2026

GLOBAL STATE OF REGULATIONS IN **BLOCKCHAIN GAMING**

Study conducted by Anuradha Chowdhary with contributions from the Blockchain Game Alliance network

BGA BLOCKCHAIN GAME ALLIANCE

DISCLAIMER

This Report is published by the Blockchain Game Alliance (BGA) for informational purposes only and does not constitute legal, regulatory, investment, or professional advice. The views and opinions expressed herein are those of the individual authors and contributors as of the date of publication and do not necessarily reflect the views or positions of the Blockchain Game Alliance, its members, partners, or affiliates. Regulatory frameworks applicable to blockchain technology and gaming are subject to change and may evolve differently across jurisdictions.

This Report does not create, and should not be construed as creating, any attorney-client or advisory relationship. While reasonable care has been taken in preparing this Report, the BGA and the contributors make no representations or warranties as to its accuracy or completeness and disclaim all liability arising from reliance on its contents. Readers are strongly encouraged to seek independent legal, regulatory, tax, and professional advice before taking any action based on the information contained in this Report.

TABLE OF CONTENTS

FOREWORD

CHRIS HEWISH

PRESIDENT, XSOLLA

The games industry has always been a space where creativity, technology, and commercial innovation converge at scale. Today, it also serves as a stress test for the digital economy. This is especially clear in blockchain-enabled games and game related infrastructure; where complex systems such as tokens, payments, wallets, identity, data, and AI operate together in live, consumer-facing environments.

At Xsolla, we see this complexity every day. We support billions in transactions across the global games ecosystem and work with studios and platforms that are already navigating a fragmented and often outdated regulatory landscape. What was once experimental is now part of daily operations. This shift demands urgency.

As gaming becomes more integrated with financial technology, it increasingly intersects with areas like finance, consumer protection, data privacy, and intellectual property. These issues are not abstract. They are embedded directly into the design and delivery of interactive experiences.

This is why the questions explored in this report are so timely and important. Asset classification, ownership rights, and the role of AI are just some of the issues shaping how games are developed, how companies are structured, and how digital economies scale. The answers to these questions carry immediate implications.

The industry can't afford to wait for regulatory perfection. Players are participating now. Studios are building now. Capital is moving now. The decision in front of us isn't whether to innovate or comply. It's whether we approach regulation with intention or fall into fragmented and reactive responses.

This report provides the clarity needed to move forward. By asking the same foundational questions across jurisdictions, the Blockchain Game Alliance has created a global snapshot of regulatory thinking. It offers a practical reference point for developers, platforms, and investors to make informed decisions.

At Xsolla, we believe that companies best positioned for sustainable success are those that treat regulation as part of the design process. The strongest innovations will not come from avoiding oversight. They will come from building systems rooted in transparency, fairness, and long-term trust.

I commend the BGA and its contributors for recognizing that good regulation is not a barrier. It is the infrastructure that allows our industry to grow with purpose and integrity.

PREFACE

By Yasmina Kaztani, President, Blockchain Gaming Alliance

The launch of this Global Regulatory Framework for Blockchain Gaming: 2026 Report comes at a pivotal moment for our industry. Across the globe, we are witnessing regulators grappling with a rapidly evolving ecosystem where digital game assets are no longer confined to the boundaries of entertainment, they intersect with financial markets, data privacy, consumer protection, and increasingly, artificial intelligence.

The approaches we observe are varied and, at times, scattered. Some jurisdictions have integrated blockchain gaming into existing financial and gambling frameworks, while others are experimenting with bespoke rules, and a few have imposed outright restrictions. This fragmented landscape highlights the urgent need for clarity and coordination, both for studios seeking to innovate responsibly and for regulators striving to protect players, particularly minors.

This report seeks to serve as a comprehensive case study on the regulation of retail and consumer-facing gaming ecosystems. By examining how different markets classify assets, define gambling thresholds, safeguard digital ownership, and apply data protection and AI governance, we aim to provide a practical resource for policymakers, industry leaders, and other stakeholders navigating this complex terrain.

At the Blockchain Gaming Alliance, we believe regulation can be a stabilizer rather than a barrier. By mapping global practices and highlighting points of convergence, this report illustrates how proportionate, technology-neutral frameworks can enable innovation while protecting players, studios, and broader digital markets.

As President of the BGA, I am proud to present this work as a shared foundation for dialogue between regulators, industry participants, and the communities we serve. Our goal is to ensure that blockchain gaming continues to evolve as a trusted, transparent, and sustainable sector, delivering value for players, studios, and society alike.

Yasmina Kaztani
President, Blockchain Gaming Alliance

INTRODUCTION

Blockchain gaming is often discussed as an entertainment vertical. In reality, it is one of the most exposed and operationally complete manifestations of the digital economy today.

Games are not closed systems. They embed tokenised value, user-owned assets, wallets, cross border participation, digital identity, and increasingly, automated decision-making. In a single consumer-facing environment, they compress many of the legal and regulatory questions confronting policymakers, institutions, and capital across the broader blockchain ecosystem. These questions surface early, publicly, and at scale. As a result, games are often the first point at which regulators, institutions, and the public encounter both the risks and the limits of existing frameworks.

This report treats blockchain gaming as a regulatory stress test for the digital economy. Rather than analysing games as products, it examines them as systems: systems where ownership is tokenised, value moves on-chain, participation is global by default, and rules are increasingly automated. The objective is not to advocate for a particular regulatory outcome, but to understand how different legal systems are responding to the same underlying challenges.

THE REPORT IS STRUCTURED AROUND FIVE CORE QUESTIONS THAT CONSISTENTLY ARISE ACROSS JURISDICTIONS:

1. Are digital assets in games securities, commodities, or simply game items? At what point do in-game assets become regulated?
2. When does blockchain gaming cross into gambling?
3. What do players actually own?
4. How are data, digital identities, and minors protected?
5. How should studios prepare for the convergence of AI and blockchain gaming?

Each chapter addresses one question, drawing on contributions from lawyers across multiple jurisdictions. Contributors respond to the same question to illustrate how similar issues are being treated globally. While regulation remains jurisdictional, the questions it seeks to answer are increasingly shared. The sixth and final chapter complements this analysis with forward-looking perspectives on how blockchain gaming is being prepared for the next five years.

The report is intended as a practical reference for founders, platforms, legal teams, policymakers, and capital. It does not offer certainty where none exists. Instead, it offers clarity, by identifying recurring questions, highlighting points of convergence and divergence, and making visible the regulatory terrain that blockchain gaming, and the digital economy more broadly, must navigate.

Anuradha Chowdhary,
Board Member, BGA;
Founder & CEO, ZeroTo3 Collective

01 ASSET CLASSIFICATION & FINANCIAL REGULATION

Are digital assets in games securities, commodities, or simply game items? At what point do in-game assets become regulated?

The "Great Classification" of 2026.

The Current State: After years of ambiguity, global regulators have shifted their focus what a digital asset claims to be to what it actually does. In 2026, the in-game item has become a legal hybrid. An asset that remains locked within a single game environment may be viewed as a simple utility; however, an asset that gains external liquidity on a decentralized exchange (DEX) is increasingly scrutinized as a financial instrument. .

Studios now face a “compliance squeeze”. Integrating deep liquidity can trigger bank-level regulations; while restricting it may diminish the core value proposition of Web3 gaming. This Chapter frames the economic reality test in the context of tokens: the moment a player’s primary motivation shifts from "entertainment" to a "reasonable expectation of profit", the studio’s legal liability transitions from standard consumer laws to complex financial oversight.

01 ASSET CLASSIFICATION & FINANCIAL REGULATION

AR

The classification of the game items depends on their features. If the game items cannot be exported outside the game or transferred to other players, generally, they will simply be game items, subject to the rights granted to users under the terms and conditions of the game.

If the game items are fungible and convey rights to participate in profits and/or rights to receive a fixed income, the game items would potentially qualify as securities under Argentine law, and their issuance and offering would be subject to the regulations of the Argentine securities exchange commission (Comisión Nacional de Valores).

Non-fungible tokens would generally fall outside the securities regulations.

The studio would be required to register as a virtual asset service provider if all of the following conditions are met:

1. if the in-game items qualify as virtual assets. For these purposes, virtual assets are digital representations of value that can be commercialized and/or transferred digitally and can be used for payments or investments (excluding digital representations of fiat currency);
2. the studio provides exchange, custody or transfer services in connection with the virtual assets; and
3. the studio has a relevant point of contact with Argentina (such as having a .ar web domain, having on-ramp agreements with local entities, the game being directed to the Argentine market, conducting marketing efforts directed to Argentina, or that 20% of the business volume of virtual asset service is derived from Argentina).

Only the provision of virtual asset services is regulated. Virtual assets themselves are not regulated by the securities exchange commission.

Author:
Juan Manuel Campos Álvarez,
SYLS

KY

Cayman does not inherently classify virtual assets as securities or commodities. While lawyers will often say "it depends upon the unique facts and circumstances applying to each token" projects and the market have moved to consider certain features higher risk and certain features lower risk.

The development of caselaws, including AA v Persons Unknown[1], the Tulip Trading v Van der Laan[2] and D'Aloia v Persons Unknown[3] cases, together with the UK Property (Digital Assets etc) Act, 2025 have set out a clear basis for digital assets to be treated as a 'third category' of property in common law countries, giving greater certainty to potential remedies when disputes arise[4]. This represents a shift from in-game assets merely being data, to which a temporary and limited licence has been granted by the game owner, but noting that web3 games still operate under the same model of granting users a licence to use the game software. The ability for part of the game, typically non-fungible tokens and/or in game currency, to be the subject of legal ownership by users is still to be widely adopted but the number of studios continuing to press ahead with projects involving digital assets signals further adoption in coming years.

Whether an in-game digital asset is regulated in Cayman involves considering two different Acts, first the Virtual Asset (Service Providers) Act (2024 Revision)[5](VASP Act) and then the Securities Investment Business Act (SIBA). The VASP Act regulates entities offering, or holding themselves out to offer, virtual asset services and provides for a two tier regulatory model. From April 2025 custody and trading platforms must be licensed, and other offerings are subject to a lighter registration regime. Under the VASP Act, a virtual asset is defined as:

a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes but does not include a digital representation of fiat currencies.

A sub-category of tokens, virtual service tokens, is expressly excluded from the definition of virtual asset, and is defined as:

a digital representation of value which is not transferrable or exchangeable with a third party at any time and includes digital tokens whose sole function is to provide access to an application or service or to provide a service or function directly to its owner.

Many traditional in-game assets are likely to qualify as virtual service tokens, but such tokens are not likely to provide the benefits of blockchain technology. A party which is providing 'virtual asset services' must be registered or licensed, these services include:

the issuance of virtual assets or the business of providing one or more of the following services or operations for or on behalf of a natural or legal person or legal arrangement-

(a) exchange between virtual assets and fiat currencies;
(b) exchange between one or more other forms of convertible virtual assets;
(c) transfer of virtual assets;
(d) virtual asset custody service; or
(e) participation in, and provision of, financial services related to a virtual asset issuance or the sale of a virtual asset;

(1) AA v Persons Unknown [2019] EWHC 3556 (Comm)
(2) Tulip Trading Ltd v Van der Laan [2023] EWCA Civ 83
(3) D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch)
(4) See Chapter 5, Bacina & Pettigrove, The Law of Code: Blockchain and the Law In Australia, LexisNexis 2025
(5)https://www.cima.ky/upimages/lawsregulations/VirtualAssetServiceProvidersAct2024Revision_1716397271.pdf

The most likely elements to apply to web3 gaming are the exchange of tokens, or custody of tokens via a wallet service offered in conjunction with a game. Transfer services, such as between users, or any financial services, such as permitting lending or borrowing of in-game assets, are on higher risk of also being VASP activities and requiring registration.

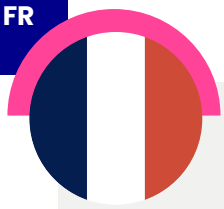
So while much depends on the features of a token, an in-game currency token which is limited to the game is likely to be outside the definition of the VASP Act, but once tradeable or usable for investment purposes, it is likely to be a 'virtual asset' and increase the risk of being regulated under the VASP Act.

These in-game assets, unless they offer passive returns or represent underlying claims on revenue or a real asset, still show more similarity to commodities than to securities. Should a token represent or be construed as a security then the issuer may find themselves falling within the scope of SIBA, which is designed to regulate certain dealings in securities, not games, and as such compliance by a game with SIBA in order to offer certain products is likely to be extremely difficult, if not impossible.

It is not uncommon to see Cayman Foundations operating as a holding company and key stakeholder in a game ecosystem, while subsidiary or related companies provide features and offerings which may fit better in other jurisdictions. We increasingly see partnerships between licensed entities and games so as to provide services like in-game token conversion, wallet and custody and other products, operating within the regulatory perimeter.

Authors:
Michael Bacina & Jonathan Turnham,
NXT Law

FR



Under EU law, digital assets used in games are not regulated per se. Their legal classification follows a principle of regulatory subsidiarity, based on the asset's economic function, attached rights, and transferability, rather than its technological form or in-game label.

At the highest regulatory level, an in-game asset qualifies as a financial instrument (or a hybrid instrument) under MiFID II where it confers rights comparable to transferable securities. This includes rights to economic returns, yield, profit participation, or governance powers akin to corporate decision-making. In line with ESMA's substance-over-form approach, an asset that functions as an investment will be regulated as such, regardless of being labelled a "game item" or an "NFT".

1. The "Closed-Loop" Exemption
In-game currencies that operate strictly within a closed ecosystem - meaning they cannot be exchanged for fiat currency or other crypto-assets and are not accepted by third parties - generally remain unregulated. Such tokens lack the character of "monetary value" in a legal sense and do not constitute financial instruments. Regulatory oversight is triggered only when a token transcends the boundaries of the game's internal economy.

2. Classification as Securities (WpPG / KWG)
If an in-game token grants the holder proprietary rights comparable to traditional capital market instruments, specifically dividend rights, profit participation, or governance rights (voting), it is classified as a security (Wertpapier) or a security-like instrument under the German Banking Act (KWG) and the Securities Prospectus Act (WpPG).

• The Criterion of Fungibility: BaFin emphasizes that for a token to be a security, it must be fungible (interchangeable) and capable of being traded on capital markets.
• MiCAR Exclusivity: Pursuant to Art. 2(4) MiCAR, tokens classified as securities are excluded from MiCAR's scope. Instead, they are subject to stringent prospectus requirements and licensing mandates under the KWG or the Investment Services Act (WpIG).

3. E-Money vs. E-Money Tokens (ZAG / MiCAR)
If a token is intended as a means of exchange and is accepted by third parties outside the original game developer's ecosystem, it may constitute E-Money under the Payment Services Supervision Act (ZAG).
• E-Money Tokens (EMT): Under MiCAR, tokens that maintain a stable value by referencing an official currency are classified as E-Money Tokens. While these are "crypto-assets" by definition, they are subject to the stricter regulatory regime of E-Money. An in-game token functioning as a cross-platform stablecoin falls into this category, requiring the issuer to hold an E-Money license.

4. Utility Tokens and Other Crypto-Assets (MiCAR)
Tokens that are based on DLT and are fungible, but do not qualify as securities or E-money, fall into the residual category of "Other Crypto-Assets" (often referred to as Utility Tokens) under MiCAR.

• Regulatory Requirement: Since the full implementation of MiCAR, issuers of such tokens must publish and notify BaFin of a "Whitepaper." For gamers and developers, this means that any fungible token that provides access to a digital service (e.g., crafting, server access) and is transferable on a blockchain is a regulated crypto-asset.

5. NFTs and the Asset Investment Act (VermAnlG)
Non-Fungible Tokens (NFTs) occupy a unique position. Because they are unique and non-interchangeable, they are generally excluded from MiCAR.

• Subsumption under VermAnlG: However, in the German jurisdiction, an NFT may be classified as an Asset Investment (Vermögensanlage) under the Asset Investment Act (VermAnlG) if it is marketed with an expectation of returns or as part of a collective investment scheme. If an NFT represents a fractionalized interest in a game's success rather than a mere collectible, BaFin may enforce prospectus obligations under national law.

Conclusion and Outlook for 2026

For stakeholders in the gaming industry, the regulatory threshold is determined by transferability and economic entitlement. By 2026, the German supervisory practice has clarified that:

1. Pure Utility (Internal): Unregulated.
2. Dividend/Equity Rights: Regulated as a Security (KWG/WpPG).
3. Third-party Payment Function: Regulated as E-Money/EMT (ZAG/MiCAR).
4. Transferable Blockchain Utility: Regulated as a Crypto-Asset (MiCAR).
5. Investment-focused NFTs: Regulated as an Asset Investment (VermAnlG).

This framework ensures market integrity but requires game developers to adopt a "Compliance by Design" approach when integrating blockchain elements.

Author:
Alireza Siadat,
Deloitte Legal

IR

In Ireland, as of 30 December 2024, digital assets (defined as crypto-assets) are regulated under the EU Markets in Crypto-Assets (MiCA) Regulation. The MiCA-Regulation applies to all digital assets that are deemed as a digital representation of a value or of a right that are able to be transferred and stored electronically using distributed ledger technology or similar technology and that are not explicitly excluded from its scope.

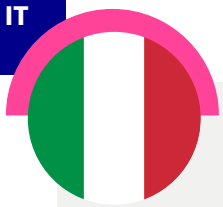
Most in-game digital assets are being used solely within a closed-loop system either as a means of payment for in-game products (like gadgets or upgrades) or as in-game items (e.g. virtual points which can boost the player's status). Under the MiCA-Regulation digital assets that are simply used as a means of access to an existing service or a product

supplied by the issuer, are deemed as utility tokens to which some key transparency and information obligations (incl. the obligation of the issuer to prepare and publish a white-paper) do not apply. The same exemption applies to digital assets that are used as a means of access to a product or a service in a limited network of merchants, who have agreed to accept it based on a contractual arrangement between them. This second exemption mirrors the exemption from the application of the Payment Services Regulations 2018, the so-called Limited Network Exemption (LNE).

Where a digital asset can be used outside the in-game ecosystem (e.g. be transferred freely to third parties and potentially be listed on a crypto-exchange), the digital asset can fall under the scope of the MiCA-Regulation as a regulated crypto-asset. In such case, the person offering digital assets to potential buyers outside the game ecosystem, may be deemed as an offeror of the crypto-assets under the MiCA-Regulation and required to comply with a number of information and transparency obligations. Entities facilitating exchange and trading in such crypto-asset, may also trigger a license obligation under the MiCA-Regulation. Further, where the digital asset in question purports to maintain a stable value by being linked to a value of another asset or an official currency, it may be deemed as a regulated stablecoin under the MiCA-Regulation (either an asset-referenced or an e-money token).

Author:
Miroslav Duric,
Taylor Wessing Partnerschaftsgesellschaft
mbB, Frankfurt

IT



Under Italian law, digital assets in games most likely can be considered as IP rights, and most probably items protected under copyright law. Furthermore it should be distinguished the copyright over the software which produces the on-line gaming from the IP over the digital asset in games at issue like the image of a character of a game or the image of a weapon.

The access to a gaming platform under a SAAS contractual agreement is similar to the access to digital books in Kindle and does not entail any legal status of digital assets in games as goods - the purchaser of the digital asset in games much likely is only obtaining a contractual right to use within the game of that digital asset but acquires no property right over it.

The idea that a digital asset in games is a commodity or a good which can be transferred under a contract of sale or barter or similar type of agreements does not violate the law but it can be mostly achieved by private contracts. From this point of view, as it is possible to sell a jpeg file or a pdf file it is also possible to sell a digital asset in games. If the digital asset in games is subject to copyright there is an issue related to the principle of exhaustion.

If the digital asset in games is an NFT the NFT can be sold as a piece of property.
Digital assets in games, apart from being regulated by IP law, can be regulated if they are incorporated into an NFT and the NFT under Regulation 2023/1114 ("MiCA") are considered from a regulatory perspective "fungible tokens" pursuant to MiCA recitals 10 and 11 (although unlikely in the case of digital assets in games).

Although many considerations herein can also be applicable to EU law as a supranational although coherent legislation, they have been mainly written in relation to Italian law.

Author:
Paolo Maria Gangi,
Gangi Law Firm

JP

The legal classification of in-game digital assets in Japan turns on economic function, transferability, and investment-like characteristics. Under the current framework, most cryptocurrencies are classified as "crypto assets" under the Payment Services Act (PSA). Type I Crypto Assets are defined as proprietary value that:

1. can be used to pay for goods or services with an unspecified party;
2. is transferable electronically; and
3. is not denominated in a legal currency.

Type II Crypto Assets can be exchanged for Type I Crypto Assets with an unspecified party and are transferable electronically. Tokens representing shares, bonds, or interests in collective investment schemes are regulated as "electronically recorded transferable rights" under the Financial Instruments and Exchange Act (FIEA) and treated as securities.
Non-fungible tokens (NFTs) occupy a distinct regulatory category. In December 2022, the Financial Services Agency (FSA) published administrative guidelines clarifying that tokens may qualify as NFTs (rather than crypto assets) if they: (i) are not intended to be used as a mode of payment for goods or services; and (ii) are priced above JPY 1,000 per unit or issued in quantities below one million. NFTs meeting these criteria are generally not subject to crypto asset regulation, although they may still fall under the PSA or FIEA if they function as payment instruments or investment schemes. The FSA's April 2025 Discussion Paper confirmed: "For NFTs that do not qualify as either crypto assets or securities, whether they should be regulated as investment targets must be considered based on what the NFT represents."

Japan's regulatory framework for crypto assets is undergoing fundamental transformation. In late November 2025, the FSA's Financial System Council Working Group finalized a report recommending that crypto assets be reclassified from the PSA regime to the FIEA regime, treating them as investment products subject to securities-level regulation. Legislation is expected to be submitted to Japan's ordinary Diet session in 2026, with implementation anticipated later that year following a transition period.

The proposed FIEA framework would introduce mandatory disclosure requirements for crypto assets listed on domestic exchanges, insider trading prohibitions with criminal penalties and surcharges, and enhanced enforcement powers against unregistered operators. A flat 20% capital gains tax (replacing the current progressive rate of up to 55%) is also under consideration as part of the broader reform package.

For blockchain gaming, the FSA has indicated that NFTs will not be moved to the FIEA framework, reasoning that their varied nature requires careful consideration before uniform financial regulation. However, in-game tokens that qualify as crypto assets under current PSA definitions would be subject to the new FIEA requirements once the reform is enacted. Studios should monitor whether their tokenomics trigger reclassification and prepare for potentially heightened compliance obligations. Early engagement with the JCBA Blockchain Gaming Subcommittee and other industry bodies would be valuable during the transition period.

Authors:
Yumi Ahn & Ryo Yamada,
Tokyo International Law Office

ME

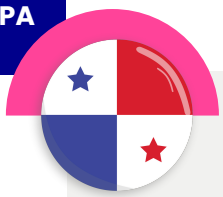
As of January 2026, the Law on the Prevention of Money Laundering and Terrorist Financing (Zakon o sprečavanju pranja novca i finansiranja terorizma) ("Montenegrin AML Act") is the primary source of regulation of crypto-assets (kriptoimovina). The term "crypto-asset" (kriptoimovina) captures various types of digital assets that are digital representations of value or rights that can be stored and transferred electronically via DLT or a similar technology, and which are not explicitly excluded from the scope of the Montenegrin AML Act. Nonetheless, when it comes to crypto-assets, the scope of the Montenegrin AML Act is solely limited to the transposition of the 5th EU AML Directive (Directive (EU) 2015/849) ("AMLD5") i.e. to the introduction of AML compliance and registration obligations for obliged entities that provide certain services in relation to crypto-assets.

Whereas the Montenegrin AML Law does not contain an explicit exclusion for crypto-assets used exclusively within a closed-loop system (like the EU MiCA-Regulation) its primary addressees are the above mentioned providers of crypto-asset related services. Further, the Montenegrin AML Act does not contain rules applicable to issuers of crypto-assets, that might be of relevance to the issuers of in-game digital assets. Therefore, where an in-game digital asset is solely used within the in-game environment, without the possibility of being transferred to third parties outside of this closed-loop system, the activity that the issuer is engaging in will generally not be be deemed as provision of crypto-asset related services. Hence, the registration obligation under the Montenegrin AML Act would generally not arrise for the issuer. Nonetheless, where an issuer facilitates transfer of in-game digital assets to third-parties or wallets outside the in-game ecosystem, this may trigger a registration obligation for the issuer that might be deemed as a provider of crypto-asset related services in such scenario.

Further, digital assets used as a means of payment in gaming, can potentially be deemed as e-money (elektronski novac) or a payment instrument (platni instrument) under the Montenegrin Payment Systems Law (Zakon o platnom prometu). Nonetheless, the Payment Systems Law provides for an exclusion from its scope of application for instruments used solely within a closed-loop system which mirrors the LNE exclusion availabile under the EU PSD2 framework.

Author: ***Miroslav Duric*** *- Taylor Wessing Partnerschaftsgesellschaft mbB, Frankfurt*

PA



Under Panamanian law, most in-game tokens, NFTs, skins, or "items" are not automatically classified as securities or commodities just because they are digital or blockchain-based. Their legal character depends on function and commercialization: what rights the asset represents, how it is sold and promoted, and whether the surrounding business model falls inside an existing regulated perimeter. Panama's main financial perimeter is the Securities regime supervised by the Superintendencia del Mercado de Valores (SMV), which defines "Securities" covering bonds, shares, participation certificates, options, and other instrument commonly recognized as a security or that the SMV determines is a security.

In parallel, Panama's gambling perimeter is led by the Junta de Control de Juegos (JCJ), which has the power to determine case-by-case whether a product is a game of chance or an activity that originates bets.

1. When digital assets are "simply game items"
An in-game asset is most defensible as a game item when it is primarily consumptive or utility, carries no investment-like rights, and is not marketed on a "profit expectation" narrative. Risk is typically lower when the ecosystem is closed-loop and transferability or secondary trading is limited or purely incidental.

2. When they can become regulated as "securities"
The critical inflection point is when the asset's economic reality resembles a Security and it is offered in a manner consistent with an investment product. Two legal triggers matter in practice: (i) the instrument, (Does it look like a security or an SMV-recognized equivalent?) and (ii) the offer. Panama requires registration of public offers or sales of securities unless an exemption applies, and it adopts a strong territorial hook: offers made to persons domiciled in Panama are treated as offers made "in Panama," and the SMV may determine when an internet offer is directed to Panama-domiciled persons.
Separately, "market activities" like intermediation and investment advice are regulated activities under the securities framework.

3. "Commodities" and derivatives exposure
Panama does not apply a universal "commodities" label to tokens the way some jurisdictions do. But assets can enter the financial perimeter when they are wrapped into investment or derivative-like structures. Notably, Panama's concept of investment vehicles explicitly contemplates investing in currencies, metals, inputs and other goods, underscoring that "the underlying" may be broad once the wrapper is an investment product.

4. The gaming and gambling overlay
Even if an asset is not a "Security," it may become regulated if the game design effectively creates wagering, or an activity that originates bets, especially online under the JCJ's electronic gaming framework.

Authors:
Teresa Carballo & Edgar Young,
Pacifica Legal

RS

Digital assets (digitalna imovina) in Serbia are regulated as of 21 June 2021 by the Digital Assets Act (Zakon o digitalnoj imovini). The Digital Assets Act has created the very first regulatory framework in Serbia that has explicitly regulated digital assets (digitalnu imovinu) which can be in one of the following forms: (i) virtual asset (virtualna imovina) the category which primarily aims to capture digital assets used as a means of exchange, and (ii) digital tokens, a catch all category for all other types of digital assets that are neither virtual assets nor excluded from the scope of the Digital Assets Act.

The Digital Assets Act does not apply to transactions with digital assets if those transactions are performed exclusively within a limited network of persons who accept such digital assets (e.g., the use of digital assets for specific products or services, as a form of loyalty or reward, without the possibility of their transfer or sale). This exclusion largely mirrors the above mentioned LNE exclusion available under the EU MiCA-Regulation.

Therefore, in-game digital assets that are solely used within a closed-loop system and which are as such solely redeemable by the issuer or a small number of persons who accept it (as a means of exchange for a product or a service or a reward supplied by them), and which are not transferable outside the in-game environment, are not regulated under the Digital Assets Act.

Where a digital asset can be used outside the in-game ecosystem and transferred freely to third parties, it may fall under the scope of the Digital Assets Act. Consequently, offering of such digital assets to persons in Serbia may constitute offer to the public of regulated digital assets to which a number of information and transparency obligations apply (incl. the obligation of an issuer to prepare and publish a white-paper). Further, where a digital asset is designed to be used as a means of payment (like e-money) it may be deemed as e-money (elektronski novac) and therefore fall under the scope of the Serbian Law on Payment Services (Zakon o platnim uslugama). The reason for this lies in the fact that unlike the MiCA-Regulation in the EU, the Serbian Digital Assets Act does not know a special category of regulated stablecoins like e-money tokens in the EU.

Author: ***Miroslav Duric,*** *Taylor Wessing Partnerschaftsgesellschaft mbB, Frankfurt*

SG

Generally, digital assets in games are not considered to be securities or commodities. While such digital assets in games are generally deemed to be in-game items, depending on the economic substance of such in-game digital assets, there are some specific instances where such digital assets may attract regulatory scrutiny and/or require licensing.

Where such in-game digital assets may be traded on an exchange or used for payment purposes, they are likely to be classified as a digital payment token ("DPT") under the Payment Services Act 2019 (the "PS Act"). Under the PS Act, the entity that provides services in relation to this in-game digital asset is likely to be deemed to be a DPT service provider and accordingly may be required to be licensed (as a standard payment institution or a major payment institution, depending on the volume processed on a monthly basis).

Such in-game digital assets may also be deemed to be a capital markets product ("CMP"), such as securities or derivative contracts. For example, if the digital asset provides the player with a share in the returns generated by the game be it in the form of revenue of the game studio, or if holding the digital asset represents a right to dividends, then such an in-game digital asset would likely be considered a CMP under the Securities and Futures Act 2001 (the "SFA").

Ultimately, such in-game assets become regulated when they are offered to the public or facilitated for exchange. Limited purpose DPTs (i.e. a digital asset that is purchasable solely for cosmetic purposes and cannot be sold outside of the game) are largely exempt from regulatory scrutiny.

For completeness, such in-game digital assets also become regulated should an element of gambling be involved. Where such an in-game digital asset is awarded through a game of chance (e.g. a randomised loot box), such an in-game digital asset may no longer be considered just a game item, but may instead be deemed to be a "money equivalent" prize (as defined in section 14 of the Gambling Control Act 2022).

Authors:
Grace Chong & Bryan Ong,
Drew and Napier LLC

KR

South Korea regulates digital assets through two separate frameworks-one for "virtual assets" and one for "securities." Whether a digital asset falls into one category or the other depends on its economic characteristics and capacity for secondary-market trading, rather than how the token is labeled or its underlying blockchain architecture.

Virtual Assets

The Virtual Asset User Protection Act (VAUPA) establishes the primary regulatory regime for virtual assets. The Act defines "virtual assets" as electronic certificates with economic value that can be electronically traded or transferred. Notably, the VAUPA explicitly excludes "game money", items obtained through gameplay under the Game Industry Promotion Act (GIPA), from the virtual asset definition. This carve-out means purely in-game currencies and items that cannot be extracted or traded externally remain outside the VAUPA's scope.

In-game assets cross into regulated territory when they exhibit characteristics beyond in-game utility. The VAUPA Enforcement Decree excludes NFTs characterized as electronic certificates that exist uniquely and are non-interchangeable among parties, primarily collected for their own value or used solely to confirm transactions between parties. However, the Financial Services Commission's NFT Guidelines specify that an NFT likely becomes a regulated virtual asset if it is issued in large quantities with high interchangeability, can be fractionalized, or can be used as a means of payment.

Securities

Digital assets exhibiting investment characteristics fall under the Financial Investment Services and Capital Markets Act (FSCMA). Tokens constitute "investment contract securities" when investors pool funds into a common enterprise expecting profits from others' efforts—a test formalized in the Financial Services Commission's (FSC) Token Security Guidelines. Security token offerings must comply with full registration and disclosure requirements.

Pending Legislation

The Digital Asset Basic Act, a bill introduced to the National Assembly in June 2025, would establish a filing regime for domestic token issuance and effectively introduce a formal regulatory framework for domestic token issuance and potentially replace the de facto administrative restrictions on initial coin offerings (ICOs) that have been in place since September 2017 through supervisory policy rather than express statutory prohibition. However, the bill remains stalled amid disagreements between the FSC and the Bank of Korea over stablecoin governance. The FSC has publicly stated that all provisions remain under consultation and debate, with nothing yet confirmed or finalized. The legislative timeline remains uncertain, and while industry commentary has suggested possible consideration beginning in or after 2026, enactment timing and final provisions remain subject to ongoing policy debate and legislative revision. Studios should treat all provisions of the proposed act as pending and subject to revision.

Practical Guidance

Studios are advised to take a conservative approach when classifying in-game assets. Assets confined to closed game ecosystems are likely unregulated, but those that can be exchanged for fiat or cryptocurrency, divided into fractional units, or promoted with profit expectations will likely attract regulatory obligations. Certain major Korean crypto exchanges require, as part of their listing review, a legal opinion from Korean counsel confirming that the token does not constitute a security under the FSCMA.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

TH

Under Thai law, digital assets used in games are generally not characterised as securities or commodities by default. Instead, they are most commonly treated as in-game items or digital property, unless they fall within the scope of regulated digital assets under the Emergency Decree on Digital Asset Businesses B.E. 2561 (2018) (the "Digital Asset Decree").

The Thai Securities and Exchange Commission (SEC) adopts a functional and substance-based approach to digital asset classification. The Digital Asset Decree recognises two principal categories of regulated digital assets: (i) cryptocurrencies, intended as a medium of exchange, and (ii) digital tokens, which may confer rights to participate in an investment, receive returns, or access specific goods or services. Importantly, the definition of a digital token is broad and technology-neutral, allowing it to capture certain blockchain-based in-game tokens if they confer transferable economic value or utility beyond purely internal gameplay.

In most blockchain games, NFTs or tokens representing characters, skins, equipment, or land are initially structured as game items rather than regulated financial instruments. These assets may constitute "property" under the Thai Civil and Commercial Code, capable of ownership and transfer, but they do not automatically fall under SEC supervision merely because they exist on-chain.

The regulatory threshold is typically crossed when an in-game asset begins to resemble a regulated digital token, particularly where:

- the token is marketed as having real-world value or resale potential;
- it is transferable outside the closed game ecosystem;
- it is tradable on secondary markets; or
- it is promoted as an investment or profit-generating asset.

Thailand does not yet have explicit legislation addressing blockchain gaming tokens, resulting in a recognised regulatory grey area. However, the SEC has consistently taken the position that where a platform offers digital tokens to persons in Thailand, it may constitute an "offering" requiring regulatory approval or licensing.

The SEC applies a targeting test to determine whether a digital asset is offered to Thai persons. Relevant factors include the use of the Thai language in marketing materials, acceptance of Thai baht, Thai-facing customer support, use of a ".th" domain, or advertising campaigns directed at Thailand. Where such targeting exists, a foreign blockchain gaming platform offering tokens may be required either to obtain a digital asset business licence or to restrict access by Thai users.

As a result, while in-game assets are not inherently regulated, tokenisation combined with transferability, monetisation, and Thai-targeted distribution can bring blockchain gaming projects within the ambit of Thailand's digital asset regulatory framework.

Author:
Dr. Jason Corbett,
Silk Legal

AE

Digital assets used in games can take several forms, ranging from purely cosmetic items such as skins, avatars, or badges to blockchain-based tokens and NFTs that may be traded externally or exchanged for real-world value.

In the United Arab Emirates, regulators adopt a substance-over-form approach, meaning in-game assets become regulated when they move beyond closed, gameplay-only use and begin to function as financial or investment instruments. For the purpose of this chapter, we will focus on the most relevant regulatory frameworks below.

DUBAI – Dubai (excluding DIFC)
In Dubai (excluding DIFC), virtual asset activities fall under the authority of the Dubai Virtual Assets Regulatory Authority (VARA). Purely cosmetic or gameplay-only items are generally unregulated where they remain confined within the game environment and cannot be transferred, traded, or converted into fiat currency or cryptocurrency. However, in-game assets become regulated where they fall outside VARA's redeemable closed-loop exemption. This occurs when tokens or NFTs are transferable between wallets, traded on secondary marketplaces, exchanged for cryptocurrency or fiat, or used within play-to-earn models. In such circumstances, the assets are treated as virtual assets, and the issuer or operator may require VARA licensing for issuance, brokerage, or marketplace activities.

DIFC
The Dubai International Financial Centre (DIFC) operates as a separate financial free zone regulated by the Dubai Financial Services Authority (DFSA). Under the DFSA framework, utility tokens and NFTs used solely to access in-game features or represent ownership of in-game items are generally treated as excluded tokens and are not regulated as financial instruments. However, in-game assets become regulated where they function as investment products, provide ownership or revenue-sharing rights, or operate as a medium of exchange or payment outside the gaming ecosystem. Even where tokens qualify as excluded tokens, issuers may still be classified as designated non-financial businesses or professions and therefore be subject to anti-money laundering and counter-terrorism financing compliance obligations.

ABU DHABI
Within the Abu Dhabi Global Market (ADGM), which is regulated by the Financial Services Regulatory Authority (FSRA), genuine in-game items are generally excluded from regulation where they are acquired primarily for gameplay and lack an investment purpose. However, assets become regulated where they are externally tradable, marketed with an expectation of profit, or structured in a way that resembles financial products rather than gameplay utilities. The FSRA also places particular scrutiny on staking and yield mechanisms, as passive income features may result in the activity being classified as regulated asset management or custody. Accordingly, while cosmetic or utility-based items remain unregulated, investment-oriented or yield-generating tokens fall within the FSRA's regulatory perimeter.

Author:
Chris Elias,
Moto Legal

UK

I. Financial Services Perimeter and Specified Investments

In the UK, the financial services perimeter captures financial instruments under the following circumstances:

In the United Arab Emirates, regulators adopt a substance-over-form approach, meaning in-game assets become regulated when they move beyond closed, gameplay-only use and begin to function as financial or investment instruments. For the purpose of this chapter, we will focus on the most relevant regulatory frameworks below.

1. An instrument (e.g. token) that is a "specified investment" under the Financial Services and Markets Act (FSMA) 2000 (Regulated Activities) Order 2001 (e.g., shares, debt instruments, units in a collective investment scheme, derivatives, certificates of deposit).
2.. Even if an instrument is not a specified investment, activities around it might be regulated under other regimes (e.g., e-money/payment services, financial promotions, or AML registration under the Money Laundering Regulations).

- Security tokens: Fall within the FCA perimeter if they possess the characteristics of specified investments.
- E-money tokens: Regulated under the Electronic Money Regulations if they meet the definition.
- Exchange/utility tokens: Generally not within the FCA's FSMA perimeter, although other regimes may still apply.

As a general guide, an in-game item that exists only within the game (i.e., it is non-transferable or only transferable within the closed ecosystem of the game) and confers consumptive gameplay utility will not be a specified investment. This remains true even if players speculate on the item's value.

An in-game item may be brought within the financial services perimeter under certain circumstances, including when the item:

- Confers profit share, dividends, or revenue participation from the studio/platform;
- Confers rights against a treasury/pool managed by others; or
- Confers tokenholder governance rights over a venture where others are doing the work.

These examples represent indicative situations where the UK analysis moves toward classification as shares/debt-like instruments or a collective investment scheme. Classification will be highly fact-dependent.

II. Commodity Classification

In the UK, "commodity" classification is mostly relevant in the context of commodity derivatives. A spot item (even if traded) is usually unregulated, regardless of an established trading market (e.g., gold or other precious metals).

Therefore, gaming items typically sit as:

- Unregulated goods/digital content, unless and until;
- Someone offers regulated financial instruments over them (derivatives), or the item itself embeds regulated rights.

III. Payments and E-Money Perimeter

Even if an item is not a specified investment, a gaming "currency" could theoretically face the risk of classification under the payments/e-money perimeter if it is used as a general means of payment or is redeemable.

However, where "gems" or other forms of in-game currency may only be used to buy in-game consumables from the issuer and cannot be redeemed or used with third parties, they benefit from a closed-loop exemption.

IV. Money Laundering Regulations (MLRs) Perimeter

A gaming asset could still be within the scope of the Money Laundering, Terrorist Financing (Information on the Payer) Regulations (2017) as amended (MLRs), even if it is not classified as a security or e-money token.

Under the MLRs, “cryptoasset” is broadly defined as a cryptographically secured digital representation of value or contractual rights that uses a form of DLT and can be transferred, stored, or traded electronically. If a gaming asset is a blockchain token/NFT, it can easily be a “cryptoasset” for AML purposes, even if it is not a security.

The key is whether an entity is acting by way of business to provide registrable cryptoasset services in the UK, such as:

- Cryptoasset exchange provider; and/or
- Custodian wallet provider (and certain other roles).

These are “relevant persons” under the MLRs and require FCA AML registration if operating in or from the UK.

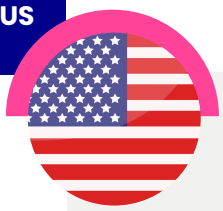
Practically, this means:

- A studio that merely issues an in-game item off-chain is often outside the MLR crypto perimeter; but
- A provider who runs a marketplace exchanging NFTs/tokens for fiat/crypto, or provides custody (hosted wallets / controls private keys) for users may be captured by the MLR regime.

The FCA explicitly requires firms providing in-scope crypto services to register and comply with AML/CTF obligations. This is highly fact-dependent, and firms should seek legal advice on this matter.

Author:
Konstantinos Adamos,
Revolut Group

US



Under United States law, most in game digital assets are not inherently classified as securities or commodities; they are usually treated as game items or licensed virtual property unless the way they are offered or traded satisfies securities or commodities law tests. The United States congress continues to develop new "market structure" legislation which, if enacted, may result in material changes to the existing requirements and guidelines applicable to both securities and commodities.

When in game items become "securities"

Whether a digital asset will be characterized as a security for purposes of the Securities Act of 1933 is determined in accordance with the now famous Howey Test. A transaction will be a sale of an "investment contract", and therefore of a "security" if the purchaser invests money in a common enterprise with a reasonable expectation of profits derived from the efforts of the issuer or promoter from whom they are purchasing.

In game assets (skins, tokens, land, NFTs, etc.) are more likely to be securities when:
• The developer or platform raises funds by selling them as an investment or "presale," emphasizing profit potential, price appreciation, or "staking"/yield.
• Purchasers rely on the game studio's ongoing managerial or entrepreneurial efforts (roadmaps, promised upgrades, monetization schemes) to increase the asset's market value.
• The primary use case is holding and trading, not playing, and there is a reasonably integrated secondary market structured and promoted by the issuer or affiliates (e.g., "buy this sword now, it will go up as our player base grows").

By contrast, ordinary game items typically are not securities where:
• They are sold for use in gameplay, with value tied to fun, status, or in game functionality rather than financial return.
• Any resale market is incidental, user driven, and not promoted as an investment opportunity by the issuer.
• There are no profit sharing rights, no revenue claims on the game or platform, and no profit expectation messaging from the issuer.

The Securities Exchange Commission recently provided "No Action" relief to two fungible token oriented enterprises, DoubleZero and Fuse Crypto Limited. Though neither of these involved an in-game-asset, they both established that where a token is primarily purchased for use or consumption that it will not be considered a security.

When in game assets look like "commodities"

Under the Commodity Exchange Act, pretty much anything can be considered a commodity. In game assets become relevant to the Commodity Futures Trading Commission when:

• They function as a generalized medium of exchange or store of value beyond a single game environment, particularly if they are tradable on off platform or DeFi style markets.
• Futures, options, swaps, or leveraged/retail margined transactions reference those game tokens or NFTs.

However:

• A closed loop game currency or item usable only in one game and redeemable solely for in game benefits is unlikely to be treated as a regulated commodity product by itself, absent a derivatives overlay.

In all cases, determining how to characterize an in-game-asset in any particular business model will be a facts and circumstances determination – meaning it will be dependent on the specific relevant particulars. It is important to remember that the in-game-assets purpose is a factor, but far from determinative as to how that asset, or the sale of that asset will be treated under US law. As always obtaining advice from qualified legal counsel knowledgeable on these matters is critical.

Author:
Josh Lawler,
Zuber Lawler

UY

In Uruguay, the legal characterization of digital assets used in video games follows a functional and economic approach, rather than a technology-driven classification.

The analysis focuses on what the asset represents in practice, how it is offered to users, and whether it performs an economically relevant role beyond the gaming environment. In the most common scenario, in-game assets are structured as licensed digital content granted under platform terms of service. Players do not acquire full ownership or autonomous proprietary rights, but rather a limited right of use subject to contractual conditions. While these assets remain confined to a closed ecosystem without fiat convertibility, institutionalized cash-out mechanisms, or use as a means of external payment or investment the applicable legal framework is primarily contract law, consumer protection, advertising standards, and data protection rules.

The regulatory threshold is typically crossed when an in-game asset acquires independent economic relevance outside the game. This occurs where assets are transferable beyond the platform, traded on secondary markets, or capable of being monetized through cash-out mechanisms or exchanges with cryptoassets or stablecoins. At this stage, the focus of the Central Bank of Uruguay (BCU) shifts from the asset itself to the services provided on a professional and ongoing basis around such assets, including purchase and sale, exchange, custody, and transfer on behalf of users.

Law No. 20,345 empowers the BCU to regulate providers of services related to virtual assets, adopting a risk-based and activity-oriented approach consistent with FATF standards. The BCU's evolving framework distinguishes between financial and non-financial virtual assets, with the latter capturing most gaming-related NFTs, such as virtual land or unique in-game collectibles, which do not by themselves grant rights to repayment, yield, or profit participation. These assets typically fall outside the strict perimeter of financial regulation. However, where token design, marketing, or economic mechanics resemble investment instruments such as through promises of returns, revenue-sharing, buy-back schemes, or value appreciation driven by the efforts of the issuer; the likelihood of regulatory scrutiny increases. Even where the asset itself remains non-financial, intermediaries facilitating its professional trading may still be subject to registration, AML, and compliance obligations.

In short, in Uruguay, in-game assets are not regulated merely because they are tokenized or blockchain-based. Regulation is triggered when their functionality, transferability, and monetization cause them to operate, in practice, as economically relevant assets circulating beyond a purely recreational environment.

Author:
Paulina Cedrola,
SYLS Ferrari

02 THE GAMBLING THRESHOLD

WHEN DOES BLOCKCHAIN GAMING QUALIFY AS GAMBLING?

The end of the "loot box loophole."

The Current State: By 2026, the "casino-fication" of gaming has reached a breaking point. Significant jurisdictions have established stricter boundaries: where randomized digital items like gacha systems or loot boxes possess secondary market value, they increasingly fall under gambling scrutiny or outright bans for minors. The "grey market" of third-party skin wagering sites is facing unprecedented enforcement, shifting the burden of responsibility directly onto studios for every "roll of the dice" within their code.

This Chapter explores the transition to provably fair standards. In 2026, transparency is no longer a "nice to have", it is a core legal defence. We examine how "safety-by-design" is being used to prevent psychological exploitation, moving from predatory "dark patterns" to sustainable, transparent economies where player protection is a primary metric of success.

02 THE GAMBLING THRESHOLD

AR

Argentina does not have a general regulation of gambling, but rather, each Argentine province and the City of Buenos Aires regulate gambling within its jurisdiction. The offering of gambling is subject to prior license in each jurisdiction.

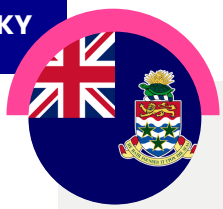
For example, in the City of Buenos Aires gambling is any game of chance, skill or betting, in which in order to obtain a prize, money or economically valuable assets that can be transferred among the participants are committed, subject to the occurrence of an uncertain result, regardless of whether there is a predominance of skill or chance. This approach is followed by other jurisdictions, such as the Province of Buenos Aires.

Based on the above, if the player is required to put money or a transferable game item at stake in order to obtain a prize, the game mechanic could be classified as gambling, regardless of whether the result depends on the player's skill or on chance.

The enforcement has been focused on traditional gambling applications such as online casinos, sports betting or lotteries. There are no local precedents involving video game mechanics such as loot boxes.

Author: **Juan Manuel Campos Álvarez,** SYLS

KY



The Cayman Islands has very strict anti-gambling laws, and gambling is effectively banned on the islands, including on cruise ships within Cayman territorial water. The Gambling Law (2016 Revision)[1] bans most form of commercial gambling, with very limited charitable exemptions. Under the Gambling Law, 'gambling' is defined very broadly:

to play at any game, whether of skill or chance, for money or money's worth

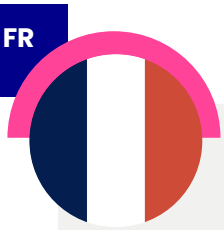
Read at it's most broad, any game which rewards players with in-game currency or items which could be cashed in at any time would qualify as gambling. However the law does not seem to have been enforced in this way with a somewhat more practical approach taken, but in 2019 there was a very visible application to non-blockchain gaming when Rockstar was required to block Cayman Islands players from accessing the in-game virtual casino in GTA V. That in-game casino permitted players to buy chips with fiat[2] currency, play with the chips and cash in any winnings for in-game items, not fiat currency. GTA V players remain free, of course, to plan and execute a heist of the virtual casino's vault.

(1) https://legislation.gov.ky/cms/images/LEGISLATION/PRINCIPAL/1964/1964-0060/1964-0060_2016%20Revision.pdf
(2) https://esports-news.co.uk/2019/08/26/countries-that-have-banned-the-new-gta-casino-and-why/

As the line blurs in many offerings between what is traditional gambling and gaming, and offerings such as prediction markets similarly seek to remain outside the scope of gambling legislation, a greater focus by regulators on how a game is presented to users and what practically is occurring in-game is likely to increase.

Authors: **Michael Bacina & Jonathan Turnham,** NXT Law

FR



Under French law, a blockchain-based game may qualify as gambling (jeu d'argent et de hasard) if it cumulatively meets the four statutory criteria defining prohibited lotteries and gambling activities.

First, the game must be offered to the public, including online. This condition is broadly construed and is generally met where the game is accessible via a website or digital platform.

Second, the player must incur a financial sacrifice, meaning that participation requires the payment of money or assets with monetary value (such as fiat currency, crypto-assets, or paid in-game credits).

Third, the game must involve an element of chance, even if randomness is not the sole or predominant factor. Any mechanism based on randomised rewards (e.g. loot boxes or random NFTs) typically satisfies this criterion.

Fourth, and most decisively, the game must generate an expectation of gain. According to the French gambling regulator (ANJ, formerly ARJEL), this condition is met only where the rewards can be monetised, whether on the operator's platform or through third-party marketplaces that are permitted or tolerated.

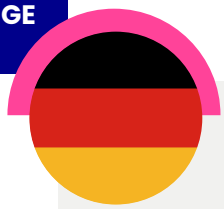
These criteria are strictly cumulative. The absence of any single criterion is sufficient to exclude the gambling qualification. In practice, regulatory risk can often be mitigated by excluding the French market (geo-blocking and no promotion in France), removing the financial sacrifice (free participation), or eliminating the expectation of gain (non-transferable and non-monetisable NFTs or tokens).

The sanction risk is significant, as gambling prohibitions are criminal in nature, the sector is heavily regulated, and the ANJ actively enforces the rules, including by blocking foreign websites and prosecuting promoters of illegal gambling activities.

Finally, France has introduced a dedicated framework for innovative digital games, the JONUM regime, which establishes a specific and lighter regulatory regime for certain Web3-based gaming models, allowing operators to achieve compliance within a proportionate legal framework

Authors: **William O'Rorke & Imane Dahmani,** ORWL, Paris

GE



The Intersection of Blockchain Gaming and German Gambling Law (GlüStV, StGB, and BGB)

In the current digital economy of 2026, the convergence of "Play-to-Earn" (P2E) models and Decentralized Finance (DeFi) has created a significant challenge for German jurisprudence. For legislators and academics, the primary task is to distinguish between legitimate gaming activities and prohibited gambling under the State Treaty on Gambling 2021 (GlüStV 2021), the German Civil Code (BGB) and the German Criminal Code (StGB).

1. The Statutory Definition of Gambling
In Germany, gambling is clearly defined and regulated. Under Section 3 (1) of German Gambling Law of 2021 (the "GlüStV 2021"), a game is classified as "gambling" if three cumulative criteria are met:

- Consideration (Stake): The player provides a contribution of monetary value.
- Chance: The outcome depends entirely or predominantly on luck/chance.
- Prize: There is a prospect of obtaining a gain of monetary value.

2. Monetary Value and the Civil Law Context (BGB)
A critical shift in the regulatory assessment of blockchain gaming involves the nature of the "prize." Unlike traditional virtual gold, digital assets or in-game-token and NFTs are recognized as "other objects" (as such a monetary value) within the meaning of Section 453 (1) Alt. 2 of the German Civil Code (BGB).

Because these assets are fungible and tradable on secondary markets for fiat currency (Euro), they possess an objective market value. Consequently, the use of such tokens as a "stake" constitutes an economic sacrifice, and their receipt as a "reward" constitutes a financial gain. This satisfies the "consideration" and "prize" limbs of the gambling definition.

3. The Dominance Principle: Skill-Gaming vs. Gambling
The distinction between a gaming or an online-gamer (which qualifies in Germany as a service contract governed by the BGB) and prohibited gambling depends on the

Dominance Principle:

- Skill-Gaming: If the outcome is determined by more than 50% through the player's cognitive or physical abilities, it is generally considered a legal game of skill.
- Gambling: If the mechanical or algorithmic chance (e.g., On-Chain Random Number Generation via Oracles like Chainlink VRF) outweighs the player's skill, the game is subject to the GlüStV 2021.

Operating such a game without a license from the Joint Gambling Authority of the German States (GGL) is prohibited under Section 4 (1) GlüStV 2021 and constitutes a criminal offense under Section 284 StGB (unauthorized organization of gambling).

4. Specific Risk Categories in Blockchain Gaming

A. Loot Boxes and Random Minting

The "minting" process, where a user pays a fixed fee to receive an NFT with randomized attributes (Rarity), is under intense scrutiny. If the NFT can be immediately liquidated on marketplaces (e.g., OpenSea), the transaction resembles a lottery. The GlüStV 2021 has indicated that "gamblification" elements—specifically those offering a chance to "win" a high-value asset for a low-value stake—are likely to be classified as gambling.

B. Betting Character under Section 762 BGB

Mechanisms where players "stake" tokens to bet on the outcome of an event (even an in-game event) may be classified as a wager (Wette). Under Section 762 of the BGB, a wager is a "non-binding obligation" (Naturalobligation). This means that while the bet is not illegal per se, the "winner" has no enforceable legal claim in a German court to compel the "loser" to pay out, unless the bet is part of a licensed gambling operation.

5. Regulatory Guidance

The GlüStV 2021 has clarified that the presence of a "cash-out" function or a vibrant secondary market is a decisive indicator of gambling. In 2026, the German authority actively monitors DLT-based platforms to ensure that "Play-to-Earn" models do not bypass player protection laws (e.g., deposit limits, social concepts).

Furthermore, BaFin (The Federal Financial Supervisory Authority) notes that if an activity is classified as prohibited gambling, any associated financial service (such as crypto-custody or exchange) cannot be licensed under MiCAR (cf. Topic 1 above), as the underlying business model violates public order (ordre public).

6. Summary for Policy Makers and Academics

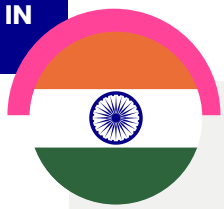
The legal classification of a blockchain game follows the principle of functional equivalence. If a token has a market price, any game mechanism based on chance that requires the use of that token enters the sphere of gambling law.

For a regulatory framework to be effective in 2026, it must differentiate between:

- Interactive Entertainment: Skill-based, no chance-based monetary gain.
- Regulated Financial Products: Tokens classified as securities (MiFID), e-money or utility/currency tokens under MiCAR.
- Prohibited Gambling: Games where chance-based distribution of valuable DLT-assets serves as the primary incentive.

Author: **Alireza Siadat,** Deloitte Legal

IN



India has no specific laws for blockchain-based gaming. Blockchain is merely the underlying technology. What matters legally isn't the technology, but whether the game itself constitutes gambling.

For decades, Indian courts distinguished between games of skill and games of chance. Skill-based games enjoy constitutional protection; games of chance do not. But in August 2025, the Parliament upended this framework by passing the Promotion and Regulation of Online Gaming Act, 2025 ("Act"), which bans all online money gaming regardless of skill.

While the Act has not been formally notified into force, the government is actively enforcing the Act's provisions administratively. Over 7,800 gambling websites have been blocked since August 2025. The Supreme Court observed recently that the entire gaming industry is in a state of suspension as most real money gaming operators have paused operations pending judicial clarity.

The Act prohibits all "online money games", defined as any online game, involving skill, chance, or both, where players pay fees, deposit money, or "other stakes" expecting to win monetary or other enrichment. Critically, "other stakes" includes "anything equivalent or convertible to money, including virtual coins and tokens". Cryptocurrencies and NFTs are convertible to fiat through exchanges, making them "stakes." This language captures blockchain gaming squarely.

The Act's emphasis on the "expectation of winning which entails monetary and other enrichment" underscores that the legislative focus is not on the form of consideration paid or rewards received, but rather on the economic substance of the transaction. The fact that such conversions occur on blockchain infrastructure rather than through traditional banking channels is immaterial under the Act's technology-neutral language.

Most play-to-earn blockchain games operating in India face direct conflict with the Act's prohibitory framework. What matters is the monetisation model: if participation requires payment in any form equivalent or convertible to money, and if players expect to receive rewards that can be liquidated, the game constitutes an "online money game" under the Act, irrespective of the skill involved.

Multiple High Courts entertained challenges on grounds of legislative competence (gambling is a State subject the Constitution and violation of fundamental rights (Articles 14, 19(1)(g)). The Supreme Court consolidated all challenges on September 8, 2025 and deferred hearings to January 2026.

Key Takeaways:

- No court has ruled specifically on blockchain gaming as gambling, but the laws relating to gaming and gambling would apply to blockchain gaming as well;
- The Act, while not formally notified, is being enforced administratively. If fully implemented, it would prohibit most play-to-earn models regardless of skill;

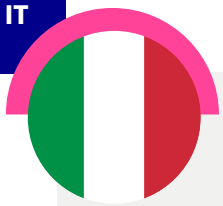
- In the meanwhile, operators should ensure VDA taxation and AML compliance (including FIU-IND registration), and monitor Supreme Court proceedings on the Act's validity; and

- Operators can consider restructuring monetisation models away from "stakes and winnings" terminology or repositioning as competitive e-sports platforms that avoid direct fiat conversion.

Ultimately, blockchain gaming's legal status in India depends not on the technology itself, but on whether the game constitutes an "online money game" under the Act. Until the Supreme Court rules on the Act's constitutional validity, operators may have to navigate administrative enforcement without formal legal clarity.

Author:
Priya Makhijani,
Zeroto3 Collective

IT



In Italy, the line between "gaming" (playful activity) and "gambling" (gioco d'azzardo) is strictly defined by both the Criminal Code and specialized administrative regulations managed by the State.

Under Italian law, an online activity is considered gambling when it satisfies two cumulative criteria: the presence of a wager and the dominance of chance.

1. The Legal Definition (The "Chance + Stake" Rule)
According to Articles 718-722 of the Italian Criminal Code, a game is classified as gambling if:

- The "Purpose of Gain": Participants stake money or other assets with economic value (the scopo di lucro).

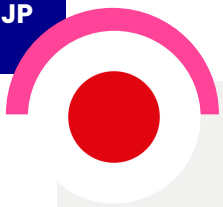
- The "Element of Luck": The outcome depends entirely or predominantly on chance rather than the player's skill or ability.

If both elements exist, the activity is considered gambling and is prohibited unless specifically authorized by the State.

2. The Role of the ADM (State Monopoly)
In Italy, gambling is a State monopoly. For an online game to be legally offered and not considered "illegal gambling," the operator must hold a specific concession (license) issued by the ADM (Agenzia delle Dogane e dei Monopoli).

Author: **Paolo Maria Gangi,** Gangi Law Firm

JP



Gambling prohibition in Japan derives from Part II, Chapter 23 of the Penal Code, which defines gambling as "an act where more than two persons bet on an outcome of a contest of chance to contend for a prize in the form of property or asset," punishable by fines up to JPY 500,000.

The Penal Code also imposes imprisonment of up to three years for habitual gambling and three to five years for operating gambling establishments for profit.

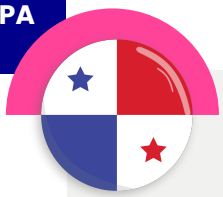
For an activity to be classified as gambling, three elements must be met: consideration (payment), chance, and prize. The Penal Code provides a narrow exception for betting items "provided for momentary entertainment", but Supreme Court precedent holds that cash, regardless of amount, never qualifies as momentary entertainment. Digital assets convertible to fiat currencies therefore receive heightened scrutiny.

"Gacha" systems have been subject to extensive regulatory scrutiny. While not directly criminalized as gambling, certain gacha implementations trigger consumer protection concerns. In 2012, the Consumer Affairs Agency banned "complete gacha" (kompu gacha) —systems requiring players to collect multiple random items for a reward—under the Act against Unjustifiable Premiums and Misleading Representations. The Computer Entertainment Supplier's Association (CESA) has issued self-regulatory guidelines, requiring probability disclosure and spending limits for gacha mechanisms.

For play-to-earn games, the critical question is how rewards are funded. Under prevailing interpretation of the Penal Code, if prize money derives from participant entry fees, the arrangement likely constitutes gambling. However, if prizes are funded solely by third-party sponsors, the activity generally remains lawful. Regulatory risk increases materially where rewards can be exchanged for any fiat currency or crypto asset with market value. Studios should ensure that rewards are funded by sponsors or operators rather than pooled player contributions, and should disclose probabilities for all randomized mechanics.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

PA



Gambling and betting in Panama are mainly regulated under Decree Law No. 2 of 1998 and the rules issued by Panama's Gaming Control Board or Junta de Control de Juegos ("JCJ"), including Resolution 11 of 2020 governing internet-based gaming and wagering.

These rules focus on activities that involve games of chance or betting and that are operated in or from Panama, or offered to players located in the country. The framework is geared toward traditional casino-style games and sports wagering, with particular attention to the "capture of bets," the presence of an operator, and the role of chance in determining outcomes.

Blockchain gaming adds complexity to this analysis because many decentralized or play-to-earn mechanics blur the line between wagering and skill-based competition. According to the attached legal opinion, Panama's regulators look primarily at three elements: (i) whether value is staked, (ii) whether outcomes are determined predominantly by chance rather than skill, and (iii) whether there is an identifiable operator acting as bookmaker, house, or betting intermediary

In Panama, blockchain gaming does not become "gambling" merely because it uses crypto, NFTs, or smart contracts, in general blockchain related developments.

The key question is whether, in substance, the activity fits the legal concept of a game of luck or chance (juego de suerte o azar) or an activity that originates bets, as applied by the Junta de Control de Juegos (JCJ) under Decree Law No. 2 of 1998 and its implementing framework. If the JCJ concludes the product is essentially wagering or chance-based gaming for value, it can fall within its regulatory competence regardless of branding.

A blockchain game is most likely to qualify as gambling when chance materially determines the outcome. Under Panamanian concepts, a game of luck or chance exists where the awarding of prizes depends totally or partially on chance, rather than predominantly on the player's knowledge, judgment, strategy, or performance. In practice, this captures mechanics such as randomized loot boxes, gacha-style draws, roulette/spin features, mystery packs, or any RNG/oracle-driven reward system, especially when the randomness is central to who wins and what is won.

A second core element is the presence of a wager or economic stake. In blockchain ecosystems, the "stake" can be more than fiat: it may include entry fees paid in tokens, staking mechanics, paid "mints," or the commitment of NFTs or other transferable assets. If players are risking value on an uncertain result whether the uncertainty comes from chance, outcomes of matches, or other contingencies, the activity begins to resemble betting.

Third, there is a heightened risk when the game offers a prize of value, not merely cosmetic points. Tokens, NFTs, or in-game assets can function as "prizes" if they have market value, can be traded, or can be cashed out. Even if rewards are "in kind," they may still be treated as valuable consideration when a secondary market or redemption path exists.

Importantly, a blockchain game can qualify even when it is skill-forward if it constitutes an activity that originates bets, meaning the wagering component is the ordinary object or main basis of participation. Examples include platforms that facilitate user-vs-user staking, pooled entry fees where winners take the pot, prediction-style contests, or systems where the operator's role resembles a house or betting intermediary.

Finally, jurisdiction matters. Under the JCJ's territorial and accessibility approach, reflected in Resolution No. 65 of 2002 as amended by Resolution No. 11 of 2020, electronic games of chance may be regulated when conducted in or from Panama, accessible in Panama, or directed to users located in Panama, even if servers or infrastructure are abroad. In assessing applicability, the JCJ tends to apply a substance-over-form analysis focused on (i) degree of chance, (ii) wagers/prizes, (iii) operator role, and (iv) Panama nexus.

Limiting or eliminating randomness tied to value, removing paid entry linked to uncertain outcomes, and ensuring rewards are non-transferable, non-redeemable, and not cash-outable could limit the jurisdiction of the JCJ on certain gaming mechanics and product features that might otherwise be characterized as games of chance or bet-originating activities, provided the overall structure does not involve wagers or prizes of economic value and is not marketed or operated as a betting product.

Authors: **Teresa Carballo & Edgar Young,** Pacifica Legal

SG

Preliminarily, gambling activities in Singapore are prohibited unless they are exempted or licensed under the law, such as under the Gambling Control Act 2022 (the "GCA") and the Gambling Control (General) Regulations 2022 (the "GCR").

Under the GCA, in-game digital assets may also be subject to regulation, as they may be deemed to be a "money equivalent" prize (as defined in section 14 of the GCA). Singapore provides a class licence regime, which is subject to certain conditions as set out in the Gambling Control (Remote Games of Chance - Class Licence) Order 2022 (the "Remote Games of Chance").

For completeness, loot boxes will likely be considered a lottery if the digital assets can be monetised in the real-world. Singapore has also taken a hardline stance, prohibiting certain games of chance, such as "online games of chance that allow players to use virtual items as a form of stake on casino games or match outcomes, such as skin-betting sites".

Authors: **Grace Chong & Bryan Ong** Drew and Napier LLC

KR

South Korea takes one of the most restrictive approaches globally toward blockchain gaming. Play-to-earn games face significant practical barriers to domestic distribution, largely due to the Game Rating and Administration

Legal Framework and Historical Context

Three statutes in South Korea are relevant to gambling analysis in gaming. The Criminal Code prohibits unlawful gambling and imposes fines or imprisonment for violations, with enhanced penalties for habitual gambling. The Game Industry Promotion Act (GIPA) prohibits games offering "gifts" or rewards convertible to real-world value as speculative. The Act on Special Cases Concerning Regulation and Punishment of Speculative Acts prohibits operating speculative businesses without authorization, with enforcement focusing on operators rather than individual players—a distinction relevant for foreign studios structuring products accessible to Korean users.

The Korean Supreme Court defines "gambling" as achieving monetary gain or loss through wagering property on chance-determined outcomes. Under the GIPA, a "speculative game" is one that involves betting, allotment, or chance-determined outcomes and causes monetary gain or loss.

The GIPA's prohibition on converting in-game results to real-world value originated in the 2007 amendments following the "Sea Story" gambling scandal, which was specifically designed to prevent games from becoming gambling vehicles by criminalizing as a business activity the conversion of in-game results to real-world value. The Enforcement Decree defines covered "game money" broadly to include points, scores, virtual currencies, and similar intangible results obtained through gameplay.

Current Regulatory Practice

All games distributed in South Korea must obtain age ratings from the Game Rating and Administration Committee. Distribution without ratings is punishable by imprisonment up to five years. The Committee has consistently refused to rate play-to-earn and blockchain games, reasoning that blockchain technology makes it easier to exchange in-game assets externally.

In 2023, the Seoul Administrative Court upheld the Committee's revocation of the rating for "Five Stars for Klaytn," holding that NFT items constituted prohibited "gifts" and that the combination of paid transactions and random structures was too close to gambling mechanisms. This administrative barrier—while not a statutory ban—effectively blocks domestic distribution of play-to-earn games in South Korea.

Proposed Reforms

A comprehensive amendment bill to the GIPA—to be renamed the "Act on the Promotion of Game Culture and Industry"—was introduced to the National Assembly on September 24, 2025. The bill would rationalize prize regulations by restricting the prize provision prohibition to location-based (arcade) game operators only, meaning online games would no longer be subject to the blanket prohibition that has historically been interpreted by courts as barring any prize provision. This change may open a pathway for play-to-earn games, as courts have previously relied primarily on the prize provision prohibition clause to reject appeals against denied play-to-earn game ratings.

However, even if the comprehensive amendment passes, play-to-earn gaming may not be fully legalized. The bill maintains a prohibition on the business of currency exchange under proposed Article 26(1)(7), which prohibits anyone from making a business of converting game results—including game money, scores, premiums, and virtual currencies—into cash, or intermediating or facilitating such conversions.

Practical Considerations for Studios

Amendments to the GIPA now require mandatory disclosure of loot-box probabilities, with subsequent amendments introducing punitive damages and shifting the burden of proof to game providers in loot-box disputes. Foreign game companies without a Korean domicile must designate a domestic agent if they meet specified scale thresholds (KRW 1 trillion global sales, 1,000 average daily Korean installations, or involvement in serious incidents disrupting the game distribution market with reporting requested by the Ministry of Culture, Sports and Tourism).

The domestic agent bears responsibility for discharging the foreign provider's statutory obligations under the GIPA and the PIPA, including submission of reports to authorities and compliance with labeling and disclosure requirements for game products, such as ratings, content descriptors, and loot-box probability information. Crucially, GIPA violations committed by the domestic agent in performing these functions are imputed directly to the foreign provider. Failure to designate a required local agent exposes providers to administrative fines of up to KRW 20 million per year.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

ES

In Spain, the starting point is that blockchain is legally neutral: a game only becomes "gambling" if it fits the generic definition of juego de azar in Law 13/2011, regardless of whether it runs on-chain or off chain.

Article 3 of Law 13/2011 defines juego as any activity where players (i) risk money or other economically valuable items, (ii) on future, uncertain results that depend at least partly on chance, and (iii) where prizes can be transferred between participants. The DGOJ has distilled this into three cumulative elements for the law to apply: payment to participate, randomness in determining the result, and a prize that is transferred to the winning participant. If those conditions are met and the activity targets Spain on a state wide basis, it is gambling and requires a licence; any non regulated modality is directly prohibited.

From the perspective of Law 13/2011 it is irrelevant whether the value involved is euros, in game currency, fungible tokens or NFTs: as soon as the asset is economically valuable and transferable, it will typically qualify as an "objeto económicamente evaluable". Accordingly, a Web3 game that requires players to pay in cryptoassets or game tokens to access randomised mechanics and offers tradable tokens or NFTs as rewards can still fall squarely under the Spanish definition of gambling, provided the cumulative elements of payment, chance and prize are met.

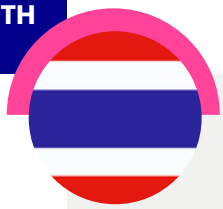
Loot boxes are the natural bridge between "classic" gambling and Web3. In its 2021–22 consultation on mecanismos aleatorios de recompensa, the DGOJ explicitly applied Law 13/2011 to loot boxes whose operation, from design to actual use, meets the statutory concept of game of chance. It then spelt out three parameters for when a loot box becomes gambling: (1) paid activation (the box must be purchased or opened for consideration, distinct from the base game), (2) random allocation of contents (the reward is future, uncertain and depends on chance), and (3) a prize that is economically evaluable and monetisable, meaning there are mechanisms inside or outside the game to convert the virtual reward into legal tender. Whether the reward is cosmetic or gives competitive advantage is irrelevant if it can ultimately be monetised.

Web3 design tends to intensify this third limb. Open secondary markets for tokens and NFTs, on chain trading and P2P swaps make it much easier to show that rewards are economically valuable and transferable in practice. A blockchain game that sells loot crates for crypto, allocates randomised NFT or token rewards, and allows or tolerates secondary trading will often satisfy the Spanish definition of gambling, even if the developer never labels it as such.

In parallel, the (still pending) Organic Law on the protection of minors in digital environments introduces a dedicated regime for mecanismos aleatorios de recompensa: it proposes a general ban on minors accessing or activating mechanisms that involve payment, chance and rewards that can be exchanged for money or other virtual objects, precisely because of their similarity to regulated gambling products. This reinforces the direction of travel: in Spain, Web3 loot boxes with tradable rewards are treated as functionally close to gambling, even where a bespoke minors protection regime is layered on top of or alongside Law 13/2011.

Authors:
Gonzalo Cantero Puig & Marina Villalonga Cladera,
Asensi Abogados

TH



Thailand maintains one of the most restrictive gambling regimes in the region, primarily governed by the Gambling Act B.E. 2478 (1935). The Act broadly prohibits "gaming for stakes," subject to limited statutory exceptions, and enforcement remains active despite the law's age.

Under Thai law, gambling is generally understood to involve three core elements:

1. Consideration, where the player provides money, property, or something of value to participate;
2. Chance, where the outcome is determined wholly or predominantly by chance rather than skill; and
3. Prizes, where the player stands to win money, property, or something of value.

Blockchain games may raise gambling concerns where tokenised mechanics replicate these elements. Examples include loot boxes with real-world value, chance-based NFT minting with secondary market liquidity, or wagering tokens on uncertain in-game outcomes.

Thai authorities do not recognise a formal distinction between "gaming" and "gambling" akin to that found in some common law jurisdictions. As a result, the presence of skill does not automatically exempt a game from being classified as gambling, particularly where chance materially influences outcomes and prizes have transferable economic value.

Where blockchain gaming assets can be converted into fiat currency or traded for other assets of value, regulators may view them as "property" for gambling law purposes. This risk is heightened when:

- players pay to participate using cryptocurrencies or stablecoins;
- rewards are NFTs or tokens with liquid secondary markets; or
- gameplay resembles lotteries, raffles, or betting mechanisms.

Notably, Thai law does not require the operator to characterise the activity as gambling for liability to arise. The substance of the mechanics is determinative. Even offshore platforms may face legal risk if Thai players can access the game and participate in gambling-like activities from within Thailand.

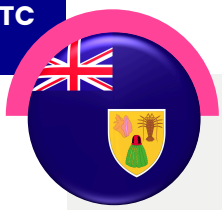
To date, there is no published guidance specifically addressing blockchain gaming under the Gambling Act. However, given Thailand's historically conservative stance, studios typically mitigate risk by:

- avoiding chance-based monetisation tied to real-world value;
- ensuring rewards are non-redeemable and non-transferable; or
- restricting access by Thai users where gambling risk cannot be mitigated.

Until legislative reform occurs, blockchain gaming projects operating in or targeting Thailand must carefully assess gambling exposure under existing law.

Author: **Dr. Jason Corbett,** Silk Legal

TC



The Turks and Caicos Islands (TCI), a British Overseas Territory, with its own constitution and a unicameral legislature currently does not have a dedicated regulatory framework specifically addressing blockchain gaming or the broader use of blockchain technology within the gaming sector.

Regulation of gambling and gaming activities falls under the Gambling Act and the Gaming Machines Act, which were not designed with digital assets or blockchain-based platforms in mind. As a result, there is significant legal uncertainty regarding how existing rules apply to blockchain-based games, particularly those involving tokens or cryptocurrencies.

There is a draft proposal for legislation covering Virtual Asset Service Providers (VASPs) which it is hoped would include Blockchain gaming and be a platform to develop such businesses in the TCI.

Key legal uncertainties and risk areas include the classification of in-game tokens or cryptocurrencies - whether they are considered as "money" or "prizes" under local law and whether certain blockchain gaming models could inadvertently fall within the scope of gambling or lottery regulations. There is also ambiguity around anti-money laundering (AML) and know-your-customer (KYC) obligations, as current statutes may not clearly address the unique features of blockchain transactions or anonymous participation.

For blockchain gaming companies considering TCI as a base or market, practical takeaways include:

(1) seeking local legal advice to assess whether your platform's activities might be captured under existing gaming or financial services laws
(2) developing robust AML/KYC procedures in anticipation of regulatory scrutiny
(3) monitoring ongoing developments, as the government may introduce specific legislation or guidance as the sector evolves, and
(4) if regulatory clarity is a primary concern consider alternative jurisdictions with more established blockchain and gaming frameworks.

Author:
Andrew Robert Mitchell KC,
FGA Law Providenciales, DM Legal Consultants RAK, UAE. 33CL Law London

AE

Under UAE federal law, gambling is a regulated activity. In Federal Decree Law No. 31 of 2021 (the UAE Penal Code), games of chance, in which profit is contingent on chance and stakes involve money or anything of monetary value, is prohibited unless conducted under specific authorisation.

The General Commercial Gaming Regulatory Authority (GCGRA), established in 2023, has exclusive jurisdiction to license and regulate commercial gaming activities in the UAE, including internet-based games such skill-based or chance-related contests. The GCGRA's remit is limited to UAE jurisdictions and does not extend internationally.
Accordingly, for a blockchain game to be classified as gambling under UAE law, it generally must meet all three of the following criteria:

1. Consideration - The player must provide something of value to participate. If a player must "pay to play," this element is satisfied (this can include fiat currency or virtual assets)
2. Chance - The outcome is determined predominantly by luck rather than skill. If the game utilizes a Random Number Generator, such as opening a "loot box," spinning a wheel, or an automated battle simulator where the player has no active control, it is likely classified as a game of chance.
3. Prize - The player receives something of value ((this can include fiat currency or virtual assets).

Blockchain gaming qualifies as gambling and would be subject to GCGRA rules when you combine these elements. A strict "Play-to-Earn" (P2E) model often falls within the scope of gambling, whereas "skill-based gaming", where the outcome depends on the player's ability, strategy, or knowledge (e.g., poker, shooter or racing game), historically falls outside the definition of gambling, provided the element of chance is negligible.

Importantly, the legal definition of "money" in this context is technologically neutral. It extends to cryptocurrency, tokens, or NFTs if they can be purchased, exchanged, or converted into monetary value. Therefore, a blockchain poker game where players wager "utility tokens" to win a pot formed by other players' tokens would be treated the same as wagering fiat currency.

Author: **Chris Elias,** Moto Legal

UK

In the United Kingdom, regulated gambling is regulated by the Gambling Commission. To date, as far as the author is aware, no firm has successfully become licenced by the Gambling Commission for gambling activities in relation to cryptoasssets or blockchain, and the regulator is generally considered as taking a very cautious approach to the industry.

As such, it is generally important for firms approaching the UK market to seek to fall outside of gambling, in the sense of being a regulated activity. The delineation of whether activity is/is not regulated gambling is determined by whether it falls within the definition of gambling as set out in the Gambling Act 2005. This defines gambling as being activity which is one of “gaming”, “betting” or “participating in a lottery”. The definition of these activities are complex, and so it is important to consider each in depth before making a determination, however in this chapter we consider the relevant activities at a very simplified, high level to give an idea of the types of activities that can be an issue, and some of the common themes we see in the context of blockchain gaming.

The starting point for a gambling analysis is generally to consider the definition of each of the types of regulated gambling that exist.

Gaming

Gaming is defined in terms of playing a game of chance for a prize. A game of chance includes:

1. a game that involves both an element of chance and an element of skill,
2. a game that involves an element of chance that can be eliminated by superlative skill, and
3. a game that is presented as involving an element of chance,

but does not include a sport, for a prize. A prize in relation to gaming (except in the context of a gaming machine) is refined as referring to money or money's worth.

It is not always clear whether there is regulated gaming. For example, whilst poker does involve skill, it is generally classified as regulated gaming.

A particular issue for gaming here has been whether in-game loot boxes should be regulated as gambling. Currently, loot boxes are not regulated as gambling due to a technical distinction in how gambling is defined in the legislation. In particular, the Gambling Act 2005 requires that for an activity to constitute gambling, prizes must be "money or money's worth".

The Gambling Commission has consistently held that in-game items obtained from loot boxes do not meet this threshold because they typically cannot be officially cashed out or converted into real money through the game operator. Even though secondary markets exist where players may trade or sell virtual items for real currency, these transactions occur outside the game's official ecosystem and are often against the terms of service. Consequently, the Gambling Commission has maintained that loot boxes fall outside the scope of gambling regulation, despite acknowledging the structural and psychological similarities between loot boxes and traditional gambling products.

However, this position has faced significant criticism and there is an ongoing debate about whether the legislation should be updated to reflect modern gaming practices and the convergence between gaming and gambling. Until such reforms are enacted, loot boxes remain in a regulatory grey area: widely recognised as gambling-like in nature, but not formally regulated as such under current UK law.

Betting

Betting is defined as making or accepting a bet on:

1. the outcome of a race, competition or other event or process,
2. the likelihood of anything occurring or not occurring, or
3. whether anything is or is not true.

It is irrelevant for these purposes whether the thing being bet on has already occurred, or whether one party to the transaction already knows the outcome being bet on.

Lottery

A lottery is a regulated lottery if either:

1. persons are required to pay in order to participate in the arrangement,
2. in the course of the arrangement one or more prizes are allocated to one or more members of a class, and
3. either the prizes are allocated by a process which relies wholly on chance, or the prizes are allocated by a series of processes, and the first of those processes relies wholly on chance.

A key consideration here is the payment requirement, and it is common therefore for lotteries to incorporate a free route of entry as an alternative to the paid route, deliberately so as to fall outside the definition of regulated gambling.

Because of this, there are detailed rules setting out what, in fact, should be considered “free”, and for example makes clear that payment does not necessarily require payment be in fiat, that it is immaterial who receives the benefit of the payment, and that for example increasing the cost of communicating a desire to participate in the lottery or requiring payment to take possession of a prize will generally mean that the competition falls within the scope of being a regulated lottery.

Taking things to the next level

The UK approach to determining whether gambling exists is similar to that in many other jurisdictions, and in that respect we have found that firms looking to incorporate an element of chance similar to approaches that work on other jurisdictions often can operate outside of regulated gambling as defined in the UK. The bigger issue for such firms is, where the prize or the cost of participating in gambling consist of tokens that are fungible and transferrable, whether there is a financial promotion capable of having an effect in the United Kingdom, which is a separate issue to gambling.

Author:
James Burnie FRSA,
Gunnercooke LLP

UY

Blockchain gaming may qualify as gambling under Uruguayan law when three core elements converge: (i) the player provides a stake or other form of economic consideration, (ii) chance predominates over skill in determining the outcome, and (iii) the game offers prizes with economically realizable value. This assessment is substance-based and applies regardless of whether the game uses fiat currency, cryptoassets, or tokenized in-game items.

Where a game is structured as a closed-loop system—meaning rewards cannot be redeemed for money, traded externally, or converted into assets with real-world value it is generally characterized as entertainment rather than gambling. The absence of a realizable economic incentive is a key factor in excluding the application of gambling regulations.

Regulatory risk increases significantly when blockchain games introduce cash-out mechanisms, enable routine trading of in-game assets on external markets, or allow tokens and NFTs to function as a bridge to third-party betting or wagering platforms. In such cases, even if the game is marketed as entertainment, its economic structure may effectively replicate a wagering activity. This risk is heightened where participation requires an upfront economic contribution and outcomes are determined predominantly by chance.

In Uruguay, gambling and betting activities are subject to prior state authorization and operate within a tightly controlled legal framework. As a result, blockchain gaming models that combine chance-based mechanics with monetizable rewards may face material enforcement and compliance risks if offered without the appropriate authorization. Additionally, where the platform itself facilitates the inflow or outflow of value related to betting activities, ancillary regulatory obligations, such as AML controls, may also be triggered.

Accordingly, the decisive factor is not the use of blockchain technology, but whether the game's design introduces an economic stake linked to chance and a realistic prospect of financial gain or loss.

Author: **Paulina Cedrola,** SYLS Ferrari

03 DIGITAL OWNERSHIP VS. INTELLECTUAL PROPERTY

CLARIFYING PLAYER RIGHTS AND INTEROPERABILITY.

The "interoperability reality check."

The Current State: 2026 marks the year the "ownership myth" matured into a more nuanced understanding of “possession rights". While blockchain allows players to "own" the token (the cryptographic receipt), it does not automatically grant ownership of the underlying IP or pixels. The interplay between new framework and traditional copyright law has clarified a vital distinction: while players have a right to transfer their digital assets, third-party developers generally have no legal obligation to receive or support them.

This Chapter deconstructs the common misconception surrounding interoperability. True cross-gaming utility is typically a commercial alliance rather than an inherent technical right. The Chapter analyses the persistent gap between marketing promises and legal reality, clarifying that what is often called 'true ownership' is effectively a token-wrapped license that grants transferability without necessarily granting autonomous control over the underlying game assets.

Concept	The Misconception	The 2026 Legal Reality
Asset Ownership	"I own this NFT, so I own the 3D model."	You own the metadata link and the right to transfer it. The 3D model is a copyrighted asset licensed to you by the studio.
IP Rights	"I can put this skin on a t-shirt and sell it."	Unless explicitly granted (like Bored Ape Yacht Club), commercializing game IP is an infringement of the developer's copyright.
Interoperability	"I can take my Game A sword into Game B."	Interoperability is a technical and business choice, not a legal right. Without a partnership agreement, Game B has no obligation to render Game A's assets.

03 DIGITAL OWNERSHIP VS. INTELLECTUAL PROPERTY

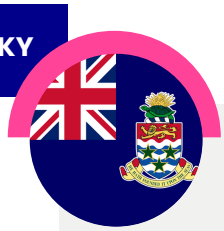
AR

With regards to simple game items, players will generally have the rights granted to them in the applicable terms and conditions.

When dealing with virtual assets, such as fungible tokens or minted NFTs, the basis for recognition of ownership of the asset would be either control (in the case of assets held in a non-custodial wallet) or the contractual agreement with the custodian of the assets (when the assets are held in custody by the studio).

Author: **Juan Manuel Campos Álvarez**, SYLS

KY



In Cayman there are no specific rules on what an in-game item can represent, but if the item represents a security or can be used for payment, there is a risk that it could be regulated under the VASP Act or under SIBA. That can impact the kind of ownership a player might seek to exercise.

Industry standards are that most non-fungible tokens (NFTs) provide a licence to the user to use (and in some licences exploit) the art associated with the NFT. Most forms of NFT and digital assets are likely to be considered property under Cayman Island common law, following AA v Persons Unknown, the Tulip Trading v Van der Laan and D'Aloia v Persons Unknown cases, together with the UK Property (Digital Assets etc) Act 2025 which set out a clear basis for digital assets to be treated as a 'third category' of property in common law countries. As such, players would likely have some proprietary ownership in most typical game-related tokens.

This will always remain framed by the terms and conditions which accompany the issue or sale of the asset, so careful drafting of terms and conditions remains key for studios wanting to mitigate the risk of disputes or claims, and Cayman law is respectful of contractual drafting, giving studios a great deal of freedom in crafting how digital assets will work and what ownership rights will be granted to users.

Authors: **Michael Bacina & Jonathan Turnham,** NXT Law

IN

As gaming has evolved from physical cartridges to cloud based platforms and now to blockchain driven ecosystems, the idea of ownership has become increasingly ambiguous. For Indian players, this confusion is not just theoretical.

It has real legal consequences. What players believe they own in a game often has little resemblance to what Indian law is willing to recognise as ownership.

Indian property law has historically been built around tangible and possessable goods. The Sale of Goods Act, 1930 operates on this premise, making it ill-suited to accommodate digital assets such as in-game items, skins, or virtual currencies. These assets cannot be possessed in the conventional sense, and as a result, player rights rarely arise from property law. That said, Indian courts have begun to recognise certain categories of digital assets as a form of intangible property. In *Rhitikumari v. Zanmai Labs (2025)*, cryptocurrencies were recognised as "virtual digital assets", capable of being owned and protected for purposes such as taxation, inheritance, and legal disputes. To the extent in game assets are structured as freely transferable tokens, this signals a positive development towards property recognition. However, this reasoning applies more readily to tradable crypto assets than to licensed game items, where access and utility remain controlled by platforms.

Most games function through End User Licence Agreements governed by the Indian Contract Act, 1872. These agreements grant players limited and revocable rights to access and use game content, not ownership over it. Indian courts have consistently upheld such arrangements, particularly where user consent is clearly established, treating the relationship between player and platform as one of licence rather than sale.

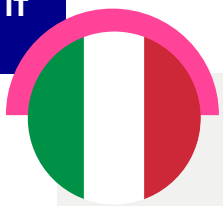
Intellectual property law further narrows the scope of what players can claim. Under the Copyright Act, 1957, game code, artwork, characters, animations, and in game assets are all protected works. Unless there is a clear written assignment that satisfies statutory requirements, copyright remains with the developer or publisher. Even where players pay for digital items or unlock them through gameplay, the transaction only grants access and does not transfer proprietary rights in the underlying work.

Blockchain gaming is often marketed as a fundamental break from this model, promising players true ownership through NFTs and on-chain assets. From an Indian legal perspective, this promise is frequently overstated. While a player may control a token through a private wallet, that control does not equate to ownership of the associated creative work. An NFT is not recognised under Indian law as a conveyance of copyright or proprietary rights. Without a valid written assignment, what the player holds is, at best, a technologically enhanced licence.

This reality weakens common assumptions around interoperability. Indian law imposes no obligation on developers to recognise third-party assets or enable cross-platform use, regardless of how ownership is marketed. As gaming ecosystems mature, clearer disclosures around player rights, IP ownership, and asset portability will be essential. Until then, digital ownership in gaming remains more narrative than legal reality for Indian players

Author:
Archana Kavil,
Zeroto3 Collective

IT



In principle, players can only access a game on the basis of a pure SAAS license, or purchase a digital asset in games without the transfer of IP over it or which include the transfer of IP over it. IT really depends on the contractual arrangement among parties.

There is also a clear distinction that has to be drawn between the ownership of a good, whether physical or digital, and the IP over that item. In this sense and in the physical world, if one buys a copy of a painting this subject can, based on the contractual arrangements with the seller, buy only the physical painting or the physical painting and the copyright of the painting or only the copyright but not the physical painting. The ownership of copyright can be and in many cases is distinguished by the physical object where it is fixated. This is true also for copyright over digital assets. Therefore, the contract of sale of digital assets in games does not automatically entail any transfer of IP right over that specific digital asset in games unless the transfer of the copyright is specifically included in the sale contract. In blockchain, famously years ago a DAO Spice DAO bought above market price a copy of the first edition of the book Dune by Frank Herbert thinking to have acquired in this way the copyright over the book: it came out immediately after that no copyright was acquired but only that physical copy of the book.

Whether or not the copyright holder of a digital asset in game whose digital asset has been sold to a third party can use the IP right to block subsequent sales of that asset in the secondary market, it depends on whether the principle of exhaustion (generally called, first sale doctrine in US law) is considered or not to be applicable to digital assets. In EU law, the principle of exhaustion is provided by Article 4, par. 2 of EU Directive 2001/29 ("InfoSoc Directive"): this principle dictates that once a copyright holder sells a specific, physical copy of their work to someone else, their right to control the further distribution of that particular copy (i.e. their right to exercise their control) is exhausted. Whether or not in EU law this is applicable to digital assets is debatable and there is not a clear answer about it - the personal opinion of who writes this piece is that the principle of exhaustion is applicable in the case of NFTs but not to digital assets in games which have not been tokenized.

The considerations herein are mainly on the basis of the EU Copyright law (on the basis of the InfoSoc Directive) but the author of this paragraph has only direct knowledge of its implementation in the Italian law.

Author: **Paolo Maria Gangi,** Gangi Law Firm

JP

Japanese law imposes significant limitations on what blockchain-based "ownership" actually conveys. The foundational principle emerges from the Tokyo District Court's August 5, 2015 decision in the Mt. Gox bankruptcy proceedings, which held that Bitcoin and similar blockchain tokens are not "objects of ownership" under Civil Code Article 85 because ownership rights can only be claimed over tangible objects. This precedent addresses the classification of digital tokens under Civil Code ownership doctrine, not the availability of contractual, restitutionary, or insolvency-related claims arising from token possession. Acquiring an NFT evidences possession of a unique digital token but does not confer property ownership under Japanese law. Nonetheless, courts will enforce the contractual rights and licenses attached to NFTs regardless of this ownership limitation.

Intellectual property rights remain firmly with creators absent explicit assignment. Under the Copyright Act, the creator holds exclusive rights to reproduce, adapt, publicly transmit, and otherwise exploit copyrighted works. The acquisition of an NFT representing digital artwork does not transfer any copyright, unless the parties expressly agree to such transfer. Article 45 of the Copyright Act permits owners of original physical artworks to publicly exhibit their works without copyright holder authorization; however, this exception does not apply to permanent installations of original works in outdoor locations open to or easily visible by the general public. However, because NFTs do not constitute "objects of ownership" under Japanese law, this exhibition right does not apply to NFT holders. Publicly displaying NFT-linked artwork - whether in virtual galleries, metaverse environments, or commercial settings - requires either explicit permission from the copyright holder or a license grant in the NFT's terms of service.

The practical scope of player rights depends entirely on contractual arrangements: platform terms of service, license agreements, and associated metadata. Without explicit licensing, NFT holders cannot reproduce, commercially exploit, or create derivative works from the underlying content. Japanese law also protects image rights (covering individual appearances) and publicity rights (covering the commercial value of celebrities' likenesses). Tokenizing such content without authorization exposes creators to infringement liability, regardless of blockchain provenance.

Claims of asset interoperability warrant careful scrutiny. Although blockchain technology enables theoretical asset portability, transferring usage rights across platforms requires separate licensing agreements with each operator. Studios promoting "true ownership" must ensure their terms of service accurately reflect the rights conferred - overstating these rights may trigger enforcement under the Act against Unjustifiable Premiums and Misleading Representations. Best practice requires explicit disclosure of the IP license scope, authorized use cases, restrictions on commercial exploitation, and any platform-specific constraints on asset functionality.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

SG

Whether players actually own any IP rights depends on the terms of service between the player and the platform provider. While we note that a huge draw for players in relation to blockchain gaming is that of "decentralisation" and that each player "owns their digital assets", we note that ownership of non-fungible tokens ("NFTs") does not necessarily mean ownership of the underlying digital asset. In addition, the value and the utility of the in-game digital asset remains largely dependent on the platform and/or service provider. Especially in the context of gaming, even if a digital asset may command a five-digit or six-digit price tag (e.g. IEM Katowice 2014 Counter Strike Stickers) , the value of such digital asset remains subject to the risk that the game platform operator continues to ensure that the game remains accessible.

The Singapore High Court has recognised cryptocurrency and NFTs as property in recent years, as evinced by cases involving an injunction against unknown persons such as Janesh s/o Rajkumar v Unknown Person [2022] SGHC 264 (the "Chefpierre Case") and CLM vs CLN [2022] SGHC 46.

Specifically, the Singapore High Court considered and affirmed the definition of property as set out by the High Court of New Zealand, that property must be: (i) definable; (ii) identifiable by third parties; (iii) capable of assumption by third parties; and (iv) have a degree of permanence or stability.

Blockchain gaming in the Web3 ecosystem also comes with the promise of interoperability. As the blockchain ecosystem continues to grow, more and more efforts are being made to ensure cross-chain and multi-chain compatibility. Currently, multi-chain support is generally achieved by the development and configuration of distinct instances of their application (be it a game or otherwise), which are subsequently bridged through the use of smart contracts. However, such "bridging" through the use of smart contracts does not necessarily mean that the "bridged" digital asset contains the same gameplay rules. The same digital asset, now in a distinct environment, may also result in unpredictable behaviour or bugs. Ultimately, this "bridged" digital asset remains an external object that merely represents an underlying asset the game that the "bridged" digital asset is transferred to remains responsible for determining how the "bridged" digital asset is recognised, classified, and by extension any and all in-game effects that it confers.

Authors: **Grace Chong & Bryan Ong** Drew and Napier LLC

KR

Korean law imposes significant constraints on rights that blockchain technology can convey. Korean courts resolve disputes through contract and intellectual property law. NFTs are treated as digital records or contractual positions, not property interests.

Copyright and Intellectual Property
The Copyright Act vests exclusive rights in creators, with copyright subsisting automatically upon creation under Korea's Berne Convention membership. Acquiring an NFT representing digital artwork transfers no copyright unless parties expressly agree to assignment in writing.

An NFT purchase constitutes, at most, acquisition of a digital token evidencing a contractual position - not the underlying creative work. Without explicit licensing, NFT holders cannot reproduce, publicly display, adapt, or commercially exploit underlying content. Studios claiming NFT ownership confers "true ownership" without corresponding license grants risk enforcement under the Act on Fair Labeling and Advertising for misleading representations.

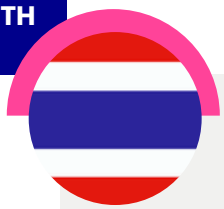
Interoperability Limitations
Blockchain enables theoretical asset portability, but legal interoperability requires separate licensing arrangements. A sword NFT from one game cannot legally function in another without the second game's operator obtaining IP licenses from the original creator and establishing technical integration agreements. Studios should avoid overstating interoperability capabilities, as technical portability does not equal legal portability. Marketing claims suggesting seamless cross-platform use without disclosing licensing requirements may trigger regulatory scrutiny.

Contractual Nature of Player Rights
Player rights derive entirely from contractual arrangements, including terms of service, end-user license agreements, and NFT metadata. Studios should explicitly disclose the scope of any IP license granted, permitted use cases, commercial exploitation restrictions, platform-specific limitations, and termination conditions together with their effect on player rights.

When a player holds an NFT representing a game item, they have a cryptographic record on a distributed ledger - but Korean law has not yet clearly recognized blockchain ledger entries as conferring independent proprietary ownership rights. In practice, Korean courts have generally treated NFTs as evidencing contractual or digital records rather than standalone property interests, leaving the scope of proprietary protection legally unsettled. Without such recognition, the NFT is functionally a database entry: the player's "ownership" exists only to the extent the game operator's terms of service permit, and can be revoked, modified, or rendered worthless if the game shuts down. Amendments to the Act on Electronic Registration of Stocks and Bonds passed on January 15, 2026 will recognize distributed ledger-registered securities as electronically registered securities, establishing transfer effectiveness upon ledger debit and credit. However, these amendments take effect in January 2027 and apply only to securities - not to game items or utility tokens - leaving most blockchain-based game asset ownership without statutory foundation. Studios must clearly disclose that NFT purchases grant only the rights explicitly specified in accompanying license terms, which typically consist of a limited, non-exclusive license for personal, non-commercial use within the specific game ecosystem. Any broader claims about "ownership" or "true ownership" require corresponding contractual grants and may trigger regulatory scrutiny if overstated in marketing materials. The absence of statutory recognition for blockchain-based ownership means players' rights remain fundamentally contractual, not proprietary.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

TH



Thai law recognises digital assets as a form of property, capable of ownership, transfer, and possession, even though the Civil and Commercial Code does not expressly address blockchain-based assets. In practice, token ownership, whether of NFTs or fungible tokens, is generally treated as ownership of intangible property rights rather than ownership of underlying intellectual property (IP).

In blockchain games, players often assume that owning an NFT equates to owning the character, artwork, or game asset itself. Under Thai law, this is not the case. IP rights remain with the developer or rights holder unless expressly assigned. Token ownership typically grants a limited bundle of rights defined by smart contracts and contractual terms, such as the right to use, trade, or display the asset within specified contexts.

Thai courts place significant weight on contractual documentation, including terms of service, end-user licence agreements, and whitepapers. Where these documents clearly state that IP ownership is retained by the studio, token holders will not acquire copyright or derivative rights merely by holding a token.

From a property perspective, however, NFTs and in-game tokens may still constitute assets capable of sale, inheritance, or enforcement against third parties. This distinction between property ownership and IP ownership is critical and frequently misunderstood by players.

Interoperability presents additional legal complexity. While blockchain technology allows assets to move across platforms, Thai law does not recognise a general right to interoperability. Any cross-game or cross-platform use of assets depends on:

- the contractual permissions granted by the original issuer;
- IP licences embedded in token metadata or terms; and
- compliance with consumer protection and misrepresentation laws.

If a game markets assets as interoperable without securing the necessary IP rights or technical support, this may expose the studio to claims of false advertising or unfair trade practices.

In summary, under Thai law, players typically own:

- the token as property; and
- the contractual rights attached to it.

They do not, absent express agreement, own the underlying IP or enjoy unrestricted interoperability.

Author: **Dr. Jason Corbett**, Silk Legal

UK

English courts have consistently held that it was at least arguable that NFTs and other digital assets were to be treated as property under English law. This has recently been codified into UK law: digital assets such as crypto-tokens and NFTs are now formally recognised as a distinct form of personal property under the Property (Digital Assets etc) Act 2025.

However, what is often misunderstood is what players actually own. NFTs, whether a weapon, skin, character or other, are essentially digital representations of value, i.e. they are a type of cryptoasset that represents an underlying tangible or intangible asset. But players are often not aware that owning an NFT or other digital asset does not necessarily mean they own the underlying intellectual property rights. While this follows the rules for traditional content, for example in the same way that owning a book does not in itself mean the owner owns the copyright in the text of the book, it is nonetheless often overlooked due to the autonomy that players otherwise enjoy in this form of gaming.

The Copyright, Designs and Patents Act 1988 is the governing framework legislation in the UK for IP rights in digital content. Under this legislation, as the default position (and ignoring fully open models, such as the original approach employed in Moonbirds), game developers and content creators (or their employers) retain the copyright in the various items depicted in or associated with the NFTs, such as character designs, skins, software code, audio and visual files, etc. Players acquiring in-game assets generally receive only a limited licence to use these assets, not actual ownership of the copyright/IP. The licence is expressed in the platform's terms of service, smart contract provisions and end-user licence agreements. These terms specify the conditions of ownership of the digital asset and determine the extent of the players' rights, for example any restrictions on use, display or commercialisation, whether there are any obligations on the player and, importantly, whether rights can be transferred with the asset. This therefore goes beyond mere ownership of the token and can significantly limit what players can actually do with their "owned" assets. Intended to embed players' ties with a platform, such restrictions can have unintended consequences, for example various third party platforms emerged to facilitate the trading of Steam in-game assets (primarily skins), effectively circumventing the limitations and restrictions of the official Steam platform.

Other limitations and misconceptions of players' rights in blockchain gaming concern permanent ownership and interoperability. While crypto-asset transactions are recorded on the publicly-available immutable blockchain digital ledger, this only records ownership of the token and does not prevent access to the game being revoked, the servers being shut down or underlying content becoming inaccessible - or data being deleted for example to save costs. Furthermore, the technical ability to transfer an NFT between wallets does not mean it will function across different games or platforms. In the UK there is no legal requirement for game developers to accept or integrate NFTs from other games, even if they exist on the same blockchain. This therefore means in practice that interoperability is reliant on licensing arrangements for IP use, compatible game engines and asset formats - and the willingness of developers to recognise third-party assets.

While, therefore, the UK's statutory recognition of digital assets as a category of personal property is slightly ahead of other jurisdictions, this does not materially change players' practical rights, or the fundamental constraint that owning an NFT token as property does not equate to owning the game, the IP rights or guarantee cross-platform functionality.

Author:
Nicky Androsov,
Gunnercooke LLP

UY

The concept of “digital ownership” in gaming is frequently misunderstood. From a legal perspective, players in Uruguay typically acquire a contractual right of use, rather than ownership in the traditional sense recognized under property law. In tokenized environments, players may hold a transferable digital record recorded on a blockchain, but this record does not, by itself, confer ownership of the underlying asset in a legal sense.

A common source of confusion concerns intellectual property rights. Holding an NFT or similar token associated with a game asset does not automatically transfer copyright or other IP rights in the underlying artwork, software, or audiovisual content. Unless there is an explicit license or assignment, IP rights generally remain with the developer or original rights holder, and the player’s rights are limited to those expressly granted by contract. Mischaracterizing token ownership as IP ownership may therefore give rise to consumer protection and misrepresentation risks.

Interoperability is another area where expectations often exceed legal and technical reality. Blockchain technology does not, on its own, ensure that an asset can be freely used across different games or platforms. Meaningful interoperability requires shared technical standards, coordinated economic design, and enforceable contractual arrangements between developers. Without these elements, claims of cross-platform usability remain aspirational and may expose studios to disputes or regulatory scrutiny.

From a regulatory standpoint, ownership narratives become particularly sensitive once assets acquire external economic value. At that point, representations about ownership, transferability, and future utility must be carefully framed to ensure accuracy and consistency with applicable consumer and financial regulations.

Author: **Paulina Cedrola,** SYLS Ferrari

04 CONSUMER PROTECTION & DATA PRIVACY

HOW ARE DATA, DIGITAL IDENTITIES, AND MINORS PROTECTED IN BLOCKCHAIN GAMING IN VARIOUS LOCATIONS?

Privacy as the ultimate competitive advantage.

The Current State: In an era of massive data breaches, the industry has realized that "data can be toxic waste" if mismanaged. New mandates for digital sovereignty – notably the EU Data Act and evolving global privacy standards – now hold studios directly liable for the handling of player data. The traditional "honey pot" model of centralised IDs is being challenged by the rise of Self-Sovereign Identity (SSI) and decentralised architecture.

A recurring regulatory challenge addressed in this Chapter is the tension between blockchain immutability and core data protection principles such as data minimisation, purpose limitation, and rights of erasure, as reflected across GDPR-inspired regimes globally. The Chapter situates these issues within broader regulatory frameworks, including laws related to data protection, consumer protection, and child-safety that can be applied to blockchain-enabled games. It focuses on the evolving duty of care regarding minors, protecting them from predatory profiling through cryptographic safeguards rather than just legal disclaimers.

INSIGHTS FROM KUCOIN

As blockchain gaming continues to scale and integrate with broader digital asset ecosystems, data protection, digital identity, and the safeguarding of minors have become central regulatory concerns. Unlike traditional games, blockchain-based games often involve transferable assets, on-chain wallets, and real economic value, which elevates identity and compliance from optional features to foundational infrastructure components.

From a regulatory standpoint, Know Your Customer (KYC) and Decentralized Identity (DID) should be viewed as complementary rather than competing frameworks. In scenarios involving fiat on- and off-ramps, secondary market trading, or assets with financial characteristics, KYC remains a core compliance requirement across most jurisdictions. It supports anti-money laundering (AML), counter-terrorist financing (CTF), and age-related safeguards, particularly where in-game assets can be traded, monetized, or transferred across platforms.

At the same time, DID introduces a forward-looking approach to identity management that better aligns with data minimization and privacy-by-design principles increasingly emphasized by regulators. Through decentralized identity frameworks, users may verify specific attributes such as age eligibility or jurisdictional compliance without disclosing full personal information. For example, zero-knowledge–based DID solutions can enable age verification without revealing a player's identity, offering a more privacy-preserving mechanism to address minors' protection in blockchain gaming environments.

For game studios and platforms, the key question is not whether to adopt KYC or DID, but how to apply the appropriate identity model across different layers of risk and functionality. Low-risk gameplay interactions may rely on DID-based attestations, while higher-risk financial or custodial activities may still require full KYC processes. This layered approach allows ecosystems to balance regulatory expectations, user experience, and data protection obligations.
From an institutional infrastructure perspective, the role of regulated platforms and service providers is to enable auditable, scalable, and regulator-compatible identity and data governance frameworks. As regulatory guidance around blockchain gaming continues to evolve, projects that integrate identity, data protection, and compliance considerations into their system design at an early stage will be better positioned to achieve sustainable and compliant growth over the long term.

Author:
Julie Zhao,
Kucoin

04 CONSUMER PROTECTION & DATA PRIVACY

AR

Argentina's data protection law requires express consent from the user to collect personal data and to make international transfers of data.

With regards to minors, Argentina has a progressive stance as to the ability to provide consent, so depending on their degree of development minors would be entitled to consent to the collection and treatment of personal data, generally since they are 13 years old. Parental consent would be required for minors under 13 years. The data protection authority has issued best practices guidelines regarding the collection of personal data from users of apps, and especially regarding minors.

International transfers of data are subject to different requirements depending on whether the recipient jurisdiction is classified as an adequate jurisdiction or not. If he recipient jurisdiction is an adequate jurisdiction, international transfers are permitted; otherwise a data transfer agreement is required to ensure Argentine users enjoy the rights granted to them under the data privacy act.[1]

Biometric data is considered sensitive data (and thus, excluded from licit collection and treatment) when it can reveal additional information regarding the user that could be potentially used in a discriminatory manner.

Under the data privacy act, Argentine users enjoy rights of access, rectification, cancellation and opposition to their personal data. The collection and treatment of personal data is subject to principles of adequacy, purpose limitation, data minimization, confidentiality and security.

Argentina's data protection law dates from 2001, and projects for its update aligned with GDPR are being considered by the National Congress.

Additionally, users of videogames are protected by the Consumer Protection law.

Author: **Juan Manuel Campos Álvarez,** SYLS

KY

In Cayman, the Data Protection Act (2021 Revision) is closely aligned with the EU General Data Protection Regulation and provides for a disclosure and consent regime in relation to personal data, which is any information relating to an identified or identifiable living individual collected by a 'data controller' (being someone who determines the purpose, conditions and manner in which data is processed) and processed by a 'data processor' (being a person or entity who collects, records and holds data). The DPA applies when someone is 'established' in Cayman (usually this means a Cayman company) and the data in question is processed in the context of the establishment.

As Artificial Intelligence enables even more metadata matching with immutable blockchain records and online digital fingerprints, it is safe to assume that nearly any user of a game is likely to be identifiable at some point and so nearly all user information will likely be personal data.

Eight data protection principles must be followed. These include:

1. data only being processed legally – there must be a legal basis to collect the data and it must be handled consistent with the DPA and other laws. Users cannot be misled as to the purpose for data collection;
2. limiting the purpose for which data is processed – documenting and communicating the purposes for data collection and only using the data for those purposes;
3. data minimization – keeping the data collected limited to only that which is adequate, relevant and necessary;
4. data accuracy - keeping data accurate and correct and updated if applicable;
5. storage limitations – keeping data for only the length of time needed;
6. respecting individual's rights – notifying users about their rights and processing data in accordance with those rights;
7. integrity and confidentiality – ensuring data is protected and kept encrypted and secure;
8. restrictions on the international transfer of data to countries which do not have adequate data protection.

For games played by minors, parental verification and consent is needed before collecting profiles, chat logs or location information and health related information (for example, collected in fitness games) require strict handing.
Great care must be taken when writing public blockchain transactions involving games given the strict rules and requirements for consent, as most of the DPA principles will be violated if personal information is written to a blockchain.

Individuals have a number of specific rights in relation to their data, including the right to:

1. be informed as to how their data will be processed and stored;
2. access their data;
3. rectify errors in their data;

1. stop or restrict processing of their data;
2. stop direct marketing;
3. the right to prevent automated individual decision-making - that is to prevent a decision which affects them significantly being made without any human involvement; and
4. complain or seek compensation.

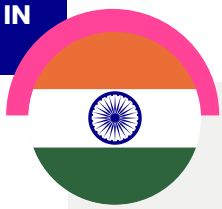
These rights are incompatible with many web3 systems, including in gaming. Rectifying errors in on-chain data is impossible for all practical purposes and restricting or stopping the processing of data by smart-contract stems on public blockchains is similarly not feasible. Automated gaming functions, lending protocols and reputation systems reliant on smart contracts and are highly likely to be inconsistent with a user's right to object to automated decision-making.

As noted above, given the increasing ease with which persons can be identified from data which might otherwise seem innocuous there seems a likely creep in the scope of the DPA / GDPR which will cause friction following the writing of data on public blockchains. A simple example might be usernames which permit real names being used in a game being used to write results of contests or matches to a public blockchain or check-ins such as traffic reports which may appear pseudonymous but may be easily combined with other data to identify an individual.

The DPA was written for a centralized data storage world, and so keeping personal information and data off-chain remains the safest path to compliance, while giving clear and broad disclosures to users as to exactly what is being written to public chains, and the risks of that occurring, is recommended to mitigate the risk of breach of the DPA.

Authors: **Michael Bacina & Jonathan Turnham,** NXT Law

IN



India has become a key market for emerging sectors in recent years. According to a report by the IMARC Group (2025), India's blockchain ecosystem was valued at over USD 650 million in 2024, while its gaming sector exceeded USD 3.8 billion in FY2024 (Lumikai report, 2024). At its intersection, blockchain gaming is making a slow, steady progress. The renewed interest in virtual digital assets ('VDAs') as well as regulatory changes in the gaming sector is likely to fuel this growth.

Blockchain gaming's DLT-first architecture offers benefits over its Web2 counterpart, which remains marked by developer-centric EULAs that confer narrow and revocable licences to players over in-game assets. On the other hand, blockchain games help in recasting EULAs into smart contracts that link assets to player-controlled wallets. They give players unqualified control on assets even if the game ceases to exist. Additionally, they obviate reliance on centralised servers that act as single points-of-failure vis-à-vis data breaches, by replacing them with tamper-resistant, auditable ledgers.

From a legal standpoint, there is no "blockchain" law in India today. A combination of laws address how data, digital identities and minors should be safeguarded. Laws like the IT Act 2000 dictate the contours of permissible content and subject platforms to due diligence and user verification obligations. The Digital Personal Data Protection Act 2023 ('DPDP Act') makes "data fiduciaries" subject to robust data security, retention and deletion standards whilst conferring "data principals" with a suite of rights. Read with the India's recent gaming law, these laws overhaul minors' interaction with games by introducing verifiable parental consent, prohibitions on behavioural monitoring, and disallowing access to certain content. Finally, VDA-related activities are now under India's anti-money laundering framework that imposes AML and CFT obligations on operators.

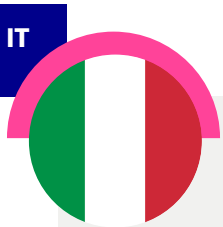
The DLT-led architecture of blockchain games however, poses a few challenges. Illustratively, holding a single 'platform' operator accountable for content on the blockchain remains difficult owing to the disparate roles played by each stakeholder. From the DPDP Act's perspective too, identifying the "data fiduciary", "data processor", and the "data principal" in each setting may be difficult. Another challenge is the identification of minors and restricting their access to prohibited content, an aspect heightened with the pseudonymity offered by blockchain. It is hence relevant for operators to rely on globally recognised regulatory guidance. For instance, 'zero-knowledge proofs' may be adopted as a baseline anonymisation measure for authenticating claims without exposing underlying datasets. Further, identifiable datasets could be stored off-chain and simultaneously linked to on-chain records via hash pointers so that data erasure is possible as per regulatory requirements. Such measures, coupled with the adoption of decentralised identity frameworks built on verifiable credentials held in player-wallets, will strengthen protections for minors by allowing them to control the modalities vis-à-vis disclosure of their identifying datasets.

While Indian laws are not customized to symmetrically apply to blockchain games today, they remain sufficiently broad to trigger applicability. While the DLT-first architecture alleviates certain data security risks that traditionally comes with centralisation, blockchain games introduce new challenge like free data visibility. With Indian laws increasingly becoming extra-territorial (i.e., applicable to entities physically located outside India), it is important that operators take a balanced approach and assess each blockchain game's compliance status and positioning from a regulatory and policy lens before they are offered and scaled in India.

Authors: **Ranjana Adhikari, Sarthak Doshi & Prateek Joinwal,**
Shardul Amarchand Mangaldas & Co



IT



Under EU law there are different laws which protect minors in relation to digital platforms including blockchain gaming.

Under Article 28 of the EU Regulation 2022/2065, known as Digital Services Act (DSA), all online platforms accessible to minors must implement "appropriate and proportionate measures" to ensure a high level of privacy and safety.

In relation to minors personal data, Article 8 of Regulation 2016/679 ("GDPR") dictates that children between 13 and 16 (depending on the member state) can legally consent to data processing. Below this age, Verifiable Parental Consent (VPC) is mandatory.
In general, it should be noted that in the EU there is a very strong consumer protection legal framework and that gaming, in most cases, will be considered as a business to consumer relationship which makes it completely applicable the EU consumer law. This means, for example, that players who access the on-line platform for the first time enjoy a right of withdrawal of 14 days.
Although many considerations herein can also be applicable to EU law as a supranational although coherent legislation, they have been mainly written in relation to Italian law.

Author: **Paolo Maria Gangi,** Gangi Law Firm

JP

The Act on the Protection of Personal Information (APPI)[1], as substantially amended effective April 1, 2022, governs data protection obligations and applies to any business operator handling personal information, including foreign companies offering services to Japanese residents.[2]

Blockchain gaming creates distinctive APPI compliance challenges. The 2022 amendments introduced the concept of "personally referable information" covering cookies, IP addresses, and device IDs—requiring consent before transferring such data to third parties who would combine it with identifying information. Wallet addresses, while pseudonymous, may constitute personal information where reasonably linkable to identified individuals. Gaming companies must clearly specify the purpose of collection before or at the time of collecting personal information,[3] and are generally prohibited from selling personal information to third parties without explicit consent.[4]

International data transfers require additional safeguards. In principle, operators must: (a) obtain informed consent after providing information about the recipient country's data protection regime; or (b) ensure the recipient has an equivalent data protection system. Additional obligations regarding pseudonymized personal information include implementing security measures to prevent data leaks, deleting data when no longer needed, and avoiding cross-referencing pseudonymized information with re-identifiers.[5]

Protection of minors requires heightened attention. While the APPI lacks specific provisions on children's personal information, Personal Information Protection Commission (PPC)'s guidelines indicate that, depending on the minor's capacity to understand the relevant information, consent should generally be obtained from the minor's legal representative.[6] Minors entering into contracts without a legal representative's consent may void those contracts under the Civil Code,[7] unless the minor deceived the other party about their age.[8] Studios should deploy robust age verification mechanisms, require parental consent for minor users, and implement spending limits.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

(1) Act on the Protection of Personal Information, Act No. 57 of 2003, as amended 2022.
(2) APPI, Art. 171.
'3) APPI, Art. 17, Art 21, paras. 1, 2.
(4) APPI, Art. 27, para 1.
(5) APPI, Art. 28.
(6) APPI, Art. 41, paras. 2, 5, 7.
(7) Personal Information Protection Commission, APPI Guidelines (General Rules) Q&A provides some guidance that depending on the relevant information, minors under the age of 15 would generally need consent from their legal representatives.
(8) Civil Code, Art. 5.
(9) Civil Code, Art. 21.

SG

While there is no specific Singapore legislation directly addressing digital identities in the context of blockchain gaming, digital identities in blockchain gaming are protected through the Personal Data Protection Act 2012 (the "PDPA") should the digital identity constitute personal data. The PDPA sets out how organisations collect, use and disclose personal data. Personal data refers to data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access. The PDPA applies to all private-sector entities that collect, use or disclose personal data in Singapore, regardless of the underlying technology.

The Personal Data Protection Commission ("PDPC") has also recognised that business and organisations across the world are starting to deploy distributed ledger technologies ("DLTs") such as blockchains. In response, the PDPC has published a Guide on Personal Data Protection Considerations for Blockchain Design ("Blockchain PDPC Guide"). In particular, the PDPC noted that DLTs may contain on-chain personal data, which refers to personal data "published on, or accessible via, a blockchain in cleartext", and the accountability and immutability issues that may arise.

The Blockchain PDPC Guide contains recommendations including, without limitation, the following: (i) ensuring that on-chain personal data is not stored on a permissionless blockchain; (ii) ensuring that any personal data on a permissioned blockchain is encrypted and/or anonymised; only storing a hash of the personal data on-chain; and (iv) conducting a data protection impact assessment to identify and assess potential risks.

The PDPC has also published Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment ("Children Personal Data Guidelines")[1]. Generally, we understand the approach to be the following:

1. children's personal data should generally be subject to a higher standard of protection and by extension enhanced safeguards. This includes basic practices such as developing and implementing an infocomm technology security policies for data protection, as well as enhanced practices such as the use of multi-factor authentication for admin access to personal data and logging all access;
2. children aged 13-17 may provide their own consent if organisations take steps to ensure that the child understands the consequences of providing and withdrawing consent;
3. organisations should minimise the amount of personal data necessary for age ascertainment purposes; and
4. organisations are encouraged to inform the child's parents and/or guardians in the event of a data breach.

Authors: **Grace Chong & Bryan Ong,** Drew and Napier LLC

(1) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-pdpa-for-children's-personal-data-in-the-digital-environment_mar24.pdf

KR

Data Protection Framework

The Personal Information Protection Act (PIPA) establishes one of the world's most stringent data protection regimes with direct implications for blockchain gaming platforms.

The Act applies extraterritorially to any personal information controller handling Korean residents' data, regardless of location. The Personal Information Protection Commission's guidelines confirm application when foreign operators provide services to Korean data subjects or process their information with direct and substantial impact.

Personal information includes wallet addresses when reasonably linkable to identified persons through exchange know-your-customer records or transaction patterns. The Act requires explicit, informed consent for collection with clearly specified purposes.

Data Subject Rights

Recent amendments have expanded data subject rights significantly. Individuals can now request transfer of their personal data to another provider in a machine-readable format, subject to technical feasibility and sector-specific rules, and data controllers must implement mechanisms such as APIs or encrypted downloads to comply. Data subjects also have rights to explanations of automated decisions and, in certain cases, rights to refuse such decisions—provisions relevant to AI-driven game mechanics. Foreign businesses without Korea offices meeting certain thresholds must designate local representatives for privacy matters.

Recognizing blockchain's inherent permanence, the Enforcement Decree permits anonymization as a method of "destroying" personal information, alongside permanent deletion. Anonymization must render data subjects unidentifiable even when combined with other information.

Protection of Minors

The Personal Information Protection Commission's Guidelines for Protection of Personal Information of Children and Adolescents recommend that services expected to be used by minors: (i) verify user age through methods such as date of birth entry or self-certification of being over 14; (ii) set default privacy settings to "high"; and (iii) refrain from designing services that require minors to provide personal information to the data controller or third parties in exchange for cash or game items. The Commission's July 2025 Consolidated Guidelines on Personal Information Processing reinforce these principles, specifying that sensitive information disclosure settings must default to "private" with users able to choose whether to make information public, and clarifying that age verification is required for "child-oriented" services rather than all data processing involving minors.

Gaming-Specific Protections for Minors

Gaming-specific protections may require implementation of spending management measures for minors in online PC games, primarily through the game rating and compliance framework administered by regulators rather than through a universally prescribed statutory spending cap. Additionally, Article 12-3 of the Game Industry Promotion Act requires online game operators to implement addiction prevention measures, including: real-name and age verification upon registration; parental consent for minor accounts; usage time restrictions upon request by minors or their guardians; notification of game characteristics, ratings, and usage details to minors and guardians; and on-screen elapsed time indicators. These measures apply to PC and console games but not to mobile games.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

ES

GDPR in Blockchain-Based Games

The EU General Data Protection Regulation (GDPR) applies fully in Spain and governs any processing of personal data in blockchain games. As a technology-neutral regulation, it requires compliance with core principles such as lawfulness, transparency and data minimisation, regardless of whether data are stored on-chain or off-chain. Developers and publishers that decide the purposes and means of processing (e.g. account creation, wallet linkage, in-game profiling) will normally qualify as controllers. Public keys, wallet addresses and avatars can constitute personal data where they are linked, or reasonably linkable, to an identifiable player. Consequently, Spanish-facing blockchain gaming projects must ensure an appropriate legal basis (often consent or contract), provide clear privacy information, and enable data-subject rights, even in decentralised or pseudonymous environments.

Digital Services Act and Gaming Platforms

The EU Digital Services Act (DSA) adds a complementary layer of obligations for online platforms, including many gaming ecosystems. Where a blockchain game hosts user-generated content or operates an NFT marketplace, it will usually qualify as an online platform and must implement notice-and-action mechanisms, content moderation and transparency duties. Crucially, the DSA prohibits targeted advertising based on profiling of minors and obliges services accessible to children to guarantee a high level of privacy, safety and security. For Spanish market operators this translates into age-assurance tools, default high-protection settings for child accounts and tight control over features such as chats, recommendations and community content.

Spanish Protections for Minors Online

Spain is reinforcing its domestic framework with a Draft Organic Law for the Protection of Minors in Digital Environments, applicable to online games and blockchain-based services. The draft raises the age of digital consent from 14 to 16, requires parental consent below that threshold and obliges device manufacturers to provide pre-installed parental controls enabled by default. Online services must deploy robust age-verification systems, potentially leveraging EU digital identity tools, and games with paid loot boxes are to be inaccessible to under-18s. The proposal also promotes child-centric design, clearer content rating and criminal responses to severe online harms such as grooming and deepfakes. In parallel, the Spanish Data Protection Agency (AEPD) actively supervises compliance and issues guidance specifically addressing minors' data in interactive services.

Without prejudice to the provisions of the above-mentioned Draft Organic Law, the fact is that the AEPD has already been adopting certain measures in this field in response to the rapid advance of new technologies and the emerging need to protect personal data in new environments, particularly that of minors.

That said, the protection of minors in web3 games operating in Spain is mainly built on three layers: (i) age and consent, (ii) the design of identities and data on blockchain, and (iii) substantive limits on game mechanics such as loot boxes.

Age, consent and access

As indicated, Spain is raising the effective minimum age for minors to consent to the processing of their data on digital platforms to 16, requiring parental authorisation below that age. The forthcoming Organic Law on the Protection of Minors in Digital Environments obliges providers to implement "effective" age-verification systems to access high-risk services such as gambling, adult content or random reward mechanisms.

From a data protection perspective, the AEPD has stressed that age-verification systems must be proportionate, respect data minimisation, and avoid models based on mass surveillance or intrusive profiling of minors. Models that provide only a "yes/no" answer on whether a user exceeds a certain age threshold are favoured, without revealing full identity or storing evidence indefinitely.

Minors' data in blockchain environments

The AEPD has specifically addressed how blockchain fits with the GDPR, especially regarding the right to erasure, and has shown through a "proof of concept" that blockchain infrastructures can comply with data protection rules when appropriate governance and technical measures are applied. In its technical notes, it highlights that the immutable nature of the chain requires moving most personal data off-chain, or using pseudonymisation and encryption techniques that, in practice, prevent identification.

Recent AEPD work shows that governance rules and technical controls can allow effective "functional erasure" while preserving ledger integrity.

Applied to web3 games targeted at, or accessible by, minors, this means avoiding anchoring on-chain any data that directly or indirectly identifies a minor (name, email, device identifiers), using rotating keys or identifiers, and processing sensitive information (age, parental status, self-exclusions) in controlled off-chain databases. The AEPD insists on documenting the architecture, the role of each node and the deletion or "unlinking" policies in order to demonstrate compliance, which is especially critical where minors' data are involved.

Age verification and digital identities in web3

Spain's new child-protection framework favours robust but "child-friendly" age-verification systems that put the burden of proof on the adult trying to access restricted content, and not on the minor. In this context, web3 games can integrate digital identity solutions (for example, verifiable credentials issued by trusted third parties or identity wallets) that allow users to prove they are adults without exposing their civil identity on the game blockchain.

The AEPD warns against solutions that involve collecting and storing copies of identity documents or biometric data without strict necessity, and recommends designing flows where the age-verification provider acts as a trusted intermediary, returning only minimal attributes (e.g. "over 18") to the game operator. In a web3 environment, this can be articulated through off-chain tokens or credentials linked to the player's wallet, so that age verification happens off-chain and the smart contract only receives an abstract "ok/not ok" signal.

Limits on loot boxes and high-risk mechanics

The Draft Organic Law on the Protection of Minors in Digital Environments introduces a general ban on minors accessing and activating loot boxes and other random reward mechanisms in video games. The restriction targets mechanisms that combine a price to activate, chance, and rewards that are transferable or convertible into money, which directly covers many blockchain game mechanics based on tradeable tokens and NFTs.

To make the ban effective, the law provides for sanctions on companies that fail to block minors' access and reinforces identity-verification requirements. In the web3 ecosystem this requires clearly segmenting "adult-only" versions or modes, limiting the tokenisation of high-risk rewards in environments accessible to minors, and, above all, integrating age checks before allowing any interaction with smart contracts that manage loot boxes or bets, even if the transaction is executed on a public network.

Regulatory Outlook for Blockchain Gaming

Spain has not yet adopted sector-specific rules for blockchain gaming, so general regimes on data protection, consumer and gambling law, together with EU instruments such as the GDPR, DSA and MiCA, form the applicable framework. Authorities are, however, clearly focused on the intersection of crypto-assets, gaming and child protection, and promote privacy-enhancing technologies (e.g. pseudonymisation, zero-knowledge proofs) for age and identity verification. Operators targeting Spain must therefore ensure that players' data and digital identities – especially those of minors – are protected by design and by default throughout the lifecycle of blockchain games.

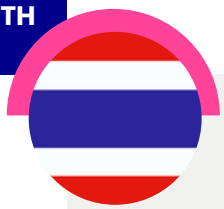
Particularly, in light of the AEPD's guidance on blockchain and the new child-protection legislation, a cautious design of web3 games for the Spanish market should:

- Keep identity and age-verification data off-chain, linking them to the game wallet only through pseudonymous identifiers.
- Implement proportionate age-verification based on minimal attributes and a strong focus on children's privacy.
- Disable loot boxes and random reward mechanisms with economic value for accounts or wallets associated with minors, while reinforcing risk information and spending controls for adults.

This approach helps reconcile the specific features of the web3 ecosystem (asset ownership, transparency, composability) with the increasingly strict requirements on data protection and child safety that are shaping the Spanish and EU regulatory agenda through 2030.

Authors: **Gonzalo Cantero Puig & Marina Villalonga Cladera,** Asensi Abogados

TH



Thailand's primary data protection framework is the Personal Data Protection Act B.E. 2562 (2019) (PDPA), which came fully into force in 2022. The PDPA closely mirrors the GDPR in structure and principles, making it directly relevant to blockchain gaming platforms handling player data.

Personal data under the PDPA includes any information relating to an identifiable individual, including usernames, wallet addresses linked to identifiable persons, device identifiers, and behavioural data generated through gameplay. Blockchain games frequently process such data for account management, matchmaking, fraud prevention, and monetisation.

A key compliance challenge arises from the immutability of blockchain records. The PDPA grants data subjects rights of erasure, rectification, and objection, which may conflict with on-chain storage. As a result, best practice in Thailand is to:

- store personal data off-chain;
- minimise on-chain personal identifiers; and
- use hashing or pseudonymisation where feasible.

Digital identities, including wallet-based identities, may constitute personal data where they can be linked to an individual. Where blockchain games implement KYC, social logins, or biometric systems, additional PDPA obligations apply, including lawful basis, transparency, and security safeguards.

The PDPA affords heightened protection for minors. While Thailand does not have a standalone children's online safety statute comparable to COPPA, consent for processing the personal data of minors under 10 years old must be obtained from a parent or legal guardian. For older minors, risk-based consent and transparency obligations apply.

In practice, blockchain gaming studios often adopt age-gating, content restrictions, and parental consent mechanisms, particularly where monetisation or token trading is involved. Consumer protection laws may also apply where minors are exposed to misleading or aggressive monetisation practices.

Cross-border data transfers are permitted under the PDPA, but require appropriate safeguards. Given the global nature of blockchain gaming infrastructure, studios targeting Thai players must ensure that overseas data processors meet PDPA-equivalent standards.

Author: **Dr. Jason Corbett,** Silk Legal

UK

The Regulatory Framework

The United Kingdom has established itself as a rigorous and proactive regulator in the intersection of digital entertainment and data privacy. For blockchain gaming studios, the UK market represents a sophisticated but high-stakes environment.

The protection of data, digital identities, and minors in blockchain gaming is governed by three principal regulatory regimes: (1) the UK General Data Protection Regulation and Data Protection Act 2018 ; (2) the Online Safety Act 2023 ; and (3) the Information Commissioner's Office Age Appropriate Design Code (commonly known as the Children's Code).

Data Protection

The UK GDPR applies to any processing of personal data of UK users, regardless of where the data controller or processor is established. Blockchain gaming presents particular challenges: on-chain wallet addresses, transaction histories, and behavioural data may constitute personal data where users can be identified. The immutability of blockchain records creates tension with data subject rights, including the right to erasure. Studios should implement privacy-by-design principles, minimise on-chain personal data storage, and clearly articulate data processing activities in transparent privacy notices.

Digital Identity

Blockchain gaming frequently involves pseudonymous wallet-based identities and NFT-based avatars. The UK Digital Identity and Attributes Trust Framework, now on statutory footing under the Data (Use and Access) Act 2025, establishes standards for digital verification services. Where studios utilise identity verification providers, using services certified against the Trust Framework provides regulatory assurance. Importantly, pseudonymous blockchain identities do not exempt studios from verification obligations; where age assurance is required under the Online Safety Act, robust identity checks must be implemented regardless of wallet-based authentication.

Protection of Minors

The Online Safety Act 2023 imposes duties on user-to-user services with links to the UK to assess risks of children encountering harmful content. Services likely to be accessed by children must deploy "highly effective age assurance" mechanisms; self-declaration of age alone is no longer sufficient. From 25 July 2025, the Protection of Children Codes of Practice require in-scope services to prevent children from accessing primary priority content.

The ICO's Children's Code establishes 15 standards applicable to "information society services likely to be accessed by children," expressly including online games. Core requirements include high privacy settings by default, data minimisation, restrictions on geolocation tracking, prohibition of manipulative "nudge techniques," and limitations on profiling.

Consequences of Non-Compliance

The penalties are substantial. Under the UK GDPR, the ICO may impose fines of up to £17.5 million or 4% of annual global turnover, whichever is greater. Ofcom's powers under the Online Safety Act reach £18 million or 10% of qualifying worldwide revenue, whichever is greater. Ofcom opened investigations into 92 services in 2025 and has imposed fines for inadequate age assurance measures.

Considerations for Gaming Studios
Studios targeting the UK market should conduct data protection impact assessments addressing blockchain-specific risks, implement robust age verification, ensure default settings are configured for maximum privacy, and avoid design features encouraging excessive data sharing by younger users.

Overseas studios should note that each regime applies extraterritorially. The UK GDPR governs processing of UK residents' data regardless of controller location. The Online Safety Act applies to services with significant UK user numbers. Compliance is essential for any studio targeting UK players.

Author:
Roshi Sharma,
LawBEAM

UY

Personal data protection in Uruguay is governed by Law No. 18,331, which is closely aligned with international standards. Game developers and platforms must comply with principles such as purpose limitation, data minimization,

The technical immutability of blockchain does not override legal obligations under data protection law. As a result, privacy-by-design and privacy-by-default approaches are essential. In practice, this often requires avoiding the storage of personal data in clear text on-chain and instead relying on off-chain storage, hashing, pseudonymization, or other architectural solutions that allow compliance with data subject rights.

Digital identity solutions integrated into games, particularly those linked to wallets or on-chain credentials, must also be proportionate to the risks involved and limited to what is strictly necessary for the intended purpose.

Minors benefit from enhanced legal protection. The processing of children's personal data requires heightened safeguards, clear and age-appropriate information, and, where applicable, valid parental consent. In addition, game mechanics and monetization models must be carefully designed to avoid encouraging financially risky behavior or exploitative practices when minors are involved

Author: **Paulina Cedrola,** SYLS Ferrari

05 THE CONVERGENCE OF AI & WEB3

HOW SHOULD STUDIOS PREPARE FOR THE CONVERGENCE OF AI AND BLOCKCHAIN GAMING?

Studios as "Digital Micro-Nations."

The Current State: As of August 2, 2026, the EU AI Act will be fully enforceable, fundamentally changing the role of the developer.

A game studio may now be viewed as a digital governance entity, responsible for the "behaviour" of its autonomous systems. When deploying AI-driven NPCs that can trade assets or algorithms that autonomously balance in-game economies, studios must navigate a complex risk-based framework.

While most gaming applications are "minimal risk," those impacting financial behaviour or minor safety require rigorous oversight.

This Chapter highlights the "compliance dividend". It argues that in 2026, speed is no longer the metric for success, legal integrity is. Studios that use regulatory sandboxes to test agentic AI and document “human-in-the-loop" processes are securing higher valuations and lower insurance premiums.

We are moving from reactive legal fire-fighting to a model of strategic governance, where the studio’s code is as scrutinized as its balance sheet.

05 THE CONVERGENCE OF AI & WEB3

AR

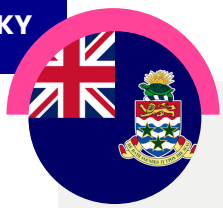
Although Argentina does not have specific guidelines, studios should focus on preparing for the use of AI which is ethical and compliant. Specifically, the use of

AI should not result in breaches to applicable laws such as data privacy and consumer protection.

Internal policies and good practices guidelines should be developed by the studio to ensure a compliant use of AI on its game mechanics.

Author: **Juan Manuel Campos Álvarez,** SYLS

KY



The speed with which AI accelerates and the impact on automation cannot be overstated.

The first step studios should have taken by now is adjusting hiring strategies to ensure that AI native and AI curious staff are identified in recruitment and brought into key roles. Training in AI usage for existing staff is key to help identify efficiencies and improvements which can be harnessed and lifting their performance. In 2025 as much as 30% of Microsoft code was AI written, and that number is only increasing, promising faster and cheaper game development than ever before.

Blockchain records will likely play a fundamental role in ensuring records can be trusted given the proliferation of AI slop and fake images and videos, and we expect authenticity and digital scarcity to rise in value in the gaming space. That authenticity and scarcity needs to be protected by studios to preserve the value being put into game development. Similarly, security against increasingly AI-bots seeking to game in-game systems is likely to need significant investment as rogue players turn to AI enhancements to automate the probing of game systems for weaknesses and opportunities to profit at the expense of others.

Authors: **Michael Bacina & Jonathan Turnham,** NXT Law

EU

Blockchain-based gaming assets are moving beyond novelty and into practical design space for studios: new use cases, new user experiences, and new revenue streams - built on a timeless driver of player behavior: ownership. When a skin, weapon, or character feels truly "mine," motivation shifts from short-session consumption toward longer-term identity, mastery, and collection.

One emerging trajectory is that these assets become the next generation of collectibles – portable in your wallet on your phone, tradeable on digital asset exchanges, and priced by global demand. Instead of being trapped inside a single game, a player could swap a rare skin for another token, can convert that into Bitcoin, and ultimately cash out into fiat (where platforms allow). The result is a global digital token market for game items - and, notably, early exposure for gamers to real market dynamics: discovery, liquidity, pricing, and online exchanges.

The bigger unlock is cross-media incentivization - linking gaming rewards to real-world experiences that, e.g., parents and educators care about. Imagine a "read-to-earn" or even "read-to-play" pathway: if a child finishes an online book (verified via comprehension questions or reading signals), they earn a themed in-game asset - perhaps a weapon skin that carries the book's narrative identity. Now motivation travels both ways: education gains a compelling reward loop, and games gain deeper meaning, status, and story. In practice, this can evolve into new family-facing models: parents subscribe to a plan that issues verified "achievement tokens" (reading, grades, sports milestones), redeemable for on-chain cosmetics, levels, or skills - tradeable later if tastes change as kids grow older.

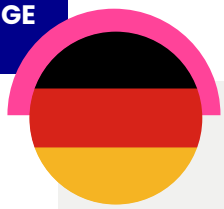
These mechanics are proven in Web3. As BCG's On Tech notes, decentralized networks can "incentivize behavior changes" by tracking actions and awarding tokenized rewards. Gaming is simply the most intuitive interface for those incentives - already fluent in progression systems, quests, and status.

Studios should also stay mindful of the European legal perimeter: depending on structure and distribution, gaming assets can intersect with EU consumer law (e.g., unfair/misleading marketing), digital content and services rules, IP licensing, the Digital Services Act, and GDPR. The implication isn't to slow down - it's to build trust through clear disclosures about what is owned (the token) versus what is licensed (the content).

Early movers are already shaping the frontier. Animoca Brands positions itself around advancing "digital property rights" in gaming. Newer entrants like One Earth Rising are building "Ownable Game Assets™" and tooling to bring on-chain skins into mainstream engines. Alongside pioneers such as The Sandbox and Immutable, the direction of this new business stream is clear: ownership-linked incentives and cross-media reward loops can become a defining innovation lever for the next wave of studio growth.

Author:
Bernhard Kronfeller,
Boston Consulting Group

GE



Studios looking to use AI systems on a standalone basis or in combination with digital assets in Germany, need to stay mindful of additional obligations that may apply to them in addition to the potential application of the MiCA-

Regulation and the national law that transposes the MiCA-framework into national law.

Same as in other EU Member States, as of 2 February 2025, the EU AI Act has partially become directly applicable in Germany as well. The EU AI Act is a comprehensive horizontal regulatory framework which applies to the supply and deployment of AI systems in the EU. To that end, the EU AI Act introduces risk-categorisation of AI systems and key transparency and operational requirements that entities supplying AI systems to persons in the EU (producers) and entities deploying AI systems (deployers) need to comply with accordingly.

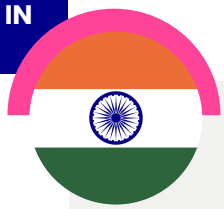
Studios utilizing AI technology on a standalone basis or in a combination with digital assets need to stay mindful of requirements under the EU AI Act that may apply to them as producers or deployers of AI systems, depending on their role in a particular structure. Further, depending on the risk categorisation of the AI system in question, the degree of the regulatory burden on studios under the EU AI Act varies quite significantly (from compliance with relatively simple transparency requirements to the prohibition of the use of an AI system). The use of some AI based practices may be particularly challenging under the EU AI Act: (i) AI systems that deploy manipulative techniques or exploiting people's vulnerabilities (like systems manipulating players to spend more in a game), are generally deemed as prohibited, (ii) AI systems which pose a significant risk of harm to the health, (like AI systems used in video games for emotion recognition, which create more personalized, and adaptive player experiences) are generally deemed as high risk AI systems and are subject to strict requirements, especially for providers (and to the lesser extent deployers of AI systems).

Where studios are using AI systems in combination with digital assets, they need to stay mindful of potential regulatory risks that may arise from the structures where an AI system is automatically minting, distributing, managing and transferring digital assets to users, since any of the aforementioned activities can potentially fall under the scope of the MiCA-Regulation. Further, in the course of implementation of the MiCA-Regulation, Germany has adopted national law that creates categories of regulated digital assets and regulated activities, that go beyond the scope of the MiCA-Regulation (especially when it comes to NFTs with an investment component – see more on this in the response to question 1). Therefore, studios looking to combine digital assets and AI technology in Germany, should stay aware of this increased regulatory complexity in the country.

Last but not least, despite the direct application of the EU AI Act to the use of AI systems, the processing of personal data of the users (players) through AI systems is subject to compliance with the German Federal Data Protection Act (Bundesdatenschutzgesetz).

Author: **Miroslav Duric**, Taylor Wessing

IN



It's no secret that AI has swept the world. And its mix with blockchain gaming is a power up no one saw coming or at least prepared for. Fuelled by Generative Adversarial Networks, agentic-AI brings real time personalization to gameplay and rewards, shapes non playable characters (NPCs), writes smart contracts, and boosts fraud detection. It also helps build simpler guides for newer players, making it easier to keep them engaged. Many blockchain games already use AI, and more plan to integrate it.

This convergence of course comes with its share of challenges. Real-time content generation or reward personalisation is tough to execute as smart contracts are typically tailored for deterministic outcomes. A surge in AI-systems on permissionless blockchains has also ensued an increase in bot-activity. Any identity-verification solution to offset these concerns may threaten the benefits of decentralisation that blockchain gaming offers. The Indian legal framework is also not a straightforward one to navigate. For instance, personalisation of assets, gameplay, and avatars offered by AI risks amplifying dark patterns and manipulative designs – a key concern under consumer protection laws. Ownership over AI-generated content is another challenge since India's copyright laws only recognise human authorship. Developers will also need to keep innovating their monetisation models with India's recent gaming law prohibiting input of money or money's worth (arguably, including cryptocurrency) with the expectation of any reward. Lastly, balancing equality and fairness among players is a task, with agentic-AI being used as a common tool during gameplay.

AI use-cases in blockchain gaming are at a nascent stage in India. It is hence the right time for studios to prepare. At a development level, studios may consider keeping AI-led inferences off-chain and linking their outputs to on-chain records via oracles. Further, botting can be addressed by maintaining oversight over unusual playing patterns and incorporating 'kill-switches' for on-chain AI-systems. From a legal and regulatory standpoint, to mitigate dark pattern-related concerns, studios should aim to adopt internal procedures that prohibit scarcity countdowns, provide opt-outs and tools to limit spending, as well as periodically audit the AI-system curating in-game rewards for players. Given the recent restrictions on game monetisation, studios could position certain game assets as utilities (access perks, cosmetics, skins etc.) and consider spreading rewards through different streams. Copyright-related risks can be handled by keeping chain-of-title and licence records for all in-game assets and training datasets, auditing AI outputs for infringement (ex: reverse-image checks), and engaging with vendors that provide indemnities with clear allocation of ownership over outputs. Finally, to offset consumer-protection related concerns, player-facing terms should transparently flag the role of AI-systems and set ownership rules for AI-assisted content.

Technology moves faster than regulation today. For AI and blockchain gaming, this cannot be truer as both have disrupted traditional sectors in recent years. Hence, it is crucial that studios take a pragmatic view and approach their game launches holistically. Demonstrating a compliance-first attitude goes a long way in India and it is crucial that studios design internal compliance standards that can keep pace with business realities and the pace of innovation.

Authors: **Ranjana Adhikari, Sarthak Doshi & Prateek Joinwal,** Shardul Amarchand Mangaldas & Co

IR

Alongside the MiCA-Regulation that may apply to the use of digital assets by gaming studios, the use of AI systems on a standalone basis or in combination with digital assets can trigger application of additional obligations under the EU Regulation (EU) 2024/1689 (commonly known as the "EU AI Act").

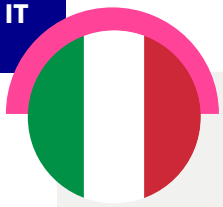
As of 2 February 2025, the EU AI Act has partially started to apply (with the remaining provisions set to start applying as of 2 August 2026). The EU AI Act is a comprehensive horizontal regulatory framework which applies to the supply and deployment of AI systems in the EU. To that end, the EU AI Act introduces risk-categorisation of AI systems and key transparency and operational requirements that entities supplying AI systems to persons in the EU (producers) and entities deploying AI systems (deployers) need to comply with accordingly.

Studios utilizing AI technology need to stay mindful of requirements under the EU AI Act that may apply to them as producers or deployers of AI systems, depending on their role in a particular structure. Further, depending on the risk categorisation of the AI system in question, the degree of the regulatory burden on studios under the EU AI Act varies quite significantly (from compliance with relatively simple transparency requirements to the prohibition of the use of an AI system). The use of some AI practices may be particularly challenging under the EU AI Act: (i) AI systems that deploy manipulative techniques or exploiting people's vulnerabilities (like systems manipulating players to spend more in a game), are generally deemed as prohibited, (ii) AI systems which pose a significant risk of harm to the health, (like AI systems used in video games for emotion recognition, which create more personalized, and adaptive player experiences) are generally deemed as high risk AI systems and are subject to strict requirements, especially for providers (and to the lesser extent deployers of AI systems).

Where studios are using AI systems in combination with digital assets, they need to stay mindful of potential regulatory risks that may arise from the structures where an AI system is automatically minting, distributing, managing and transferring digital assets to users, since any of the aforementioned activities can potentially fall under the scope of the MiCA-Regulation. Last but not least, despite the direct application of the EU AI Act to the use of AI systems, the processing of personal data of the users (players) through AI systems is subject to compliance with the Irish Data Protection Act 2018 (GDPR implementation in Ireland).

Author: **Miroslav Duric,** Taylor Wessing

IT



Studios should probably be aware that in EU it is already in force the Regulation 2024/1689 or AI Act, a regulation specifically dedicated to put on the market into the EU of products which make use of AI. The regulation contains various rules including the obligation of AI to respect IP rights of EU residents. This regulation might impact studios and they should be aware of it in relation to their activity in the EU.
Although many considerations herein can also be applicable to EU law as a supranational although coherent legislation, they have been mainly written in relation to Italian law.

Author: **Paolo Maria Gangi,** Gangi Law Firm

JP

AI agents are not recognized as separate legal persons in Japan. Even if an AI agent autonomously creates or manages its own crypto wallet, the cryptocurrencies in such wallet are legally owned by the human or corporate entity that controls the AI agent. Japan enacted its first comprehensive AI legislation in May 2025: the Act on the Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies, which became fully effective in September 2025. In contrast to the EU AI Act, Japan's framework prioritizes innovation over restriction through a principles-based approach. The absence of criminal penalties or administrative fines is a deliberate policy choice, not a regulatory gap.

Persons or entities that develop or deploy AI agents may be held liable in civil actions for negligence, although proving causation may be difficult. Product liability claims may also arise, though establishing that harm was caused by a lack of security of the AI agent itself presents evidentiary challenges. The AI Guidelines for Business (version 1.01, March 2025), published by METI and MIC, provide practical operational guidance calling for executive-level responsibility.

Article 30-4 of the Copyright Act permits non-expressive uses—including AI training—without rights-holder consent, so long as outputs do not reproduce protected expression. The Agency for Cultural Affairs' 2024 guidance further clarified that replicating the "style" of source materials does not constitute infringement. Notably, AI-generated content is not eligible for copyright protection absent human creative effort. Training AI on gameplay data does not require game developer authorization under Article 30-4; however, studios should consider seeking permission from professional players whose distinctive techniques may inform the training data.

Recommended best practices include: documenting AI decision-making processes and training data origins; maintaining human oversight over material determinations; embedding explainability features in systems that affect asset distribution; and tracking regulatory developments in AI governance and consumer protection.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

ME

Studios focusing on Montenegro that are combining blockchain and AI must be prepared to navigate a regulatory landscape that is currently in a state of rapid transition as part of the country's rapid alignment with the EU acquis that will continue throughout the coming period.

First, where intending to stay outside the scope of the Montenegrin AML Act as well as the Montenegrin Payment Systems Law (see more on this in response to question 1 above), studios must ensure that digital assets are solely used within the closed in-game environment (thereby falling under the LNE exclusion under the Payment Systems Law and avoiding triggering application of the registration regime applicable to providers of crypto-asset related services).

Regarding the use of AI, there is currently no standalone designated regulatory framework for the use of AI in Montenegro. However, as of January 2026, the country has officially begun implementing the Strategy for the Development of Artificial Intelligence (2026–2030). This strategy represents the first step towards the potential creation of the Law on Artificial Intelligence, which would ensure alignment of the Montenegrin law with the EU AI Act as part of the Montenegro's final push for EU accession. Therefore, conscious of the accelerated EU accession process, studios focusing on Montenegro will highly likely have to deal with very similar requirements on AI systems that will highly likely be equivalent to those stipulated by the EU AI Act. Aside from the horizontal regulation of AI systems, studios shall keep in mind that processing of personal data of the users is subject to compliance with the Montenegrin Act on Protection of Personal Data (Zakon o zaštiti podataka o ličnosti) which largely transposes the GDPR into Montenegrin legislation.

Studios should stay mindful of risks that may arise from the structures that utilize AI for the purposes of automatic minting, distribution and management/transfer of digital assets, that may bring the structure at hand in the scope of the Montenegrin AML Act.

Author: **Miroslav Duric,** Taylor Wessing Partnerschaftsgesellschaft mbB, Frankfurt

RS

Gaming studios that are combining blockchain and AI in gaming need to stay mindful of several important points when operating in Serbia:

First, they need to ensure compliance with the Serbian Digital Assets Act (Zakon o digitalnoj imovini) (as explained in more detail in response to question 1). To that end, when it comes to in-game digital assets that shall be solely used within the in-game ecosystem, the most crucial point would be ensuring exemption from the scope of application of the Serbian Digital Assets Act and, where the digital asset is designed as a means of payment, the Serbian Payment Services Act (Zakon o platnim uslugama).

When it comes to the use of AI, there is currently no designated regulatory framework on the use of AI in Serbia. The processing of users' data however through AI systems is subject to compliance with the Serbian Act on Protection of Personal Data (Zakon o zaštiti podataka o ličnosti).
In January 2025 Serbia adopted the Strategy for the Development of Artificial Intelligence for the period 2025–2030 which defines the goals and measures for the further development of AI in the country and serves as the foundation for the future Law on Artificial Intelligence.

The Ministry of Science, Technological Development, and Innovation of Serbia has formed a working group currently drafting the law, which shall largely use as a basis the EU AI Act. Once this framework is finalised, studios will need to factor in any potential limitations especially in terms of permitted use cases (particularly where the future Serbian Law on Artificial Intelligence, implements the risk categorisation of AI systems from the EU AI Act). Last but not least, using AI systems which automatically mint, distribute and potentially manage digital assets, may expose the studios to a risk of being deemed as either offerors of digital assets or as providers of regulated services related to digital assets, depending on the structure.

Author: **Miroslav Duric,** Taylor Wessing Partnerschaftsgesellschaft mbB, Frankfurt

SG

Given the constantly evolving technology landscape, entities should response to the convergence of AI and blockchain gaming through being prepared to explore emerging use cases. We set out below a non-exhaustive list of trends

recently observed in the blockchain gaming industry. At this juncture, it is important to remain cognisant that AI is more than just generative AI; AI also encompasses computer vision, such as facial recognition capabilities, as well as augmented reality and virtual reality capabilities.

Agentic AI

On 22 January 2025, Singapore launched the Model AI Governance Framework for Agentic AI.[1] Agentic AI typically refers to systems that are able of some degree of independent planning over multiple steps to achieve a user-defined goal. In the same way that ChatGPT has drastically improved since its launch in November 2022, Agentic AI can be expected to drastically improve in capabilities as the technology stack continues to evolve and improve. In the context of blockchain gaming, entities could possibly leverage such technologies to manage in-game economies and/or work towards cross-chain capability through the use of smart contracts.

AI integration with the game environment

Entities should invest in capabilities that allow the games to support AI-generated in-game digital assets, such that players may be able to create bespoke items. Some projects, such as Astra Nova, have gone one step further, exploring the possibility of such AI-generated in-game digital assets to be minted as NFTs.

Another emerging use case is to integrate non-playable characters ("NPCs") with large language models. In contrast to Web2 games, where NPCs are bound by scripts and/or Boolean input, integration of AI with NPCs may allow for such NPCs to learn from their interactions with the player and respond differently over time.

(1) https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf

Together, the use of AI may allow game developers to provide a tailored experience for each and every single player, manifesting itself in forms such as customised quests and reward structures.

Entities may prepare for and respond to these emerging use cases by ensuring that they are technically ready to explore such emerging use cases. Entities should be prepared to implement sandboxes and/or other governance frameworks while exploring such emerging use cases. For example, entities could tag each Agentic AI with a unique traceable identity linked to a human supervisor and/or wallet address. Entities could also implement a "checkpoint" system where human oversight is required, especially where high-risk and/or high-value actions are involved. This would be consistent with the Model AI Governance Framework for Agentic AI, where such deployment should involve clear allocation of responsibilities within and outside of the organisation such that meaningful human oversight is always present.

Authors: **Grace Chong & Bryan Ong,** Drew and Napier LLC

KR

The AI Basic Act

The Framework Act on Artificial Intelligence Development and Establishment of Trust (the "AI Basic Act") establishes Asia-Pacific's first comprehensive AI legislation with significant implications for blockchain gaming studios.[1]

The AI Basic Act applies to both AI development business operators, who create and offer AI systems, and AI utilization business operators, who deliver products or services that integrate AI technology. The Act contemplates application to foreign AI operators meeting specified user or revenue thresholds in Korea, primarily through local agent designation and compliance obligations.

High-Impact AI Requirements

AI systems that significantly affect human life, safety, or fundamental rights face heightened requirements. In blockchain gaming, several applications could fall under this category because they directly impact players' financial interests and access: AI used for player evaluation affecting rewards or rankings, matchmaking systems influencing competitive outcomes, automated moderation impacting account status, and dynamic pricing or changing the probability that players can receive certain items, rewards, or loot.

Under the AI Basic Act, operators of high-impact AI must review in advance whether their AI qualifies as high-impact and may request confirmation from the Ministry of Science and ICT if uncertain.[2] They must establish plans to provide users with meaningful explanations of AI-generated outputs, including the key criteria used to derive those outputs and an overview of the learning data, to the extent technically feasible.[3]

(1) Framework Act on Artificial Intelligence Development and Establishment of Trust (Act No. 20676), passed December 26, 2024, effective January 22, 2026 ("AI Basic Act").
(2) AI Basic Act, Art. 33.
(3) AI Basic Act, Art. 34(1)(2).

Operators must also establish and operate user protection measures[1] and ensure human management and supervision of high-impact AI systems.[2] Additionally, operators are expected to assess in advance the impact of their AI on fundamental rights, though this is framed as an effort-based obligation rather than a strict mandate.[3] Finally, they must prepare and maintain documentation demonstrating the measures taken to ensure AI safety and reliability. [3]

Generative AI Transparency

Mandatory labeling applies to generative AI. Operators must notify users if products or services are developed using AI and must label whether content was produced by generative AI.[4] This requirement is relevant for AI-generated game assets, characters, or narratives.

AI and Copyright

South Korea's Copyright Act currently lacks an explicit text-and-data mining (TDM) exception for AI training purposes. In the absence of specific TDM provisions, the legality of using copyrighted works for AI training must be assessed under Article 35-5 of the Copyright Act, which establishes a general fair use framework modeled on U.S. law. This provision sets out four factors for determining fair use: (1) the purpose and nature of the use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used; and (4) the effect on the potential market or value of the work. However, unlike the United States, Korea lacks a substantial body of case law interpreting fair use in the AI context, creating significant legal uncertainty. The Korea Copyright Commission's 2023 Guide on Generative AI and Copyright provides non-binding guidance encouraging AI developers to obtain licenses for training data and to prevent output infringement, but expressly excludes detailed treatment of training-phase copyright issues. For AI-generated outputs, infringement liability turns on whether the output constitutes "actual copying" and is "substantially similar" to a copyrighted work. Current Korean copyright practice generally requires meaningful human creative contribution for copyright protection. As a result, purely AI-generated assets are unlikely to qualify for copyright protection under prevailing interpretations, although Korean courts have not yet issued definitive rulings specifically addressing AI authorship.

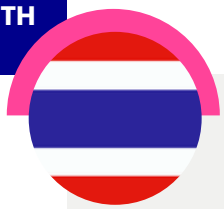
Practical Guidance

Studios should audit AI systems for high-impact classification, implement transparency notices for AI-driven features, document human oversight mechanisms, and ensure AI-generated assets have sufficient human creative input for copyright protection.

Authors: **Yumi Ahn & Ryo Yamada,** Tokyo International Law Office

(1) AI Basic Act, Art. 34(1)(4).
(2) AI Basic Act, Art. 35.
(3) AI Basic Act, Art. 34(1)(5).
(4)AI Basic Act, Art. 31(1) & (2).

TH



The convergence of artificial intelligence and blockchain gaming presents both regulatory opportunity and risk in Thailand. While Thailand does not yet have a comprehensive AI statute, regulators have made clear that AI will increasingly fall within existing legal frameworks, including data protection, consumer protection, cybersecurity, and digital platform regulation.

From a blockchain gaming perspective, AI is already being deployed in procedural content generation, player analytics, fraud detection, NPC behaviour, and dynamic economies. These use cases often rely on large-scale data processing, triggering PDPA compliance obligations relating to transparency, lawful basis, and automated decision-making.

Studios should anticipate future regulatory developments by adopting AI governance practices now, including:

- clear documentation of AI use cases;
- human oversight of automated decision-making affecting players;
- bias and fairness testing in AI-driven systems; and
- explainability where AI materially affects gameplay, rewards, or enforcement actions.

There is also likely to be regulatory overlap between AI and digital asset frameworks. AI-driven token economies, automated market mechanisms, and agent-based trading systems may attract scrutiny from both the SEC and data protection authorities, particularly where they affect pricing, access, or player outcomes.
Thailand has signalled its intention to align with international AI principles, including risk-based regulation and responsible AI deployment. Blockchain gaming studios that proactively align with these principles will be better positioned to adapt as formal AI governance emerges.
In practical terms, studios should treat AI not as an unregulated frontier, but as an extension of existing compliance obligations—particularly where AI systems intersect with token economics, personal data, and consumer trust.

Author: **Dr. Jason Corbett,** Silk Legal

UK

A.
Elon Musk claims that AI will change everything. Well, sort off... technically, it repeats everything.

The mystique surrounding AI is in overdrive, and so it is best to start by looking at what it actually is, before getting carried away. Generally, AI (which currently generally refers to large language models) is the use of a model over a large amount of data to organise that data in response to prompts, i.e. questions, posted to the AI model. In this respect, AI is doing something akin to an educated guess to responding the question asked, the guess being made effectively by the programmers who train the model who seek to get the AI to convincingly respond to the problem question without knowing what it is in advance.

The accuracy of this guess is disturbingly accurate, albeit still a guess so not entirely accurate. It is akin to getting a newbie to "have a go". More concerningly, not being human, AI lacks the capacity to think, and more fundamentally to be unsure. As such, inaccurate and accurate thoughts are given equal footing.

What does this mean for blockchain gaming?[3]
The speed of AI means that a result can be reached quickly, however the guessing nature of the technology means that the result may not be correct. As such, whilst it may speed up grunt tasks, and tasks which can be afforded a certain amount of latitude in terms of making mistakes (e.g. maybe AI generated co-participants in a game), for more important functions it will need to be heavily checked and reviewed. This is for example important for anything involving in-game payments, where there can be a tangible loss in the event of an error. A key question game providers will also need to consider is the extent that they are willing to tolerate bugs to reduce cost – as buggier games may command less premium value, particularly in a market that will likely become increasingly saturated over time.

It also means that there will be a heavier premium in innovation. Whilst AI can regurgitate, it cannot innovate. Genuine innovation (rather than simply applying existing innovation) will therefore trade at a greater premium, being an intrinsically human attribute. Game developers will therefore have to put particular care as to how they safekeep innovation – particular in light of the speed at which Studio Ghibli's artwork style was effectively pirated by AI, reducing its value. As well as the traditional approaches towards safekeeping intellectual property, we may also see new approaches, and in this respect the original approach to intellectual property in Moonbirds, which used a fully open model, is interesting.

Dial-a-regulator?
Whilst the temptation for participants in a new industry can be to call for regulation, as a way of gaining legitimacy and protection, that is not always smart – as clearly shown by the fact that most regulation of cryptoassets does not really cater for the blockchain gaming industry, and the cost of compliance, as well as the assumptions on which regulation was based, meant that many games struggled.

With respect to AI, we can see an interesting split of approach. The EU has rushed forwards with regulation, arguing that regulation provides for consumer protection and the comfort they derive from it benefits the industry as they are more likely to use AI. The US has taken the reverse approach, seeking not to regulate AI arguing that the cost of regulation prevents innovation. The UK has been an interesting jurisdiction in this respect, as it has departed from its historic approach of aligning with the EU, and aligned much more with the US innovation first approach. Looking at the EU regulation, much of it is focussed on data and also risk if AI falls, and again we can see that it is not created with blockchain gaming in mind. It generally does not deal with the issues for gaming companies outlined above, and so regulation is unlikely to be helpful to the sector, and so in our view studios should avoid encouraging regulation of AI.

So what to do?
AI will doubtless impact studios, and so studios should look to see how it can be used to save cost and to scale games, whilst keeping sufficient oversight over AI to stop issues from breaking the value of the game. The focus should also be on innovation[3], enabled by AI, and how to protect the studio's edge given that imitation is now easier than ever. Because whist imitation may be the best form of flattery, it is not a lucrative one.

Author: **James Burnie FRSA,** Gunnercooke LLP

B.
Studios focusing on the UK market that are looking to use AI systems in combination with digital assets, need to be prepared to navigate rapidly changing regulatory environment, especially when it comes to the emerging regulatory framework on cryptoassets in the UK (see more on this in the response to question 1).

This may be particularly challenging where studios use AI systems that shall automatically mint, distribute and transfer digital assets, given that any of the aforementioned activities may fall under the scope of the future regulated activities related to cryptoassets under the new UK regulatory framework on crypotassets that is currently in the making.

When it comes to the use of AI systems, unlike the EU, the UK currently does not have a designated regulatory framework on the use of AI. Currently, the UK Government does not intend to create horizontal AI regulation that would be equivalent to the EU AI Act. Instead, the UK Government is looking to support sectoral regulators with the development of sector-focused, principles-based approach to the regulation of AI use.

Regardless of the lack of horizontal regulatory framework, studios should stay mindful of technology-neutral legal obligations that may impact their use of AI systems including, in particular: (i) copyrights limitations, when training their AI systems based on a non-proprietary data; (ii) legal processing of personal data of their users in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Author: **Miroslav Duric,** Taylor Wessing Partnerschaftsgesellschaft mbB, Frankfurt

UY

Studios operating in Uruguay should address regulatory exposure from the design phase, rather than attempting to retrofit compliance after launch. This includes properly classifying digital assets and value flows, assessing whether certain activities could qualify as virtual asset services, and determining when AML, consumer protection, or financial regulatory obligations may arise.

Clear governance and accountability structures are particularly important where smart contracts, automated economic rules, or AI-driven systems play a central role. Even in highly automated environments, responsibility does not disappear: studios must be able to identify who controls system parameters, updates, and risk management decisions.

The integration of AI increases exposure to fraud, manipulation, market abuse, and money-laundering typologies, especially when combined with transferable digital assets and secondary markets. As a result, monitoring, traceability, and internal controls become increasingly relevant, not only for compliance purposes but also as[3] evidence of reasonable diligence.

Finally, transparency toward users is critical. Overstated or unsupported claims regarding ownership, interoperability, AI-generated content, or asset appreciation can quickly translate into consumer complaints, regulatory scrutiny, and reputational damage. In Uruguay, effective preparation means ensuring that a project remains clearly positioned as entertainment before it begins to operate, in practice, as a regulated value-based ecosystem.

Author: **Paulina Cedrola,** SYLS Ferrari

06 FUTURE OUTLOOK

FUTURE-PROOFING BLOCKCHAIN GAMING: LEGAL PRIORITIES FOR THE NEXT FIVE YEARS

As we look toward 2030, "future-proofing" has evolved beyond simple NFT ownership; it is now about the institutional professionalisation of the game economy. Based on the BGA's 2025 State of the Industry Report and recent global discourse in London and Abu Dhabi; the BGA advocates for a structural shift: studios move away from functioning as accidental, unlicensed financial institutions. Instead, the industry gravitating toward a "decentralized entertainment stack" – a model where creative studios build the "worlds", while specialized, compliant infrastructure layers handle the "money."

The BGA Core Pillars for Economic Consistency

To ensure the long-term viability of the sector, the BGA identifies three critical drivers that will transform gaming from niche crypto-projects into global entertainment powerhouses:

1. Stablecoins as the Universal Native Currency: The industry is pivoting away from volatile, speculative utility tokens. The BGA views stablecoins (regulated under frameworks like the US GENIUS Act and EU MiCA) as the standard "payment rail". This shift provides developers with predictable revenue models and players with a trusted medium of exchange that maintains its value outside the game.

2. The "Open Money Stack" Architecture: To survive the 2026 funding winter, successful studios are adopting an "infrastructure-first" approach. By integrating with pre-compliant rails (like those on Polygon or Ronin), studios offload the burden of KYC, AML, and fiat on-ramps. This enables small, innovative team to run a global economy without the overhead of a bank-grade compliance department.

3. Entertainment-DeFi Convergence: Gaming is the "front-end" for the next-generation finance. We are seeing DeFi protocols – such as staking, lending, and yield – abstracted into game mechanics. These are no longer presented as complex financial spreadsheets, but as intuitive elements of gameplay and "social money" within entertainment communities.

XSOLLA

The blockchain gaming space has matured past the point where legal teams can afford to be simply reactive. Five years ago, the question was whether regulators would pay attention to our requests for meaningful regulatory guidance. Now the question is which frameworks will stick-and the good news is that companies willing to invest in compliance infrastructure are increasingly well-positioned to shape those answers.

From our perspective at Xsolla, four legal priorities will define the next half-decade.

First, token classification will remain the central fault line. The utility-versus-security debate isn't going away, and the answer will continue to vary by jurisdiction. But this ambiguity is also an opportunity. Companies, like Xsolla, that design with optionality-tokens that function cleanly under multiple classification regimes-won't just survive regulatory divergence; they'll have a competitive advantage over those who bet on a single favorable outcome.

Second, consumer protection will overtake securities law as the primary enforcement vector. Regulators have figured out that going after token issuers is resource-intensive. Going after platforms and other infrastructure layers for deceptive practices, unfair terms, or inadequate disclosures is faster and plays better publicly. The flip side? Companies that genuinely prioritize transparency and fair dealing will stand out-and that differentiation is starting to matter to players and partners alike.

Third, the gambling question isn't settled-it's expanding. We've spent years debating whether loot boxes constitute gambling. Now add secondary markets, token staking mechanics, and prediction features to that mix. Regulators in multiple jurisdictions are revisiting these questions with broader definitions.

The opportunity here is to get ahead of it: if your game has any mechanic where players risk something of value for an uncertain outcome, building a defensible position now means you're ready when clearer rules arrive-not scrambling to catch up.

Fourth, cross-border complexity will force operational choices. The dream of a single global product serving all markets is increasingly incompatible with regulatory reality. But that's not necessarily a bad thing. Legal teams that help their businesses make smart, strategic calls about where to operate and where to geo-fence aren't limiting growth-they're focusing it. Sometimes the most valuable legal advice is knowing which markets offer the best risk-reward balance and doubling down there.

At Xsolla, we've approached blockchain with legal and compliance embedded from inception-not bolted on after product or business decisions were made. That's not a burden; it's a foundation. When your platform touches payments, digital assets, minors, and multiple jurisdictions simultaneously, early investment in compliance becomes a genuine asset. It's what allows you to move faster when opportunities emerge, not slower.

The companies that will thrive are the ones building fully compliant structures flexible enough to adapt when greater clarity arrives-and confident enough to lead while the rules are still being written.

The next five years belong to the prepared. That is our motto in the Legal department at Xsolla.

Author:
Carla Bedrosian,
Xsolla

EXCLUSIBLE

Roblox is a perfect reminder that digital ownership is not a small detail. When the platform recently announced it would move away from classic 2D faces and push dynamic faces as the new standard, the community reaction was immediate. It showed how attached players are to the assets that represent them, and how fragile trust becomes when those assets can be changed, removed, or redefined by the platform itself.

This isn't only emotional, it's economic. Players spend real money building their avatar identity and portfolio over time. Creators and studios build entire businesses designing and selling these assets, with real costs, real payroll, and real expectations of long-term value. When a platform shifts the rules, it impacts consumer confidence, but it also puts creator businesses at risk overnight.

That's why I'm optimistic about blockchain gaming. Ownership should mean stability. It should mean that what players earn, buy, and build keeps its value over time, and doesn't depend entirely on one company's decisions. Over the next five years, the legal priorities are clear: protect users, clarify rights around digital assets, and make sure creators and communities can build in ecosystems that feel lasting and fair.

Author:
Olivier Moingeon,
Exclusible

DREW AND NAPIER LLC

Nobody knows what the next five years will entail- as alluded to above, the rate of improvement and the rate of change is constantly increasing, especially in a technology related industry. Despite this, it is likely that the next five years entails developments in relation to autonomous AI, whether self-driving cars finally become a reality, or whether it comes in the form of increased incidences of "rogue AI". It is also likely that DPTs be used in the context of payments, as the entire world moves from a Web2 society to a Web3 society.

With that in mind, companies should be improving their tech stack. In the near future, it is likely that companies will be expected to be able to segregate each and every customer asset not just from that of the company (which is the current obligation), but also from that of other customers. Given the immutability and the transparency that DLTs afford, it is likely that companies, in particular DPT service providers, will be expected to be able to segregate the specific assets of a strata of users, a sub-strata of users, of even just that of a specific individual. This would directly allow for better audits, preventing double spend and ensuring that unexpected outcomes (resulting from a bug, or otherwise) may be promptly detected and if necessary, remediated.

Companies may also be expected to adopt programmable money. The Monetary Authority of Singapore has already signalled this through Project Orchid, which is a multi year, multi phase exploratory project examining the various design and technical aspects pertinent to a possible digital Singapore dollar; including its functionalities as well as its interaction with existing payment infrastructures.

Under the currently regulatory landscape, limited purpose DPTs are subject to less stringent regulatory and licensing burden. Programmable money would thus directly lighten the regulatory burden of any entity that seeks to use DPTs solely for in-game functions.

Simultaneously, the adoption of programmable money would likely lead to a flourishing economy within the game itself, as it would allow for automatic player-to-player trades to be possible. For example, a player seeking to purchase a high value in-game digital asset would no longer have to trust the seller, as the programmable money (through the use of a smart contract) would be able to only release the funds once the smart contract has confirmed that the transfer of the high value in-game digital asset is complete.

Authors: **Grace Chong & Bryan Ong,** Drew and Napier LLC

NXT LAW

Cayman is fortunate to have a Government supportive of innovation and a regulator which has taken sensible steps to protect consumers but keep innovation in Cayman, in contrast to the pivots required in recent years in the USA and other countries.

While sandboxes are useful for light-touch regulatory approaches, they have had limited adoption globally.

At a first-principles position, the structure of a Cayman Islands Foundation, coupled with British Virgin Island token issuer subsidiary, has proven to be the most popular and robust form of token and project launch structure to date. As such, the legal priorities around this framework as a driver of innovation is key to ensuring it retains, and grows, that position.
Cayman Islands Foundations are governed by the Foundation Companies Act (2025 Revision) and are incredibly flexible, typically having an independent board and a supervisor with power to remove and replace that board.

The law provides no express prohibition on conflicts of interest between the supervisor and the board, and we have seen some pushing 'one-stop shops' where the supervisor is controlled by the same persons who control the board. This is a situation which should be avoided and ideally legislated against to preserve the valuable governance framework that foundations can provide.

While foundation companies can have a founder (who typically has power to change the supervisor) and beneficiaries as well as members, we typically do not see those roles in new foundations, as the supervisor/independent board combination is (subject to there being no conflicts) a robust basis for good governance.

We would like to see a light touch VASP approach to interface any regulated aspects of games in the Cayman Islands emerge to help match regulation to risk and to see greater certainty around the use of, and integration of stablecoins into games and other platforms in the near future.

Market confidence in stablecoins and their integration into games and other platforms remains, in our view, one of the greatest coming drivers of user adoption of web3 and blockchain gaming.

Close attention to these matters will be key to ensuring the future of gaming in the Cayman Islands will be ready not only for player one, but for all the players yet to come.

Authors: **Michael Bacina & Jonathan Turnham,** NXT Law

MOTO LEGAL

As the digital asset landscape matures, the era of regulatory ambiguity is ending. For in-house counsel, the next five years will require a pivot from reactive defence to proactive architectural alignment with specific virtual asset regulations and gaming laws.

To future-proof your blockchain gaming portfolio, we advise focusing on three strategic pillars:

1. Conduct a product-level assessment before you commit to building and deploying
If your strategic intent is to remain outside the perimeter of gambling regulation, reliance on general terms and conditions is no longer sufficient. The "sweepstakes" or "prize pool" nature of many blockchain based games creates inherent friction with UAE penal codes, virtual asset laws and global gaming laws.

Recommendation: In-house teams should engage external specialists to conduct a high-level assessment of the game design and associated products, before committing time and resources to building the wrong product. It is not uncommon for developers inadvertently trigger securities or gambling legal issues, or any unwanted virtual asset regulatory obligations. Good counsel that can advise on product detail can go a long way in avoiding unwanted regulatory issues. This is not just about compliance; it is about risk mitigation. The next step would be to obtain a third-party legal opinion on your game's design, which will serves as a defence, should a regulator ever inquire about your status.

2. Leaning Into Regulation

The market demand is shifting. We are seeing an explosion of interest in prediction markets, high-stakes wagering, and complex GameFi economies. Attempting to shoehorn these products into gaming exemptions is becoming a liability that limits growth and a game developer's ability to be creative.

Recommendation: Rather than engineering loopholes, developers should consider "leaning in" to regulation. Operating under a recognized body, such as the UAE's General Commercial Gaming Regulatory Authority (GCGRA), offers a distinct competitive advantage: legitimacy!
Other benefits of leaning into regulation include:

- Banking Access - Licensed operators can secure tier-1 banking and payment processing, a major hurdle for unregulated blockchain based businesses;
- User Trust - In a market plagued by "rug pulls," a license is a powerful marketing asset;

- Freedom to Innovate – by understanding the scope and limitations of your authorization, you gain the freedom to build the betting and prediction products the market actually wants, without the constant fear of enforcement actions.

3. Keep your finger on the global pulse

The regulatory landscape is not uniform. In-house counsel must maintain a 360 degree view of global changes in regulations to get ahead of trends. In our opinion (which is debatable), the two most influential jurisdictions are:

- The United States: Remains the primary source of enforcement risk. Watch the SEC and CFTC's treatment of "gamified" DeFi, prediction markets and other blockchain based games. Their aggressive stance often defines the "high-water mark" for compliance globally.
- The UAE: Is rapidly becoming the primary source of opportunity. With the GCGRA and VARA, the UAE is building the world's first cohesive framework for blockchain based gaming. Aligning your corporate structure with UAE standards often creates a "gold standard" compliance posture that is exportable to other emerging markets.

In summary, the winners of the next cycle will not be those who hide from regulation, but those who architect their business around it. Whether you choose to avoid or lean in to regulation, you should make a calculated, informed and deliberate decision.

Author: **Chris Elias,** Moto Legal

SKALE FOUNDATION

Building successful Web3 games is no longer just about creativity or technology. Games increasingly involve real economic value, real users, and real regulatory oversight. As a result, teams must design their products to be compliant, secure, and easy to use from the very beginning. Treating these aspects as core product requirements, rather than retrofitting any of these later, reduces risk and supports long-term growth.

Gambling and DLT Regulations: overlapping but distinct frameworks

Online gambling, digital casinos, and prediction markets continue to grow globally, and many Web3 games now sit close to this regulatory space. Regulation in this area is strict and varies significantly by jurisdiction. As a result, Web3 gaming teams must consider licensing requirements, geofencing, KYC and AML obligations, age verification, and responsible gaming measures early in the product design process.
In Europe, the legal treatment of a Web3 game often depends on factual details, such as whether outcomes are driven by skill or chance and whether in-game assets are purely functional or have monetary value. Small design choices can materially change a game's regulatory classification, making careful assessment essential.

Alongside gambling laws, DLT regulations (such as MiCAR) establish harmonized frameworks across the globe for issuing and offering crypto-assets. While those do not regulate gambling activity, it applies to Web3 games that issue or use tokens as part of gameplay. Many gaming tokens may qualify as utility tokens if they provide access to a digital service and are not marketed as investment products. This triggers obligations around disclosures, fair marketing, and transparency.

DLT regulations and gambling regulations often address different risks. MiCAR for example focuses on crypto-asset issuance, market integrity, and user protection at the EU level, while gambling laws focus on player protection, fairness, and addiction prevention and are enforced nationally. For Web3 games, this means that compliance with DLT regulations does not remove exposure to gambling regulation. Both frameworks must be assessed in parallel to ensure a sustainable and compliant product launch.

Betting and Prediction Markets in Web3

Betting and prediction markets are currently among the most visible and fast-growing consumer Web3 applications. They have attracted significant user activity around sports, political events, and other real-world outcomes. While traditional DeFi use cases such as stablecoins and DEXs still account for a large share of on-chain activity, prediction markets stand out due to their rapid growth and public attention.

This trend matters for Web3 gaming because many games include mechanics that resemble wagering or outcome-based rewards. As soon as players can stake tokens or assets on uncertain results, games may start to overlap with gambling or prediction market regulation.

Conclusion

Web3 gaming increasingly sits at the intersection of entertainment, finance, and regulation, requiring teams to balance innovation with security, usability, and legal compliance. Projects that embed compliance, reduce user friction, and design for regulatory flexibility from the outset are best positioned for sustainable, long-term success.

Author:
Fabio Tomaschett,
SKALE Foundation

SERGIO VARONA

From my perspective, future-proofing blockchain gaming over the next three to five years will depend on how effectively the industry integrates open financial infrastructure into games while managing regulatory risk in a scalable and predictable way.

One of the most significant shifts I see today is the growing adoption of stablecoins as a standard payment instrument in gaming and consumer applications more broadly. As stablecoins become familiar, trusted, and increasingly regulated forms of digital money, they enable a new era of global, internet-native payments within games. For developers, this creates opportunities for new business models, ranging from seamless global monetization and secondary markets to incremental revenue streams that extend beyond traditional in-app purchases. However, as stablecoins move from being a niche crypto asset to a widely used payment rail, gaming economies begin to intersect directly with payments regulation, consumer protection, and financial compliance frameworks.

In practice, a key hurdle for game studios remains access to fiat on-ramps and off-ramps. These functions trigger regulatory requirements that most studios are not structured to manage directly. To address this, the industry is moving toward a modular infrastructure where licensed Payment Service Providers (PSPs) and compliance functions are integrated at the infrastructure layer, rather than leaving individual game studios to navigate complex requirements on their own. By leveraging these regulated interfaces, developers can access compliant fiat-to-stablecoin rails while preserving the benefits of public, interoperable networks.

Looking ahead, I expect embedded compliance to become the industry standard. Wallets, payment layers, and products built on-chain will increasingly perform regulatory checks, based on jurisdiction, transaction type, and risk, by default. This approach better protects developers from regulatory exposure while improving consumer safeguards, without undermining the openness of public blockchains.

Finally, interoperability and composability will require regulators to move beyond siloed frameworks built for closed platforms. Games are becoming entry points to a broader digital economy, not isolated environments. Future-proof regulation should recognize this reality and support proportionate, technology-neutral approaches that enable innovation while managing risk.

Author:
Sergio Varona

OUR CONTRIBUTORS

Juan Manuel Campos Álvarez, SYLS

Head of Venture Capital and Finance Regulation; with more than 20 yeas of experience, area of practice covers blockchain, fintech, venture capital and technology businesses.

Michael Bacina & Jonathan Turnham, NXT Law

The co-founders of NXT Law are avid games and have been involved in nearly 400 crypto projects since 2016, they have incorporated more Cayman Foundation structures than any other lawyers and love ensuring that their clients build on a strong foundation. Globally recognized and respected, the NXT Law team are seen as the go-to Cayman and global counsel by leading web3 gaming projects.

William O'Rorke & Imane Dahmani, ORWL, Paris

Co-founder of ORWL, William O'Rorke is recognized as one of France's leading experts in crypto-asset regulation. For nearly ten years, he has been advising players in the crypto-finance sector, combining high-level legal expertise with a deep understanding of blockchain technologies.

Imane supports financial institutions and Web3 stakeholders across all regulatory matters (MiCA, MiFID, AML/CFT, and payment services), drawing on extensive experience in new technologies and compliance.

Alireza Siadat, Deloitte Legal

Alireza Siadat is a German lawyer and digital finance expert, currently serving as a Partner at Deloitte Legal. He specializes in banking and finance law, with a particular focus on Distributed Ledger Technology (DLT), blockchain, and crypto assets. Alireza is contributing to the DLT ecosystem as board member of the German Blockchain Association and co-publisher in digital-assets at Wolters Kluwer.

Miroslav Duric, Taylor Wessing Partnerschaft sgesellschaft mbB, Frankfurt

Multi-jurisdictionally qualified legal professional advising clients on various aspects of the EU and the UK financial regulation. As a trusted advisor of fintech companies and incumbent financial institutions he is particularly specialising in advising clients on complex legal questions related to the integration of emerging technologies like crypto-assets, DeFi, Artificial Intelligence, and cloud computing in finance.

Paolo Maria Gangi, Gangi Law Firm

Paolo Maria Gangi is an Italian lawyer who provides legal advice to crypto foundations, DAOs and web 3:0 companies for regulatory issues (including MiCA) and company formation, DeFi, governance and IP.

Yumi Ahn & Ryo Yamada,
Tokyo International Law Office

Yumi Ahn is a California-qualified lawyer based in Tokyo specializing in legal issues surrounding emerging technologies including blockchain technologies and cross-border M&A. Yumi is currently working as Counsel at Tokyo International Law Office (TKI) and is a registered foreign lawyer member of the Daini Tokyo Bar Association.

Ryo Yamada is an associate at Tokyo International Law Office (TKI), advising clients on cross-border M&A, regulatory, and dispute matters. His work includes legal analysis of emerging regulatory issues, including those relating to blockchain-related businesses. Ryo is qualified to practice in Japan and is a member of the Daini Tokyo Bar Association.

Teresa Carballo & Edgar Young,
Pacifica Legal

Teresa Carballo is a Panamanian lawyer focused on bridging technology and law, with a practice centered on advising blockchain and virtual-asset projects on their legal and regulatory strategy, particularly in Panama and also Mexico. She is a co-founder of Pacífica Legal, where her work frequently involves designing compliant corporate structures, commercial operations, all with a pragmatic, prevention-oriented approach grounded in real-world risk management.

Dr. Edgar Young is a Panamanian attorney with more than a decade of experience in multi-jurisdictional legal practice. He holds a Ph.D. and an LL.M. in International Private Law from RUDN University, as well as an LL.B. from the University of Panama.
As a Partner at Pacifica Legal, Edgar focuses on Emerging Technologies, Blockchain, IT, FinTech, and venture-backed startups. His practice includes offshore corporate structuring, regulatory compliance, fundraising, token offerings, and comprehensive legal advisory services.

Grace Chong & Bryan Ong,
Drew and Napier LLC

Grace Chong heads the Financial Services Regulation practice in Drew & Napier LLC. She has extensive experience advising on cross-border and complex regulatory matters, including licensing and conduct of business requirements, regulatory investigations, and regulatory change. A former in-house counsel at the Monetary Authority of Singapore (MAS), she regularly interacts with key regulators, is closely involved in regional regulatory reform initiatives and has led discussions with regulators on behalf of the financial services industry.

Grace Chong heads the Financial Services Regulation practice in Drew & Napier LLC. She has extensive experience advising on cross-border and complex regulatory matters, including licensing and conduct of business requirements, regulatory investigations, and regulatory change. A former in-house counsel at the Monetary Authority of Singapore (MAS), she regularly interacts with key regulators, is closely involved in regional regulatory reform initiatives and has led discussions with regulators on behalf of the financial services industry.

Dr. Jason Corbett,
Silk Legal

Dr. Jason Corbett is the Managing Partner of Silk Legal, a Bangkok-based law firm
advising on blockchain, Web3, fintech, and technology-driven corporate matters. He
has over 15 years' experience in commercial and insolvency law, with more than five
years focused on digital asset regulation and Web3 ecosystems.

Chris Elias,
Moto Legal

Chris is passionate about blockchain, fintech, Ai and emerging tech and has worked with over 250+ blockchain and emerging tech companies from start-up, scale-up to enterprise. These include RWAs, AI, payments, cyber security, technology defence,, crypto exchanges, DeFi, Gaming, DAOs, Layer 1s and 2s, token raises and so much more. Chris also has experience founding, operating and exiting his own startup and knows firsthand the journey of the founders. Chris prides himself on providing practical advice and solutions.

Konstantinos Adamos,
Revolut Group

Konstantinos is a financial services regulatory lawyer focusing on fintech and in particular cryptoassets. He is the Group Head of Legal for Revolut Digital Assets responsible for the group's regulatory strategy on cryptoassets, advising the business on licensing, product structuring and regulatory compliance. Konstantinos also serves as a Non-Executive Director on the Board of Revolut's MiCA licensed CASP.

Josh Lawler,
Zuber Lawler

Josh Lawler, Partner at Zuber Lawler, a minority owned law firm, is an expert in digital asset regulation, securities law, intellectual property rights, mergers and acquisitions and commercial transactions with a strong focus on crypto, NFTs and other digital assets and related systems. As a dedicated futurist, Josh leads the firm's New Technology Practice Group, focusing on novel issues presented by developing technology including Blockchain (distributed ledger), artificial intelligence, robotics, virtual/augmented reality and internet of things.

Paulina Cedrola,
SYLS Ferrari

Lawyer specialized in corporate law, currently pursuing a Master's degree in Digital Law and Technology, with a focus on blockchain, AI governance, data protection, and tech industry legal frameworks.

Roshi Sharma,
LawBEAM

Roshi Sharma is a senior lawyer and the founding partner of LawBEAM. LawBEAM is a leading international firm focused on crypto and digital assets and blockchain gaming. Roshi provides legal advice and solutions to technology companies and regulated firms in the UK and internationally.

Gonzalo Cantero Puig & Marina Villalonga Cladera,
Asensi Abogados

Gonzalo Cantero is a lawyer specializing in blockchain, digital assets, and financial regulation. With a strong academic background and hands-on experience, he advises companies on regulatory compliance, licensing, legal structuring, and risk management within the fintech ecosystem.

Marina Villalonga is leading the corporate and digital assets departments at Asensi Abogados. Marina has wide expertise in M&A, contractual law, insolvency and touristic law. She is a qualified lawyer, too, in blockchain, fintech, e-commerce and data protection, advising both national and international clients on complex regulatory, transactional, and strategic matters in these fast-evolving sectors.

Andrew Robert Mitchell KC,
FGA Law Providenciales, DM Legal Consultants RAK

Legal practitioner of over 40 years with offices in TCI, Dubai, London and access to other legal markets, experienced in compliance, regulation and practical solutions to complicated factors.

James Burnie FRSA, Nicky Androsov, Gunnercooke LLP

James is a ranked Band 1 in Chambers FinTech Legal: Blockchain and Cryptocurrencies, and is a partner at gunnercooke llp. He has been involved in crypto for around 10 years, since advising on the first successful UK-based ICO, and has been involved in drafting around 3% of the global regulation of cryptoassets. He has acted for well over 300 Web3 companies.

Nicky is a recommended lawyer in Legal 500 for Intellectual Property. A partner at gunnercooke, she has substantial expertise in Intellectual Property, Information Technology and Data Protection mattersand her clients include providers and customers of AI, software and other technology solutions, as well as players across the Web3 ecosystem, from NFT artists and layer 1 blockchains to metaverses and gaming platforms.

Bernhard Kronfeller, Boston Consulting Group

Bernhard is a Partner & AD at Boston Consulting Group (BCG), where he has been advising leading institutions, regulators, and digital-native companies since joining the firm in 2007, following earlier experience at J.P. Morgan in London. He co-leads BCG's Digital Assets business and is responsible for the global lead Marketing in Web3. Beyond BCG, Bernhard is a founder, co-founder, and angel investor in multiple FinTech and Web3 start-ups. He is also a university lecturer at TU Wien and the University of Vienna, and advises regulators in Austria and Qatar on digital-asset regulation.

Ranjana Adhikari, Sarthak Doshi & Prateek Joinwal, Shardul Amarchand Mangaldas & Co

Ranjana Adhikari is a Partner in the Technology, Media and Telecommunications ('TMT') practice at SAM & Co., specialising in advising global tech, Web3, gaming, and OTT platforms on regulatory compliance, data protection, and multi-jurisdiction launches. She is routinely engaged by businesses in their go-to-market strategy from a regulatory and corporate perspective and has advised companies (including crypto exchanges) on data breach matters.

Sarthak Doshi is a Principal Associate in the TMT practice group at SAM & Co., and specialises in advising digital-first businesses across Web3, online gaming, financial services, and e-commerce. On the Web3 front, he advises leading crypto exchanges, Web3 gaming guilds and payment solution providers on licensing, token issuances, monetisation, and liaisoning with regulatory authorities.

Prateek Joinwal is an Associate at SAM & Co. in the TMT practice. He advises clients across digital and regulated sectors, including gaming, banking, e-commerce, and Web3 on regulatory, compliance and commercial matters. He focuses on licensing and regulatory approvals advisory, platform compliance and commercial enablement for banks, gaming operators and digital platforms. He routinely drafts and negotiates technology contracts spanning software development, API and SDK licensing, cloud and data partnerships, and content/platform integrations.

Fabio Tomaschett SKALE Foundation

Fabio Tomaschett is Vice President of Business Operations at the SKALE Foundation, where he focuses on scaling Web3 infrastructure and driving

Olivier Moingeon,
Exclusible

After 18 years as an executive in the Luxury Industry, Olivier co-founded Exclusible in 2021. Specialized in immersive technologies, Exclusible is an award-winning Roblox studio helping Brands and IPs launch impactful experiences on Roblox. Our clients include Care Bears, Sesame Street, Winx Club, Rabbids, e.l.f. Beauty and many more!

Archana Kavil &
Priya Makhijani,
Zeroto3 Collective

Archana is a lawyer specialising in IP prosecution and commercial contract drafting for media, entertainment, Web3, blockchain, and gaming companies. Her work spans regulatory, compliance, and transactional support for technology-driven businesses.

Priya Makhijani is a highly experienced corporate lawyer advising startups and investors on venture capital fundraising and broader corporate matters and commercial contracts, including cross-border transactions. She also advises on Web3 fundraising and innovative financing structures, including token offerings.

Carla Bedrosian &
Chris Hewish
XSolla

Carla Bedrosian, Esq. is an award-winning C-suite executive and globally recognized legal leader who (very happily) serves as Global Chief Legal Officer at Xsolla, overseeing legal operations across multiple continents, while spearheading strategic new business lines, M&A activity and partnerships critical to global expansion. With 25 years of executive experience in the private and publicly traded sectors, she has earned prestigious recognition, such as the LA Times In-House Counselor of the Year, Women We Admire 2025 Award Recipient,and Oncon Legal ICON 2025 Awards Recipient, and is a California and New York licensed attorney with a distinguished litigation background from Sullivan & Cromwell LLP and Loeb & Loeb LLP.

Chris Hewish operates at the intersection of game technology, digital commerce, and platform infrastructure. Throughout his career, he has focused on building scalable, player-first systems that empower creators, support sustainable economies, and function reliably across borders and markets at Activision, DreamWorks, and Xsolla.