion of the Metabirkins, d) stop collecting royalties for the NFTs already purchased, and e) transfer to Hermès any profits yielded from the Metabirkins project since the beginning of the trial.

[1]Hermès International SA v. Rothschild, S.D.N.Y., No. 1:22-cv-00384, verdict 2/8/23.

https://doi.org/10.54934/ijlcw.v2i3.61

The Court declined explicitly to order the transfer of any Metabirkins left in the possession of Rothschild to Hermès, for them to be destroyed. This has been found unnecessary to protect Hermès' interests and "unwise", since Metabirkins are "at least in some respects works of art". Therefore, their removal from the channels of commerce and destruction would cause "constitutional issues". Notably, no order has been sought against the Metabirkins' purchasers compelling them to refrain from any use and to transfer their NFTs to the aggrieved company.

1.3 Framing the issues of concern from the perspective of EU law

The law applied in the above case is very similar to the corresponding EU rules in force. In particular, according to Directive 2004/48 on the enforcement of intellectual property rights[2], articles 10-13, in case of a registered trademark infringement, the right-holder establishes claims for cease and desist. The cease of the offence is in principle enforced through the removal from trade or even the destruction of the infringing sign and/or any products bearing it. When it comes to desist, the competent judicial authorities may issue injunctions by which the defendant is ordered to refrain from using the infringing material in the future, subject to monetary penalties. The infringer's liability is strict, while the existence of fault justifies concurrent claims for damages.

The above claims may be raised against any user of the infringing material, regardless of whether s/he is the manufacturer, a purchaser, a licensee, a trustee, etc.[3] It is also insignificant what are the objectives pursued by the acquisition of the critical subject matter, i.e., whether the user acts on a commercial scale or not. The competent judicial authorities are bound to the principle of proportionality[4] and have discretion to consider such parameters in the context of ordering appropriate corrective measures and setting the damages in each given case.

Based on recital 14 Directive 2004/48, it is individually argued that end users of signs and products infringing third-party trademark rights, as consumers, are not subject to the above claims [8]. This view is supposedly reinforced by the fact that the preliminary version of Directive 2004/48 explicitly limited its scope to "illegal activities carried out for commercial purposes or causing significant harm to the right holder". It should be noted, however, that these reservations have been heavily criticized [15] and were

[2] OJ L 157, 30.4.2004, p. 45–86.
[3] See also C-62/08 of 19.02.2009, UDV North America, ECLI:EU:C:2009:111, rec. 48.
[4] See rec. 22 and Articles 10 para 3, 12 and 13 Directive 2004/48.

https://doi.org/10.54934/ijlcw.v2i3.61

ultimately withdrawn from the final text of the Directive. This can only indicate the EU legislator's ultimate intent for broader harmonization. In the same vein, recital 14 Directive 2004/48, as it currently stands, prescribes a narrow scope of application, restricted to "acts carried out on a commercial scale", only for articles 6(2), 8(1) and 9(2) of the Directive. This seems to imply, by contrast, that other provisions apply uniformly to commercial and non-commercial uses of infringing signs. In any case, the exemption introduced by recital 14 refers to acts carried out by end-consumers "acting in good faith". In view of the right to publication of judicial decisions enshrined in Article 15 Directive 2004/48, an end-consumer's good faith must be regarded as negated as soon as a publicity measure is enforced in the case, following a conviction against the trademark counterfeiter.

The above observations justify the assumption that, within the EU, end users of NFTs are in principle passively legitimated in proceedings concerning trademark violations, i.e., individually subject to claims for cease and desist, as well as potentially for the payment of damages [13]. Therefore, apart from their obvious significance from the perspective of IP law, trademark litigations concerning crypto artworks also raise questions in the light of contract law. More specifically, it transpires that the violation of third-party trademark rights may affect the performance of sale or licensing agreements concerning the infringing NFT, by restricting or precluding its rightful use to the detriment of its current right holder.

In such cases, it is to be examined what claims does the aggrieved party establish and on which legal basis. In this respect, the relatively newly released Directive 2019/770 on contracts for the supply of digital content[5] has attributed specific rights to consumers. However, its applicability in the case of NFT supply agreements is still unexplored.

1.4 Objectives of the analysis

In view of the above, the study at hand approaches the Metabirkins case in the light of EU IP and consumer protection law. It contemplates whether the critical facts would have established a trademark infringement from the perspective of Directive (EU) 2015/2436[6] and Regulation (EU) 2017/1001[7]. It then presents Directive (EU) 2019/770 and examines the claims attributed to the aggrieved trademark owner

[5] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019, p. 1–27.
[6] Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trademarks, OJ L 336, 23.12.2015, p. 1–26.
[7] Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trademark, OJ L 154, 16.6.2017, p. 1–99.

https://doi.org/10.54934/ijlcw.v2i3.61

as an instance of improper performance of NFT supply agreements concluded between the Metabirkins' digital artist (author) and end users (consumers). The objective of this analysis is to clarify the rights and obligations of the contracting parties in such cases and to comment upon the challenges posed to their enforcement by the particularities of blockchain.

2. NFT ART SUPPLY AGREEMENTS FROM THE PERSPECTIVE OF EU CONSUMER LAW

Modern EU legislation recognizes "digital content" as an individual subject matter of economic transactions, which is distinct from tangible and intangible goods, rights, and services. The term refers to "data produced and supplied in digital form"[8] and comprises computer programs, as well as any type of digital files, e.g., text, image, audio and/or video [13]. Digital content may be transferred in storage mediums, like CD-ROMs and DVDs, or be downloaded directly from the internet. It is not disputed that NFTs fall within the pertinent concept [14], since they consist of digital data and cryptographic software.

2.1 The regulation of consumer contracts for the supply of digital content

Directive (EU) 2011/83 on consumer rights[9] was the first to regulate the obligations of traders supplying digital content to consumers. In this respect, the Directive prescribes pre-contractual information in favor of the purchaser of digital content (articles 5 and 6) and establishes certain formalities for the valid conclusion of the relevant agreements by electronic means at a distance (article 8). Moreover, it regulates the consumer right of withdrawal from digital content supply agreements without giving any reason (articles 9-16). The pertinent provisions have been recently amended by Directive (EU) 2019/2161, also known as the "Omnibus" Directive[10].

In addition to the above, Directive 2019/770 regulates the proper performance of consumer contracts for the supply of digital content. This entails the trader's obligation to make the digital content available (article 5), as well as to provide digital content that complies with the ("subjective") requirements agreed upon with the consumer (article 7). The digital content supplied must be also fit for the purposes

[8] See Article 2(1) Directive 2019/770.
[9] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88.
[10] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28.

https://doi.org/10.54934/ijlcw.v2i3.61

for which digital content of the same type would normally be used in accordance with any standards, open technical specifications, good practices, and codes of conduct applying in the pertinent field ("objective" conformity requirements). Besides, it must possess the qualities and performance features reasonably expected by the consumer, considering any public statement made by or on behalf of the trader (article 8). The trader has the obligation to keep the digital content updated for the entire duration of a fixed-term license agreement, otherwise for the period that the consumer may reasonably expect (article 8 para. 2), given the type and purpose of the digital content and considering the circumstances and nature of the contract [27].

Interestingly, the Directive designates explicitly as an indication of improper performance on the part of the trader, the provision of digital content whose use is subject to limitations in accordance with IP law, e.g., due to a violation of third-party IP rights (article 10). Indeed, when the IP holder rightfully compels the trader to discontinue offering the controversial digital content, any purchasers or licensees cannot use that content without infringing the law (recital 54). In such cases, the consumer is entitled to remedies for lack of conformity of the supply agreement according to article 14 Directive 2019/770, unless national law provides for its nullity or rescission.

In particular, article 14 entitles the consumer to have the defective digital content brought into conformity, unless this would be impossible or entail disproportionate costs considering, e.g., the gravity of the defect and the value of the digital content without the defect. If the restoration of conformity is impossible or unprofitable, belated, or unsuccessful, the consumer is entitled to receive a price reduction. This shall be proportionate to the reduction in the value of the digital content due to the lack of conformity. The consumer has the alternative right to terminate the contract unless the lack of conformity is insignificant.

2.2 Crypto art purchasers as "consumers"

The application of the above legal framework to NFT artwork supply agreements is subject to the condition that the purchaser/licensee is a consumer. The consumer concept is interpreted narrowly and "functionally" in EU law. In particular, the consumer status is attributed only to natural persons acting for purposes which are outside their trade, business, craft, or profession[11]. Consequently, an individual is

[11] See article 2(6) Directive 2019/770.

https://doi.org/10.54934/ijlcw.v2i3.61

considered a consumer only for those transactions which serve subsistence needs. The professional status and financial capacity of the individual, any previous experience in the pertinent field, as well as the value of the critical transaction are irrelevant in the context of this assessment.

There are certain adversities when applying the functional criterion for ascribing the consumer status. For instance, legal theory has been occupied with the so called “dual purpose” contracts, i.e., transactions serving partly private and partly professional purposes. This is the case, for instance, of a lawyer purchasing a laptop with a view to covering both professional and recreational needs. According to the European jurisprudence, in such cases the "predominant" transaction purpose prevails[12], which is identified based on objective criteria [6].

In the same vein, it is problematic whether nonprofessionals purchasing products or services as an investment, i.e., with a view to generating future income, retain the consumer status. This is the case for instance with individuals purchasing property with a view to reselling or hiring it out. According to the pertinent guidelines of the European Commission (2016)[13] and the European jurisprudence[14], speculative objectives do not suffice to negate the consumer status. Only when the commercial exploitation of the purchased goods becomes a quasi-professional activity, does the purchaser become de facto a “trader”, which shall be examined on a case-by-case basis [26]. For instance, whether the exploitation of real estate through short-term rentals is an economic activity for an individual is conditional upon its duration and intensity, in terms of the financial turnover yielded, the number of immovables promoted, and leases concluded. In this context, the individual turns into an undertaking when s/he must hire staff and set up business premises to cope with demand[15].

Considering the above, it must be noted that often NFT purchasers are legal entities, thus being precluded from any consumer protection. On the other hand, whether a natural person purchasing crypto art is a consumer or not, should be considered on a case-by-case basis. Neither the high value of the transaction, nor the speculative motives of the purchaser negate this capacity per se. However, if the purchaser has turned investments in NFT artworks into a business, the consumer status may be successfully contested. Indicative of such a de facto commercial activity is, for instance, the methodical

[12] See recital 17 Directive 2001/83/EU.
[13] Commission staff working document, Guidance on the implementation/application of Directive 2005/29 on unfair commercial practices. SWD(2016) 163 final.
[14] C-105/17 of 04.10.2018, Komisia za zashtita na potrebitelite v Evelina Kamenova, ECLI:EU:C:2018:808, rec. 38.
[15] BGH of 20.02.2018, XI ZR 445/17, VersR 2019, pp. 691-694, rec. 21.

https://doi.org/10.54934/ijlcw.v2i3.61

and repetitive conduct of similar transactions, the establishment of infrastructure for promoting the purchased NFTs for resale, e.g., hiring an intermediary, setting up a marketplace, etc.

3. IP VIOLATIONS BY PURCHASED NFT ARTWORKS AS AN INSTANCE OF CONTRACTUAL "NON-CONFORMITY"

A crypto art supply agreement does not have fixed and predetermined content in all cases. It is commonly divided into two parts, i.e., one concerning the NFT as a cryptogram, and another referring to the digital file represented by the NFT on the blockchain [7]. As a rule, the contract provides for the sale of the NFT, i.e., the transfer of its ownership to another blockchain user (node) in exchange for a price paid in cryptocurrencies. The new beneficiary shall also assume the costs for maintaining the NFT on the blockchain, e.g., energy consumption charges, platform fees, etc.

Regarding the other part of the transaction, which deals with the digital file as an artistic expression to the outside world, the supply contract has a less standardized content. The parties may specify the type of the supplied file, e.g., sound, video, etc., as well as its individual features, e.g., that the video has a minimum duration. Variations also arise regarding the permitted use of the digital artwork by the purchaser [18]. Indeed, some agreements allow only non-commercial use, while others a limited commercial exploitation of the artwork, by specifying, for instance, a maximum profit margin per year. The supply agreement for the famous "Bored Apes" NFTs, in contrast, grands rights to unlimited use and full commercialization of the artwork to the purchasers[16]. Consequently, they are free to resale it, use it as a logo, embed it in digital text, in multimedia, etc.

3.1 Objective conformity requirements of an NFT Digital Art Supply Agreement

The dual character of NFT artworks, according to the above, also determines the objective conformity requirements pertaining to agreements for their supply to consumers, within the meaning of Directive 2019/770. Technically, the artwork is expected to have a unique encrypted fingerprint on the blockchain. Consequently, the vendor is supposed to have taken all the necessary measures for the tokenization of the critical content, as well as its maintenance on the blockchain, e.g., by paying the necessary renewal fees. The vendor is also expected to retain ownership of the NFT at the time of the conclusion of the supply contract, i.e., to not have already transferred it to a third party.

[16] See the relevant terms and conditions: https://boredapeyachtclub.com/#/terms.

https://doi.org/10.54934/ijlcw.v2i3.61

3.1.1 Non-fungibility vs originality

The conceptual content of the term “non-fungible” is of great importance when outlining the objective conformity requirements of NFT artworks. This concept reflects the distinction between "replaceable" and "non-replaceable" things, which is prescribed in several legal orders in the context of property law[17]. Accordingly, as replaceable are regarded all movable things which are interchangeable with other things of the same genus. In contractual relations, such things are rather identified by their quantity (number), weights and measures, than by their individual features. Here fall, for instance, coins and banknotes, securities, consumable goods (e.g., agricultural and cattle products, fuel), mass-produced industrial products (e.g., electrical, and electronic devices, vehicles), etc. Conversely, as irreplaceable are regarded all immovables, as well as those movable things, which are unique and can be individualized in transactions. Here fall works of art, custom-made items, second-hand goods, etc.

Considering the above definitions, a “non-fungible” token, unlike cryptocurrencies, is a non-replaceable crypto asset. On the one hand, it has been attributed a unique hash value and metadata which differentiate it from any other entry on the blockchain. On the other hand, an NFT is meant to represent individualized content, i.e., non-replaceable things[18].

An issue to be addressed is whether the NFTs’ non-replaceability also guarantees the originality of their content from the perspective of IP law, i.e., as a prerequisite for its copyright protection. In this regard, it should be reminded that the concept of originality does not adhere neither to qualitative assessments nor to quantitative calculations. Namely, for a creation to be deemed original, it is insignificant whether it is tasteful, large-sized, etc., as well as whether its production required the expenditure of substantial resources. On the contrary, at an international level copyright seems to adhere to the causality between the author and the creative effect. Therefore, in the EU and the USA an original work is expected to reflect the author’s personality. Similarly, in the Anglo-Saxon legal orders a protectable work is a product of the author’s labor, skill, and judgment [23].

As derived from the above, a copy of an earlier work cannot be deemed original. However, originality is not synonymous with uniqueness. Certain legal orders do ascribe "statistical uniqueness" to

[17] See, for instance, article 950 of the Greek Civil Code (AK) and article 91 of the German Civil Code (BGB).
[18] See Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 (MiCA), (2020/0265(COD)), final version 05.10.2022, rec. 6c.

https://doi.org/10.54934/ijlcw.v2i3.61

original works[19]. This is a hypothetical value, based on the assumption that no one else apart from the author himself could ever generate the same expressive output, under the same conditions, without copying. In other words, the concept of statistical uniqueness refers to the capacity of an original work to manifest a unique personality. However, the fact that an object is "one of its kind" does not make it original per se since its features may be dictated by technical function or be banal.

Consequently, the uniqueness of an NFT does not imply the originality of the content it represents. The latter is non-replaceable, i.e., individualized, and distinct from other items of the same genus. Whether it also meets the originality standards shall be examined on a case-by-case basis according to the criteria prescribed by IP law.

3.1.2 The fit for purpose test in the light of the exhaustion principle

According to Directive 2019/770, an NFT artwork supplied by a trader to a consumer must be suitable for the use agreed upon by the parties. This may be private or commercial, limited, or unlimited. If the rightful use is not explicitly determined in the contract, then the NFT must be fit for the purposes for which digital content of the same type would normally be used and possess the qualities and performance features normal for digital content of this type.

In the case that the NFT artwork is subject to copyright as an original work according to the above, the scope of its reasonably expected use is conditional upon any IP rights retained by the author after the conclusion of the supply agreement [16]. According to the "principle of exhaustion", as prescribed by EU law[20], after the first sale of a work by its author or with his consent within the EU, the author cannot control or prevent the subsequent distribution of the work, i.e., its resale or further licensing by the new beneficiary to third parties. Whether this principle applies also to digital content in the form of NFT artworks, remains unclear.

With reference to digital content, exhaustion is provided for in article 4 par. 2 of Directive 2001/29 (InfoSoc). The same provision of Directive 2009/24/EC enshrines the principle of exhaustion for software. According to the EUCJ jurisprudence, to the extent that there is a software "sale", i.e., an agreement by

[19] This is true for the Greek legal order. See, for instance, the decisions of the Greek Supreme Court (Άρειος Πάγος) no. 196/2010, ΕπισκΕΔ 2011, pp. 919 et seq., as well as no. 537/ 2010, ΕπισκΕΔ 2010, pp. 1047 et seq.
[20] See Article 15 of the Regulation (EU) 2017/1001, as well as the identical provision of Directive (EU) 2015/2436, Article 4 par. 2 of Directive 2001/29 (InfoSoc) and rec. 33 Directive 96/9 on the legal protection of databases.

https://doi.org/10.54934/ijlcw.v2i3.61

which one acquires its permanent use[21], the exhaustion principle applies without exception, i.e., irrespective if the software is delivered in a storage medium, or by download[22]. When it comes to digital content, however, the principle of exhaustion applies only to data files incorporated into physical carriers [21]. This derives from the literal interpretation of art. 4 par. 2 InfoSoc Directive in the light of its recitals 28 and 29, and it is also teleologically justified.

Indeed, the first sale of a computer program enables the copyright holder to obtain an appropriate remuneration. Thus, giving him the right to control the resale of any copies downloaded from the internet would go beyond what is necessary to safeguard his intellectual property[23]. On the contrary, online digital content can be easily and inexpensively reproduced in counterfeit copies, which cannot be distinguished from the original. Therefore, the recognition of exhaustion in this case would affect the author's interest to receive fair remuneration for his works, while not even contributing to the creation of a secondary market of "second-hand goods", as is the case with tangible objects[24]. The application of the exhaustion principle in the case of composite material shall be determined by their "essential" element. Thus, for instance, eBooks comprising digital data backed by software shall be treated as digital content as a whole and be subject to the above restrictions[25].

The consistency of the above distinction is disputed [29]. In any case, it does not seem to affect the rights of an NFT artwork purchaser. Arguably, the essential element of NFT artworks consists in the digital content rather than the cryptographic software they comprise [5]. Unlike other types of digital content, however, digital files attached to the blockchain as NFTs are not susceptible to replication and unlicensed use by multiple users. Instead, as analyzed above, NFTs are unique, traceable, and tamper-proof. Therefore, they can be in the possession of only one person at a time and be distributed exclusively by their rightful owner.

Consequently, NFTs possess qualities pertaining rather to tangible goods than to digital data. Therefore, the principle of exhaustion should be applied without exemption in their case. This means that, unless it is differently determined in the supply contract, the purchaser of an NFT artwork subject to copyright is in principle entitled to unlimited use.

[21] C-128/11 of 03.07.2012, UsedSoft GmbH vs Oracle International Corp., ECLI:EU:C:2012:407, rec. 72.
[22] Ibid, rec. 60.
[23] Ibid, rec. 63.
[24] C-263/18 of 19.12.2019, Nederlands Uitgeversverbond and Groep Algemene Uitgevers, ECLI:EU:C:2019:1111, rec. 58.
[25] Ibid, rec. 59.

https://doi.org/10.54934/ijlcw.v2i3.61

3.2 Falling foul of the conformity requirements of Directive 2019/770 in the Metabirkins case

In the Metabirkins case, Rothschild made three allegations that have been intensively debated in the US legal order [12]. First, he pointed out that Hermès' trademarks at issue had not been registered for digital representations of the Birkin bag. Therefore, the use of a similar sign for Metabirkins, i.e., for completely different products than the physical Birkin handbags, could arguably not establish an infringement from the perspective of trademark law. Moreover, the critical creations were meant to make a statement for the world of luxury fashion, thus being protected by the freedom of artistic expression. After all, a disclaimer had been placed on the website where the Metabirkins were exhibited for sale, stating that their designer is not related to Hermès. This section endeavours to subsume the facts of the Metabirkins case under EU trademark law.

3.2.1 Substantiating a violation of Hermès' trademark rights under EU law

Regarding the first above speculation, it should be noted that the Birkin trademark is a reputation mark, i.e., it enjoys high recognition among the interested public. For reputation marks EU law provides increased protection, simplifying the establishment of an infringement. Indeed, both Directive (EU) 2015/2436 on trademark law (Article 10 par. 2c), and Regulation (EU) 2017/1001 on the EU trademark (Article 9 par. 2c) grant a reputation mark owner the right to prohibit the use of any similar sign by third parties, irrespective of whether it relates to goods or services which are identical, similar, or dissimilar to those distinguished by the reputation mark. This presupposes that the use of the similar sign could take unfair advantage of the distinctive character or the repute of the reputation mark or be detrimental to these capacities. An infringement is not established, where there is sufficient "due cause" for the use of the similar sign.

The risk of a sign taking unfair advantage of the distinctive character, or the commercial recognition of a reputation mark is established where there is a "likelihood of association" between the sign and the trademark. This likelihood relates to the assumption that the interested public would probably recall the reputation mark immediately, spontaneously, and subconsciously when perceiving the critical sign. Under these circumstances, the sign can appropriate the positive disposition of the interested public towards the reputation mark. From another perspective, by visually, audibly, or conceptually approximating a well-established trademark, the sign becomes promptly, effortlessly, and inexpensively visible and identifiable in the market [2].

https://doi.org/10.54934/ijlcw.v2i3.61

It could be argued that the Metabirkins demonstrate visual and phonetic similarities with the Birkin bag, which suffices to substantiate a likelihood of association by the interested public. Under these circumstances an infringement of Hermès' reputation mark is established, irrespective of the fact that the infringing undertaking does not sell handbags or other physical accessories, but rather digital representations of these bags on the blockchain. This is also true, despite the placement of a disclaimer on the Metabirkins marketplace, that the NFTs do not relate to the renowned fashion brand. As analyzed above, when it comes to reputation mark counterfeiting, there is no need to substantiate a "likelihood of confusion" of the interested public, that the infringer commercially relates to the right holder of the trademark. The offense is rather established by the fact that a sign becomes visible and gains an unfair competitive advantage by parasitizing on the reputation of an earlier trademark without due cause (free riding).

3.2.2 Artistic expression as a "due cause" legitimizing a trademark infringement

The burden of alleging and proving that the unauthorized use of the non-proprietary trademark serves a "due cause" is borne by the infringer. According to the recitals 27 of Directive (EU) 2015/2436, and 21 of Regulation (EU) 2017/1001, the use of a trademark for the purpose of artistic expression should be considered fair if at the same time it is in accordance with honest practices in industrial and commercial matters. Moreover, both these pieces of EU legislation, pursuant to their article 14 respectively, legitimize the use of non-proprietary trademarks for the purpose of "referring" to the goods or services they distinguish, if that use conforms with honest practices in industrial or commercial matters.

Based on the above provisions, the use of third-party trademarks in the discourse of artistic expression, criticism, or parody is acknowledged as a "due cause" in abstracto. However, if such use shall be deemed legitimate in concreto, is conditional upon an "honest practices test". This is in essence a balancing test to be carried out between, on the one hand, the financial interests of the trademark owner and, on the other hand, the freedom of expression as a fundamental right [22].

The reconciliation of these conflicting interests is one of the most controversial issues in EU trademark law. EU Courts have not had the opportunity to formulate a clear methodology for this purpose yet. It is however convincingly argued that the artistic or parodic use of non-proprietary trademarks shall not be deemed fair, if it is exercised "in the course of trade, in relation to goods or services".

https://doi.org/10.54934/ijlcw.v2i3.61

In more detail, artistic expression may well coexist with speculative objectives. Therefore, mocking or criticizing a non-proprietary trademark in an artistic context remains in principle lawful even though the generated artwork may be offered for sale. However, when a non-proprietary trademark is modified in a parodic way, only to be used as a trademark for the infringer's products or services, invoking the freedom of expression would only constitute an excuse to circumvent trademark law [2]. If this is the case shall be examined on a case-by-case basis. In this context, factors to be considered shall be the gravity of the offense, as well as the subjective perceptions of the offender (knowledge, negligence, intent), as deduced, e.g., from the particularities of his artistic activity (occasional or systematic), and style.

In view of the above, it cannot be argued with certainty whether the unauthorized use of Hermès' trademark would be deemed lawful within the EU as justified by a "due cause". It should be reminded that the word "Metabirkins" is used to distinguish a series of digital representations of the Birkin bag, which are offered for sale on the blockchain as NFTs. Consequently, it is used "in the course of trade", in relation to tradeable goods [16]. The social message from the illustration of the famous product, invoked by the artist before the US courts, does not seem obvious to the average consumer. Instead, Metabirkins appear to herald the advent of an augmented reality universe ("Metaverse"), where every material object can have a digital avatar with distinct utility and commercial value (Uhlenhut & Bernhardt, 2023). From this perspective also, it might be argued that the Metabirkins usurp from Hermès a potential future use of the Birkin trademark.

3.2.3 The infringement's impact on the originality of the NFT artworks

To the extent that a trademark infringement is not excluded under EU law, it should be considered what its impact might be on the "qualities and performance features" of the critical NFTs. A relevant concern is whether Hermès' trademark claims may affect Metabirkins' character as copyrighted works. In broader terms, it should be examined whether the phonetic or/and visual resemblance to an earlier trademark, may negate the original character of an NFT artwork.

From a contract law perspective, the finding that the supplied digital content is not original may firstly contradict the pertinent subjective conformity requirements within the meaning of Directive 2019/770. This may occur when specific properties, such as that the digital content has been created by the vendor himself, that it is "authentic", etc., have been stipulated between the parties by contractual

https://doi.org/10.54934/ijlcw.v2i3.61

terms. Besides, originality may also constitute an objective compliance requirement, i.e., a reasonably expected quality, within the meaning of Directive 2019/770.

Indeed, as developed above, not all NFTs represent "works" subject to copyright, since their non-fungibility does not make them original per se. However, when it comes to digital content created with the very objective of being sold as digital art, such as depictions, musical compositions, animation, etc., originality usually occurs. This is also supposed to be the reason why such artifacts are getting increasingly tokenized. Their registration on the blockchain, is namely meant to certify their origin from a specific author and to endow them with traceability, which prevents their replication and unauthorized use. This emphasizes and shields their character as works of art, which in the digital environment is in principle challenged [20].

Reasonable expectations on the part of the consumer regarding the originality of a purchased NFT artwork may have been also prompted through the artist's public statements and especially his marketing practices. In this context, the price of the promoted NFT also plays a significant role. No doubt, the value of crypto assets is fluctuating under the influence of many factors, including how much energy-consuming their production is, the forces of supply and demand in the relevant market, etc. Nevertheless, the offer price of NFT artworks is in many cases so high that it disposes the public to consider the promoted subject matter as a piece of contemporary art with timeless artistic value, which can function as an investment tool [17].

Either as a subjective or an objective conformity requirement, originality arguably affects the market value and marketability of the NFT artwork. In this sense, the finding that the supplied NFT is not protectable by copyright, whenever it might occur after the conclusion of its supply contract, would degrade its merits and pose restrictions on its rightful use. Therefore, it would constitute a defect, giving rise to consumer claims under the Directive 2019/770.

As regards the above, it is acknowledged that a work may remain original, as a unique expression of the author's intellect, even though it infringes third-party rights, i.e., offends somebody's personality, incorporates non-proprietary content, establishes a likelihood of confusion with a third-party trademark, or a likelihood of association with a reputation mark. In such cases, the controversial work is subject to copyright and the author is entitled to exercise the negative powers deriving from his intellectual property, e.g., inhibit any unauthorized use of his work by third parties. However, s/he is not allowed to

https://doi.org/10.54934/ijlcw.v2i3.61

exercise the positive economic powers of reproduction, presentation, and distribution of the work to the public without permission by the offended third parties.

The above means that Metabirkins may remain original works despite offending Hermès' trademark. In that case, however, their author shall be obliged to restrict himself on private use and not to exploit them commercially without Hermès' consent[26]. The impact of these restrictions on the performance of any supply agreements concluded by the artist with third parties, shall be assessed on a case-by-case basis.

3.2.4 The infringement's impact on the rightful use of the NFT artwork

As argued above, in the case of a trademark violation the trademark owner is entitled to raise claims of cease and desist against any user of the infringing material according to EU law. This is true, even if that user represents a consumer in the context of the transaction by which s/he acquired the critical subject matter. This means that, in the Metabirkins case, Hermès would have the right to prohibit any Metabirkins' purchaser or licensee from using their NFTs. However, claims for removal or destruction would rather be denied by courts due to the nature of Metabirkins as copyrighted artistic works. This would ultimately result in a hybrid situation, where the Metabirkins holders would be entitled to keep the infringing NFTs in their possession, but also obliged to refrain from any non-private, let alone commercial use of them.

Whether the above state of affairs would contadict the agreed or reasonably expected use of the NFT on the part of a Metabirkin purchaser in his capacity as a consumer, thus violating the respective subjective or objective conformity requirements of the pertinent supply agreement within the meaning of Directive 2019/770, could be only deemed in concreto [19]. It is for instance possible that the commercial exploitation of the Metabirkins by their purchasers has been contractually excluded in advance. In that case, Hermès' trademark claims would not affect the purchasers' rights. On the other hand, if the supply agreement does not provide for specific restrictions, Metabirkins should conform with the normal use for digital content of the same type. As argued herein, this use is primarily commercial since this type of crypto assets usually functions as an investment tool. Besides, the IP rights of the digital artists get exhausted as long as an NFT supply agreement prescribes full transfer of their ownership rights to the purchaser[27].

[26] See art. 10 para 3 Directive 2015/2436 and 9 para 3 Directive 2017/1001.
[27] C-128/11, rec. 42.

https://doi.org/10.54934/ijlcw.v2i3.61

4. ENFORCING THE RIGHTS PRESCRIBED BY ART. 14 DIRECTIVE 2019/770 IN THE CASE OF NFT SUPPLY AGREEMENTS

According to article 10 Directive 2019/770, where a restriction resulting from a violation of a third-party IP right prevents or limits the use of the digital content, the consumer is entitled to the remedies for lack of conformity provided for in Article 14. If the applicable national law provides for the nullity or rescission of the contract in such cases, it shall prevail. As far as article 14 of Directive 2019/770 is concerned, it awards three separate remedies to consumers which cannot be exercised cumulatively. In particular, the consumer is entitled to firstly have the digital content brought into conformity. Only where the restoration of conformity is impossible, or unsuccessful, the consumer is entitled to receive a proportionate reduction in the price, or to terminate the contract [28].

As analysed in the preceding section, under certain circumstances a commercial exploitation ban imposed by Hermès on the purchasers of Metabirkins may constitute a legal defect of the pertinent supply agreement in the light of Directive 2019/770. In that case, the aggrieved parties in their capacity as consumers may take advantage of the above remedies. In this respect, it could be argued that restoration of conformity is inherently impossible in the scrutinized case. It would namely entail the replacement of the purchased Metabirkin with another which does not infringe Hermès' trademark. However, the entire Metabirkins collection follows a uniform concept and artistic style. Thus, they do not differ from each other regarding the controversial qualities determining the infringement. In any case, the individual pieces of the Metabirkins collection, as non-fungible tokens, are not substitutable with one another. Consequently, the aggrieved consumer could select only between price reduction and contract termination.

4.1 Price reduction

According to article 14 par. 5, in conjuction with the recital 66 Directive 2019/770, a reduction in price shall be proportionate to the decrease in the value of the digital content due to the defect and to the time during which the consumer was unable to enjoy the digital content in conformity. In the context of the pertinent calculation, it should be taken into consideration that the infringement of third-party rights by an NFT artwork does not negate per se its originality. Thus, it may be still protected by copyright as a work of art in the Metaverse and be enjoyed privately by its owner. Any restrictions posed by the infringement refer to the commercial exploitation of the artwork. It should be also kept in mind that the value of crypto assets experiences large ups and downs, irrespective of their uniqueness, rarity, and

https://doi.org/10.54934/ijlcw.v2i3.61

copyright protectability. These fluctuations relate to energy expenditure rates, as well as to the forces of supply and demand in the relevant market, which in turn depend on consumer trust and the contemporary economic and geopolitical scene.

The value of the defective NFT, as shaped under the above influences, shall be subtracted from the value that the same NFT would have had if it were in conformity. This assessment shall take into account the selling price of non-defective NFT artworks of the same type at the time when the price reduction claim is raised. This is true, unless the relevant market experiences inflation at that time. In such a case, the price difference an aggrieved purchaser can claim shall be calculated based on the lower selling price recorded at the time when the NFT supply agreement was concluded.

4.2 Contract termination

The right to termination refers to a declaration of intent which has the legal consequence of overturning a contract, thus discharging the parties from their unperformed obligations. Moreover, contract termination establishes reciprocal claims between the parties, on the one hand, for the return of the digital content that has been already unduly delivered and, on the other hand, for the reimbursement of any part of the price that has been paid in advance, which corresponds to the period that would have remained had the contract not been terminated[28]. Because of these consequences, the right to termination can only be exercised where lack of conformity is deemed "not minor". The materiality of the defect relates to its impact on the rightful use of the digital content and shall be evaluated based on objective criteria. The relevant burden of proof lies with the trader and not with the consumer who exercises the termination right[29].

As argued herein the inability to exploit commercially a purchased NFT artwork may represent under certain circumstances a substantial restriction of its rightful use, thus justifying the termination of the pertinent supply agreement by the consumer. However, the exercise of the termination right in the case of NFT supply agreements poses certain adversities. The reason is that, on the one hand, their subject matter is registered in the blockchain. On the other hand, they are commonly executed automatically by means of smart contracts.

[28] See articles 16 and 17 Directive 2019/770.
[29] Article 14(6) Directive 2019/770.

https://doi.org/10.54934/ijlcw.v2i3.61

Indeed, within the blockchain ecosystem the reciprocal return of performances between the parties may be hindered by intermediaries refusing to process the transfer, as well as by smart contracts not having been programmed to recognize legal defects caused by third-party IP rights as a cause of contract unraveling. In such cases, the parties may raise reimbursement claims against non-cooperative intermediaries. Also, the mutual obligations for return may need to be executed manually, thus bypassing the deficient smart contract. The normative challenges posed by these processes must be meticulously investigated by jurisprudence.

5. CONCLUDING REMARKS

In the discourse of the above analysis, it has been concluded that an NFT artwork purchase agreement may be subject to EU consumer law, as a consumer contract for the supply of digital content. This is subject to the condition that the purchaser is a natural person and that the way s/he engages in the transaction does not pertain to a de facto professional activity. Moreover, under EU law an NFT artwork demonstrating acoustic, optical, or conceptual similarities with a reputation mark violates in principle the IP rights of the trademark owner. Freedom of expression cannot override these rules if the infringing material is meant to distinguish the NFT artwork as a tradeable product in the Metaverse. In any case, the infringement does not deprive the NFT artwork of its originality, i.e., its copyright protectability, but rather impedes its commercial exploitability.

As long as their supply agreement does not contain specific restrictions, NFT artworks must be suitable for unlimited and in principle commercial use by their owners. This assumption is not overridden by the EUCJ jurisprudence declining the application of the exhaustion principle in the case of digital content not incorporated in physical storage media. The pertinent interpretation of InfoSoc Directive does arguably not conform to the particularities of NFTs, which simulate on the blockchain the qualities and performance features of tangible irreplaceable objects. Consequently, any limitation of commercial use posed to the NFT by a third-party right, constitutes a legal defect of the pertinent supply agreement, thus establishing the non-conformity claims provided by Directive 2019/770 in favor of the purchaser as a consumer.

The Metabirkins case has unveiled how awkwardly NFT transactions fit into the latter rules. Small investors and collectors should be aware when purchasing art tokens, that third-party IP right violations may render their NFTs unbacked. In such cases it is inherently impossible to bring the NFT into

https://doi.org/10.54934/ijlcw.v2i3.61

conformity. Hence, purchasers shall be obligated to initiate lengthy procedures to enforce their rights for price reduction or reimbursement against the vendor. How the pertinent adversities shall be tackled is still an open issue to be set under scrutiny. On the part of NFT market stakeholders, it would be wise to safeguard consumer rights in advance, e.g., by including appropriate general terms in crypto art supply agreements and by correctly adjusting smart contracts, so that claims arising by an eventual NFT depreciation may be fairly reconciliated. Foresight and transparency safeguards consumer trust, thus preventing a collapse of the crypto art trade.

REFERENCES

[1] M. Alber, & A. Brandi-Dohrn, „Auswirkungen der Digitale-Inhalte-Richtlinie auf die Erschöpfung des urheberrechtlichen Verbreitungsrechts bei unkörperlichen digitalen Inhalten“, IT-Rechtsberater, vol. 12, no. 11, pp. 261-267.

[2] M. Bohaczewski, “Conflicts between trademark rights and freedom of expression under EU trademark law: Reality or illusion?”, International Review of Intellectual Property and Competition Law (IIC), vol 51, published online, pp. 856-877.

[3] M. Bohaczewski, “Special Protection of Trademarks with a Reputation under European Union Law”, (Kluwer Law International, 2020).

[4] E. Bonadio, & L. McDonagh, “Artificial intelligence as producer and consumer of copyright works: evaluating the consequences of algorithmic creativity”, Intellectual Property Quarterly (I.P.Q.), 2020, no. 2, pp. 112-137.

[5] E. Bonadio, & R. Mohnot, “NFTs and copyright: some burning issues”, European Intellectual Property Review (E.I.P.R.), 2023, vol. 45, no. 3, pp. 150-153.

[6] J. M. Carvalho, “Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771”, Journal of European Consumer and Market Law (EuCML), vol. 9, no. 5, pp. 194-201.

[7] J. Hugendubel, “Technische und rechtliche Grundlagen von Non-Fungible Tokens (NFTs)”, IPRB, 2022, pp.135-139.

[8] J. Miosga, „Vernichtungs- und Rückrufansprüche, §18“, in A. Kur, V. v. Bomhard, & F. Albrecht (Eds), Kommentar zum MarkenG – UMV, 4. Auflage 2023, C.H.Beck.

https://doi.org/10.54934/ijlcw.v2i3.61

[9] R. Moskat, & R. Schaar, „Kryptokunst - eine steuerliche Einordnung“, Betriebsberater, vol. 32, no. 1, pp. 28-31.

[10] J. Moringiello, & C. Odinet, “The property law of tokens”, Florida Law Review, vol. 74, no. 4, pp. 607-670.

[11] D. Rapp, & C. Bongers, „Kryptokunst in der Steuerbilanz“, Deutsches Steuerrecht (DStR), 2021, pp. 2178-2185.

[12] M. Ryan, “Intellectual property considerations and challenges in the metaverse”, European Intellectual Property Review (E.I.P.R.), 2023, vol. 45, no. 2, pp. 80-84.

[13] L. Kuschel, & D. Rostam, „Urheberrechtliche Aspekte der Richtlinie 2019/770: Eine Analyse der Bereiche: EULA, Second Hand Market, Overblocking und Nutzung nach Vertragsbeendigung“, Computer und Recht, vol. 36, no. 6, pp. 393-400. https://doi.org/10.9785/cr-2020-360613

[14] J. Lai, “Cryptoassets: goods, services, digital content, or a sui generis category?”, International Company and Commercial Law Review (I.C.C.L.R.), 2023, vol. 34, no. 5, pp. 287-300.

[15] C. - H. Massa, & A. Strowel, “The scope of the proposed IP enforcement directive: torn between the desire to harmonise remedies and the need to combat piracy”, European Intellectual Property Review (EIPR), 2004, vol. 26, no. 6, pp. 244-253.

[16] K. Middelhoff, & A. Zarm, “NFTs - marken-, urheber- und persönlichkeitsrechtliche Facetten des Phänomens”, IPRB, 2022, pp. 270-274.

[17] M. Molins, Blockchain technology, foundations, protocols and aesthetic considerations, Technoetic Arts, vol. 19, no. 3, pp. 349-364.

[18] M. Murray, “NFT ownership and copyrights”, Indiana Law Review, vol. 56, pp. 367-391.

[19] L. Oprysk, & K. Sein, “Limitations in end-user licensing agreements: is there a lack of conformity under the new Digital Content Directive?”, International Review of Intellectual Property and Competition Law (IIC), 2020, vol. 51, no. 5, pp. 594-623.

[20] E. Perot, “NFTs: copyright foe or friend?”, European Intellectual Property Review (E.I.P.R.), 2021, vol. 43, no. 12, pp. 793-799.

[21] E. Rosati, “Online copyright exhaustion in a post-Allposters world”, Journal of Intellectual Property Law & Practice, vol. 10, no. 9, pp. 673-681.

[22] M. Senftleben, "Robustness check: Evaluating and strengthening artistic use defences in EU trademark law", International Review of Intellectual Property and Competition Law (IIC), vol. 53, no 4, pp. 567 – 603.

[23] T. E. Synodinou, "The concept of authorship in international copyright law", in: T. E. Synodinou (ed.), "Pluralism or Universalism in International Copyright Law", Kluwer Law International (2019), pp. 563-583.

[24] E. Tzoulia, The blockchain ecosystem in the light of intellectual property law, JIPITEC, 2022, vol. 13, no. 3, pp. 290-301.

[25] T. Uhlenhut, & J. Bernhardt, „Markenrecht im Metaverse", Wettbewerb in Recht und Praxis, vol. 19, no. 2, pp. 139-146.

[26] S. Weidert, Verbraucher oder Unternehmer? Umfassende Einzelfallbetrachtung erforderlich, GRUR-Prax, vol. 10, no. 21, p. 510.

[27] M. Witzel, Der neue Mangelbegriff für digitale Produkte, IT-Rechtsberater, vol. 12, no. 12, pp. 289-292.

[28] N. Zdraveva, "Digital content contracts and consumer protection: status quo and ways further", EU and Comparative Law Issues and Challenges Series (ECLIC), 2021, no. 5, pp. 398-421.

[29] A. Sattler, „Neues EU-Vertragsrecht für digitale Güter: Die Richtlinie (EU) 2019/770 als Herausforderung für das Schuld-, Urheber- und Datenschutzrecht", Computer und Recht, vol. 36, no. 3, pp. 145-154. https://doi.org/10.9785/cr-2020-360305

ABOUT THE AUTHOR

Eleni Tzoulia – Lecturer for commercial law at the Law School of the Aristotle University, Thessaloniki, Greece
e-mail: elena.tzoulia@gmail.com
ORCID ID: https://orcid.org/0000-0001-5449-151X

ABOUT THIS ARTICLE

Conflict of interests: Author declares no conflicting interests.

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.54

NFTS, DIGITAL WORLDS AND BRAND PROTECTION IN FASHION: A UK/ EUROPEAN INTELLECTUAL PROPERTY PERSPECTIVE

Ioanna Lapatoura
Nottingham Trent University, Nottingham, UK

Article Information:

Received
July 19, 2023
Approved
July 29, 2023
Accepted
October 3, 2023
Published
November 30, 2023

Keywords:

intellectual property,
NFTs,
metaverse,
fashion,
designers

ABSTRACT

Two years into the metaverse utopia and with the promising launches of metaverse Fashion Weeks for two years in a row, the creative industries have not yet lost their enthusiasm for experimenting with digital worlds. In practice, brand owners 'mint' non-fungible tokens, or NFTs, associated with their real-world or purely digital assets that most commonly enjoy intellectual property (IP) protections, such as fashion designs. Those can be sold at dedicated NFT marketplaces, but are often interoperable, or capable of being used across a number of different digital worlds. This article endeavours to shed light into the following key question: to what extent intellectual property rights vested into real-world creations can be transposed into the digital and by extension, whether the legal protection offered can be given its full effect in a digital unregulated space, where users' identities are anonymous or pseudonymous. By weighing the expected benefits and losses from a UK & EU intellectual property perspective, the author questions: Are NFTs and the metaverse more than a gimmick? And hence, is the metaverse a market worth investing for fashion brands? The article first explores the metaverse for fashion, as well as designers' and brands' activity in this novel market space, followed by an in-depth discussion on the intellectual property question posed.

FOR CITATION:

Lapatoura, I. (2023). NFTs, Digital Worlds and Brand Protection in Fashion: A UK/ European Intellectual Property Perspective. International Journal of Law in Changing World, Special Issue NFTs, 141-152. DOI: https://doi.org/10.54934/ijlcw.v2i3.54

1. INTRODUCTION TO FASHION NFTs AND THE METAVERSE

Following last year's success, in March 2023 the second metaverse Fashion Week took place across 3 different virtual interconnected worlds: Decentraland, Spatial and Over (MVFW, 2023). Global fashion brands of the likes of Diesel, Tommy Hilfiger, DKNY, Balenciaga and Dolce & Gabbana were among the 60 designers and artists who showcased their collections in the virtual runways, expanding their collections to blockchain-based digital twins. Other than long-established fashion giants, Web3 native brands that exclusively sell digital fashion, such as the Institute of Digital Fashion and The Fabricant, were also present. Digital fashion is the by-product of tokenization of real-world or purely digital assets, or else fashion designs, that most commonly enjoy a range of intellectual property protections. In 2021, digital fashion amounted to approximately $498 million and '*is predicted to grow into a $4.8 billion market by 2031*' (Linares, Vogue Business, 2023; Allied Market Research, 2023). Brand owners showcase or market their creations in the form of non-fungible tokens or NFTs, permanently stored and verified in a blockchain network, i.e. commonly in the Ethereum blockchain [1]. The blockchain token essentially is a digital certificate of authenticity of its associated IP protected asset, i.e. a digital fashion design, rather than an embodiment of the asset. The latter is typically stored outside of the blockchain – often in a secure server or other cloud storage solution, while the NFT's metadata typically contain a URL link that points to this location. A fashion NFT can be accompanied by a digital wearable item for users' virtual avatars, that can be used in a multitude of virtual worlds, including gaming and metaverse platforms.

The metaverse is a virtual reality environment that blends the digital with the physical world, where users of networked computers can interact in real time (Oxford English Dictionary, 2023; [4]; Guadamuz, 2023). While one could perceive it as the future of gaming, it also is the latest market space for fashion [3]. Gonzalo Brujó, from Interbrand Group explains:

"*At its most ambitious, the metaverse is imagined as a single, digital universe that people can inhabit, bodily, through the use of virtual reality (VR) – a space that will be used to exist: to shop, to play, to go to school or to work*" (Seares, 2022).

Users are equipped with digital avatars, similar to those used in video games, that they can dress up with the latest fashion. They can immerse themselves in countless experiences, from unlocking physical fashion week experiences, to attending musical shows and after-parties, or sitting at the 'virtual' front row

https://doi.org/10.54934/ijlcw.v2i3.54

of the most well-known fashion shows, contributing to the strengthening of brands' relationship with consumers. And all, or at least most, of those experiences can be accessed for free, opening the floodgates to a global audience of online users, curious enough to test the waters of this new digital territory. More recently, the Council of Fashion Designers in America launched a 60-year-anniversary exhibition on metaverse platform The Sandbox, featuring looks from among others, Carolina Herrera and Diane von Furstenberg, with accompanying NFTs for purchase that also unlocked experiences (Schultz, Vogue, 2023). For instance, purchasers of Diane von Furstenberg's NFT fashion will enjoy exhibition access and pre-collection viewings, a physical dress, as well as an exclusive meeting with the designer herself.

Luxury brands Ralph Lauren, Dolce & Gabbana and Gucci were among the first to actively experiment in metaverse and Web3 spaces and appreciate the possibilities that exist within this technology. Since summer 2021, Ralph Lauren collaborated with one of the largest Asian social networking and NFT avatar platforms, Zepeto (Ralph Lauren, 2021). In late 2022, Gucci launched its own metaverse world and game called 'The Vault' in metaverse gaming platform, The Sandbox (Marr, Forbes, 2022). Two of the most successful brands in this new market frontier are luxury brand Dolce & Gabbana, generating a striking 5.7$ million from its NFT couture apparel collection in 2021 (Thomas, The NY Times, 2021), as well as sportswear brand Adidas, with over 30,000 digital wearable items and a trading volume of $138.6 million (Linares, Vogue Business, 2023). Adidas has collaborated with several digital native brands, including virtual avatar company Genies in 2021 and most recently, with the bespoke Bored Ape Yacht Club NFT collectibles, launching an exclusive collection of virtual hoodies that sold for $35 up to approximately $8,000 (OpenSea, 2023).

While initially viewed as a "*trillion-dollar revenue opportunity*" (Holmes, 2021) in late 2021, the metaverse has declined in popularity. Among other things, the incompatibility of its software with certain devices or programmes makes it difficult to access all of its available features and instances of technical issues, such as drop in performance of certain online games or game server lags, have further contributed to this phenomenon (Farrukh, 2023). However, this decline does not seem to particularly affect the fashion sector's activity in this virtual environment. To the contrary, despite the popularity of the metaverse declining by over 85% between October 2021 and January 2022 (Google Trends, 2023), the first metaverse Fashion Week was launched in March 2022 and the substantial attention it attracted led to its second edition in 2023 with more than 60 participating brands, both emerging and established fashion houses. In terms of participation, however, less than 50,000 users attended the virtual event, which is approximately

https://doi.org/10.54934/ijlcw.v2i3.54

half of last year's numbers (Linares, Vogue Business, 2023). Nonetheless, retailers and fashion are still actively involved with the metaverse to this day, indicating that there is still potential for revolutionising the way fashion players make profit, in this new and uncharted territory that is the metaverse, potentially extending to a more diverse consumer base.

1.1. Fashion NFTs and their diverse consumer base

A large part of the popularity of fashion NFTs is owed to the fact that their buyer is the owner of a scarce version, much like a limited-edition, of the underlying fashion design associated with it. But a fashion NFT is not just a blockchain-based certificate that can be traded as a collectible, although in various instances the value of NFTs has tremendously grown in the resale market (Lapatoura, The IPKat, 2021; McDowell, 2021). When considering fashion NFTs' associated digital wearables, they could appeal to gamers and the long-established in-game purchases of outfits, such as the so-called Fortnite 'skins', for their videogame characters. The norm with in-game items is that they are pre-determined by the developers, with limited scope for customisation. Also, they are typically at the disposal of end-users by means of a license, that allows their use within a specific online gaming environment. NFTs could revolutionise things, as their code supports interoperability and are compliant with several metaverse or gaming platforms. This means that buyers of fashion NFTs could not only have additional choice as to how they want to express themselves through their virtual avatars' attire, but also have proof of ownership of their digital wearable items, carry them across different platforms or even resell them. A promising development in this sphere comes from gaming platform The Sandbox and its announcement that thousands of popular NFT collections, including Bored Ape Yacht Club, World of Women and Cool Cats, could be played as avatars (The Sandbox, 2023). Nevertheless, while it is technically feasible for a digital wearable to be transferred to and recognised by another online game, such transfer could impact on how those assets appear and incorporating user generated content that is not part of the game could slow down its performance (Glegg, 2022). In fact, one of the key reasons for the metaverse's recent decline in popularity is the unexpected experiencing of bugs and drop in metaverse games' performance by some users, impacting on their overall experience (Farrukh, 2023).

Equally, fashion-conscious consumers, technology enthusiasts and 'Gen Z' individuals – alongside the increasing tendency of the latter to engage in virtual communications [5] – could be attracted to purchasing fashion NFTs to showcase their virtual fashion collections to others. Given their digital nature, NFT fashion items can be modified and customised using 3D modelling software without the costs of

https://doi.org/10.54934/ijlcw.v2i3.54

designing and producing physical items. This provides both designers and consumers with a unique opportunity to express their creativity and unique identities with less time-related and financial restrictions. With minimal production costs, no packaging or shipping fees, the price tag of fashion NFTs could arguably be substantially lower than their real-world counterparts, making fashion more accessible. Although it is not surprising that there are exceptions when it comes to more 'exclusive' luxury brands, where the metaverse has enabled brands to profit more than in the real world, with fashion NFTs selling for more than their 'real' value. For instance, in 2021 a tokenised Gucci handbag sold for approximately $4,500 in Roblox, while the identical physical counterpart sells for $800 less (The Fashion Law, 2021). At last, it is important to note that the popularity of digital fashion could also have a significant impact on reducing carbon emissions and waste, the by-products of producing physical fashion goods, meaning that it could also appeal to the environmental-conscious segment of fashion consumers.

2. FASHION NFTs AND UK/EU INTELLECTUAL PROPERTY LAW CHALLENGES IN THE METAVERSE

The second part of this article endeavours to shed light into the following key question: to what extent intellectual property rights vested into real-world creations can be transposed into the digital and by extension, whether the legal protection offered can be given its full effect in a digital unregulated space, where users' identities are anonymous or pseudonymous (Section 2.1.). Through the exploration of potential infringement instances in the metaverse and beyond, there comes the issue of effective legal enforcement (Section 2.2.).

2.1. Copyright and Trademark protection in the metaverse

Under the EU intellectual property regime, real-world fashion items can be protected as trademarks, designs or copyright, while it is possible to receive cumulative protection from more than one of the above-mentioned rights. In theory, brand owners and designers arguably maintain the exclusive right to exploit their works in the digital domain. Therefore, use of a tokenized digital wearable, even in the metaverse, must abide by the intellectual property rules that apply to those digital assets [4]. Nevertheless, very commonly the buyer of a fashion NFT will be granted certain limited usage rights in relation to the work associated with the NFT, by way of licensing. This does not automatically entail an assignment of any intellectual property rights vested in the said asset to the buyer, though it may be possible. Smart contracts embedded with the NFT code dictate the rights and interests that will be passed

https://doi.org/10.54934/ijlcw.v2i3.54

on upon purchase and those are pre-determined by the right holders themselves. This section will particularly focus on the UK and EU copyright and trademark regimes and the available protections to fashion NFTs.

Copyright may subsist in a fashion design the moment it becomes created and for 70 years after the designer's death, provided that the sole criterion of *originality* is satisfied (Directive 93/98/EEC, Art. 1). In other words, the fashion design would need to be the original expression of their *author's own intellectual creation*, or else, a reflection of their personality that stems from their *free and creative choices* (Infopaq, 2009; Painer, 2012). While some EU national laws (such as Portugal and Italy) stipulated those industrial designs, including fashion, needed to meet a higher threshold of originality, the CJEU has recently departed from this requirement, making it easier for fashion designs to satisfy the EU originality threshold (Derclaye, Kluwer Copyright Blog, 2019). The 2019 *Cofemel* CJEU judgment established that copyright protectable subject-matter may not necessarily possess an artistic value or aesthetic appeal, while in *Brompton Bicycles* the Court accepted the copyrightability of functional shapes, thereby opening the floodgates of protection for different types of fashion items, including clothing or accessories (Cofemel, 2019; Brompton Bicycle, 2020).

But what about subsistence of copyright in digital NFT fashion? In theory, the fashion design itself is protected, irrespective of the products, or 'vessels', it is applied to. Moreover, *Levola* has established that a copyright work "*must be expressed in a manner which makes it identifiable with sufficient precision and objectivity, even though that expression is not necessarily in permanent form*" (Levola, 2018). Therefore, fixation of the fashion design in any medium in a precise and objective way would suffice, including in digital form. The same cannot be said for UK law, which necessitates fixation of the work in a tangible medium. As such, while real-world physical tokenised fashion and its digital twin metaverse wearable could both enjoy copyright law protection under both regimes, digital-born fashion would fall outside the scope of copyright protection in the UK.

On the other hand, if we strictly focus on the copyrightability of the fashion NFT itself, rather than its associated digital design (or its copy), which is stored off-chain, things may differ. The NFT is comprised of computer code and under such circumstances, it cannot be regarded as an embodiment of the protected asset itself, unless the actual copy of the protected fashion design is stored within the same blockchain block that stores the NFT and its metadata. This is rarely the case, as popular NFT platforms, like OpenSea, operate in the Ethereum blockchain, where the larger the size of the NFT's metadata to be

https://doi.org/10.54934/ijlcw.v2i3.54

minted, the higher the chances that the minting timeframe and payable gas fees by the minter are going to increase. Incorporating a copy of the protected fashion design within the NFT would, therefore, be a costlier and more time-consuming exercise and hence, the NFT would likely only be comprised of computer code and a link pointing to the off-chain location of the asset, rather than contain the actual IP asset.

In terms of UK and EU trademark law, any signs, including words, letters, designs, prints or shapes, that are capable of distinguishing one's brand from their competitors' may be protected (Regulation 2017/1001, Art. 4; Directive 2015/2436, Art. 3; Trade Marks Act 1994 (TMA), s.1(1)). They can either be registered and protected for renewable 10-year periods, provided that they can satisfy a series of absolute and relative grounds for refusal (TMR 2017/1001, Art. 7-8(1)(a)-(b); Directive 2015/2436, Art. 4-5(1)(a)-(b), 11, 40; Directive 2008/95 Art. 4(4)(b)-(c); TMA, ss. 3, 6, 42, 43), or remain unregistered, with varying levels of protection. In terms of registrable fashion items, they need to possess distinctiveness or acquire it through successful and continuous use in the EU market. For instance, the Louboutin red sole is now protected as a position mark in the EU (Louboutin, 2018). Nevertheless, trademark protection is territorial in nature, so how can fashion designers protect their creations in the metaverse? Its borders have not been yet defined, in the sense that it is not expressed in any fixed territory other than being an online environment. And its notable popularity since the end of 2021 has resulted in countless NFT mintings, though the initial hype has gradually settled.

The landmark *Hermès v Rothschild* case from the US – involving digital 'MetaBirkin' handbags that closely imitated Hermès' 'Birkin' word mark as well as the shape mark of their iconic Birkin bags range – illustrates the complexity in brand protection in the borderless metaverse territory (*Hermès v Rothschild* (2023)). Despite the artist's counterclaims for fair use, some important factors that led the US Court to find trademark infringement, were the enormous popularity of the digital 'MetaBirkin' NFT wearables and the fact that they were selling at premium prices, between $450 – $46,000 each. In one instance, a 'Baby Birkin' NFT was auctioned for $23,500, exceeding the average $9,500 price of original Hermès 'baby' Birkins sold by the luxury fashion house [3]. Given that Hermès' had no involvement with NFTs or the metaverse at the time, the importance of the decision is substantial in this sphere, making it clear that copyists are not immune from trademark infringement liability in the metaverse. Moving forward, as in the case of Hermès, brands may be able to rely on their established reputation and argue for extended protection, beyond the Classes of goods or services for which they have secured trademark

https://doi.org/10.54934/ijlcw.v2i3.54

registrations. But would this precedent be followed in relation to all types of brands? Arguably, small emerging fashion designers and fashion SMEs would be in a flawed position nonetheless, as they could not rely to their established reputation, and especially a global reputation that Hermès enjoys for many years.

So how can brands respond to metaverse-related threats to their IP? First, brands have soon realised that they may need to expand their trademark portfolio and register for other Classes of goods and services, that cover virtual goods, including digital fashion wearables and uses in virtual environments, to strengthen their position in a potential legal dispute over use of their signs in the metaverse. Among the first fashion industry players to do so was Nike, expanding their trademark to cover "downloadable virtual goods" (Class 9), "retail store services featuring virtual goods" (Class 35), and "entertainment services, providing on-line, non-downloadable virtual footwear, clothing, […]and accessories for use in virtual environments" (Class 41) (USPTO, (2021)). The EU has followed suit, recognising that "*virtual goods are proper to Class 9 because they are treated as digital content or images*" (EUIPO, 2022). In fact, from January 1, 2023, the 12th Edition of the Nice Classification has recognised the term 'downloadable digital files authenticated by non-fungible tokens' in Class 9.

Speed is of the essence in ensuring that an extended trademark portfolio is in place, as another concern for securing trademark protection in a global, borderless metaverse environment is the increased likelihood that similar marks will be registered for virtual products and services beforehand, that could give rise to revocation claims. And the *Hermès* case illustrates that some will not lose the chance to register trademarks that resemble other's for use in the metaverse. Failing to expand a trademark portfolio in time, alongside the numerous freshly minted fashion NFTs daily, could put brands in a difficult position. Not only could they be exposed to IP legal disputes, but also find it more difficult to secure IP protection for their digital collections.

2.2. Copyright and Trademark infringement and enforcement in the metaverse

When it comes to NFT-related intellectual property infringement and enforcement, an anonymous, international, and decentralised environment is far from ideal. The ease of tokenising fashion designs and the straight-forward NFT minting process means that anyone can mint NFTs. Given the lack of any thorough user identity checks from the existing popular NFT platforms, a high volume of fraudulent minting or "copyfraud" has emerged [1]. Copyists have been presented with a window of opportunity to

https://doi.org/10.54934/ijlcw.v2i3.54

not only profit from the sale of NFTs to a global and more diverse consumer base, but also '*incur substantially less costs than those required for producing physical counterfeit goods*' [3]. This ultimately poses the risk of a new wave of digital 'counterfeit fashion'. According to popular NFT platform OpenSea, host of approximately 80 million NFT listings, "*more than 80 percent of the items created with [its free NFT minting] tool were plagiarized works, fake collections, and spam*" (OpenSea, 2022). Amongst them, protected fashion designs, such as tokenised versions of popular Cartier 'love bracelets', are being sold as NFTs on NFT platform Roblox (Roblox, 2023).

In practice, "copyfraud" refers to the instance where, other than the rightful IP owner of the token's underlying asset, a fashion NFT is created by a third party, with no interest in the work and no authorisation to use the work. The newly minted NFT may be tied to someone else's intellectual property [1] [3]. The imminent question is whether this act would qualify as IP infringement.

There are certain instances where the minting of someone's trademarked or copyright work in NFT form would be permitted. For instance, where the third party is the holder of a license or some other form of authorisation to use the work, or where the NFT falls within some of the exceptions from liability, i.e. if used for personal and non-commercial purposes. If this is not the case, the act of minting an NFT which is tied to someone else's protected trademark would likely be infringing, especially if brands have expanded their trademark portfolios to cover Classes of digital goods and uses of their marks in digital environments.

In terms of copyright infringement, it was previously discussed that the NFT is simply a digital receipt, or else a digital certificate of authenticity of the underlying asset, rather than an embodiment of the asset, as no actual copy of the work would typically be stored within the NFT's metadata. This would mean that the NFT would not violate the author's reproduction right. However, NFTs usually do contain a URL link, pointing to the off-chain location of the protected work (or its copy). In such a case, the NFT would be arguably violating the author's exclusive right of public communication, given that any online user would be able to access the blockchain and hence, access the copyright work by clicking on the URL link at any time (Bonadio and Mohnot, 2022).

In case of IP infringement, blockchain decentralisation effectively means that regulation falls on the individual NFT platform used for minting the infringing token in question. But, achieving effective IP enforcement is inherently difficult, as NFT minters maintain their anonymity and most key NFT platforms

https://doi.org/10.54934/ijlcw.v2i3.54

do not verify their users' identities. Since the ability to take legal action against unauthenticated users who mint others' protected works cannot be guaranteed, this gives copyists leeway to infringe without being held accountable for their actions and at the same time, leaves IP holders with little choice to protect their brands and very few or no legal remedies available to them. Other than policing the NFT marketplaces against infringing digital uses, designers are faced with the option of filing a 'notice-and-takedown' request to the NFT platform's complaints team, for the allegedly infringing listing to be removed from the marketplace; to disable access to the illicit content; or to disable the infringers' platform accounts (Directive 2000/31/EC, Art. 13-14; InfoSoc Directive, Art. 8(3); Directive 2004/48/EC, Art. 11; Directive (EU) 2019/790, Preamble). In terms of the latter, while disabling the online accounts of the platform users may be effective, it is only a temporary measure, as infringers can easily re-appear with a new identity and counterfeit goods listings may be back again. A proactive measure from the platforms' side to request for users' identity verification, if universally applied, could play a critical role in disincentivising infringers from signing up to NFT platforms and engaging with counterfeit sales, in fear that their revealed real-world identities could result in being held accountable for their unauthorised uses of IP protected assets, within or outside the metaverse.

Another hurdle in effective enforcement in this context is lack of timeliness. Under EU law, once platforms are notified of infringement, they are under an obligation to take action in a timely manner. But, how promptly can NFT platforms respond to a takedown request? Especially when being the recipient of numerous requests, given the plethora of newly minted NFTs daily, some of them being potentially infringing. It is possible that the infringing NFT could have been bought before the NFT platform even gets the chance to review the incoming complaints. And what if the infringing NFT has a digital 'resale royalty' embedded within its metadata? [3]. It quite possibly means that the infringer continues to profit indefinitely, or for as long as the specific 'resale royalty's' terms are.

And even in the event that the infringing NFT is delisted in time and before being purchased, the effectiveness of such a measure is questionable. Because of blockchain's immutability, the information stored within the blockchain, namely the fashion NFT code alongside the link pinpointing to the off-chain location where the infringing copy of the garment is stored, are part of the blockchain ledger. This means that, in theory, users could access the link contained within the NFT's metadata and access the infringing copy of the protected work indefinitely, provided that the link still works. Recently the CJEU has ruled, however, that online platforms may be under an obligation to remove any other content that is equivalent

https://doi.org/10.54934/ijlcw.v2i3.54

to the infringing content in question, meaning that the infringing copy located off-chain and any other related NFTs could be subject to a removal request (Glawischnig-Piesczek v Facebook, 2019).

3. CONCLUSION

The metaverse and its compilation of virtual interconnected worlds undeniably present an exciting opportunity for fashion designers to not only express their creativity in new ways and experiment with fashion in digital form, that was previously largely reserved to the gaming industry, but also attract a diverse and global consumer base, interact with their audience through virtual experiences and build their brand image. But where there is opportunity, there also lies risk. Risk for an investment that may sink, alongside the gradually decreasing popularity of the metaverse and the failure to keep its promise to users for a seamless interoperable experience, though several fashion brands are still actively engaged in this digital market space for the second year in a row. But most importantly, the serious threat posed by the metaverse's anonymity to the preservation of creators' rights and the risk of uncontrollable unauthorised minting of copyright or trademark protected fashion designs in NFT form, without the power to seek effective IP enforcement.

There is arguably a long way to go for ensuring that IP holders' rights are safeguarded. While there are certain steps that designers can take to maximise protection of their IP assets in the metaverse, their effectiveness is limited to instances where infringers identities are not hidden. Whether the metaverse is here to stay is yet to be seen. For the time being, if complete anonymity prevails, we could be witnessing an unprecedented wave of tokenised fashion fakes, that mirrors the longstanding counterfeiting phenomenon of physical 'real world' fashion.

https://doi.org/10.54934/ijlcw.v2i3.54

REFERENCES

[1] Guadamuz A. (2021b), "The treachery of images: Non-fungible tokens and copyright," Journal of Intellectual Property Law & Practice, vol. 16, no. 12 (2021), pp. 1378-1382.
[2] Idelberger F., Mezei P., "Non-fungible tokens," Internet Policy Review, vol. 11, no. 2 (2022), https://doi.org/10.14763/2022.2.1660
[3] Lapatoura I., "Fashion beyond physical space: NFTs and intellectual property challenges in the metaverse," Entertainment Law Review, vol. 33, no. 6 (2022), pp. 197-202.
[4] Mezei P., Arora G. C., "Chapter 11 - Copyright and Metaverse," in M. Cannarsa & L. A. Di Matteo (eds): "Research Handbook on Metaverse and the Law," (Edward Elgar, 2023) (forthcoming), pp. 1-3, 6, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4444608 (last visited 12.05.2023)
[5] Park S. M., Kim Y. G., "A Metaverse: Taxonomy, Components, Applications, and Open Challenges," 10 IEEE Access (2022), p. 4209

ABOUT THE AUTHOR

Ioanna Lapatoura – Ph.D. Candidate and Postgraduate Teaching Assistant in Law, University of Nottingham School of Law, Nottingham, United Kingdom and H-P Lecturer in Law, Nottingham Trent University School of Law, Nottingham, United Kingdom.
e-mail: ioannalapatoura1@gmail.com

ABOUT THIS ARTICLE

Conflict of interests: Author declares no conflicting interests.

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.37

THE IMPACTS OF THE BRAZILIAN CRYPTOASSETS LAW IN NFT SOLUTIONS

Daniel Becker
Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, Brazil

Aylton Gonçalves
Centro Universitário de Brasília (UniCEUB), Distrito Federal, Brazil

Article Information:

Received
June 13, 2023
Approved
June 13, 2023
Accepted
October 10, 2023
Published
November 30, 2023

Keywords:

NFT,
Smart Contract,
regulation,
cryptoassets,
Brazilian law

ABSTRACT

This article aims to establish the applicability of Law No. 14,478, enacted on December 21, 2022 (hereafter referred to as the Brazilian Cryptoassets Law), to the trading of non-fungible tokens (NFTs) that utilize Blockchain and Smart Contract technologies. The article covers (i) the use of Smart Contracts and Blockchain in relation to NFTs, (ii) the current state-of-the-art NFT solutions, and (iii) the key articles and legal obligations outlined in the Brazilian Cryptoassets Law. It's important to note that the Brazilian Cryptoassets Law applies differently to various NFT solutions depending on their intended use, which is the distinguishing factor in determining whether the law is applicable to a particular NFT transaction.

FOR CITATION:

Becker, D., & Gonçalves, A. (2023). The impacts of the Brazilian Cryptoassets Law in NFT solutions. International Journal of Law in Changing World, Special Issue NFTs, 153-170. DOI: https://doi.org/10.54934/ijlcw.v2i3.37

1. INTRODUCTION

Throughout history, people have collected a wide range of items, from old coins and baseball cards to watches and other valuable objects. In the digital age, this tradition continues, with people seeking out exclusive and unique items in what is often called the Internet of Value Era. One significant difference between NFT trading and the physical selling of items like baseball cards is that NFT trading is conducted entirely online and without the need for a trusted third party. NFT solutions are known for their unique and exclusive qualities, which have generated significant interest since 2021.

As with traditional cryptoasset trading, NFT exchanges require a way to ensure the validity of transactions, and this is achieved through Blockchain technology, which provides auditability and traceability. Most NFT solutions also rely on Smart Contracts, a technology that enables order-sensitive executions. It's important to note that not all NFTs are considered cryptoassets under the Brazilian Cryptoassets Law, as will be explained further in this paper. This distinction is critical in delimiting consumer rights in NFT transactions within the Brazilian jurisdiction. To establish the applicability of the Brazilian Cryptoassets Law to NFTs, this paper will explore the most important use cases for NFTs and shed light on the regulation of these assets.

2. SMART CONTRACTS

Since most NFT solutions rely on the technologies of Blockchain and Smart Contracts, it's essential to analyze these technologies to investigate the usage of NFTs and their treatment under the Brazilian Cryptoassets Law. The term "Smart Contract" was coined by Nick Szabo in 1996, who described it as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." In simpler terms, a Smart Contract is a program that automatically executes based on digital input. Szabo envisioned that Smart Contracts could translate the terms of an agreement into code, making it self-executing and minimizing the cost of contracting between transacting parties. The main idea behind a Smart Contract is that a clause is executed automatically when predefined conditions are met. In contrast, traditional arrangements require centralized completion by a trusted third party, adding to the implementation time and cost [27]. To explain the entire cycle of a Smart Contract, it can be divided into four steps, which are:

https://doi.org/10.54934/ijlcw.v2i3.37

(1) Creation. The creation of a Smart Contract, much like a traditional contract, involves defining prohibitions, obligations, and rights. These terms are then translated by software engineers into a computer language with auto-execution triggers. For instance, in NFT solutions, when an individual transfers their cryptoassets to NFT ownership, the ownership of the NFT changes automatically [9].

(2) Deployment. Typically, this step is carried out on a Blockchain. When a Smart Contract is stored on a Blockchain, it cannot be altered due to the immutability characteristic, as further explained in the next section. If changes need to be made to the Smart Contract, a new contract must be created. In the context of NFTs, the deployment step is triggered when cryptoassets are blocked to ensure payment for the acquisition of the NFT [4].

(3) Execution. The execution step involves fulfilling the conditions set out in the Smart Contract. Once the contractual terms are met (such as the transfer of the required sum of cryptoassets to pay for an NFT), the contractual procedures are automatically executed, and the payee receives their NFT [22].

(4) Completion. The completion step of the Smart Contract cycle involves updating the states. For instance, in the case of NFT solutions, the completion step confirms that the ownership of an NFT has been transferred to a new party.

The rational construction exposed in this paper, such as the above steps division, is grounded on very specific literature on Smart Contracts. In this sense, it is important to highlight some recent studies about this theme, such as (i) the presentation of comprehensive surveys regarding Blockchain and Smart Contracts [28]; (ii) the survey of the vulnerabilities on Ethereum Smart Contracts programming [18]; (iii) the survey about the verification methods of Smart Contracts languages [7]; (iv) the report of teaching Smart Contracts programming and students mistakes [12]; (v) the empirical study regarding Smart Contracts [16].

3. BLOCKCHAIN

Ten years after the early stages of the Smart Contracts idealization, in 2008, Satoshi Nakamoto, a pseudonym, publicized the paper *Bitcoin: a peer-to-peer cash system*, introducing the cryptoasset Bitcoin and the new technology that would make possible transactions with this *new money*: the Blockchain, a term that was not mentioned in Satoshi's paper but is widely used in the crypto market.

https://doi.org/10.54934/ijlcw.v2i3.37

The technology presented by Satoshi called Blockchain is capable of preventing historical problems in the development of a new type of currency apart from Central Banks: the double-spending and the Byzantine fault.

The double-spending problem arises from the need to establish clear ownership of a cryptoasset and its transfer. For example, if person A sends an e-mail to person B with a document attached, this document does not disappear from person's A computer. However, in financial transactions, double-spending cannot occur. If person A send ten dollars to person B by a banking transaction, person A will lose these ten dollars. The same that happens with dollars needs to occur with cryptoassets transactions [17].

The Byzantine fault has a connection with the decentralization of the validation of a transaction. Once Bitcoin and the cryptoassets were created based on decentralization, they are exchanged without a trusted third party, such as a bank, and the validation of the transaction is executed by several decentralized computers. In spite of this decentralization, the decision regarding the validation of the transaction needs to be convergent. It refers to a situation where a group of people or computers need to make a decision together, but some members of the group may be giving out false information or trying to sabotage the decision-making process. It is like a group of friends trying to decide on a restaurant to eat at, but some members of the group are secretly working for a competing restaurant and are trying to sway the decision in their favor. This is the Byzantine problem. In simple words, the problem is to converge a decentralized system [15].

The technology of Blockchain deals with these two problems and solve them via a Proof-of-Work (PoW) system — a species of competition among computers in a decentralized system in order to find a solution to a complex equation by CPU power.

Blockchain, as a decentralized ledger technology, has some determined characteristics, such as (i) immutability, (ii) transparency; (iii) permanency, and (iv) security [21] [1].

It is essential to indicate, in this part of this paper, that there is not just one Blockchain. Satoshi's creation was the Bitcoin system, but there are other Blockchains applicable to other types of transactions. For instance, as mentioned, the NFT solutions are based on Ethereum Blockchains, as we will discuss henceforward. There are public and permissioned Blockchain based on its openness. In this sense, Bitcoin

https://doi.org/10.54934/ijlcw.v2i3.37

and Ethereum are public Blockchains— everyone can read, write, and mine depending on CPU power (in the case of PoW).

A public Blockchain, as commonly used on NFT solutions, has four advantages defended by the specialized works of literature in comparison with permissioned Blockchain [11]:

a) **Transparency.** All nodes (computers) involved in the Blockchain have access to all to transactions carried out.

b) **Information preservation.** As the Public Blockchain is decentralized, it is challenging to destroy the information maintained in each node.

c) **Tamper-resistance**. Because each transaction's validity depends on the validation of the preceding transaction, it becomes increasingly difficult, and eventually almost impossible, to tamper with a public blockchain as the number of transactions grows.

d) **High fraud cost**. The costs associated with PoW, particularly in terms of CPU power, make fraudulent activities economically unviable, making it an unwise decision to attempt to defraud the system.

Furthermore, it is important to note that Smart Contracts and Blockchain are not the same technology: a Blockchain can operate without Smart Contracts, and, maybe more importantly, Smart Contracts do not need a Blockchain in order to function. However, there is a common thread among these technologies, namely Ethereum, the network where almost all NFTs are created on a daily basis.

4. THE POINT OF CONNECTION – ETHEREUM

Smart contracts on a Blockchain are strongly connected to the history of Ethereum. Back in 2011 or 2012, a few years after Satoshi's famous publication, several new cryptoassets were presented, reportedly trying to correct some flaw in the Bitcoin system. In 2013, Vitalik Buterin, a seventeen-year-old boy looking at the potential of smart contracts, released a white paper where he proposed a new Blockchain called Ethereum [3].

https://doi.org/10.54934/ijlcw.v2i3.37

The Ethereum Blockchain has supported Smart Contracts as a priority. Buterin does not focus his Blockchain on a cryptocurrency, besides his creation of the cryptocurrency Ether, but on several types of decentralized applications, such as the NFT solutions. This network is the Ethereum Virtual Machine (EVM).

In the Ethereum system, all NFT solutions are based on Blockchain and Smart Contracts. The details of most NFT are determined by a technical standard, the ERC-721 (ERC-721 Non-Fungible Token Standard, 2018). This document establishes the required metadata of the NFT and the executable functions needed in the NFT Smart Contracts used on Ethereum.

5. NFT

From the beginning, NFT emerged from the gaming community [24] and the visual arts. As mentioned in this paper, NFTs are blockchain-based assets and represent ownership of exclusive items [29].

NFT has some important differences compared with traditional cryptoassets such as Ether [25]. Ether is a standard asset where all units are equivalent and indistinguishable from one another. In other words, one Ether is never more valuable than another Ether. On the other hand, NFTs are unique and non-interchangeable, possessing a non-fungible characteristic. By utilizing NFTs in smart contracts, the creator of the NFT can easily demonstrate the existence of digital assets such as images, videos, and even event tickets.

Moreover, the inventor, utilizing Blockchain and Smart Contracts, may earn a fee for the success of this creation in the market. Outstandingly in the entrepreneurship area, NFT is appointed as one of the most prominent disruptive technologies by researchers.

By introducing the idea of digital scarcity, NFTs are able to expand the use cases of blockchain technology, particularly by providing a new form of ownership that adds significant value to digital assets [5].

NFT solutions are a type of decentralized application [3], and, as such, they offer the benefits discussed in the previous section, particularly in terms of Public Blockchains. The chart below summarises the most important proprieties of NFT.

https://doi.org/10.54934/ijlcw.v2i3.37

NFT characteristic	Details
Verifiability	The proof of ownership of an NFT resides in a Public Blockchain, allowing everyone to check all information about it.
Transparent Execution	Once the NFT is traded by a Public Blockchain, the activities, including purchasing and selling, are always accessible.
Availability	The system that allows one to buy or sell an NFT operates 24/7, with no interruptions.
Tamper-resistance	The use of public blockchains in NFT solutions provides a high degree of security and transparency, making it more difficult for fraudulent activity to occur.
Usability	The trading of NFT solutions is generally very user-friendly in comparison with others cryptoassets transactions.

The scope and purposes of NFTs are now extremely varied [8] [2]. However, it is possible to indicate categories of NFT solutions that are more widespread than others.

a) **Games.** NFT has its origins in gaming enthusiasts. For instance, there are crypto games such as CrytpoKitties and Axie Infinity using this kind of asset. A very interesting mechanism in this games is called "breeding". The users are able to raise and spend much time breeding new offspring. As well, the users can be able to buy a rare virtual pet and sell it for a high price. Another important function of NFT is to create a history of the usage of a game item as a skin. The ownership history of an NFT has the potential to increase its value, making it a potentially lucrative investment.

https://doi.org/10.54934/ijlcw.v2i3.37

b) Virtual Events. Generally, events depend on a trusted third party. In these situations, there is a possibility of, for instance, buying fraudulent event tickets, which will be canceled, causing real concerns for the owner. "NFT-based ticket" represents an event ticket in a Blockchain and is able to ensure access to a culture or sports event, for example. Once the NFT-based ticket is exclusive, there is no possibility of the ticket buyer resell the ticket after it is sold.

c) Digital Collectibles. Digital collectibles are the foundation of the entire NFT concept. Some examples of NFT solutions in digital collectibles are (i) historical moments images; (ii) virtual videos; (iii) trading cards; and even (iv) wines.

d) Metaverse. Metaverse is a term used to describe a collective virtual shared space, typically created using advanced technologies like virtual reality (VR) and augmented reality (AR). It is a hypothetical concept that describes a fully immersive and interactive digital universe where people can interact with each other and with digital objects and environments in a seamless way. The NFT solutions could be implemented and traded in the metaverse in many ways, such as to furnish a metaverse home or to give a unique skin to an avatar.

e) Music Industry. The principal function of NFT solutions in the music industry is to ensure intellectual property. This usage is able to minimize litigation about this theme — something frequent in this market.

f) Art Industry. NFT solutions are able to increase the value of an asset, ensuring its exclusivity, scarcity, and uniqueness. In this manner, NFT creates a new spectrum of possibilities for artists. Historically, the usage of NFT solutions represents a total paradigm change in the art industry.

g) Loyalty Points and Rewards. In order to incentivize and foster the consumption of their products, companies are issuing NFTs that can be redeemed for discounts and other special buying conditions. The unique feeling provided by owning an NFT can incentivize higher quantities and more expensive purchases.

These characteristics and usages of NFT solutions are determined by the specialized literature. There are notable studies regarding the NFT area, such as the (i) research of land pricing in Decentraland

https://doi.org/10.54934/ijlcw.v2i3.37

[30] [8], (ii) research of a structural model of valuation for CryptoKitties [13]; (iii) research of the CryptoPunks, a popular NFT collection, using hedonic models [14]; research regarding fan tokens [23]; (v) research of the data from all of the NFT transactions on OpenSea up to 2021 [19]; (vi) research about how NFT will transform the way businesses operate and is already reaching a disruptive impact in markets such as sports, escrow, law, digital collectibles, crypto, and gaming and it has the inherent force to extend to real state, financial markets, and the entire digital world in the future [6]; (vii) research that argues that while NFT has the force to support several new ways of digital ownership and creative sponsorship, the market activity has so far been dominated by speculative transactions. If it cannot be further improved and corrected, it faces the risk of failure [5]; and (vii) research regarding the art sector, which is very important to NFT solutions, which has found that the emerge of NFT has strongly changed the resale market [31].

6. BRAZILIAN CRYPTOASSETS LAW

Since 2015, with the presentation of a bill on the subject in the Brazilian National Congress, the regulation of cryptoassets has been considerably discussed in the Brazilian jurisdiction. Some of the biggest concerns expressed by lawmakers were (i) money laundering; (ii) money smuggling; and (iii) consumer rights violations through the usage of cryptoassets.

Issues related to money laundering with cryptoassets are part of an intense international agenda oriented by FATF. In June 2013 and June 2015, respectively, the organization published the first Risk-Based Approach (RBA) guidelines applicable to the crypto asset market, namely: (i) Guidance for a Risk-Based Approach - Prepaid Cards, Mobile Payments, and Internet-Based Payment Services, and (ii) Guidance for a Risk-Based Approach - Virtual Currencies. At that time, FATF pointed out the importance of economic agents paying attention to the possibility that cryptoassets could serve illicit practices.

In October 2018, FATF released a statement called Regulation of virtual assets, which addressed updates to its Recommendations and Glossary. Additionally, on June 30, 2022, the intergovernmental organization published the document Targeted Update on Implementation of FATF's Standards on VAs and VASPs, which deals with the implementation of FATF's Recommendations related to cryptoassets in various jurisdictions around the world, based on the FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers - a guide published in 2019 and updated in 2021.

https://doi.org/10.54934/ijlcw.v2i3.37

More recently, in November 2022, the bankruptcy of FTX, one of the largest exchanges in the world, caught the attention of Brazilian lawmakers, who expedited the approval of the Brazilian Cryptoassets Law.

Brazilian Cryptoassets Law establishes fundamental concepts regarding the legal framework applicable to NFT solutions in the Brazilian jurisdiction.

Firstly, it is necessary to note that the Brazilian Cryptoasset Law does not use the term *cryptoasset*. In fact, the law determines what is (i) a *virtual asset* and (ii) a *virtual asset service provider*, which is aligned with the Recommendations and Guidelines of the Financial Action Task Force (FATF), the global money laundering and terrorist financing prevention watchdog.

However, the definition of virtual assets utilized by the Brazilian Cryptoasset Law is similar to the cryptoasset definition. In a recent paper published by the Financial Stability Board called Regulation, Supervision, and Oversight of "Global Stablecoin" Arrangements for Innovation, cryptoassets are defined as "a type of private digital asset that depends primarily on cryptography and distributed ledger or similar technology" [10].

Indeed, in documents issued by the most important authorities on financial regulation and supervision, such as the Bank For Internacional Settlements, the term cryptoasset is elected instead of virtual asset. The term cryptoasset can express one of the most common connection points between assets like Bitcoin, Ether, and NFTs: the usage of cryptography.

Under the terms of the Article 3 of the Brazilian Cryptoassets Law, virtual assets are digital representations of value that can be traded or transferred via electronic means and used for making payments or investments, except for (i) Brazilian and foreign currencies; (ii) electronic currency, under the terms of Law No. 12,865 of October 9, 2013 — the electronic representation of the Brazilian currency; (iii) instruments that provide their holders with access to specific products or services or any benefits thereof, such as loyalty program points and rewards; and (iv) representations of assets whose issuance, recording, negotiation, or liquidation is provided for in laws or regulations, such as securities or financial assets.

Throughout this definition, made via exclusion, it is possible to point out the first assumption about the applicability of the Brazilian Cryptoasset Law on NFT matters: if an NFT only provides access to

https://doi.org/10.54934/ijlcw.v2i3.37

specific products or services, or any benefits associated with them, without a purpose of investment or making payments, it will not be considered a cryptoasset (or a virtual asset).

This hypothesis is not the most common on NFT solutions. As previously mentioned in this paper, NFT solutions are generally open to token ownership transfer through negotiation , including with the purpose of investment.

On the other hand, there are examples of NFT solutions that are focused on granting benefits. For instance, consider an NFT solution for a book, where ownership of the NFT grants the owner access to a special version of the book. However, the NFT does not allow the owner to sell it to someone else. In this specific case, there is no usage as an investment or payment purpose of the NFT solutions, so it will not be classified as a cryptoasset (virtual asset) by the Brazilian Cryptoassets Law.

Another vital concept in the Brazilian Cryptoassets Law is related to the *virtual asset service provider*, the companies that deal with cryptoassets. Thus, Article 5 of the Brazilian Cryptoassets establishes that a virtual assets service provider is defined as a legal entity that performs at least one of the following virtual asset services on behalf of third parties: (i) exchanges of virtual assets and Brazilian or foreign currency; (ii) exchanges of one or more virtual assets; (iii) virtual assets transfers; (iv) custody or administration of virtual assets, or instruments that allow control over virtual assets; or (v) financial services and services related to the offer of virtual assets by an issuer or the disposal of virtual assets.

Considering the text of the Brazilian Cryptoasset Law, there is a second assumption regarding NFT solutions: taking into consideration the chance that an NFT does not fit in the cryptoasset (or virtual asset) definition, it is possible that a legal entity provider of NFT solutions is not considered a virtual asset service provider, pursuant to the law

Notwithstanding, as mentioned, the most common NFT solutions are based on the possibility of free negotiation and, consequently, usage as an investment or a way of making payments. For instance, it is possible to offer an NFT for an NBA video that gains value depending on the performance of the basketball player. In this scenario, the legal entity that deals with NFT solutions will be considered a virtual asset provider under the terms of Article 5 of the Brazilian Cryptoasset Law.

https://doi.org/10.54934/ijlcw.v2i3.37

The difference between NFT solutions that are considered cryptoassets (or virtual assets) and those that are not, which focuses on the usage of the asset as an investment or payment method, is essential mainly because of the legal treatment by legal entities.

In fact, there are three items of concern for legal entities that are considered virtual asset providers: (i) they will be regulated by the Central Bank of Brazil and will face a degree of regulatory requirements similar to those applied to Brazilian financial institutions; (ii) they will need to submit an authorization request and provide information on risk assessment parameters and market knowledge; and (iii) they will have a legal obligation to report suspicious activities related to money laundering to the Brazilian Financial Intelligence Unit (COAF). However, these legal entities will not be subject to some of the legal obligations of the Brazilian Consumer Defense Code due to the material impossibility of compliance, as expressed in Article 13 of the Brazilian Cryptoasset Law.

For example, the Brazilian Consumer Defense Code states in its Article 49 that consumers have the right to cancel a contract within seven days of signing or receiving a product or service if it was contracted outside of a commercial establishment, such as through a phone call or house visit (referred to as the "right of regret"). However, if an NFT solution is used as an investment, this right cannot be guaranteed due to the inevitable price volatility of the asset.

The virtual asset service provider also needs to ensure that their services are compliant with the following principles : (i) free enterprise and free competition; (ii) good governance practices, transparent operations, and a risk-based approach; (iii) information security and personal data protection; (iv) consumer and user protection; (v) the protection of popular savings and investments; (vi) efficient transactions; and (vii) the prevention of money laundering, terrorism financing and the proliferation of weapons of mass destruction, aligned with international standards.

https://doi.org/10.54934/ijlcw.v2i3.37

In order to summarize what was explained in this topic, it is possible to utilize the chart below.

Legal Obligation	**Legal entity provider of NFT solution classified as a cryptoasset (investment or payment purpose)**	**Legal entity provider of NFT solution not classified as a cryptoasset**
Submitting a prior authorization request in order to function (Article 2 from the Brazilian Cryptoasset Law)	Shall comply with the law	Shall not comply with the law
Complying with the Central Bank of Brazil Regulation (Article 7 from the Brazilian Cryptoassets Law)	Shall comply with the law	Shall not comply with the law
Following principles of virtual assets services (Article 4 from the Brazilian Cryptoassets Law)	Shall comply with the law	Shall not comply with the law
Ensuring the right of regret (Article 49 from the Brazilian Defence Consumer Code)	Shall not comply with the law	Shall comply with the law

7. CONCLUSIONS

The first objective of this research was to provide an overview of the technology involving NFT, notably Smart Contracts, Blockchain, and Ethereum.

Thus, it can be noted that Smart Contracts, whose concept was created in 1996, focus on creating a kind of contract that has self-executing clauses. An operation by a Smart Contract, such as that of an NFT solution, has a high level of security since, once the condition established in the contract is achieved, the predetermined activity will be executed. In the case of NFT, which is usually transacted via

https://doi.org/10.54934/ijlcw.v2i3.37

cryptocurrencies, the Smart Contract allows a certain amount of cryptocurrency in a wallet to be locked to ensure payment of the amount required to obtain ownership of the NFT.

Still, in an effort to solidly understand the NFT solution, we proceed to discuss Blockchain technology. One relevant point highlighted by the research was that, although related, Blockchain technology and Smart Contracts are different and independent.

The development of Blockchain dates back, as we studied, to the year 2008 and the Bitcoin project coined by the pseudonym Satoshi Nakamoto. Blockchain technology deals with two important problems for the security of transactions involving NFT solutions, which are the double-spending problem and the Byzantine problem. Other attempts to establish new currencies outside the state failed to overcome these issues.

At the end of this cognitive foundation construction for the study of NFT and its regulation in the Brazilian jurisdiction, we understand that the Ethereum system is responsible for connecting Blockchain and Smart Contracts technologies as we know them. In 2013, Buterin significantly expanded the scope of the project presented by Satoshi Nakamoto by including not only forms of money but also other assets, such as NFTs, that could be transacted on a Blockchain.

In a specific study of NFT solutions, we extracted the necessary understanding of the benefits involved in these tokens. It was also possible to gain clarity on the various use cases involving NFT, demonstrating that, in many cases, NFT can be used as an investment or payment method.

Understanding the most common ways of using NFT solutions enabled us, in the last chapter of this paper, to clarify the incidence of the Brazilian Cryptoassets Law on these assets. It was observed that NFT solutions could be considered cryptoassets (or virtual assets). When NFT solutions are used as an investment or payment method, their value can appreciate or depreciate, as with a token representing an NBA video based on the player's performance.

The understanding that NFT solutions may be cryptoassets for the purposes of the Brazilian Cryptoassets Law assisted in the main purpose of this work: to evaluate the impacts of the law on NFT solutions in the Brazilian jurisdiction.

https://doi.org/10.54934/ijlcw.v2i3.37

Therefore, it was found that if a legal entity is considered a virtual asset service provider - for example, conducting operations with certain NFT solutions - it will need to observe a series of precautions, specifically the need to (i) submit a prior authorization request; (ii) comply with general rules issued by the Central Bank of Brazil, (iii) observe principles for the provision of services involving virtual assets.

For companies that operate in the Brazilian jurisdiction with NFT solutions but do not fit the virtual asset service provider profile, attention must be paid to consumer rights, notably the right of regret. In cases where NFT solutions are not cryptocurrencies, without the natural possibility of volatility, the exercise of the right of regret may be demanded by the consumer.

The categorization of NFT solutions as cryptoassets, given their complexity, must always be made based on the specific case, evaluating the specifics of the business model presented.

REFERENCES

[1] Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open Blockchain*. O'Reilly Media, Inc.: Sebastopol, CA.

[2] Bao, H., & Roubaud, D. (2022). Recent Development in Fintech: Non-Fungible Token. *FinTech*, 1(1), 44–46.

[3] Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. 36p. Available at: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

[4] Sillaber, B., & Waltl, B. (2017). Life cycle of smart contracts in blockchain ecosystems, *Datenschutz Datensicherheit* – DuD, 41(8), 497–500.

[5] Chalmers, D., Fisch, C., Matthews, R., Quinn, W., & Recker, J. (2022). Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? *Journal of Business Venturing Insights,* 17, e00309.

[6] Chohan, R., & Paschen, J. (2021). What marketers need to know about non-fungible tokens (NFTs). *Business Horizons*, 66(1), 43-50.

https://doi.org/10.54934/ijlcw.v2i3.37

[7] Harz, D. & Knottenbelt, W. (2018). *Towards safer smart contracts: A survey of languages and verification methods*. arXiv preprint arXiv:1809.09805. Available at: https://arxiv.org/pdf/1809.09805.pdf

[8] Dowling, Michael (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, 44, 102097.

[9] Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). Evaluation of logic-based smart contracts for blockchain systems, in: *International Symposium on Rules and Rule Markup Languages for the Semantic Web*, RuleML, Springer, 167–183.

[10] FSB (2020). *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations*, October.

[11] Iansiti, M., & Lakhani, K. R. (2017). The truth about Blockchain. *Harvard Business Review*, 95(1), 118–127.

[12] Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, in: *Proceedings of International Conference on Financial Cryptography and Data Security*, 79–94.

[13] Kireyev, P., & Lin, R. (2021). *Infinite but Rare: Valuation and Pricing in Marketplaces for Blockchain-Based Non-fungible Tokens*. INSEAD Working Paper No. 2021/60/MKT. Available at: https://flora.insead.edu/fichiersti_wp/inseadwp2021/2021-60.pdf

[14] Kong, D-R., & Lin, T-C. (2021). Alternative investments in the Fintech era: The risk and return of Non-Fungible Token (NFT). Available at: https://acfr.aut.ac.nz/__data/assets/pdf_file/0010/690409/Draft-20220829-NFTs.pdf.

[15] Lamport, L., Shostak, R., & Pease, M. (2019). The byzantine generals problem. In: *Concurrency: the Works of Leslie Lamport*, 203–226.

[16] Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns, in: *International Conference on Financial Cryptography and Data Security*, Springer, 494–509.

[17] Musan, D. I., Knottenbelt, W. J., & Gervais, A. (2020). *NFT.Finance Leveraging Non-Fungible Tokens*. Meng Individual Project. Imperial College London: London.

[18] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smartcontracts (SoK), in: *Proceedings of International Conference on Principles of Security and Trust*, 164–186.

https://doi.org/10.54934/ijlcw.v2i3.37

[19] Nadini, M., Alessandretti, L., Di Giacinto, Martino, F. M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the NFT revolution: market trends, trade networks and visual features. *Scientific Reports*, 11(1), 20902.

[20] Satoshi, N. (2008). *Bitcoin: A Peer-to-Peer Eletronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf

[21] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press, Princeton, NJ.

[22] Koulu, R. (2016), Blockchains and online dispute resolution: smart contracts as an alternative to enforcement. *SCRIPTed*, 13(1).

[23] Scharnowski, M., Scharnowski, S., & Zimmermann, L. (2021). Fan Tokens: Sports and Speculation on the Blockchain. *Journal of International Financial Markets, Institutions and Money*, 101800.

[24] Serada, A., Sihvonen, T., & Harviainen, J. T. (2021). CryptoKitties and the New Ludic Economy: How Blockchain Introduces Value, Ownership, and Scarcity in Digital Gaming. *Games and Culture*, 16(4), 457–480. https://doi.org/10.1177/1555412019898305.

[25] Shirole, M., Darisi, M., & Bhirud, S. (2020). Cryptocurrency token: An overview. *IC-BCT 2019*, 133–140.

[26] Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, (16) 18(2).

[27] Wood, G. (2023). Ethereum: A secure decentralised generalised transaction ledger. Berlin Version. *Ethereum project yellow paper*, 1–32. Available at: https://ethereum.github.io/yellowpaper/paper.pdf

[28] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends, in: *2017 IEEE International Congress on Big Data, BigData Congress*, IEEE,557–564.

[29] Franceschet, M. (2021). HITS hits art. *Blockchain: Research and Applications*, 2(4), 100038.

[30] Goldberg, M., Kugler, P., & Schär, F. (2021). *Land Valuation in the Metaverse: Location Matters*. Available at: https://dx.doi.org/10.2139/ssrn.3932189

[31] van Haaften-Schick, L., & Whitaker, A. (2022). From the Artist's Contract to the blockchain ledger: New forms of artists' funding using equity and resale royalties. *Journal of Cultural Economics*, *46*(2), 287-315.

ABOUT THE AUTHORS

Daniel Becker Paes Barreto Pinto
Lawyer at BBL Advogados, student at Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, RJ, Brazil
e-mail: daniel.becker@bbladv.com.br
ORCID ID: https://orcid.org/0009-0007-3486-9061

Aylton Gonçalves Junior
Lawyer at Opice Blum (Opice Blum, Bruno Advogados Associados), student at Centro Universitário de Brasília (UniCEUB), Brasília, DF, Brazil
e-mail: aylton.goncalves@bbladv.com.br
ORCID ID: https://orcid.org/0009-0007-4879-0805

ABOUT THIS ARTICLE

Conflict of interests: Authors declare no conflicting interests.

https://doi.org/10.54934/ijlcw.v2i3.37

International Journal of Law in Changing World

Special Issue: NFTs and the Legal Landscape (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i3.55

NON-FUNGIBLE TOKENS:
AN ARGUMENT FOR THE OWNERSHIP OF DIGITAL PROPERTY?

Matteo Alessandro
MK Fintech Partners, Birkirkara, Malta

Article Information:

Received
July 19, 2023
Approved
July 29, 2023
Accepted
October 3, 2023
Published
November 30, 2023

Keywords:

digital property,
digital ownership,
digital assets,
non-fungible tokens,
blockchain technology

ABSTRACT

The paper examines the concept of ownership and its potential application to digital assets, particularly Non-Fungible Tokens (**"NFTs"**). Technological advancements which allow the creation, storage, and sale of unique digital assets in a purely digital manner have raised many questions about the concept of 'digital ownership'. However, the legal frameworks regulating the ownership, sale, and legal classification of digital assets have not evolved at the same pace as technology. This leads to legal uncertainty in the digital landscape, and weakened protection for the users of this technology, particularly in the European Union (**"EU"**). Although the concept of digital property has been discussed theoretically, practical recommendations for the implementation of this concept are still scarce. This paper discusses the concept of digital property after providing a contextual understanding of NFTs and the technology behind them. Finally, the author offers recommendations for a harmonised EU-level framework for the legal classification of NFTs, and for the concept of digital property.

FOR CITATION:

Alessandro, M. (2023). Non-Fungible Tokens: An Argument for the Ownership of Digital Property? International Journal of Law in Changing World, Special Issue NFTs, 171-201. DOI: https://doi.org/10.54934/ijlcw.v2i3.55

1. INTRODUCTION

The blockchain cannot be described just as a revolution. It is a tsunami-like phenomenon, slowly advancing and gradually enveloping everything along its way by the force of its progression.

—William Mougayar

Although many in this fast-emerging industry wax lyrical about the mathematical, trust-based system which needs no regulation, the stark reality is, as Aristotle pointed out many years ago – "law is order, and good law is good order." Technological advancements have fast out-paced the law, with many scholars advocating for the implementation of future-proof, technologically neutral regulation. The law has regulated what we can own, and what we can do with it since its very inception. However, blockchain technology now provides opportunities and challenges which jurists of the past could not even begin to imagine. Regulating for the digital age requires a delicate balance of knowledge of the law, as well as of the technologies which it seeks to regulate. Understanding both these fields will ensure that the law simultaneously regulates technology, while ensuring that technological innovation is not stifled by unnecessary bureaucratic and regulatory burdens.

The purpose of the paper is to analyse the concepts of digital ownership, and how it is currently being approached in a number of jurisdictions. The paper shall particularly focus on non-fungible tokens (**"NFTs"**), a recently developed technology which allows for the creation of unique digital assets – something which was not possible before. Although arguments have been made for the development of this concept, and frameworks have been created on national levels, no practical recommendations have yet been made for the development of a European Union (**"EU"**) level framework. Furthermore, by analysing the legal classification of NFTs under different legislations, the paper aims to provide recommendations for a framework which will harmonise the classification of such digital assets under EU law.

The paper shall first provide a contextual understanding of NFTs and their use-cases. The second part of the paper will provide a wide-ranging comparative legal analysis of the legal classification of NFTs, as well as the approaches taken to digital assets and digital property across a number of jurisdictions – with a focus on Liechtenstein and the United Kingdom (**"UK"**). The third section of the paper shall also examine the traditional concept of ownership and possession, as well as the arguments for and against the

https://doi.org/10.54934/ijlcw.v2i3.55

development of the legal concept of digital ownership, then applying these concepts to NFTs. In the fourth section, the paper will utilise the findings of the comparative analysis to develop recommendations for an EU level framework for the legal classification of NFTs, and for the development of the legal concept of digital ownership.

This paper is not intended to provide the final solution for the issues being examined, but rather, it is aimed to be the basis of further discussion and analysis. However, through analysing the current legal landscape and considering different possible approaches, the paper aims to provide practical and applicable solutions, rather than purely theoretical arguments.

2. UNDERSTANDING NFTS

2.1 Non-Fungible Tokens and their rise to popularity

Although NFTs have been around since 2014, their recent meteoric rise to popularity has been well-documented in the nascent pool of literature about NFTs [5] [30]. People who are not well-versed with the technology behind NFTs are likely to know them simply as art collectibles and tend to be sceptical of the concept. CryptoPunks and CryptoKitties were two of the first projects to gain widespread popularity between 2017 and 2018 (EUBOF, 2021). Although NFTs did not immediately gain mainstream popularity, in the third quarter of 2021, the NFT market exploded with sales amounting up to 10.7 billion USD, compared to 1.2 billion USD in the first quarter of the same year, and 28 million USD in the third quarter of 2020 (Howcroft, 2021). These statistics clearly demonstrate the ever-increasing popularity of the NFT market, highlighting the stark necessity for an adequate regulatory framework.

However, it is clear that many scholars, particularly those who do not have a technological background, struggle to understand what an NFT truly is. Some have described NFTs as a smart contract [18] [28], while others have held that they are always tied to "real-world objects" (Dalai, 2022). Both of these assertions fail to understand what an NFT actually is. NFTs are, in and of themselves digital assets, or tokens which can be proven to be unique, and are not fungible (EUBOF, 2021). The common *acquis* in literature is that NFTs are a type of crypto-token, which are different from other 'traditional' crypto-assets as a result of their non-fungibility [5] [7] [23] [12]. Before this, the concept of uniqueness was limited to physical objects, since digital objects could be easily replicated without any provenance.

https://doi.org/10.54934/ijlcw.v2i3.55

The NFT itself is a token which usually points to a metadata file which contains information about the digital asset, most importantly the tokenID and contract address. The file itself does not usually contain the underlying asset (in the case of digital assets), but rather a link to it [17]. The NFT itself is 'minted' (or created) using a smart contract, which then registers it as a digital ledger entry on a particular blockchain, and it is stored in the respective cryptographic wallet [32].

2.2 The characteristics of NFTs

Due to the variety of use-cases for NFTs which shall be discussed in the subsequent heading, it is often difficult for legal scholars, as well as laypersons to understand what the NFT actually represents. Broad questions such as "Are NFTs securities?" are often put forward when analysing the legal classification of NFTs. Although this may seem to be a fair question, it makes just as much sense as asking if a piece of paper is a security, simply because of its ability to be used as such. The majority of literature has been focused on attempts to classify NFTs within existing legal definitions, mostly to understand the legal implications under current regimes of applicable law (Moritz et al., 2022). Instead of adopting this approach, the characteristics of NFTs will be examined, to be able to understand the tokens, and what differentiates them from other forms of digital assets. This approach will allow the paper to develop a technologically neutral classification, rather than one which is based on pre-existing concepts.

Two main sources were used when analysing the characteristics of NFTs, namely a report by the EU Blockchain Observatory and Forum (**"EUBOF"**) (2021), and a journal article by blockchain expert Popescu (2021). The study has focused on these sources because of the thorough understanding of blockchain technology and NFTs which the respective authors of the papers have. Both papers offer five properties, of which four are congruent, and which the paper shall examine first. The first, perhaps most obvious, characteristic is that of uniqueness and non-fungibility. While EUBOF refer to this characteristic as "uniqueness", Popescu referred to it as "non-interoperable". This characteristic is needless to say eponymous to NFTs, and is also set as the basis for the classification set out by the England and Wales Law Commission (**"EWLC"**) (2022). The second characteristic, which is agreed upon by both papers, is that of rarity, which EUBOF further expands to develop the concepts of artificial, numerical and historical rarity. Since NFTs are produced in a limited supply, the NFT owned will always be one out of a finite number. The third characteristic is that of immutability, which is the basis of all blockchain-based tokens, meaning that the token is tamper-resistant, and may not be removed or destroyed by anyone. The fourth and final agreed upon characteristic is that of authenticity, referring to the ability to verify information on

https://doi.org/10.54934/ijlcw.v2i3.55

the ledger, as well as provide provenance for the asset. EUBOF referred to this characteristic as "ownership", which this paper will refrain from using for the sake of clarity.

Popescu holds that the final characteristic is indivisibility, meaning that the NFT must be represented as a whole, and cannot be divided into smaller denominations. The present author argues that this falls under the scope of non-fungibility, in the sense that if the NFT is inherently not interchangeable, it could not logically be divided. It should be noted however, that NFT fractionalisation is possible through the creation of tokens which represent 'shares' in the original NFT, which remains undivided itself. On the other hand, EUBOF hold that the last characteristic is programmability, arguing that NFTs can be programmed just like any other programmable software. The example provided refers to residuals and royalties being paid to artists even after the first sale, as well as experimental applications of NFTs to Decentralised Finance (**"DeFi"**). Two categories of programmability are defined by EUBOF, (i) basic token functionalities such as the ability to transfer the token, as well as 'burn' (or destroy) it, and (ii) token information functionalities which allow one to query about the holder of an NFT, as well as the metadata of the NFT itself.

2.3 The myriad use-cases of NFTs

Regardless of the hype surrounding NFTs, awareness and knowledge about them remains considerably low. In a study by Pew Research Centre (Faverio and Massarat, 2022), it was shown that less than half of adults in the United States of America (**"USA"**) have heard at least a little about NFTs, with 2% saying that they have bought NFTs. With these statistics, it is hardly surprising that most people's perception of NFTs is either that they are cryptocurrencies, or only used for digital arts. For a number of reasons, namely the considerable influx of people jumping onto the NFT bandwagon during the final quarter of 2021 and the first of 2022, and their eventual abandonment, the NFT market's volume of sales has decreased considerably - with many happy to declare them a fad which is dying out (Brooks, 2022; Kharif, 2022). However, this is far from being a novel phenomenon, with Mao (2022) comparing it to a number of historical events such as tulip mania in the 1600s and the Dotcom bubble in the late 1990s. Others have profusely criticised NFTs as being "a solution in search of a problem", even arguing that NFTs should not be considered as tokens [27]. However, these arguments are based on NFTs being used in their most mainstream nature, that of digital arts or as being created through a third-party platform. As will be demonstrated below, this interpretation falls short of considering the myriad possible use-cases for

https://doi.org/10.54934/ijlcw.v2i3.55

NFTs in a number of industries. On the other hand, some have heralded the so-called "NFT meltdowns" as an opportunity to explore more dynamic and applicable use-cases for NFTs (Stein Smith, 2022).

Certain authors have attempted to provide categorical and paradigmatic approaches, mostly based around the current applications of NFTs, rather than their potential use-cases. Chiu and Allen (2022) propose three paradigms: (i) the consumption of NFTs, (ii) commercial exploitation of the non-financial underlying asset, and (iii) the financialisation of NFTs. The concepts being considered were more theoretical than practical and were also limited to the integration of NFTs in legal systems, rather than their potential use-cases in different industries. A similar approach was adopted by Mao (2022), who advocated for a technologically neutral approach, understanding that a blanket approach would be "over-reductionist" due to the rapid development of the technology at hand. Mao proposed four categories which aim to conceptualise the use-cases of NFTs at present day: (i) digital certificates of provenance, (ii) pure consumables, (iii) speculative instruments, and (iv) digital shares. Although the analysis is a thorough one, and rather more encompassing than the one proposed by Chiu and Allen, Mao did note that these categorisations only consider present use-cases and should only serve as a reference for potential future use-cases.

Building off the framework proposed by Mao (2022), it is pertinent for the study to analyse a few potential use-cases, to further demonstrate the need for technological neutrality when regulating NFTs. However, an in-depth analysis of all such potential use-cases would merit a study in and of itself, so for the purposes of brevity, this paper shall focus on a few choice topics which illustrate the variety of use-cases for this technology. The use-cases chosen are those which display the more innovative applications of NFTs, rather than their more well-documented use-cases. The paper shall also avoid discussing the use-cases of NFTs in art, entertainment and consumption of digital media since these are already well established, and well documented. The first use-case, and perhaps one which may be implemented in the near future, is the application of NFTs to real estate. Transfers of ownership can be easily implemented through a transfer of a token representing a property title which is automatically registered on a public database, a process which currently takes a considerable amount of time. NFTs can also be used to create better systems for fractional property ownership, mortgages, and even rent agreements with automatic payments [4].

Apart from the more obvious applications of NFTs to DeFi, Financial Technology (**"FinTech"**), and other activities of a commercial nature such as securities and shares, NFTs can be used to streamline

https://doi.org/10.54934/ijlcw.v2i3.55

and improve processes in the medical industry, while also providing for the safer storage of sensitive medical data. A similar argument is proposed for the use of NFTs to unlock the concept of self-sovereign identity, allowing for a more secure system which could later also include processes such as voting (Shilina, 2022; Luca, 2022; EUBOF, 2021). The final potential use-case being considered is the application of NFTs to already existing applications of blockchain technology to supply chain management by introducing unique, non-fungible tokens for items being tracked (Shilina, 2022; EUBOF, 2021; Sophir et al., 2021). This wide variety of potential use-cases clearly demonstrate the inapplicability of a broad regulation which simply regulates NFTs as a technology, and even, one would argue, regulation which merely categorises NFTs into digital assets and digital asset securities in the way that the proposed Digital Asset Market Structure and Investor Protection Act of the USA would. The author agrees with Mao (2022) who argues that NFTs, and digital assets as a whole, should not simply be pushed into the same schemes which provide for traditional financial assets while relying on 'catch-all' clauses.

3. A COMPARATIVE LEGAL ANALYSIS OF NFTs, DIGITAL ASSETS AND DIGITAL PROPERTY

3.1 The legal classification of NFTs across jurisdictions.

Although a considerable number of jurisdictions have now regulated cryptocurrencies and virtual financial assets in one way or another, not many have implemented a tailored approach to NFTs. The existing frameworks focus, some argue excessively, on the form the asset takes, rather than the substance of the asset itself (CCAF, 2020). No common system has yet been adopted, which scholars have outlined the need for, considering the cross-jurisdictional nature of NFTs. This section will examine the legal classification of NFTs in a number of jurisdictions from across the world, also focusing on their classification under current EU legislation.

3.1.1 European Union Legislation.

The EU's focus on digital transformation can be witnessed in the proposal for the regulation of *Markets in Crypto-assets* (**"MiCA"**), the EU's first attempt to regulate crypto-assets which do not fall under financial regulation. This regulation defines three types of crypto-assets: (i) utility tokens, (ii) asset-referenced tokens, and (iii) electronic money tokens. Utility tokens are defined to have non-financial purposes, and usually provide digital access to goods or services. Asset-referenced tokens are used to

https://doi.org/10.54934/ijlcw.v2i3.55

maintain a stable value by referencing several currencies, commodities, or crypto-assets to stabilise their value and in turn to be used as a payment form. This is differentiated by the EU from crypto-assets which are purely used for payment and stabilise their value using only one fiat currency. The regulation defines a crypto asset as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology." Although recent amendments to the proposal have made its application to NFTs possible in certain scenarios, it would broadly not apply to NFTs as a whole.

3.1.2 European Union Jurisdictions.

The legal classification of NFTs in France is based on a case-by-case analysis which depends on the particular NFT's classification as a digital asset or a token. France began regulating digital assets with the implementation of the *5th Anti-Money Laundering Directive* (**"AMLD V"**), opting to create a global regime which considers digital assets as a whole – including virtual currencies and tokens. Under French law, tokens are defined as "an intangible good representing, in digital form, one or more rights that is recorded on a distributed ledger technology" (European Network, 2022). For the most part, the application of securities regulation to NFTs is not considered under French law, however the way in which they are marketed may lead to their qualification as securities, even though they do not fulfil all the necessary characteristics.

In Germany, there is no specific regulation of NFTs, however the specific characteristics and functionalities of the NFT in question are to be considered, since they may lead to the application of a number of regulatory provisions. Germany defines crypto-assets in the *German Banking Act* (**"KWG"**), which holds that they are:

> digital representations of value that has not been issued or guaranteed by a central bank or public body and does not have the legal status of currency or money, but is accepted by natural or legal persons as a means of exchange or payment or serves investment purposes on the basis of an agreement or actual practice and which can be transmitted, stored, and traded electronically (Engelmann and Brunotte, 2022).

The widest interpretation of this definition would mean that NFTs fall under its scope, since they may be seen as serving investment purposes. However, it has been argued that the simple fact that NFTs

https://doi.org/10.54934/ijlcw.v2i3.55

can be sold should not mean that they are considered as an investment, but rather the "investor-like expectation of the performance of the NFT" should be considered (Engelmann and Brunotte, 2022). It has also been argued that NFTs are not tradable, since this would require exchangeability - which is not the case with NFTs due to their non-fungible nature. Engelmann and Brunotte (2022) go on to argue that NFTs should not be considered as securities, asset investments, or units of account under German law, an argument reiterated by Lorenz et al. (2022).

3.1.3 Liechtenstein.

The Liechtenstein 'container model' introduced by the *Liechtenstein Token and Trusted Technology Service Provider Act* (the **"Liechtenstein Token Act"**), is an innovative one, in which the token is a legal object which can represent any type of rights. Since the token is considered a 'container', it is possible to have an 'empty' container (LLV, 2019). The Liechtenstein Token Act did away with the traditional necessity of a physical information carrier and replaced them with digital register-based information carriers to create a future-proof system [22]. However, it is to be noted that the tokens must be backed by "trustworthy technology systems", such as Distributed Ledger Technology (**"DLT"**) to ensure legal certainty in transactions (LLV, 2019). Under this law, the NFT would be considered as a token, however, the way in which it is treated by the law will depend on its functionality, rather than its form.

3.1.4 United Kingdom.

In the UK there is currently no bespoke framework for NFTs, but they would be considered as a crypto-asset, of which three categories are recognised in the UK: (i) security tokens, (ii) e-money tokens, and (iii) unregulated tokens. For an NFT to be considered a security token it must "provide rights and obligations specified investment which included shares, deposits and insurance" [21]. However, in a recent landmark consultation paper held that NFTs should be considered as crypto-tokens, which are a type of crypto-asset. The paper defined crypto-tokens in such a way that there is no distinction based on the taxonomy or the use of the crypto-token, providing a technologically neutral approach (EWLC, 2022). The following definition of a crypto-token is provided:

Crypto-token means a particular, individuated data structure which:

https://doi.org/10.54934/ijlcw.v2i3.55

1. is constituted by the Protocol Rules of the Crypto-token System in which it is instantiated using one or more distributed ledgers or structured records; and

2. is recognised by the Protocol Rules of the Crypto-token System in which it is instantiated as, at any one time:

    a. capable of being uniquely attached to or associated with a particular Data Address; and

    b. capable of Authentication of an operation in respect of the particular instantiation of the data structure

In the proposed definition, *authentication* refers to cryptographic authentication via computational means. The *crypto-token system* refers to the system manifested by the operation of the Protocol Rules. *Data address* is defined as a unique individuated data structure or a set of such, recognised by the Protocol Rules. *Protocol rules* refer to the software code which defines the rules and algorithms for the particular crypto-token system (EWLC, 2022).

Although this definition is not enacted into law yet, it has the potential of putting the UK at the forefront of NFT legislation and regulation. It distinguishes between the NFT as a crypto-token in and of itself, and the NFT as a crypto-asset – considered as a crypto-token linked to a thing or rights external to the crypto system (EWLC, 2022). Further, it is recommended that the fungibility of an NFT depends on what contractual counterparties are willing to accept as mutually interchangeable, rather than the objective quality of the token itself. On this point, it is argued that fungibility is a subjective quality, and that although bank notes are usually considered as fungible objects, they are individually numbered, meaning that each note is unique (EWLC, 2022).

3.2 Digital assets and digital property across jurisdictions

3.2.1 The non-disruptive Liechtenstein model.

In the report issued by the Liechtenstein National Administration (**"LLV"**) (2019), it was noted that the concept of ownership of an object is limited to physical objects. It was argued that the extension of the concept of ownership beyond physicality would require the rewriting of many provisions of property law. This was deemed to be undesirable since property law regulates many other aspects over and above

https://doi.org/10.54934/ijlcw.v2i3.55

the ownership of property. Thus, the Liechtenstein Government adopted an approach which autonomously regulated the ownership of tokens and the associated legal consequences, which in turn does not affect the established system of property law while still providing much needed legal certainty. This is compared to the Swiss approach to the regulation of intermediated securities in that there can be a direct assignment of assets to legal entities at any time (LLV, 2019).

The Liechtenstein model introduces two key concepts: (i) the person entitled to dispose of the token, and (ii) the holder of the power of disposal of the token. The former may legally dispose of the tokens and is considered as the owner, therefore making them the legal holder of the right represented by the token. The latter is considered to be any person who knows the private key which allows access to the token, without necessarily being the person entitled to dispose of it (LLV, 2019). With the creation of the token as a new legal object, the Liechtenstein Token Act "side-stepped the doctrinal civil law difficulties of recognising intangible objects as objects of property rights and instead created a standalone, specific statutory regime" (EWLC, 2022).

3.2.2 The UK's third category of personal property.

The proposals of the EWLC and a recent judgement have highlighted the UK's willingness to recognise property rights over digital assets. It is argued by the EWLC (2022) that "digital assets [do not] fit neatly into either of the existing common law categories of personal property." However, it is noted that "the law of England and Wales is highly flexible," allowing for incremental developments. In the case of *Osbourne v. Persons Unknown and Ozone Networks t/a Opensea*, the plaintiff filed a lawsuit stating that NFTs were stolen from her digital wallet [3]. Judge Pelling held that there was "at least a realistically arguable case that [NFTs] are to be treated as property as a matter of English law." For the purposes of context, it should be noted that in a previous decision by the same Court in *Fetch.ai Ltd and another v Persons Unknown Category A and Others*, the Court departed from the reasoning proposed by the UK Jurisdiction Taskforce (**"UKJT"**)'s Legal Statement (2019), and held that crypto-assets could be considered as choses in action. This is contrasted with the position taken in *AA v Persons Unknown*, which endorses the UKJT Legal Statement, and is argued to be the preferred position [3].

The EWLC (2022), alongside a number of other authors (Palka, 2016; 2017; CCAF, 2020), calls for the development of a third category of property, the *tertium quid*, being data objects. Three criteria are proposed to determine which things fall into this new category: (i) composed of data presented as an

https://doi.org/10.54934/ijlcw.v2i3.55

electronic medium, (ii) exists independently of persons and exists independently of the legal system, and (iii) rivalrousness (EWLC, 2022). The first criterion is used to distinguish from personal property in possession, as well as recognising that the object is "constituted of data that is uniquely instantiated within a particular network or system." The second criterion is based on the *Ainsworth* criteria defined below, making the object definable, identifiable, stable and capable of being transferred. The requirement of existence independently of the legal system distinguishes these things from those considered as things in action (EWLC, 2022). The final criterion follows the principles of rivalrousness and excludability examined in Section 3 of this paper.

3.2.3 Commonwealth jurisdictions' interpretation of digital property.

The application of property law to digital assets was examined by the Singapore International Commercial Court in the case of *B2C2 Ltd v Quoine Pte Ltd*, in which there was an attempt to "bridge the gap between a purely contractual perspective [...] towards blockchain technology and a property law informed approach by classifying electronic currencies as intangible property with identifiable value" [20]. Although the court of first instance seems to recognise the third category of personal property by relying on the *Ainsworth* criteria to determine if such things are an "identifiable thing of value", the appellate court adopted an approach similar to the *Mt. Gox* case, which held that ownership can only relate to tangible things.

The New Zealand High Court examined the same issue in the case of *Ruscoe v. Cryptopia Ltd*, in which the Court quoted the Legal Statement made by the UKJT (2019), finding that crypto-assets were "a species of "intangible personal property" and "clearly an identifiable thing of value […] capable of being the subject matter of a trust"" [3]. In its decision, the Court also quoted the Canadian case of *Shair.com Global Digital Services Ltd v Arnold*, which held that crypto-assets can be considered as property for the purposes of a proprietary freezing order [3].

4. CAN NFTs ATTRACT PROPERTY RIGHTS?

4.1 Questions of ownership and possession

"The first problem in any analysis of property rights is the lack of any coherent definition of 'property'." [10]. Although property law has been a fundamental area of law since Roman times, no set, unilateral definition of the legal concept of property has ever been established (EWLC, 2022). In English,

https://doi.org/10.54934/ijlcw.v2i3.55

the word 'property' is used interchangeably to describe an object of property (the actual thing), as well as the relationship between a person and a thing, and the rights which the person has over that thing (Palka, 2016; EWLC, 2022). Palka (2016) also holds that the 'concept of property' can refer to three things: (i) the concept of an object of a property right, (ii) the concept of the type of social ordering, and (iii) the concept of a type of property right. It is also widely agreed upon that 'property' is "not a thing at all but a socially approved power-relationship in respect of socially valued assets, things or resources" (Gray, 1994; EWLC, 2022). This understanding of the social aspect to property has been widely endorsed through case law and literature (Palka, 2016; [24]; EWLC, 2022).

Breaking this down, a widely accepted understanding of this concept is that it contains three elements: (i) the existence of a thing which can be subject to property rights, (ii) the right of the person to use the thing, and (iii) the right of the person to exclude others ([24]; EWLC, 2022). It is important to understand the way in which law attempts to regulate reality. Palka (2016; 2017) argues that the law states what reality should be, thus referring to reality through legal concepts. Legal terms get their meaning from the concepts which are constituted by norms, being able to refer to actual objects. On the other hand, the norms are established by the features of the actual objects, creating a dialectical relation. This concept is important to understand because the categorisation of a thing will affect the way in which it is dealt with in law. When interpreting the law, legal professionals' reason *per analogiam,* attempting to find similarities in classifications, rather than differences (Palka, 2016; 2017). However, this approach may not apply when the things being considered are of a nature which has not yet been dealt with by law – as is the case with digital property.

4.1.1 What are things?

Although nearly two millennia have passed, the understanding of what can be considered as the object of rights, or the basis of it, has remained the same. The Roman jurist Gaius described the concept of *res*, things which can be the objects of rights. Gaius then makes the distinction between things which are tangible – *res corporales* – and those which are intangible – *res incorporales* – but still exist in law. In present day law, the delineation between material and immaterial objects is still based on this concept, both in common and civil law jurisdictions (Palka, 2016; 2017). However, common and civil law jurisdictions differ in the way they treat objects in terms of ownership, with common law systems being more flexible in their interpretation, while civil law systems tend to have a set definition of what can be

https://doi.org/10.54934/ijlcw.v2i3.55

considered as *res* (CCAF, 2020). While common law systems recognise ownership in intangible objects, civil law systems recognise rights in them, but not actual ownership [29].

A number of approaches have been proposed with regard to the determination of a thing's ability to attract property rights. The paper will consider the approaches proposed by the EWLC (2022), and by Marinotti (2021). The former considers the following characteristics: (i) compatibility with the *Ainsworth* criteria, (ii) excludability, (iii) rivalrousness, (iv) separability, and (v) value. Quoting Lord Wilberforce's judgement in the case of *National Provincial Bank v. Ainsworth*, four characteristics were proposed:

> Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability.

These criteria are not considered an exhaustive list, and it has also been noted that the criteria are not easily applicable to intangible things in which there is no physical indication (EWLC, 2022). Regardless, when applying these criteria to 'crypto-tokens', both the EWLC, and the UKJT agree that 'crypto-tokens' are able to attract property rights. The concepts of excludability and rivalrousness are similar in nature. When a thing is *rivalrous*, it means that if one person has a thing, the other does not. If the use or consumption of a thing by a person inhibits others' use and consumption, it is considered to be rivalrous. On the other hand, *excludability* refers to a person's ability to control or deny access of others to the thing or its benefits. *Separability* considers the ability of a thing to have independent existence, meaning that things such as talents cannot be subject to property rights since they would fail to exist without the respective person. With regard to *value*, it is noted that this does not only refer to economic value, but also realisable value, which means that the thing should be transferable, and has the potential to be paid for (EWLC, 2022).

Marinotti (2021) adopts an iterative approach in creating a technologically neutral formula which can be applied to a thing to determine its ability to attract property rights. The process is based on the owner's right to use a thing, adopting the approach that the right should have an "obvious boundary". Rather than considering it the owner's right to exclude, Marinotti phrases it as the duty of all non-owners not to interfere with the thing. However, Marinotti disagrees with the opinion of Douglas and McFarlane (2013) who held that a thing must be tangible for others to be able to know their duty not to interfere.

https://doi.org/10.54934/ijlcw.v2i3.55

Marinotti argues that tangibility is not the only manner in which boundaries can be delineated, meaning that in and of itself it is not a requisite. Marinotti goes on to argue that a technologically neutral approach would once again focus on the obvious boundaries of the thing, which may be determined through other means. To determine such boundaries, Marinotti argues that these should be derived from shared social customs and intuitions. The non-exhaustive list of examples provided are similar to the criteria determined by the EWLC, in that they recognise separability, value, and transferability. The final working definition provided by Marinotti to define the ability of a thing (*t*) to be able to attract property rights is the following:

1. Is *t* a rival asset?
2. From shared social customs and intuitions:
    a. Can owner X discern the boundary of their right to use *t*?
    b. Can non-owner Y discern the boundary of their prima facie duty not to interfere with *t*?

Marinotti's proposed system provides a clear formula to determine a thing's ability to attract property rights, which the present author agrees with since it does away with the need for tangibility – providing a much needed technologically neutral approach.

4.1.2 Traditional concepts of ownership and possession.

Now that a framework to determine which things can attract property rights has been established, what are the property rights that they can be subject to? An understanding of the traditional applications of ownership and possession will serve as the basis for the discussion of the application of these concepts – or variations thereof – to digital assets and NFTs. The concept of ownership is treated differently in common and civil law jurisdictions, which is a result of the historical development of the legal concepts in different jurisdictions [29]. Merrill (2017) defines ownership as "a legally enforceable right to exclusive control of a thing", noting that it is broader than possession since it is not always limited to tangible things. On the other hand, possession refers to the physical control over a thing, which for obvious reasons can only apply to tangible things [16].

Although many different legal theories of ownership have been developed, for the purposes of this paper it is enough to understand the main differences between the two legal traditions. In civil law, the

https://doi.org/10.54934/ijlcw.v2i3.55

concept of ownership is considered one which is absolute – affording total appropriation, and allowing the owner to use, benefit from, dispose of, and even destroy the thing [29]. Thus, in civil law, the property right is *erga omnes*, against all. On the other hand, in common law, a legal relation is considered a property right if a person has a better title when compared to another [35]. While certain property rights can be afforded to intangible objects in civil law systems, ownership in and of itself – generally speaking – cannot [16].

This is due to the fact that in most civil law jurisdictions, only things which can be possessed can be subject to proprietary rights. On the other hand, in common law jurisdictions property rights can be attributed to tangibles and intangibles. It should however be noted that possession can never be used to acquire property rights over intangibles [16]. In common law, property rights over movables are considered choses in possession, while property rights over intangibles are considered as choses in action, since they can only be enforced through legal action ([16]; EWLC, 2022). It is abundantly clear that neither system provides for digital assets as things which can be interpreted through the traditional concepts of ownership and possession, with many calling for the creation of a third type of personal property (Palka, 2016; 2017; CCAF, 2020; EWLC, 2022).

4.1.3 The case for digital ownership.

Digital assets and debates about their ownership are far from being a new phenomenon, being considered as early as 2013 as a new type of asset (Toygar et al., 2013). This section of the paper will focus on the general arguments in favour and against the development of the concept of digital ownership, rather than focusing on a comparative analysis of legislation and case law or an analysis of practical applications, which will be conducted in subsequent sections. The technology behind NFTs has provided an opportunity which was not considered possible before – the creation of unique, non-fungible digital assets. Currently, the only legal regimes which recognise the concept of the ownership of digital assets (aside from Liechtenstein) are based on copyright laws ([12]; Goldman, 2022). Fairfield, a great advocate of digital ownership, held that the "extension of property principles to digital assets is [...] inevitable" [11]. However, it is clear, and widely accepted, that digital assets cannot be governed by traditional concepts of property [1], and that the development of a *sui generis* (or unique) regime is necessary (Szilagyi, 2018). The current approaches have been criticised, with Moon (2018) holding that "centuries old legal categories and classifications of 'things' are out of date", making them "inadequate and in urgent need of updating."

https://doi.org/10.54934/ijlcw.v2i3.55

This sentiment was echoed by Fox and Green (2019), who describe the current regimes as "increasingly untenable."

Although this would require considerable legislative efforts, which will be discussed in the following sections, the main recommendation is the adoption of a "single, unified, and tech-neutral definition of legal thinghood in property law" [24]. It is argued that "the law ought to be able to take a principled, nuanced, and idiosyncratic approach to the legal treatment of new technology" which will allow the law to "facilitate and protect the development of a completely new type of data object" (EWLC, 2022). Palka (2016) argues that as time goes by, new concepts based on new, more fitting analogies are necessary, an argument which Fairfield (2021) reiterates profusely in his work. Allen (2018) holds that this will "make our law of property in general more future-proof, as a large and increasing proportion of our economy is concerned with such immaterial objects." One of the main arguments put forward by proponents of this development is the inapplicability of tangibility as a sufficient method of determining thingness, arguing that importance should instead be given to the characteristics of the things at hand [24] [12] [25].

This is not to say that the proposal for the legal concept of digital property has no critics. Bridge et al. (2021) held that the debate brought forward is a "red herring", and that intangibles could be classified as choses in action. Moringiello and Odinet (2021) argue that NFTs do not present any reason to be given the legal status of a token in their current constitution. They argue that NFTs are not rivalrous, because they "are freely available for download by anyone with a computer". The authors go on to hold that NFTs are "a case of attempting to create novel and overly complex property rights by contract", and that a holder of an NFT lacks "any kind of meaningful right to exclude others." The critique goes on to hold that NFTs are not compatible with the progressive property theory since they are "harmful to the environment." Although these criticisms will be analysed in further detail below, it is beneficial to consider the approach presented by Moringiello and Odinet (2021).

The study was conducted by referencing the terms of service of a number of NFT platforms, and only by considering the use-case of NFTs as representations of digital art. While it is agreed that the NFT in and of itself does not necessarily transfer any rights in underlying assets, the interpretation based on a select amount of market practices does not provide a technologically neutral assessment. The study also holds that NFTs are available for download by anyone. Even though the token's metadata and linked asset *may* be downloaded, this is not the token itself. The token itself is stored on the blockchain and cannot

https://doi.org/10.54934/ijlcw.v2i3.55

simply be claimed by anyone who downloads it. The logic behind the argument that NFTs should not be considered as property because of their environmental impact can also be argued against. Many other industries pose environmental concerns, and yet their products are still considered to be property. The author agrees that there are plenty of misrepresentations being represented by NFT platforms and sellers alike, however one cannot assess technology based on one use-case while not considering its actual technological potential.

4.2 An argument for digital property

The main argument for digital ownership is legal certainty. For the 'owners' of digital assets, many questions are left unanswered in an unregulated space. Fairfield (2021) argues that the legal regimes which regulate digital assets currently have "all but eradicated ownership interests online in favor [sic] of a contract and licensing regime." One of the main issues considered are the remedies available to the 'owners' of digital assets in cases of theft and similar offences (LLV, 2019). Other considerations are related to the bankruptcy of service providers storing digital assets on behalf of their customers (LLV, 2019). This lack of legal certainty and regulation, in turn, weakens the legal protection of users of this technology (EWLC, 2022). Fairfield (2021) argues that "[the] legal regime for digital personal property must evolve to support purchaser expectations for a kind of online ownership that has until now not been available." The applicable regimes to the transaction of such goods are also obscured, since if they cannot be considered as things, the law of sales of goods would not apply, even though users "clearly intend to convey an ownership interest in digital property" [12].

The LLV (2019) argues that legal certainty is necessary on two levels. First, since the digital assets can represent not only the purely digital assets, but also rights to physical objects, a buyer needs to have legal certainty with regard to their rights over such objects. Second, legal certainty is necessary with regard to the obligations of service providers, and the remedies available to their customers should they be necessary (LLV, 2019). They hold that:

Greater legal certainty at these two levels may help create an efficient ecosystem for digital assets and transactions and thus enable full exploitation of the potential of the token economy.

Fairfield (2021) argues that better analogies are to be used when assessing digital property, and that the "analogy to physical personal property is clear and compelling." He advocates a shift from "pure

https://doi.org/10.54934/ijlcw.v2i3.55

license characterizations [sic], which have plagued digital objects." Fairfield (2021) holds that "[law] proceeds by analogy, and technology law is no different," and that the key to doing so is to provide grounding examples. He argues that digital assets, particularly NFTs are "sold with precisely the rights of ownership [...] that come attached to real-world ownership." The LLV (2019) argues that it is not the software itself which should be regulated, since this "would stifle innovation and is therefore not effective," a sentiment which was echoed by the EWLC (2022). The development of this concept is only the beginning of a long process of creating legal certainty for this technology, and further clarifications will be necessary with regard to the transfer and acquisition of such things, control and custody over them, and the remedies available (CCAF, 2020; [14]; EWLC, 2022).

However, these theories are not without their critics. Most notably, Moringiello and Odinet (2022) have argued that NFTs, and other digital tokens as a whole, do not "embody property rights in a reference thing" by comparing them to current applications of tokenisation such as bills of lading and deeds of real property. They argue that NFTs "do not provide any link to an underlying asset, and therefore do not facilitate the transfer of any asset". The author agrees that NFTs ability to attract property rights is subject to a number of considerations, namely their intended use. Thus, a clear-cut answer which provides a final answer is difficult to achieve when considering the variety of use-cases. This being said, if regulation focuses on present use-cases of a technology, the law would need to be rewritten every time a new application is developed (LVV, 2019).

Palka (2016) argues that the problem with legal understanding is that "[legal scholars] tried so hard to make the new phenomena fit into existing concepts that an absurd conclusion still seemed the most plausible one." Palka (2016) argues that the unwillingness to create novel legal concepts which reflect reality will result in laws which are not representative of society's expectations and practices, and which are made redundant through the development of technology. The present author agrees with the EWLC (2022), in that the objective should be to "create a facilitative and legally certain environment in which [digital] assets can flourish." The present author argues that the development of a harmonised framework, especially at an EU level, will be essential to establish legal certainty in the single market due to the cross-jurisdictional nature of digital transactions.

https://doi.org/10.54934/ijlcw.v2i3.55

4.3 NFTs as things able of attracting property rights

Now that the theoretical importance of establishing the legal concept of digital property has been considered, the paper will apply the formula developed by Marinotti (2021) to NFTs. This approach is similar to the one proposed by the EWLC (2022), however it is preferred due to its clear, formulaic nature. Although Marinotti (2021) performed this assessment on a number of specific case-studies, no assessment was conducted on a generic NFT. It is to be noted, however, that the following analysis is a purely theoretical exercise, and does not necessarily apply across the board. It is merely the application of a formula proposed through literature, which aims to establish the *possibility* of NFTs attracting property rights. The author argues that in practice, a unified classification of the ability of these digital assets to attract property rights is impossible, since many other considerations must be made. For the purposes of defining what is considered as an NFT, the definition of a crypto-token proposed by the EWLC (2022) shall be utilised. This definition is being used due to its comprehensive nature, which allows the crypto-token to be differentiated from other crypto-assets such as cryptocurrencies.

First, are NFTs rival assets? Cutts (2021) defines rivalrousness as "if use or consumption by one person, or a specific group of persons, inhibits use or consumption by one or more other persons." The rivalrousness of NFTs is innate to their technological design, in that they are unique. Only one copy of the token exists, and if one person holds it and uses it, another cannot. This is due to the ability of an NFT to be "uniquely attached to or associated with a particular Data Address" (EWLC, 2022). This is contrasted with other digital objects, such as text files or audio files which can be easily copied and used by a number of people. Thus, it is clear that NFTs satisfy the first criterion.

Second, can the owner of an NFT discern the boundary of their liberty-right to use it? The owner of an NFT, through the technological framework which it is found on, in essence, has the ability to keep it, transfer it, or destroy it. The shared social customs and institutions which are defined by Marinotti (2021) are enforced by the blockchain itself, since these actions are only allowed by a person who has the data address with which the NFT is associated. Unlike other digital assets, such as virtual in-game items, these are not dependent on the interface to determine their usage, or limitations thereof. This means that owners of NFTs are able to discern the boundary of their liberty-right to use.

Third, can non-owners of an NFT discern the boundaries of their duty not to interfere? The technological framework behind the blockchain on which an NFT is found provides that no individual can

https://doi.org/10.54934/ijlcw.v2i3.55

interfere with the NFTs owned by another. These limitations are "cryptographically created and enforced, so too is the [NFT's] non-owner's duty not to deliberately interfere" [24]. Without having the data address, one cannot exercise any rights over an NFT held by another. Marinotti (2021), when examining Bitcoins, holds that "non-owners need not even actively acknowledge the boundary of their duty not to interfere because the boundary is functionally impenetrable." The same line of reasoning can clearly be applied to NFTs. Further, once again using the same reasoning applied to Bitcoins, it can be held that "[each] non-owner knows or should know that it is socially and legally wrongful" to use, transfer or destroy another's NFT – demonstrating a shared social custom.

This demonstrates that all the criteria proposed by Marinotti (2021) can be satisfied by a generic NFT, theoretically allowing NFTs to be things which are capable of attracting property rights. For further emphasis, NFTs also satisfy the *Ainsworth* criteria in that they are: (i) definable, (ii) identifiable by third parties, and (iii) capable in their nature of assumption by third parties. It must once again be noted that this analysis is theoretical and is based on a generic NFT. It does not consider use-cases in which such a token would not satisfy these criteria, such as identification tokens, which are analysed by the EWLC (2022). Finally, the legal treatment of these digital assets relies heavily on their intended use, and how they are being used, which requires case-by-case analysis, which is not achievable through this analysis. However, this analysis does provide a potential theoretical backing for the concept of digital property and its application to these tokens.

5. AN EU FRAMEWORK FOR DIGITAL PROPERTY

5.1 A harmonised classification of digital tokens

To be able to regulate digital tokens at an EU level, it is important to develop a clear legal classification of these items. The term 'digital asset' is often widely used to describe any asset which is represented in a digital or electronic form. Not all digital assets may be able to attract property rights, and due to this paper's focus on NFTs, the classification will be focused on digital tokens. The proposal of the Cambridge Centre for Alternative Finance (**"CCAF"**) (2020) to create a framework in which assets are completely separate from their form offers a technologically-agnostic approach in which regardless of the form, an asset has the same legal standing. The present author argues that this is, although admirable, nigh on impossible to practically implement. Rather, following the logic proposed by the EWLC (2022), a classification which defines particular digital assets, notably those which are potentially able to potentially

https://doi.org/10.54934/ijlcw.v2i3.55

attract property rights, is more desirable. This classification should focus on the characteristics of the token, rather than its intended use. This will then allow other regulations to apply to the token based on its usage. For example, securities and financial markets laws would only apply to the tokens being used for those purposes, rather than tokens as a whole. Also, this would not negatively impact already implemented regulations with regard to cryptocurrencies or other types of crypto-assets. This technologically neutral approach does away with the need to update regulations consistently.

Before defining the classification of these digital assets, one must first attempt to define the technology at their core. This is important to distinguish these assets from others, such as mutable digital files. In this regard, the *Liechtenstein Token Act* adopts a broad definition, that of "trustworthy technologies" (**"TT"**), being "technologies through which the integrity of tokens, the clear allocation of tokens to a TT identifier, and the transfer of tokens can be ensured." The LLV (2019) argues that the term 'blockchain' would not be technologically neutral since this depends on the "serial logging of transactions in a distributed ledger and [...] block-based verification", which is only one potential technical implementation. Nor does it consider the term 'DLT' to be sufficient, since "it cannot be ruled out that in future blockchain systems will be developed without a decentralised ledger." The Liechtenstein model also strays away from using terms such as 'crypto-systems' since cryptographic methods are used in information systems as a whole, and methods other than cryptography can be used for blockchain systems.

On the other hand, the definition proposed by the EWLC (2022) is more specific, referring to crypto-token systems which are reliant on protocol rules. These protocol rules are the technological framework which provide for:

1. The generation, authentication, sending and validation of data within the particular crypto-token system;

2. Determining and effecting changes to the distributed ledger or the structured record of the particular crypto-token system by a process of authentication such that the state of the relevant distributed ledger or structured record is capable of verification by other participants in the crypto-token system; and

3. Determining and effecting changed to the particular crypto-token system and/or the protocol rules themselves.

https://doi.org/10.54934/ijlcw.v2i3.55

The author holds that this definition provides a clear classification based on the characteristics of the token. It can be argued that this definition, being more specific, could afford more legal certainty.

With regard to the digital asset itself, the Liechtenstein model creates a new legal object – the token, which is defined as "every connecting point of rights on a [trusted technologies] system, regardless of whether they are technologically implemented as a "token", or whether the token is "filled" or not" (LLV, 2019). It is a container, which may or may not hold any rights. A similar approach is adopted by the EWLC (2022), in that the particular technological implementation itself is not considered, nor is the necessity for the crypto-token to be "filled" with anything. The author agrees with this approach, in that it does not limit the digital tokens to those which are a representation of value.

Based on a mixture of both these models, the author proposes the following characteristics for consideration when regulating. It should be noted that these recommendations are not exhaustive, and only provide a guideline for classification. For the purposes of technological neutrality, the term 'digital token' shall be used, as the author agrees with the LLV (2019) in that cryptography is not the only feasible method. Thus, for the purposes of creating a harmonised classification, the following characteristics are outlined.

A Digital Token is a particular, individuated data structure which:

1. is rivalrous;
2. exists independently of persons;
3. is constituted by the Protocol Rules of the Digital Token System in which it is instantiated using one or more distributed ledgers or structured records;
4. is capable of being attached to or associated with a particular Data Address; and
5. is capable of Authentication (cryptographically or otherwise) of an operation in respect of the particular instantiation of the data structure.

In the proposed classification, the term Digital Token System takes on the same definition as that of Crypto-token System provided by EWLC (2022). All other definitions are those proposed by the EWLC (2022), except for Authentication, which has been broadened to include authentication by methods other

https://doi.org/10.54934/ijlcw.v2i3.55

than cryptography. This classification is technologically neutral, in that it caters to future technological advancements, while still providing for a degree of legal certainty. Further, this will encompass applications such as NFTs and cryptocurrencies, while allowing them to be subject to other regulations, depending on their application.

5.2 A harmonised EU framework for digital property

Creating a harmonised classification for digital tokens is a far less challenging prospect than creating an EU-wide framework for digital property. As discussed above, civil and common law jurisdictions adopt different approaches with regard to ownership, and what can be considered the subject of ownership. Even between civil law jurisdictions, approaches vary in the classification of things which are subject to proprietary rights [3]. Now that the UK has left the EU, only Ireland remains as a pure common law jurisdiction amongst member states, with Malta and Cyprus having mixed legal systems. Thus, when one is attempting to create a framework which can apply to all EU member states, a system which is equally applicable to common and civil law jurisdictions has to be created. Although common law jurisdictions can add a third category of personal property with relative ease (as will be discussed in reference to the EWLC (2022) proposals), civil law jurisdictions would likely have to face a costly upheaval of established property law (LLV, 2019; CCAF, 2020; [3]). Further, it is clear that the traditional concept of possession cannot apply with regard to digital assets, with other concepts such as custody being proposed instead (CCAF, 2020; EWLC, 2022). This section will first analyse the proposals of the EWLC (2022) and the Liechtenstein model. Based on this, recommendations will be proposed to establish a framework for digital property in the EU.

As examined in Section 2, the EWLC (2022) proposes the creation of a third category of personal property. This would lead to a number of legal developments, namely the concept of control which is described as “an analogue to the common law concept of possession” (EWLC, 2022). This is determined by analysing if “a person in control of a data object enjoys a level of control over that asset that would satisfy the control element of possession, were the object in question tangible” (EWLC, 2022). Further, it is argued that the mechanism for the factual transfer of crypto-tokens is different from that which is applied to the transfer of legal title over tangibles and intangibles. Based on this, the EWLC (2022) argues that the distributed ledger is not necessarily a definitive record of superior legal title, since the “legal system is external to a crypto-token system.” Finally, the EWLC (2022) argues that the causes of action and

https://doi.org/10.54934/ijlcw.v2i3.55

remedies which are applicable to other types of objects of property rights can be easily applied to this third category of legal property.

On the other hand, the Liechtenstein model provides an "insulated special regime" (CCAF, 2020) which "autonomously [regulates] ownership of the token and the associated legal consequences only for TT systems" (LLV, 2019). The LLV (2019) argues that:

> [this] does not affect the established system of property law and creates a clear and well laid-out legal framework for tokens in relation to TT systems, which can also be understood by non-lawyers.

In order for this system to work, innovative legal concepts needed to be introduced. The first is the "person entitled to dispose of the token", which is defined as the owner of the token, the legal holder of the right represented, and the person who may legally dispose of the token (LLV, 2019) The law then introduces the "holder of the power of disposal" (LLV, 2019). The disposal of a token requires a private key to the wallet containing the token (or TT key). In this regard, any person who knows the private key is considered as the holder of the power of disposal, although they may not necessarily be the person entitled to dispose of the token (LLV, 2019). Tokens can contain any type of right, and "[any] transfer of a token on a TT system constitutes a binding transfer of the represented right, whether a pre-existing right or the right to digital information [22]. It is further held that "the legal effect of the transfer of a token has to be based on the underlying legal transaction and it depends on the design in each individual case" [22]. This means that depending on the content of the token, different laws will apply. Thomas Dünser, from the Liechtenstein Office for Financial Market Innovation explains this, by saying:

> This means that if a security is represented in a token, security laws apply. If a financial instrument is represented in a token, financial market laws may apply, and so on (Liechtenstein Impuls, 2020).

To ensure legal certainty, further amendments were also made to the Liechtenstein Persons and Companies Act and the Liechtenstein Trade Act, to cater for this system [22].

Based on these findings, it is argued that a framework similar to that developed in Liechtenstein proves to be the least disruptive solution which can cater for both civil and common law jurisdictions. In this way, member states will not incur substantial legislative costs, while still providing for an adequate

https://doi.org/10.54934/ijlcw.v2i3.55

degree of legal certainty and harmonisation. Although this will allow for the tokenisation of all assets and rights, if certain areas of law require specific formal procedures – such as the registration of the transfer of land with a public register – this law would not apply. Once again, it is to be noted that the following recommendations are far from exhaustive, and merely provide a conceptual basis upon which regulation should be built. Thus, the following concepts should be used to build a framework for digital property in the EU:

1. A Digital Token can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights;

2. A Digital Token which represents no rights is subject to the same provisions as a Digital Token which does;

3. The person who has the right of disposal over a Digital Token is considered as the owner of the Digital Token, as well as the legal holder of the right represented by the Digital Token (if any);

4. Any person who holds the private key has the power of disposal over the Digital Token, even though they may not be entitled to do so;

5. The disposal of a token is considered as the transfer of the right of disposal over the Digital Token or the justification of a securities or a right of usufruct over a Digital Token;

6. Disposal of a Digital Token also results in the disposal of the rights represented by the Digital Token;

7. The disposal of a Digital Token must be conducted in line with the protocols of the Digital Token system; and

8. A person who receives a Digital Token in good faith is to be protected in their acquisition even if the transferring party was not entitled to the disposal of the Digital Token unless the recipient was aware, or should have been aware of the lack of right of disposal.

The definitions in these recommendations are those established in the previous section. This proposed framework will also have to be accompanied with relevant provisions to cater for conflict of laws, as well as the introduction of the concept of a Physical Validator, which the *Liechtenstein Token Act*

https://doi.org/10.54934/ijlcw.v2i3.55

defines as "a person who ensures the enforcement of rights in accordance with the agreement, in terms of property law." The author argues that this system provides an opportunity for the EU to develop a concept of digital property, in a way which will not be problematic for member states. This also allows for the application of regulatory provisions to digital tokens based on their use, rather than their technological form. Fairfield (2021) argues that "[we] should regulate technologies according to how humans use them." Such a technologically neutral approach will allow for legal certainty, without stifling innovation.

6. CONCLUSION

Fairfield (2021), one of the greatest advocates for the development of the legal concept of digital personal property held that "[if] NFT technology had been available at the advent of the internet, law would have taken a vastly different arc [...] It is time for a late-breaking course of action.

This paper is but a humble contribution to the discussion of digital property, aiming to provide recommendations which pave the way towards legal certainty in today's – and tomorrow's – digital era. The findings of this paper are far from being the final solution to the concept of digital property. The recommendations proposed are merely meant to provide a basis for further research, discussion, and hopefully, regulation. The legal concepts developed in years gone by do not reflect the reality of today's digital world. With technology evolving daily, it no longer makes sense to stubbornly shelter under the comfort of established legal norms. Legal scholars and legislators are now provided with the opportunity (and the considerable challenge) to create avant-garde legal concepts which foster innovation while providing legal certainty. In this regard, a mere understanding of the law is no longer enough. Technological understanding, and even code literacy, have become essential skills in developing the regulations which govern technology.

It is impossible to overstate the importance of future-proof, technologically neutral regulations. Further research about the procedural law, enforcement, and conflict of laws with regard to digital assets and digital property will be essential in developing comprehensive legal frameworks. If the EU truly wishes to develop a digital single market, it can no longer ignore the technology which can truly change how we transact online. The blockchain era is well upon us, it is time to acknowledge it, embrace it, and regulate it.

https://doi.org/10.54934/ijlcw.v2i3.55

REFERENCES

[1] Allen, J. (2019). Property in digital coins. *European Property Law Journal, 8*(1) http://dx.doi.org/10.1515/eplj-2019-0005

[2] Allen, J. G., Rauchs, M., Blandin, A., & Bear, K. (2020). *Legal and Regulatory Considerations for Digital Assets*. Cambridge, United Kingdom: University of Cambridge Centre for Alternative Finance. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf

[3] Allen, J. G., Wells, H., & Mauer, M. (2022). *Cryptoassets in Private Law: Emerging Trends and Open Questions from the First 10 Years*.SMU Centre for AI & Data Governance. https://dx.doi.org/10.2139/ssrn.4206250 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4206250

[4] Appelmans, A. (2022). *The potential of NFTs in real estate markets The potential of NFTs in real estate markets.* Crypto Valley Journal. https://cvj.ch/en/focus/blockchain/nfts-in-the-real-estate-market/

[5] Behzadi, E. (2022). The Fiction of NFTs and Copyright Infringement. *University of Pennsylvania Law Review Online, 170* https://dx.doi.org/10.2139/ssrn.4025604

[6] Bridge, M., Gulliger, L., Low, K., & McMeel, G. (2021). *The Law of Personal Property* (Third ed.). Sweet & Maxwell.

[7] Chiu, I. H., & Allen, J. G. (2022). Exploring the Assetisation and Financialisation of Non-Fungible Tokens (NFTs): Opportunities and Regulatory Implications. *Banking and Finance Law Review, Upcoming* https://dx.doi.org/10.2139/ssrn.4051912

[8] Cutts, T. (2021). *Possessable Digital Assets.*LSE Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895404

[9] Douglas, S., & McFarlane, B. (2013). Defining Property Rights. In J. E. Penner, & H. E. Smith (Eds.), *Philosophical Foundations of Property Law*. Oxford University Press.

[10] Edelman, J. (2015). Property rights to our bodies and their products. *University of Western Australia Law Review, 39*(2) http://classic.austlii.edu.au/au/journals/UWALawRw/2015/20.html

[11] Fairfield, J. (2017). *Owned: Property, Privacy and the New Digital Serfdom*. Cambridge University Press.

[12] Fairfield, J. (2022). Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property. *Indiana Law Journal, 97*(4) https://www.repository.law.indiana.edu/ilj/vol97/iss4/4

[13] Fox, D., & Green, S. (2019). *Cryptocurrencies in Public and Private Law*. Oxford University Press.

[14] Garcia-Teruel, R. M., & Simon-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review, 41* https://doi.org/10.1016/j.clsr.2021.105543

[15] Gray, K. (1994). Equitable Property. *Current Legal Problems, 47*(2) https://doi.org/10.1093/clp/47.Part_2.157

[16] Graziadei, M. (2017). The structure of property ownership and the common law/civil law divide. In M. Graziadei, & L. Smith (Eds.), *Comparative Property Law: Global Perspectives*. Edward Elgar Publishing.

[17] Guadamuz, A. (2021). The treachery of images: non-fungible tokens and copyright. *Journal of Intellectual Property Law & Practice, 16*(12) https://doi.org/10.1093/jiplp/jpab152

[18] Guadamuz, A. (2022). Perspectives on NFTs from the EU and UK. *The Columbia Journal of Law & the Arts, 45*(3) https://doi.org/10.52214/jla.v45i3.10010

[19] Ibanez, L., Hoffman, M. R., & Choudhry, T. (2022). *Blockchains and Digital Assets*.EU Blockchain Forum. https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchains_and_digital_assets_june_version.pdf

[20] Kulms, R. (2020). Blockchains: Private Law Matters. *Singapore Journal of Legal Studies, March 2020* https://ssrn.com/abstract=3646920

[21] Kumar, S., Rigg, G., & Green, K. (2022). The NFT Collection: The Rise of NFTs - Copyright Strikes Back? (Part 3). *The National Law Review, 12*(256) https://www.natlawreview.com/article/nft-collection-rise-nfts-copyright-strikes-back-part-3

[22] Lins, B., & Praicheux, S. (2021). Digital and Blockchain-Based Legal Regimes: An EEA Case Study Based on Innovative Legislations - Comparison of French and Liechtenstein Domestic Regulations. *Financial Law Review, 22*(2) https://www.ejournals.eu/pliki/art/19446/

[23] Mao, C. (2022). Imperfect Digital Certificates of Provenance - A Categorical Risk-Based Approach to Non-Fungible Tokens (NFTs). *SSRN Electronic Journal,* https://dx.doi.org/10.2139/ssrn.4060436

[24] Marinotti, J. (2021). Tangibility as Technology. *Georgia State University Law Review, 37*(3) https://readingroom.law.gsu.edu/gsulr/vol37/iss3/3

[25] Michels, J. D., & Millard, C. (2022). The New Things: Property Rights in Digital Files? *The Cambridge Law Journal, 20*(1) https://doi.org/10.1017/S0008197322000228

[26] Moon, K. (2018), Is Software Goods, or even Property? A Recommendation for Sui Generis Categories. *Society for Computers and Law Magazine,*

https://www.scl.org/articles/10240-is-software-goods-or-even-property-a-recommendation-for-sui-generis-categories

[27] Moringiello, J. M., & Odinet, C. K. (2021). The Property Law of Tokens. *Florida Law Review, 74*(607) https://dx.doi.org/10.2139/ssrn.3928901

[28] Nevi, G. (2022). *NFT - Non-Fungible Tokens how react the consumers? An exploratory analysis for a future integrated acceptance model.* Unpublished manuscript. http://archives.marketing-trends-congress.com/2022/pages/PDF/023.pdf

[29] Pierre, B. (1997). Classification of Property and Conceptions of Ownerships in Civil and Common Law. *Revue Generale De Droit, 28*(2) https://www.erudit.org/fr/revues/rgd/1997-v28-n2-rgd02413/1035639ar.pdf

[30] Pinto-Gutierrez, C., Gaitan, S., Jaramillo, D., & Velasquez, S. (2022). The NFT Hype: What Draws Attention to Non-Fungible Tokens? *Mathematics, 10*(3) https://www.mdpi.com/2227-7390/10/3/335/html

[31] Popescu, A. (2021). Non-Fungible Tokens (NFT) - Innovation beyond the craze. *Proceedings of Engineering & Technology Journal, 66* https://www.academia.edu/50920483/Non_Fungible_Tokens_NFT_Innovation_beyond_the_craze

[32] Steiner, A. (2021). The Paper It's Printed On: NFTs, Ownership and Conceptual Art. *SSRN Electronic Journal,* https://dx.doi.org/10.2139/ssrn.3997352

[33] Szilagyi, K. (2018). A Bundle of Blockchains? Digitally Disrupting Property law. *Cumberland Law Review, 48*(9) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3161151

[34] Toygar, A., Rohm Jr., C. T., & Zhu, J. (2013). A New Asset Type: Digital Assets. *Journal of International Technology and Information Management, 22*(4) https://scholarworks.lib.csusb.edu/jitim/vol22/iss4/7

[35] van Erp, S. (2017). Ownership of Data: the numerus clausus of legal objects. *Brigham-Kanner Property Rights Conference Journal,* (6) https://cris.maastrichtuniversity.nl/en/publications/ownership-of-data-the-numerus-clausus-of-legal-objects

ABOUT THE AUTHORS

Matteo Alessandro – Associate at MK Fintech Partners, Birkirkara, Malta
e-mail: matteo@matteoalessandro.com

ABOUT THIS ARTICLE

Conflict of interests: Author declares conflicting interests.

https://doi.org/10.54934/ijlcw.v2i3.55

International Journal of Law in Changing World

Special Issue 1: NFTs (2023) ISSN 2764-6068

In the ever-evolving digital landscape, Non-Fungible Tokens (NFTs) have emerged as a disruptive force, challenging the traditional paradigms of digital asset ownership and control and as such we considered the subject worth of an entire issue dedicated to it. This issue serves as a testament to the multifaceted legal challenges and opportunities presented by NFTs. Through the insightful contributions of our esteemed authors, we hope to foster a deeper understanding and stimulate further discourse on this pivotal topic.

Editorial Team