frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 20 October 2025
DOI 10.3389/fbloc.2025.1675735

OPEN ACCESS

EDITED BY
Eda Sahin-Sengul,
Bath Spa University, United Kingdom

REVIEWED BY
Beril Taşkın Kapusuzoğlu,
Boğaziçi University, Türkiye
Ghulam Mustafa,
University of the Punjab, Pakistan

*CORRESPONDENCE
Ana Mercedes López Rodríguez,
amlopez@uloyola.es

RECEIVED 29 July 2025
ACCEPTED 25 August 2025
PUBLISHED 20 October 2025

CITATION
López Rodríguez AM (2025) Consumer protection in blockchain-based metaverses: a comparative study of cross-border legal gaps and platform governance.
Front. Blockchain 8:1675735.
doi: 10.3389/fbloc.2025.1675735

Consumer protection in blockchain-based metaverses: a comparative study of cross-border legal gaps and platform governance

Ana Mercedes López Rodríguez*

Departamento de Derecho, Facultad de Ciencias Jurídicas y Políticas, Universidad Loyola Andalucía, Seville, Spain

Blockchain-based metaverse platforms such as Decentraland and The Sandbox offer a vision of decentralized digital ownership and seamless cross-border interaction, yet expose users to significant legal and security risks due to fragmented consumer protection frameworks. This article undertakes a comparative legal analysis of six major jurisdictions—the European Union, United States, China, Singapore, Brazil, and South Korea—focusing on jurisdictional issues, data privacy, liability, and dispute resolution within decentralized virtual worlds. The findings reveal a fragmented regulatory landscape, with ongoing gaps that contribute to declining user trust and engagement. These unresolved legal challenges, alongside persistent security vulnerabilities, undermine the long-term viability of metaverse ecosystems. To address these problems, the paper proposes a hybrid governance framework that integrates blockchain-native tools, such as smart contract arbitration, with enforceable legal standards. This approach aims to align innovation with accountability and foster a more trustworthy, sustainable, and user-centered metaverse.

KEYWORDS

blockchain-based metaverse, consumer protection, jurisdiction and conflict of laws, decentralized governance (DAOs), smart contracts, dispute resolution (ADR/ODR/BDR), comparative legal analysis

1 Introduction

As consumer activity continues to grow within virtual environments—particularly blockchain-based metaverse platforms such as *Decentraland* and *The Sandbox*—the legal challenges surrounding digital transactions, ownership, and user rights are becoming increasingly complex. In these immersive settings, users routinely buy, trade, and create digital assets, including virtual land, non-fungible tokens (NFTs), in-game currencies, and subscription-based services (Belk et al., 2022). These interactions often carry real financial value and involve the exchange of personal and sensitive data, yet they frequently occur beyond the reach of traditional regulatory oversight (Falchuk et al., 2018).

Despite the expanding scale and economic relevance of these platforms, most existing consumer protection laws remain rooted in frameworks designed for physical goods or conventional e-commerce. As a result, they are ill-equipped to address the distinctive risks posed by decentralized and immersive digital ecosystems. Issues such as the enforceability

of digital ownership, the opacity of terms of service, vulnerability to fraud, and inadequate data safeguards are becoming more pressing (Mourtzis et al., 2022). The decentralized and pseudonymous nature of blockchain-based systems, integral to many metaverse platforms, further complicates enforcement efforts by limiting the effectiveness of traditional legal remedies (Bonomi et al., 2023).

Addressing the emerging risks of consumer interaction in metaverse environments requires more than simply extending traditional consumer protection frameworks. It requires a reexamination of core legal concepts—such as ownership, consent, and liability—in light of the technical and social architecture of decentralized virtual worlds (Corrales Compagnucci et al., 2022). Among the most urgent concerns is jurisdictional uncertainty: transactions in the metaverse frequently span multiple legal systems, yet offer little clarity about which laws apply, or which authorities hold jurisdiction. This legal fragmentation exposes users to uneven protections and makes cross-border enforcement a persistent challenge (American Bar Association, Committee on Cyberspace Law, 2000).

This article explores both dimensions of this problem. First, it analyzes how consumer protection laws in six major jurisdictions—the European Union, United States, China, Singapore, Brazil, and South Korea—are responding to legal ambiguities in blockchain-based metaverse contexts. Second, it investigates how leading platforms have structured their internal governance and dispute resolution systems. By bridging these two perspectives—the external regulatory landscape and the internal architecture of metaverse platforms—the study reveals how platform practices both reflect and reinforce broader regulatory fragmentation. The findings make a strong case for developing harmonized, blockchain-aware legal frameworks that can effectively operate within an increasingly decentralized and global digital economy.

2 Methodology

This study employs a doctrinal legal methodology to assess the capacity of current regulatory frameworks to address cross-border consumer protection challenges in blockchain-based metaverse environments. Its contribution is fourfold.

First, the analysis offers an integrated examination of how legal systems address critical risks in digital markets, including data governance, contractual fairness, and AI-driven service provision. Unlike many existing studies that treat these areas in isolation (Yadav, 2024; Rosenberg, 2022), this paper presents a holistic view of the legal landscape as it applies to the metaverse.

Second, the study adopts a comparative perspective, contrasting legal developments across six major jurisdictions: the European Union, the United States, China, Singapore, Brazil, and South Korea. While prior efforts—such as the International Bar Association's metaverse report—tend to treat each jurisdiction independently (Figueiredo, 2025), this analysis identifies both points of convergence and key divergences, offering insight into broader global patterns in consumer protection regulation.

Third, the paper addresses the complex jurisdictional and conflict-of-law issues that arise in decentralized environments. It interrogates the limits of traditional legal assumptions—such as the existence of identifiable parties or a fixed locus of legal authority—in the face of borderless, pseudonymous, and immutable systems.

Finally, the study supplements legal analysis with a close examination of governance and dispute resolution mechanisms used by decentralized metaverse platforms. Special attention is given to alternative and blockchain-based dispute resolution methods (ADR and BDR), evaluating their effectiveness in securing consumer redress in decentralized, transnational settings. By integrating doctrinal and comparative legal analysis with real-world platform practices, this methodology offers a comprehensive and practice-oriented understanding of consumer protection in the evolving metaverse economy.

3 Findings

The findings of this study stress a growing mismatch between existing consumer protection frameworks and the realities of blockchain-based metaverse environments.

3.1 Regulatory challenges

Across jurisdictions, regulatory systems consistently fall short in addressing the legal and practical risks posed by decentralized platforms, pseudonymous user identities, and smart contract-based transactions.

First, privacy and data protection laws—such as the EU's General Data Protection Regulation (Regulation (EU) 2016/679, 2016), the California Consumer Privacy Act (California Consumer Privacy Act, 2018), and China's Cyberspace Administration measures—struggle to align with the fundamental characteristics of blockchain technology. The immutability and distributed nature of public ledgers are at odds with key consumer rights, including the right to be forgotten and the ability to withdraw consent. These tensions become even more pronounced when biometric and behavioral data, often collected through immersive metaverse experiences, are stored on-chain in ways that cannot be reversed or easily redacted.

Second, traditional contract and liability regimes offer limited recourse in metaverse contexts. Smart contracts—automated and self-executing by design—generally lack built-in mechanisms for consumer redress, cancellation, or revision. This challenges core protections found in laws the EU Directive on Unfair Terms in Consumer Contracts (Directive 93/13/EEC, 1993), like the EU Consumer Rights Directive (Directive 2011/83/EU, 2011), the U.S. Federal Trade Commission Act (Federal Trade Commission Act, 2018), and similar statutes in Brazil and South Korea. Furthermore, when digital assets such as NFTs or virtual services malfunction or cause harm, existing product liability laws provide little guidance—especially when the party responsible is unidentified or legally unaccountable.

Third, jurisdiction and conflict-of-law doctrines remain poorly suited for decentralized systems. Whether under the EU's Brussels I Recast Regulation (Regulation (EU) No 1215/2012, 2012), the U.S. "minimum contacts" standard, or domicile-based rules in parts of Asia, traditional tests for asserting legal authority break down when users interact through pseudonyms, and when activities occur on

platforms operated by DAOs with no fixed location or legal personhood.

Fourth, the redress landscape is fragmented and opaque. Alternative and online dispute resolution (ADR and ODR) mechanisms are often overridden by platform-imposed arbitration clauses, many of which direct users to remote jurisdictions with weak consumer safeguards. For instance, major platforms such as *Decentraland*, *The Sandbox*, and *Axie Infinity* include mandatory arbitration clauses tied to Panama, Malta, and the Cayman Islands—often undermining international principles of fair access to justice, such as those articulated in Brussels I Recast.

Finally, emerging platform governance systems—particularly DAO-led models—present further legal uncertainty. While blockchain-native tools like *Kleros* show potential as decentralized dispute resolution mechanisms, their legitimacy, enforceability, and compatibility with national legal standards remain unresolved. These systems currently lack procedural transparency and oversight, raising concerns about fairness, due process, and consumer trust.

3.2 Consumer issues

Real-world user experiences in blockchain-based metaverse platforms highlight the practical implications of the identified regulatory gaps. In *Decentraland*, users have reported significant technical challenges, including laggy servers, poor draw distance, and a "clunky" user interface, which detract from the platform's marketed immersive experience (Cryptonator's, 2025). Additionally, the lack of robust governance and oversight has created opportunities for abuse, raising ongoing concerns about the viability and security of the *Decentraland* ecosystem (Ravenscraft, 2021). These technical shortcomings, combined with low concurrent user numbers (Smith, 2024)—reinforce the risk of unmet consumer expectations, potentially leading to disputes over purchased virtual goods or services.

Similarly, *Axie Infinity* has faced user dissatisfaction due to economic volatility and governance challenges (Jordan and Vidan, 2025). The devaluation of its in-game token, *Smooth Love Potion* (SLP), which became "useless" due to a lack of mechanisms to burn excess tokens, led to significant financial losses for players who invested heavily in the play-to-earn (P2E) model (Ramos, 2023). At its peak in August 2021, *Axie Infinity* generated $215 million in revenue, but the subsequent decline in SLP value and high entry costs—requiring players to purchase three Axies at hundreds of dollars—frustrated users and contributed to a drop in engagement (Manoylov, 2022). Furthermore, *The Ronin network* hack exposed serious security flaws in *Axie Infinity*'s platform, undermining user trust and raising concerns about the safety of digital assets in decentralized metaverse environments (Wilson and Howcroft, 2022). These cases illustrate how technical, economic, and security issues amplify consumer risks in decentralized metaverses, particularly when clear redress mechanisms are absent.

In *The Sandbox*, similar consumer vulnerabilities have emerged from governance shifts and disputes over virtual assets. In 2024, *The Sandbox*'s platform updates, such as changes to LAND staking rewards and rendering capabilities, raised user concerns about the devaluation of virtual land parcels, potentially leading to disputes over misrepresentation under consumer laws like truthful advertising standards ("Adjustment to LAND Staking Multipliers," 2024). Users expressed frustration over limited recourse under the platform's terms, with some seeking remedies like freezing injunctions against anonymous actors. However, *The Sandbox*'s Maltese jurisdiction complicated enforcement, particularly for non-EU residents, highlighting the challenges of applying legal remedies in decentralized metaverse environments (see infra, 3.5.1). Additionally, IP conflicts have arisen from unauthorized recreations of brands in user-generated experiences, resulting in takedowns and financial losses, as seen in disputes over voxel-based NFTs where smart contract ambiguities prevented clear ownership resolution (Legal Clarity, 2025).

Governance changes in metaverse platforms like *The Sandbox* have aimed to address consumer issues but highlight ongoing tensions. The Sandbox DAO, launched in May 2024, empowered SAND and LAND holders to vote on ecosystem decisions, such as content moderation and asset rules, through Snapshot voting and delegation systems ("[The Sandbox DAO]," 2024). By mid-2025, the DAO supported community initiatives, including funding for creators to enhance user trust, though early Sandbox Improvement Proposals (SIPs) revealed centralization risks, with large token holders influencing outcomes and slowing dispute resolutions, such as those related to token devaluation (O'Sullivan, 2024).

Similarly, *Decentraland*'s DAO evolved through 2024–2025 governance proposals to improve efficiency and accountability, including adjustments to voting mechanisms and debates on reducing centralized control (*Decentraland DAO, 2025*).

Taken together, these findings reveal the urgent need for coordinated legal innovation—one that incorporates interoperable rules and blockchain-sensitive instruments capable of addressing the unique challenges of decentralized virtual environments.

4 Discussion

4.1 Blockchain as the backbone of the metaverse

Blockchain technology forms the essential foundation for many metaverse platforms by enabling key features such as digital assets—including NFTs and cryptocurrencies—smart contracts, and decentralized governance. This architecture fundamentally reshapes how users interact within these virtual worlds, making peer-to-peer transactions seamless, fostering decentralized marketplaces, and reducing reliance on traditional intermediaries (Chen et al., 2024).

But blockchain's impact goes beyond its technical capabilities. It is increasingly recognized as the critical pillar for creating a decentralized, democratic virtual society where users have greater control and agency (Fernandez and Hui, 2022). The rise of Decentralized Autonomous Organizations (DAOs) exemplifies this shift, introducing innovative governance models and new ways to coordinate economic activity within the metaverse (Martha et al., 2023; Ghosh et al., 2024). These structures not only enhance user participation and autonomy but also promote collective decision-making, helping to build virtual environments that are secure, trustworthy, and fair (Santana and Albareda, 2022).

However, the transparency and immutability that make blockchain so powerful also bring fresh challenges. For example, irreversible transactions can complicate dispute resolution, and the public nature of ledgers demands new approaches to privacy and usability (Rodrigues, 2019). Addressing these challenges is crucial as blockchain continues to shape the evolving landscape of the metaverse.

4.2 Consumer risks in blockchain-based metaverse environments

The integration of blockchain technology into metaverse platforms—such as *Decentraland*, *The Sandbox*, and *Axie Infinity*—opens exciting possibilities but also introduces a range of consumer risks that challenge current regulatory frameworks (Konyalioglu, 2023).

Unlike more centralized metaverses like *Roblox* or *Horizon Worlds*, these decentralized platforms operate on blockchains such as Ethereum, Polygon, and Solana, allowing users to truly own digital assets like NFTs, participate in governance through Decentralized Autonomous Organizations (DAOs), and engage in secure transactions (Ghosh et al., 2024).

However, this innovation also magnifies potential dangers. These risks are compounded by issues of user trust and engagement, which directly impact the consumer experience. For instance, *Decentraland* has faced criticism for low user engagement, with reports indicating as few as 38 active users performing currency transactions in a 24-h period in 2022, despite claims of 8,000 daily users (Tangermann, 2022). This discrepancy, coupled with technical issues like laggy servers and a "clunky" interface, erodes user trust and increases the likelihood of disputes over virtual goods or services that fail to meet expectations (Mazafaka, 2024). Similarly, *Axie Infinity*'s $615 million Ronin network hack in March 2022 exposed vulnerabilities in its infrastructure, undermining confidence in the security of digital assets and highlighting the risks of financial loss in play-to-earn models (Wilson and Howcroft, 2022).

Users also face risks of losing assets due to vulnerabilities in smart contracts, compromised wallets, or phishing attacks (Sayeed et al., 2020). NFTs, in particular, bring their own challenges—questions of authenticity, price volatility, and disputes over ownership remain prevalent (Lince, 2022). Furthermore, because transactions are permanently recorded on public blockchains, serious privacy concerns arise around personal and behavioral data (Falchuk et al., 2018). The pseudonymous nature of these systems, coupled with weak identity verification, increases exposure to identity theft and fraud (McAmis et al., 2025).

On top of these blockchain-specific issues, the immersive, data-rich environments of metaverse platforms introduce further complexities (Jiayi Sun et al., 2022). These spaces collect sensitive biometric and behavioral data—ranging from eye movements and facial expressions to real-time emotional reactions—which can be used to build detailed psychological profiles (Ozkaynar, 2023). Such insights enable hyper-personalized and often subtle advertising techniques, like Virtual Product Placements (VPPs) and AI-driven virtual agents ("veeples"), that may influence user behavior without their conscious awareness (Rosenberg, 2022). These practices, combined with business models centered on monetizing user data, raise significant ethical questions and demand stronger regulatory oversight.

Given that many of these platforms attract younger, more vulnerable groups—such as Generation Z—there is an urgent need for transparent advertising standards and robust data protection measures to prevent exploitation and ensure users can give informed consent (Kaur et al., 2024).

Finally, the decentralized and cross-border nature of blockchain-based metaverses creates a legal grey area. Jurisdictional ambiguity and a lack of clear dispute resolution mechanisms leave consumers with limited options to seek legal recourse when problems arise (Comenale, 2021).

4.3 Legal challenges: applying and adapting existing frameworks

Existing legal frameworks for consumer protection face significant difficulties when applied to blockchain-based metaverses. The decentralized, pseudonymous, and immutable characteristics of these platforms often mean there is no clearly identifiable service provider or accountable legal entity (Table 1).

4.3.1 Intermediary liability and content moderation

The EU's Digital Services Act (DSA) (Regulation (EU) 2022/2065, 2022) and e-Commerce Directive (Directive 2000/31/EC, 2000) impose liability and transparency obligations on centralized intermediaries (Articles 4–6, 16–17 DSA; Article 5 e-Commerce Directive), which are difficult to enforce in blockchain-based metaverses governed by DAOs lacking identifiable providers.

Similarly, in the US, Section 230 of the Communications Decency Act (*47 U.S.C. § 230*) and DMCA safe harbors (United States Congress Senate Committee on the Judiciary, 1998) rely on centralized entities to moderate content or respond to takedown notices, a process undermined by blockchain's immutability and DAO-driven automation. The absence of a responsible party in decentralized systems complicates compliance, highlighting the need for blockchain-specific liability frameworks.

Transparency obligations present additional hurdles. California's Consumer Privacy Act (CCPA) (California Consumer Privacy Act, 2018), for example, imposes requirements on businesses to inform users about data collection and use. However, in decentralized metaverses with pseudonymous actors and no clearly responsible "business," enforcing these transparency rules becomes problematic.

China's Cyberspace Administration Regulations on Internet Information Services (Cyberspace Administration of China, 2022) similarly mandate platforms to monitor and remove illegal content, assuming centralized control and responsibility. Yet, blockchain-based metaverses governed by DAOs lack such centralized entities, and the immutability of blockchain records further complicates efforts to comply with content removal mandates.

4.3.2 Data protection and privacy

Data protection laws, particularly the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679, 2016), are built on

TABLE 1 Comparative overview of consumer protection challenges in decentralized metaverse environments across selected jurisdictions.

Jurisdiction	EU	U.S.	Brazil	Singapore	China	South Korea
AI regulation	Binding rules under the AI Act; enforcement limited by lack of identifiable actors.	FTC Act (15 U.S.C. § 45) applies, but pseudonymous automation complicates oversight.	No AI-specific legislation; general consumer protection applies. Bill No. 2338/2023, known as the "Brazilian AI Act," is currently under review	No comprehensive AI law; regulated via sectoral and privacy frameworks.	Draft AI governance rules focus on transparency; enforcement uncertain in decentralized settings.	AI Basic Act (Law No. 20676, 2025) mandates risk-based oversight; assumes identifiable system operators.
Product liability	Revised product liability directive (Directive (EU) 2024/2853) includes digital goods; decentralized systems challenge attribution.	§ 402A of the Restatement (Second) of Torts applies; requires identifiable manufacturer.	Strict liability applies under the Consumer Defense Code; enforcement weakened by pseudonymity.	Legal status of smart contracts under product liability is unclear; contractual recourse limited.	Product liability focuses on platforms; less effective with distributed codebases.	Enforcement difficult without a centralized producer; DAOs fall outside traditional definitions.
Smart contracts and redress	Consumer rights laws apply, but enforcement across borders and pseudonymous actors is weak.	FTC enforcement is limited in blockchain contexts due to transaction finality and anonymous parties.	Refunds and remedies are limited when smart contracts self-execute across pseudonymous networks.	Existing consumer protection laws do not address irreversible, automated contracts.	Current contract and tort frameworks are not adapted to blockchain-based execution.	Legal redress mechanisms are underdeveloped for automated, cross-border smart contract disputes.
Digital goods and guarantees	Unclear whether NFTs or virtual items qualify as "goods"; value often subjective and enforcement is weak.	UCC's application to NFTs is debated; Yuga Labs v. Ripps recognized NFTs as protectable goods.	Uncertain if digital assets fall under existing definitions; weak recourse for non-functional items.	Consumer protections for digital goods are not clearly defined in law.	Recognition of digital goods remains cautious; redress depends on centralized intermediaries.	Lack of legal clarity around virtual items; defectiveness and enforceability difficult to establish.

the assumption that centralized entities—data controllers—can be held accountable for enforcing user rights. These include core principles such as data minimization (Art. 5(1)(c)), storage limitation (Art. 5(1)(e)), and the right to erasure (Art. 17). However, blockchain-based metaverses pose structural challenges to these principles. The immutability of blockchain records and the decentralized nature of distributed ledgers make it nearly impossible to fully comply with data erasure obligations. Once data is recorded on-chain, it cannot be deleted—directly contradicting Article 17 of the GDPR.

Moreover, while users often interact through pseudonymous identities, this does not ensure true anonymity. On-chain data can potentially be linked back to individuals, creating significant risks of re-identification and undermining privacy protections. This issue is particularly pressing in metaverse environments where sensitive personal data—such as biometric and behavioral information—is collected through immersive VR and AR technologies. Article 9 of the GDPR, which protects special categories of personal data, becomes highly relevant in these contexts.

Emerging privacy-enhancing technologies, such as zero-knowledge proofs (ZKPs) and hybrid on-chain/off-chain storage models, offer promising workarounds. However, their implementation across platforms remains inconsistent, and many users remain exposed to risks like behavioral profiling and data misuse (Zhou et al., 2024).

Similar challenges arise under the California Consumer Privacy Act (CCPA) (California Consumer Privacy Act, 2018), which also guarantees users rights to data access and deletion. In decentralized and pseudonymous ecosystems, identifying a responsible party to fulfill these obligations becomes difficult, if not impossible.

Further complexities emerge with the application of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689, 2024), which categorizes certain AI-driven systems—such as personalized advertising via AI avatars or "veeples"—as "high-risk." In theory, such systems are subject to strict oversight. In practice, however, the lack of centralized control in decentralized metaverse platforms makes enforcement of these safeguards highly problematic. Without a clearly accountable actor, ensuring compliance with transparency, fairness, and user consent requirements is a major regulatory challenge (Lopez-Tarruella and Rodríguez de las Heras Ballell, 2025).

4.3.3 Consumer contracts and smart contracts

Smart contracts promise automation and efficiency—but at a cost to consumer protection. Their self-executing nature leaves little room for redress in cases of fraud, misrepresentation, or error (Weber, 2020). Once initiated, these contracts typically cannot be altered or reversed, which means consumers often have no meaningful recourse if something goes wrong.

In the EU, instruments like the Consumer Rights Directive (Directive 2011/83/EU, 2011) and the Unfair Commercial Practices Directive (Directive 2005/29/EC, 2005) are meant to protect consumers from unfair terms (Durovic, 2024). Yet these frameworks struggle in decentralized environments, where parties transact pseudonymously across borders (Moslein, 2020).

The jurisdictional limits of current law were highlighted in (Commodity Futures Trading Commission, 2022), where U.S. regulators faced serious hurdles in establishing jurisdiction and assigning legal responsibility to a decentralized collective. The case underscored the fundamental issue: in the absence of a

centralized actor or legally recognized entity, accountability becomes diffuse, and enforcement mechanisms lose their effectiveness.

The Federal Trade Commission Act (Federal Trade Commission Act, 2018), also prohibits deceptive commercial practices but is difficult to enforce in blockchain-based platforms. Pseudonymous sellers and irreversible transactions make refunds or cancellations nearly impossible—especially in NFT markets, where misleading descriptions or non-functional assets can lead to real financial harm.

These issues reflect a deeper regulatory gap. Consumer protection laws were not built for systems where contracts execute automatically, actors are anonymous, and legal remedies are out of reach. Bridging that gap will require a fundamental rethink of enforcement strategies and legal design (De Filippi and Wright, 2019).

4.3.4 Sales and guarantees

Traditional consumer protection laws struggle to keep pace with the sale of digital assets. The EU's Consumer Sales and Guarantees Directive (Directive 1999/44/EC, 1999) was built to ensure that consumers receive goods that meet expectations and are free from defects. But whether virtual assets like NFTs or metaverse land qualify as "goods" under this framework remains unclear—and even when they do, enforcement is complicated by pseudonymous sellers and irreversible blockchain transactions.

The U.S. faces similar uncertainty. Article 2 of the Uniform Commercial Code (Uniform Commercial Code, 1951) provides implied warranties, but its application to digital property like NFTs is still unsettled. A recent ruling in Yuga Labs v. Ripps (Yuga Labs Inc, 2023) recognized NFTs as protectable goods in trademark law, potentially opening the door to broader protections. Still, real-world enforcement in decentralized markets remains challenging.

Assigning responsibility is particularly difficult when smart contracts automate sales and sellers conceal their identities. Unlike physical products, virtual items do not degrade, and their "defectiveness" is often subjective—tied to market hype, visual appeal, or scarcity (Wang et al., 2022).

As digital goods become central to consumer interaction in the metaverse, existing frameworks must adapt. Without clearer rules and enforcement tools, consumers face growing risks with little chance of redress when virtual assets are misrepresented or fail to function as promised (Fairfield, 2022).

4.3.5 Financial transactions and payments

Traditional payment regulations, such as the EU's Payment Services Directive 2 (Directive (EU) 2015/2366, 2015), the US's Consumer Financial Protection Act (Consumer Financial Protection Act, 2010) and the Electronic Fund Transfer Act (EFTA) (Electronic Fund Transfer Act, 1978), ensure fraud protection and refund rights in fiat-based systems but struggle to apply to cryptocurrency transactions in decentralized metaverses. Autonomous smart contracts and the absence of intermediaries limit oversight and consumer redress.

Recent US case law (Nero v. Uphold HQ Inc, 2023; Rider v. Uphold HQ Inc, 2023), and a 2025 CFPB interpretive rule extend EFTA protections to digital assets, recognizing them as "funds." However, enforcement remains challenging in pseudonymous, decentralized environments, highlighting the need for blockchain-specific payment safeguards.

4.3.6 Product liability

The revised EU Product Liability Directive (Directive (EU) 2024/2853, 2024) marks a major shift by including digital products and software within its scope. In theory, this could extend to smart contracts and AI features in metaverse platforms. But in practice, applying product liability to decentralized code is fraught with difficulty.

When smart contracts malfunction or AI behaves unpredictably, assigning legal responsibility is nearly impossible. Code is often developed by anonymous actors or governed by DAOs, raising the question of who qualifies as a "producer" or "manufacturer" under the Directive (Zetzsche et al., 2017). Without a central entity, enforcement collapses.

Proving defectiveness in code is equally complex. Unlike physical goods, software operates in dynamic, interdependent systems, making causation and foreseeability highly technical and uncertain (Frommelt, 2021).

U.S. law faces the same problem. Section 402A of the Restatement (Second) of Torts (Restatement Second of Torts, 1965) and California's Consumer Legal Remedies Act (Consumer Legal Remedies Act, 1970), impose strict liability—but only when a responsible party can be identified. In decentralized ecosystems, that's rarely the case.

Brazil's Consumer Defense Code (Consumer Defense Code, 1990) also covers defective digital goods, yet enforcement breaks down in pseudonymous, smart contract–based systems.

Legal recognition of digital products is advancing, but enforcement still lags behind. Without centralized actors, product liability regimes—however modernized—struggle to protect users from harm in the metaverse.

4.3.7 Consumer protection frameworks for AI

Applying traditional consumer protection laws to AI systems in blockchain-based metaverses is proving unworkable. In the EU, the AI Act (Regulation (EU) 2024/1689, 2024) sets out clear rules for high-risk AI, including transparency (Art. 13), human oversight (Art. 14), and risk management (Art. 9). But these requirements are difficult to enforce when platforms are decentralized, governed by DAOs, and run on autonomous smart contracts. Without an identifiable operator, enforcement breaks down. The same problem undermines the EU's revised Product Liability Directive (Directive (EU) 2024/2853, 2024), which struggles to assign responsibility when AI code is created by anonymous contributors.

In the U.S., consumer laws like the Federal Trade Commission Act (Federal Trade Commission Act, 2018) and the California Consumer Privacy Act (California Consumer Privacy Act, 2018) require transparency and accountability in AI-driven services. Yet in decentralized metaverses, where pseudonymity and automation dominate, regulators face serious blind spots. Many AI agents operate entirely without human intervention, leaving no clear path for redress.

Traditional liability frameworks such as Section 402A of the Restatement (Second) of Torts, built around centralized producers, also collapse under decentralized conditions. In both the EU and the U.S., the law presumes the presence of a legal actor who can be held accountable—an assumption that does not hold in blockchain-native environments.

Other jurisdictions face similar dilemmas. South Korea's AI Basic Act (AI Basic Act, 2025), mandates transparency and risk controls for high-impact systems (Shivare and Park, 2025), but again relies on centralized enforcement. In metaverses built on code and anonymity, these frameworks lose traction. Legal norms may be well developed, but without structural accountability, liability remains theoretical.

4.3.8 Tensions between decentralization and enforceable regulation

The decentralized architecture of blockchain-based metaverses inherently produces tensions with enforceable regulation, as platforms like *Decentraland* and *The Sandbox* prioritize user autonomy, pseudonymity, and immutability over centralized accountability. These structural choices enable innovative governance models but also obstruct regulatory oversight, leaving consumer protections fragile and uneven. The conflict between decentralization and enforceable regulation manifests across four critical dimensions.

First, jurisdictional ambiguity undermines the applicability of existing laws. Because transactions and interactions in metaverses are borderless, regulators struggle to assert authority, and users lack clarity over which courts or laws govern their rights (see infra, 3.4). Traditional jurisdictional anchors—territory, domicile, or place of business—are obscured by DAOs and smart contracts, leaving consumers caught between platforms' global reach and fragmented national laws.

Second, privacy protections clash with blockchain's immutability. The GDPR's right to erasure (Art. 17) is fundamentally incompatible with the permanent, on-chain storage of user activity. In *Decentraland*, behavioral data tied to immersive experiences creates long-lasting risks of re-identification, while in *The Sandbox*, voxel-based data collection poses similar threats. Although techniques such as zero-knowledge proofs offer partial mitigation, their adoption remains inconsistent, leaving users vulnerable to profiling and surveillance ("Blockchain Data Protection and Privacy Compliance: A deep dive on GDPR and HIPAA requirements," 2024). This creates a persistent tension between regulatory mandates for privacy and the technical realities of blockchain systems.

Third, smart contract rigidity undermines consumer redress. Self-executing agreements, while efficient, leave little space for legal intervention when disputes arise. For instance, in The Sandbox, a flawed in-game transaction cannot be reversed through consumer-friendly remedies such as refunds or withdrawal rights. This directly conflicts with regulatory frameworks like the EU Consumer Rights Directive, which requires meaningful remedies for consumers in digital transactions (Zafar, 2025). Thus, the very feature that ensures automation and trustlessness in decentralized ecosystems simultaneously obstructs consumer protection mandates.

Finally, DAO governance illustrates the paradox of decentralization. Although presented as egalitarian, DAOs often replicate or even exacerbate centralized power structures. In *Decentraland*, the 2025 proposal for "Dynamic Voting Thresholds" sought to reduce the dominance of large token holders ("whales"), yet concentrated voting power persists, allowing influential actors to steer governance outcomes (*Decentraland DAO, 2025*). Similarly, *The Sandbox* DAO has reinforced decision-making hierarchies rather than achieving meaningful decentralization ("The Sandbox DAO," 2024). These governance flaws weaken accountability while simultaneously shielding decision-makers from regulatory oversight, producing a double tension: insufficient decentralization for fairness, yet too much decentralization for enforceability.

Taken together, these conflicts underscore the broader regulatory dilemma of blockchain-based metaverses: their defining features—immutability, borderlessness, automation, and decentralized governance—are precisely what render traditional consumer protection regimes difficult to apply. Regulators thus face a structural challenge: how to safeguard users without undermining the decentralization that underpins the metaverse's value proposition.

4.4 Cross-border complexities

The decentralized and transnational architecture of metaverse platforms poses profound challenges to established legal doctrines governing jurisdiction, applicable law, and enforcement. Features such as pseudonymity, governance by Decentralized Autonomous Organizations (DAOs), and the global circulation of digital assets like non-fungible tokens (NFTs) strain the capacity of traditional legal frameworks—including the EU's Rome I and Brussels I (Recast) Regulations, U.S. jurisdictional standards, and comparable conflict-of-law provisions in jurisdictions such as China, Singapore, South Korea, and Brazil.

4.4.1 Jurisdiction

The EU's Brussels I Recast Regulation (Regulation (EU) No 1215/2012, 2012), in Articles 17–19 allows consumers to sue in their home state if a professional targets their jurisdiction (Court of Justice of the EU, 2015), but DAOs' pseudonymity and lack of domicile undermine this protection.

Indicators like language or marketing (Court of Justice of the EU, 2010) are indeterminate in borderless metaverses, and platform jurisdiction clauses often violate Article 19's requirements—typically requiring post-dispute agreement or parties domiciled in the same Member State (see below). It is further observed that the definition of 'consumer' under the Brussels I Regulation is presently contingent upon the existence of a direct contractual relationship. This requirement is notably absent in scenarios such as the resale of non-fungible tokens (NFTs) on secondary markets, where no contractual link exists between the original issuer and the subsequent purchaser. As a result, in the event of a dispute with the issuer, the ultimate purchaser would be excluded from the jurisdictional protections afforded to consumers under the Regulation (European Parliament, 2024).

Compounding this issue, the CJEU's jurisprudence under Article 7(2) of Brussels I Recast allows jurisdiction in NFT disputes at the consumer's domicile where damage occurs (Court of Justice of the EU, 2011) or the issuer's location, if identifiable (Court of Justice of the EU, 2014). The referred new Directive on liability for defective products (Directive (EU) 2024/2853, 2024) explicitly covers digital products like NFTs, potentially applying to defects by analogy (Court of Justice of the EU, 2017), but decentralized metaverse anonymity and jurisdictional gaps challenge enforcement.

In the US, personal jurisdiction requires "minimum contacts" (International Shoe Co, 1945) or targeted effects (Calder v. Jones, 1984), but pseudonymity and decentralization complicate attribution. State long-arm statutes (*New York CPLR § 302, 2024*) face similar challenges, limiting enforcement against anonymous actors.

In Asia, similar issues arise. China's Civil Procedure Law (Articles 22–35) (Civil Procedure Law of the People's Republic of China, 2023) provides jurisdiction based on domicile, contract performance, or tort location. The Supreme People's Court's 2022 Interpretation on Internet-Related Disputes extends jurisdiction to platforms accessible within China (Supreme People's Court of the PRC, 2022), but again, pseudonymity and decentralization frustrate enforcement. Singapore's Rules of Court 2021 (Order 10) (Rules of Court, 2021) permit jurisdiction where the defendant is present, submits voluntarily, or causes harm within the jurisdiction, applying a "substantial connection" test. However, identifying such a connection in the metaverse—especially involving DAOs—remains problematic. Similarly, South Korea's Private International Act (Private International Law Act, 2022) and Civil Procedure Act (Civil Procedure Act, 2016) prioritize domicile or contract performance location but face analogous obstacles where services are provided by pseudonymous or decentralized actors using cryptocurrency.

In Latin America, Article 22 of Brazil's Code of Civil Procedure (Code of Civil Procedure, 2016) and Article 101 of the Consumer Protection Code (*Consumer Protection Code*, Brazil, 1990, *Art. 101*) allow consumers to sue in their domicile for online transactions. Nonetheless, the fluid and anonymized nature of blockchain transactions and the lack of asset situs impede the application of these rules to metaverse-based disputes involving DAOs or smart contracts. Even if a consumer secures jurisdiction in their domicile, enforcing judgments against pseudonymous entities or DAOs is difficult. Blockchain-based assets may be held in decentralized wallets, inaccessible to traditional court orders, reducing the practical benefit of suing locally.

4.4.2 Choice of law (conflict of laws)

Determining the applicable law in metaverse-related transactions presents similar legal uncertainties. Traditional conflict-of-laws frameworks, premised on identifiable parties, territorial connections, and clearly defined places of contracting and performance, often falter in this context—particularly in business-to-consumer (B2C) relationships involving smart contracts, digital assets, or decentralized autonomous organizations (DAOs).

Within the European Union, the Rome I Regulation (Regulation (EC) No 593/2008, 2008) governs contractual obligations, with Article 6 providing special rules for consumer contracts. Where no choice of law has been made, the default rule favors the law of the consumer's habitual residence, provided that the professional directed its commercial activities to that country. Even when parties agree to apply another law, Article 6(2) ensures that consumers cannot be deprived of the mandatory protections of their home jurisdiction. However, it remains unclear whether smart contracts, NFTs, or decentralized financial (DeFi) services even fall within the traditional definition of a "contract" as contemplated by Rome I (Borgogno, 2018). For example, Article 6(4)(a) excludes certain services performed entirely outside the consumer's country—an exclusion that raises real doubts in the context of metaverse interactions, which often lack any fixed territorial footprint.

Further complexity arises from overriding mandatory provisions, such as those in the Digital Services Act (Regulation (EU) 2022/2065, 2022), which may apply regardless of the chosen law, under Article 9 of the Rome I Regulation. Additionally, Article 11(4) Rome I Regulation places formal validity under the law of the consumer's habitual residence, meaning many "click-to-agree" platform contracts must meet that jurisdiction's standards. Yet, as platform Terms and Conditions often include sweeping choice-of-law clauses, courts may need to scrutinize whether such clauses unjustifiably strip consumers of Article 6(2) protections (see below).

Outside the EU, similar tensions exist. In the United States, the governing framework comes from the Restatement (Second) of Conflict of Laws (Restatement Second of Conflict of Laws, 1971), which applies the law of the state with the "most significant relationship" to the transaction (Section 188). But this standard is difficult to apply in metaverse contexts. Where is the contract formed if one party is pseudonymous? Where is performance when the service is executed by autonomous code on a distributed ledger? While the Uniform Commercial Code (UCC § 1-301) (Uniform Commercial Code, 1977) may govern certain sales transactions, such as the sale of NFTs, its application to blockchain-based smart contracts and DAOs remains legally untested (Fairfield, 2022). Moreover, federal and state consumer protection statutes like the California Consumer Privacy Act (California Consumer Privacy Act, 2018) may impose mandatory rules, but their extraterritorial reach is limited and often insufficient in metaverse contexts involving foreign or anonymous actors.

China's conflict-of-laws framework, codified in the Law on the Application of Laws to Foreign-Related Civil Relations (Law on the Application of Law for Foreign-Related Civil Relations, 2010) permits party autonomy in the selection of applicable law under Articles 41–42, defaulting to the law of the jurisdiction with the closest connection—typically the consumer's domicile in B2C relationships. The Supreme People's Court's 2022 Interpretation on Internet-Related Disputes expands consumer protections to digital platforms accessible within China (see above). Still, these frameworks face the same hurdles: identifying contracting parties, defining territorial nexus, and enforcing rules in a pseudonymous and borderless environment.

Singapore applies common law conflict-of-laws principles supplemented by statutory rules under the Application of English Law Act 1993 (Woon, 1999). Parties may designate the applicable law, but in the absence of such agreement, courts will apply the law with the closest and most real connection to the dispute (Pacific Recreation Pte Ltd, 2008). Although the Consumer Protection (Fair Trading) Act (Consumer Protection Fair Trading Act, 2009) enshrines mandatory protections for consumers, its applicability to decentralized metaverse platforms is legally unsettled.

In South Korea, the Private International Act (Articles 45–55) (Private International Law Act, 2022) follows a similar path, allowing parties to choose applicable law or defaulting to the law most closely connected to the transaction—often the consumer's domicile. It is supplemented by the Consumer Protection in

Electronic Commerce Act (Consumer Protection in Electronic Commerce Act, 2018). Yet again, enforcement is impeded by the lack of centralized actors or territorial presence in most blockchain-based environments.

Brazilian law, through the Introductory Law to the Civil Code (Decree-Law No. 4,657, 1942)— applies the law of the place where the contract was formed—or, in consumer contracts, the consumer's domicile. However, these provisions, too, are strained by blockchain-based interactions. Smart contracts and NFTs are created and executed through pseudonymous, often autonomous systems that operate independently of any identifiable "place" (Becker and Gonçalves Junior, 2023).

Across jurisdictions, the same core problem emerges: traditional legal tools—designed for physical transactions between identifiable parties—are ill-equipped to handle decentralized, extraterritorial systems like the metaverse. As blockchain and AI-driven platforms become more integral to consumer life, private international law may need a paradigm shift. Without international regulatory harmonization or the development of blockchain-specific legal frameworks, consumers will remain vulnerable, and legal certainty will continue to erode in digital environments that defy territorial logic.

4.5 Dispute resolution and redress mechanisms

Dispute resolution within metaverse platforms presents a fragmented and often legally problematic landscape, particularly for consumer protection. Leading platforms such as *Decentraland*, *The Sandbox*, and *Axie Infinity* operate under DAO governance or hybrid structures that frequently impose mandatory arbitration and exclusive foreign jurisdiction clauses—clauses that often conflict with the referred international consumer rights standards.

4.5.1 Platform-specific dispute resolution

Decentraland, *The Sandbox*, and *Axie Infinity* impose centralized dispute resolution mechanisms for user-platform conflicts, often conflicting with consumer protections. *Decentraland*'s Terms of Use (*Decentraland, Terms of Use, 2025*), mandate a 30-day informal resolution followed by ICC arbitration in Panama under Panamanian law, while user-to-user disputes rely on variable LAND or District terms, creating legal uncertainty. Recent governance updates in *Decentraland* demonstrate attempts to address these conflicts and enhance user experience. Key 2025 proposals, such as "Decentraland POIs: Categorization and Guidelines" (*Decentraland POIs: Categorization and Guidelines*, 2025) and "Add the location 84,40 to the Points of Interest" ("Add the location 84,40 to the Points of Interest," 2025), targeted conflicts over virtual space allocation and underrepresentation of areas, respectively. However, ongoing issues persist, especially related to intellectual property infringements in virtual replicas. Delays in DAO voting on these disputes have often forced users to pursue external arbitration, highlighting broader challenges in governance and enforcement within decentralized metaverse platforms (*Decentraland DAO*, 2025). *The Sandbox* (*The Sandbox Terms of Use, 2024*) requires disputes with TSB Gaming Ltd. to be litigated in Malta under Maltese law, with no provision for user-to-user conflicts, which may fall to Sandbox DAO governance. The DAO's 2024 launch introduced SIPs for community-driven resolutions ("[The Sandbox DAO]," 2024), but user-to-user disputes, like those over misrepresented NFTs or land utility changes, often lack clear pathways, exacerbating risks in a volatile economy. *Axie Infinity* (*Axie Infinity Terms of Use, 2024*) stipulates a 30-day negotiation period, followed by AAA arbitration in the Cayman Islands under Cayman law, with user-to-user Marketplace disputes left to the parties' responsibility. These foreign arbitration or jurisdiction clauses (Panama, Malta, Cayman Islands) likely violate EU consumer rights under Brussels I Recast (Art. 18) and Rome I (Art. 6), as well as protections in the US, Singapore, China, South Korea, and Brazil, limiting access to local courts. The absence of standardized mechanisms for user-to-user or B2C disputes exacerbates regulatory fragmentation.

4.5.2 Alternative dispute resolution (ADR) mechanisms

To address the identified challenges, a new generation of cross-border conflict resolution mechanisms is essential, tailored to the decentralized architectures of blockchain-based metaverses. The fragmented governance models of platforms like *Decentraland* and *Axie Infinity*—where user-to-user disputes rely on inconsistent LAND terms or lack clear resolution pathways—reflect the urgency of standardized, blockchain-native solutions.

Scholars have proposed various models. Giacalone and Arnone (2024) advocate for dispute resolution protocols embedded directly within blockchain platforms, enabling rapid and cost-effective arbitration of conflicts over digital assets, such as non-fungible tokens (NFTs) or virtual land in metaverses like *Decentraland*. Their proposed model utilizes smart contracts to automate dispute initiation and resolution, reducing the need for centralized intermediaries. For example, a smart contract could escrow disputed funds or assets and release them based on predefined arbitration outcomes, ensuring trustless enforcement. This approach aligns with the ethos of decentralization, as it minimizes reliance on traditional legal systems, which often falter in cross-border contexts due to jurisdictional ambiguity.

Taking this concept further, Gangemi (2023) proposes a sophisticated, privacy-preserving protocol built on the Ethereum blockchain, integrating zero-knowledge proofs (ZKPs), quadratic voting, and soulbound tokens to create a reputation-based adjudication system. Zero-knowledge proofs allow parties to verify transaction details or dispute evidence without revealing sensitive data, addressing privacy concerns inherent in public blockchains (e.g., GDPR's right to erasure, as discussed in Section 4.3.3). Quadratic voting is a way of voting where the influence of each participant grows with the square of the tokens they spend. This means that people who have a bigger stake in the platform—like owners of LAND in *Decentraland*—get a proportionate say in decisions. Meanwhile, soulbound tokens are special NFTs that cannot be transferred and are linked to a user's identity. These help create a reputation system that encourages honest and fair behavior when resolving disputes. Together, this approach helps make sure the dispute resolution process in metaverse marketplaces is fair and accountable, without needing a central authority to oversee everything.

Awan et al. (2023) describe a practical model of smart contract-based trust and decentralized arbitration tailored for avatars and organizations in metaverse environments. Their system employs algorithmic trust management, where smart contracts automatically verify the integrity of transactions (e.g., NFT trades in *Axie Infinity*'s Marketplace) and trigger arbitration processes if predefined conditions—such as non-delivery or fraud—are detected. For instance, a smart contract could lock disputed assets in an escrow until a decentralized panel of arbitrators, selected based on reputation or stake, reaches a consensus. This approach mitigates risks like phishing attacks or smart contract vulnerabilities (Section 4.2) by embedding redress mechanisms directly into the platform's infrastructure, offering consumers a faster and more accessible alternative to traditional litigation.

Real-world implementations are beginning to test these theoretical frameworks, demonstrating both their potential and their limitations. A notable example of such implementation is *Kleros*, a blockchain-based arbitration platform that operationalizes decentralized dispute resolution through crowd-sourced juror panels and cryptographic evidence submission (Aouidef et al., 2021). *Kleros* leverages Ethereum smart contracts to manage disputes, allowing users to submit evidence (e.g., transaction records, NFT metadata) and select jurors from a pool of pseudonymous participants incentivized by the platform's native token (PNK). Jurors vote on outcomes, and the blockchain ensures transparency and immutability of the process. In the context of metaverses, *Kleros* could resolve disputes over virtual goods, such as a misrepresented NFT in *The Sandbox*'s Marketplace, by providing a decentralized forum that operates independently of national jurisdictions. However, *Kleros*'s reliance on pseudonymous jurors and token-based incentives raises concerns about bias, juror expertise, and procedural fairness, particularly for complex consumer disputes involving significant financial stakes (Bergolla et al., 2022).

Despite their promise, these blockchain-native dispute resolution mechanisms remain legally fragile, (López Rodríguez, 2025). Platforms like Kleros lack formal legal recognition in most jurisdictions, limiting their enforceability under traditional legal frameworks. For example, a *Kleros* ruling on a disputed NFT transaction may not be recognized by a court in the EU or US, especially if it conflicts with mandatory consumer protections (e.g., Brussels I Recast, Art. 18). Without backing from state institutions or international legal harmonization, these systems risk being perceived as private experiments rather than legitimate alternatives to conventional dispute resolution. This fragility is particularly problematic in metaverse platforms, where arbitration clauses tied to remote jurisdictions (e.g., Panama for *Decentraland*, Cayman Islands for *Axie Infinity*) already restrict consumers' access to local courts (Section 4.4).

To address these limitations, scholars emphasize the need for hybrid legal-technical frameworks that integrate blockchain-native mechanisms with enforceable legal standards. Alomari (AlLouzi and Alomari, 2023) argue that such frameworks should combine the efficiency and transparency of on-chain ADR with procedural safeguards aligned with national consumer protection laws. For instance, a hybrid model could require platforms to embed smart contracts with standardized arbitration protocols that comply with international principles, such as the EU's Consumer Rights Directive (Directive 2011/83/EU, 2011) or the US's Federal Trade Commission Act (*15 U.S.C. § 45*). These protocols could include mandatory disclosure of arbitration processes, clear criteria for juror selection, and appeal mechanisms to ensure due process. Additionally, integrating interoperable digital identity systems, such as the European Digital Identity Wallet (EUDI) under the eIDAS 2.0 Regulation (Regulation (EU) 2024/1183, 2024), could enhance accountability by linking pseudonymous users to verifiable identities without compromising privacy, facilitating compliance with jurisdiction-specific laws.

The development of such hybrid frameworks requires collaboration between platform developers, regulators, and researchers to ensure scalability and legal legitimacy. For example, piloting Kleros-like systems in metaverse platforms like *Decentraland* could test their effectiveness in resolving user-to-user disputes, while international agreements on mutual recognition of blockchain-based rulings could enhance enforceability. These efforts are critical to closing the consumer protection gap in decentralized metaverses, where traditional legal tools are ill-equipped to address the unique challenges of pseudonymity, automation, and cross-border interactions.

While on-chain dispute resolution mechanisms have a lot of promise, they still face serious limitations. These issues point to a bigger challenge in the metaverse: the need for legal systems that are built for digital spaces—ones that can adapt to new technologies and are recognized across borders. At the same time, fewer people are using metaverse platforms. That drop-off is likely due to too much hype early on, unclear benefits, and a market that's become overcrowded and confusing (Rai and Khandelwal, 2023). Together, these problems make it even harder for users to handle disputes when things go wrong. Until better systems are in place, consumers will continue to face uncertainty and risk in virtual worlds.

5 Conclusion and future avenues

As blockchain-based and immersive platforms increasingly mediate transnational interactions, the fragmentation of legal authority across jurisdictions has become one of the most pressing challenges for consumer protection. These decentralized ecosystems, often structured around smart contracts and DAOs, displace traditional notions of territoriality, rendering established conflict-of-law principles inadequate. Legal uncertainty arises not only from the anonymity and pseudonymity of users, but from the absence of a stable legal forum to adjudicate disputes that transcend borders.

To address these challenges, there is a need for a new generation of cross-border conflict resolution mechanisms adapted to the unique features of decentralized architectures. Existing private international law frameworks, predicated on identifiable parties, geographic location, and contractual choice-of-law clauses, struggle to accommodate transactions that are governed by code, executed autonomously, and often lack any identifiable locus. The widespread practice of imposing arbitration clauses tied to obscure or strategically selected jurisdictions—such as Panama, Malta, or the Cayman Islands—further compounds this issue by limiting users' access to effective remedies.

As blockchain platforms continue to expand across borders, an international framework for consumer protection must evolve to meet the challenges of decentralization. A key priority should be ensuring that user rights are enforceable regardless of the platform's formal legal seat. This includes recognizing consumers' right to bring legal action in their country of residence, even when platform terms require disputes to be resolved through foreign courts or arbitration. Accessible forums are especially critical where users face information asymmetries and the technical complexity of blockchain ecosystems, which can amplify power imbalances between platforms and consumers.

To enhance trust and transparency, harmonized disclosure requirements for virtual goods and services should be introduced. These would help reduce regulatory arbitrage and ensure users receive clear, consistent information. Cross-border enforcement of such obligations would be greatly strengthened through mutual recognition agreements between national authorities, allowing regulators to coordinate more effectively—particularly important in pseudonymous environments, where traditional legal tools like identity verification or service of process are difficult to apply (Jabotinsky and Lavi, 2024).

On the technical side, embedding dispute resolution mechanisms directly into blockchain infrastructure can support fair outcomes without requiring users to exit the ecosystem. For example, smart contracts can be designed with automated triggers for third-party arbitration or escalation in cases of fraud or failed transactions. Decentralized arbitration protocols are also emerging as viable alternatives, offering resolution pathways that are native to the blockchain environment. However, to ensure these mechanisms are legitimate and effective, they must operate under oversight standards that guarantee procedural fairness and enforceability (Guillaume and Riva, 2023).

A solid consumer protection regime will also require interoperable digital identity systems that balance the need for legal accountability with the right to privacy. Such systems would allow users to assert rights and facilitate compliance with jurisdiction-specific laws—without relying on centralized identity databases. In this context, the European Digital Identity Wallet (EUDI), introduced by the eIDAS 2.0 Regulation, represents a major step forward. In force since May 2024 and set for mandatory implementation by 2026, EUDI provides a secure, privacy-preserving identity layer that can function across borders. Its design supports trusted transactions in the metaverse and could serve as a global benchmark for digital identity governance—though its long-term impact will depend on how widely it is adopted and integrated by platforms.

In the end, resolving cross-border disputes in decentralized systems will require a hybrid regulatory model—one that pairs international legal harmonization with technical tools built into the architecture of blockchain platforms. For example, platforms like *Decentraland* and *Axie Infinity* could integrate on-chain ADR mechanisms (e.g., Kleros) with standardized governance rules to address user complaints more effectively, ensuring fairness and transparency. This model must strike a delicate balance: flexible enough to respect the decentralization ethos of blockchain, but solid enough to uphold user rights across jurisdictions. Regulatory innovation, driven by international collaboration and informed by the realities of decentralized technology, is essential to building a digital future where rights do not disappear at national borders—or on the blockchain itself.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

AL: Conceptualization, Investigation, Methodology, Resources, Supervision, Validation, Writing – original draft, Writing – review and editing.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that Generative AI was used in the creation of this manuscript. In the preparation of this manuscript, I utilized generative artificial intelligence tools, specifically ChatGPT (GPT-4o) and Perplexity (both in free versions), for proofreading and translation purposes. These tools were employed to facilitate the comparative analysis by enabling direct engagement with original sources in their native languages. All substantive analysis and interpretation were conducted by the author.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

AlLouzi, A. S., and Alomari, K. M. (2023). Adequate legal rules in settling metaverse disputes: hybrid legal framework for metaverse dispute resolution (HLFMDR). *Int. J. Data Netw. Sci.* 7, 1627–1642. doi:10.5267/j.ijdns.2023.8.001

AI Basic Act (2025). *AI Basic Act (Republic of Korea), Law No. 20676, promulgated January 21, 2025; effective January 22, 2026*. Republic of Korea: Publisher: Ministry of Government Legislation.

American Bar Association, Committee on Cyberspace Law (2000). Achieving legal and business order in cyberspace: a report on global jurisdiction issues created by the internet. *Bus. Lawyer* 55 (4), 1801–1946. Available online at: http://www.jstor.org/stable/40687955.

Aouidef, Y., Ast, J., and Deffains, B. (2021). Decentralized justice: a comparative analysis of blockchain online dispute resolution projects. *Frontiers in Blockchain* 4, 564551, doi:10.3389/fbloc.2021.564551

Awan, K. A., Din, I. U., Almogren, A., and Seo-Kim, B. (2023). Blockchain-based trust management for virtual entities in the metaverse: a model for avatar and virtual organization interactions. *IEEE Access* 11, 136370–136394. doi:10.1109/ACCESS.2023.3337806

Becker, D., and Gonçalves Junior, A. (2023). The impacts of the Brazilian cryptoassets law in NFT solutions. *Int. J. Law Changing World* 2, 153–170. doi:10.54934/ijlcw.v2i3.37

Belk, R., Humayun, M., and Brouard, M. (2022). Money, possessions, and ownership in the metaverse: NFTs, cryptocurrencies, Web3 and wild markets. *J. Bus. Res.* 153, 198–205. doi:10.1016/j.jbusres.2022.08.031

Bergolla, L., Seif, K., and Eken, C. (2022). Kleros: a socio-legal case study of decentralized justice and blockchain arbitration. *Ohio State J. Dispute Resolut.* 37, 55–98.

Brazil (1990). Consumer Protection Code *Código de Defesa do Consumidor*. Available online at: https://www.g-regs.com/downloads/BRGenConsProtection8078.pdf (Accessed October 7, 2025).

Bonomi, A., Lehmann, M., and Lalani, S. (2023). "Introduction: the blockchain as a challenge to traditional private international law," in *Blockchain and private international law* (Leiden: Brill Nijhoff), 1–9. doi:10.1163/9789004514850_002

Borgogno, O. (2018). Smart contracts as the (new) power of the powerless? The stakes for consumers. *Eur. Rev. Private Law* 26, 885–902. doi:10.54648/ERPL2018060

Calder v. Jones (1984). Calder v. Jones, 465 U.S. 783 (1984).

California Consumer Privacy Act (2018). *California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. Enacted 2018; as amended*. Publisher: State of California.

Chen, H., Duan, H., Abdallah, M., Zhu, Y., Wen, Y., Saddik, A. E., et al. (2024). Web3 metaverse: state-of-the-art and vision. *Commun. Appl.* 20 (1), 1–42. doi:10.1145/3630258

Civil Procedure Act (2016). *Civil Procedure Act (Republic of Korea), Act No. 14103, enacted March 22, 2016*. Republic of Korea: Publisher: Ministry of Government Legislation.

Civil Procedure Law of the People's Republic of China (2023). *Civil Procedure Law of the People's* Republic of China, *as amended September 2023; effective January 1, 2024*. Publisher: National People's Congress, PRC.

Code of Civil Procedure (2016). *Code of Civil Procedure, Law No. 13.105, enacted March 16, 2015; entered into force March 18, 2016*. Publisher: Official Gazette of Brazil.

Commodity Futures Trading Commission (2022). Commodity Futures Trading Commission v. Ooki DAO, No. 3:22-cv-05416-WHO (N.D. Cal. 2022).

Comenale, A. P. (2021). *METALAW: El Metaverso Jurídico y los Derechos de los Consumidores Avatares*. Observatorio Blockchain. Available online at: https://observatorioblockchain.com/metaverso/el-metaverso-juridico-y-los-derechos-de-los-consumidores-en-el-espacio-metalaw/ (Accessed October 7, 2025).

Consumer Financial Protection Act (2010). *Consumer Financial Protection Act of 2010, 12 U.S.C. §§ 5481 et seq. Enacted July 21, 2010*. Publisher: United States Congress.

Consumer Defense Code (1990). *Consumer Defense Code, Law No. 8,078, enacted September 11, 1990*. Publisher: Official Gazette of Brazil.

Consumer Protection in Electronic Commerce Act (2022). *Act on the Consumer Protection in Electronic Commerce, Etc. (Republic of Korea), Act No. 6704, promulgated March 30, 2002; last amended by Act No. 15323, February 13, 2024*. Republic of Korea: Publisher: Ministry of Government Legislation.

Consumer Protection (Fair Trading) Act (2009). *Consumer Protection (Fair Trading) Act, Chapter 52A, originally enacted as Act 27 of 2003; revised ed. 2009*. Publisher: Government of Singapore.

Consumers Legal Remedies Act (1970). *Civil Code §§ 1750 et seq. (California), Consumers Legal Remedies Act, enacted 1970*. Publisher: State of California.

Corrales Compagnucci, M., Kono, T., and Teramoto, S. (2022). Legal aspects of decentralized and platform-driven economies. *SSRN*. doi:10.2139/ssrn.4027412

Court of Justice of the EU (2011). Court of Justice of the EU, eDate Advertising and Others, Joined Cases C-509/09 and C-161/10, 2011, ECLI:EU:C:2011:685.

Court of Justice of the EU (2010). Court of Justice of the EU, Pammer and Hotel Alpenhof, Joined Cases C-585/08 and C-144/09, 2010, ECLI:EU:C:2010:740.

Court of Justice of the EU (2014). Court of Justice of the EU, Kainz v. Pantherwerke AG, Case C-45/13, 2014, ECLI:EU:C:2014:7.

Court of Justice of the EU (2015). Court of Justice of the EU, Hobohm, Case C-297/14, 2015, ECLI:EU:C:2015:844.

Court of Justice of the EU (2017). Court of Justice of the EU, N.W. and Others v. Sanofi Pasteur, Case C-621/15, 2017, ECLI:EU:C:2017:484.

Cryptonator's (2025). I logged into the metaverse in 2025 and found a ghost town with lag *Medium*. Available online at: https://medium.com/@cryptonator_s/i-logged-into-the-metaverse-in-2025-and-found-a-ghost-town-with-lag-a589492e0a6d (Accessed October 7, 2025).

Cyberspace Administration of China (2022). *Provisions on the Administration of Deep Synthesis Internet Information Services (China), Order No. 12, promulgated November 25, 2022; effective January 10, 2023*. Publisher: Cyberspace Administration of China.

Directive 93/13/EEC (1993). Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. *Official Journal of the European Communities, L 95*, 29–34.

Directive 1999/44/EC (1999). Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees. *Official Journal L 171*, 12–16.

Directive 2000/31/EC (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. *Official Journal L 178*, 1–16.

Directive 2005/29/EC (2005). Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive). *Official Journal L 149*, 22–39.

Directive 2011/83/EU (2011). Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights. *Official Journal L 304*, 64–88.

Directive (EU) 2015/2366 (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2). *Official Journal L 337*, 35–127.

Directive (EU) 2024/2853 (2024). Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. *Official Journal L 2024/2853*, 1–11.

Decree-Law No. 4,657 (1942). *Decree-Law No. 4,657 (Introductory Law to the Brazilian Civil Code), enacted September 4, 1942*. Publisher: Official Gazette of Brazil.

De Filippi, P., and Wright, A. (2019). *Blockchain and the law: the rule of code*. Harvard University Press.

Durovic, M. (2024). "Adaptability of the unfair commercial practices directive to the metaverse," in *Research handbook on the metaverse and law*. Editors Romero Moreno F. and Rodríguez-Barbero D. (Cheltenham: Edward Elgar Publishing), 311–334. doi:10.4337/9781035324866.00029

Electronic Fund Transfer Act (1978). *Electronic Fund Transfer Act, 15 U.S.C. §§ 1693 et seq., enacted November 10, 1978*. Publisher: United States Congress.

European Parliament (2024). Resolution of 17 January 2024 on policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues. *Official Journal of the European Union*, Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202405720 (Accessed October 7, 2025).

Fairfield, J. A. T. (2022). Tokenized: the law of non-fungible tokens and unique digital property. *Indiana Law J.* 97 (4), 1261–1312.

Falchuk, B., Loeb, S., and Neff, R. (2018). The social metaverse: battle for privacy. *IEEE Technol. Soc. Mag.* 37, 52–61. doi:10.1109/MTS.2018.2826060

Federal Trade Commission Act (2018). *Federal Trade Commission Act of 1914, 15 U.S.C. § 45*. Publisher: United States Congress.

Fernandez, C. B., and Hui, P. (2022). Life, the metaverse and everything: an overview of privacy, ethics, and governance in metaverse. *Proc. IEEE ICDCSW*, 272–277. doi:10.1109/ICDCSW56584.2022.00058

Figueiredo, T. D. (2025). *Digital regulations in the metaverse era: metaverse guide*. London: International Bar Association. Available online at: https://www.ibanet.org/metaverse-guide-digital-regulations-in-the-metaverse-era (Accessed October 7, 2025).

Frommelt, E. (2021). Liability challenges in the blockchain ecosystem. *UC Davis Bus. Law J.* 21, 165–222.

International Shoe Co. (1945). International Shoe Co. v. Washington, 326 U.S. 310 (1945).

Gangemi, A. (2023). Towards a privacy-preserving dispute resolution protocol on ethereum. arXiv:2303.00533.

Ghosh, A., Lavanya, Hassija, V., Chamola, V., and El Saddik, A. (2024). A survey on decentralized metaverse using blockchain and web 3.0 technologies, applications, and more. *IEEE Access* 12, 146915–146948. doi:10.1109/ACCESS.2024.3469193

Giacalone, M., and Arnone, G. (2024). Dispute resolutions for digital assets in a decentralized virtual world. *Eur. J. Priv. Law and Technol.*, 117–135. doi:10.57230/ejplt241MGGA

Guillaume, F., and Riva, S. (2023). "Blockchain dispute resolution for DAOs: the rise of decentralized justice," in *Blockchain and private international law*. Editors L. Bonomi and Lalani (Leiden: Brill Nijhoff).

Jabotinsky, H. Y., and Lavi, M. (2024). *Regulating the metaverse: reducing diffusion of trader responsibility*. University of Michigan Journal of Law Reform. (forthcoming). Available online at: https://ssrn.com/abstract=4753418 (Accessed October 7, 2025).

Jiayi Sun, W. G., Chen, Z., Li, J., and Yu, P. S. (2022). Big data meets metaverse: a survey. arXiv:2210.16282

Jordan, A., and Vidan, G. (2025). Playing, earning, crashing, and grinding: axie infinity and growth crises in the Web3 economy. *Big Data and Soc.* 12, 20539517251357296. doi:10.1177/20539517251357296

Kaur, J., Mogaji, E., Paliwal, M., Jha, S., Agarwal, S., and Mogaji, S. A. (2024). Consumer behavior in the metaverse. *J. Consumer Behav.* 23, 1720–1738. doi:10.1002/cb.2298

Konyalioglu, F. I. (2023). "Consumer behavior in the metaverse," in *Consumer psychology in digital contexts* (Springer), 161–175. doi:10.1007/978-981-99-4641-9_11

Law on the Application of Law for Foreign-Related Civil Relations (2010). *Law of the People's* Republic of China *on the Application of Law for Foreign-Related Civil Relations, adopted October 28, 2010; effective April 1, 2011*. Publisher: National People's Congress, PRC.

Lince, T. (2022). OpenSea: how trademark infringement is rampant on the biggest NFT marketplace. *World Trademark Review*, 37(2), Available online at: https://www.worldtrademarkreview.com/article/opensea-how-trademark-infringement-rampant-the-biggest-nft-marketplace (Accessed October 7, 2025).

Legal Clarity (2025). Do brands have legal ownership of user-generated content?. *LegalClarity*. Available online at: https://legalclarity.org/do-brands-have-legal-ownership-of-user-generated-content (Accessed October 7, 2025).

López Rodríguez, A. M. (2025). *Resolución de Conflictos en el Metaverso*. Madrid: Tecnos.

Lopez-Tarruella, A., and Rodríguez de las Heras Ballell, T. (2025). A European regulatory framework for the metaverse. *SSRN Res. Pap. No. 5024023*. doi:10.2139/ssrn.5024023

Manoylov, M. (2022). Play-to-earn game Axie Infinity's revenue continues to slide, *The Block*, Available online at: https://www.theblock.co/linked/150320/pay-to-earn-game-axie-infinitys-revenue-continues-to-slide (Accessed October 7, 2025).

Martha, G. I. R., Gaol, F. L., Supangkat, S. H., and Ranti, B. (2023). "Utilization of DAOs for virtual property transaction governance in metaverse," in *Proceedings of ICICyTA 2023* (IEEE), 306–311. doi:10.1109/ICICyTA60173.2023.10429035

Mazafaka (2024). This is why decentraland have no future, Mirror. Available online at: https://mirror.xyz/mazafaka.eth/XqhwRqa9d7F98iNkDp-yke3Vu0342F90onvNwLaxCYo (Accessed October 7, 2025).

McAmis, R., Durak, B., Chase, M., Laine, K., Roesner, F., and Kohno, T. (2025). Handling identity and fraud in the metaverse. *IEEE Secur. and Priv.* 23, 27–37. doi:10.1109/MSEC.2024.3399699

Moslein, F. (2020). "Legal boundaries of blockchain technologies: smart contracts as self-help?," in *Digital revolution – new challenges for law*. Editor Franceschi A., Schulze R., Graziadei M., Pollicino O., Riente F., Sica S. et al. (Munich: Verlag C.H. Beck), 313–326.

Mourtzis, D., Panopoulos, N., Angelopoulos, J., Wang, B., and Wang, L. (2022). Human centric platforms for personalized value creation in metaverse. *J. Manuf. Syst.* 65, 653–659. doi:10.1016/j.jmsy.2022.11.004

Nero v. Uphold HQ Inc. (2023). Nero v. Uphold HQ Inc., 688 F. Supp. 3d 134 (S.D.N.Y. 2023).

O'Sullivan, J. (2024). The Sandbox launches the sandbox DAO with 25M SAND treasury. *Cointelegraph*, Available online at: https://cointelegraph.com/news/the-sandbox-launches-dao-25m-sand-treasury (Accessed October 7, 2025).

Özkaynar, K. (2023). Consumer behavior, marketing approach, branding, advertising, and new opportunities in the metaverse areas, in *Advances in Digital Marketing and eCommerce* Editors R. Gonzalo), 151–159.(Singapore: Springer). (Accessed October 7, 2025). doi:10.1007/978-981-99-4641-9_10

Private International Law Act (2022). *Act on Private International Law (Republic of Korea), Law No. 18041, promulgated January 4, 2022; entered into force July 5, 2022*. Republic of Korea: Publisher: Ministry of Government Legislation.

Ramos, M. (2023). Stung by losses, Filipino players ditch Axie Infinity crypto game. *Context*, Available online at: https://www.context.news/big-tech/stung-by-losses-filipino-players-ditch-axie-infinity-crypto-game (Accessed October 7, 2025).

Ravenscraft, E. (2021). The metaverse land rush is an illusion. *Wired*, 26. Available online at: https://www.wired.com/story/metaverse-land-rush-illusion/ (Accessed October 7, 2025).

Rai, V., and Khandelwal, P. (2023). Metaverse in crisis: analyzing its decline and contributing factors. Pune: Zensar Technologies. Available online at: https://www.zensar.com/insights/white-paper/technology/it-services/metaverse-in-crisis-analyzing-its-decline-and-contributing-factors?tagType=insightCard (Accessed October 7, 2025).

Regulation (EC) No 593/2008 (2008). Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). *Official Journal L 177*, 6–16.

Regulation (EU) 2016/679 (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). *Official Journal L 119*, 1–88.

Regulation (EU) No 1215/2012 (2012). Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I bis). *Official Journal L 351*, 1–32.

Regulation (EU) 2022/2065 (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal L 277*, 1–102.

Regulation (EU) 2024/1689 (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal L 168*, 1–156.

Regulation (EU) 2024/1183 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the framework for a European Digital Identity. *Official Journal of the European Union, L*(2024). 1183. Available online at: https://eur-lex.europa.eu/eli/reg/2024/1183/oj (Accessed October 7, 2025).

Rider v. Uphold HQ Inc. (2023). Rider v. Uphold HQ Inc., 657 F. Supp. 3d 491 (S.D.N.Y. 2023).

Restatement (Second) of Conflict of Laws (1971). *Restatement (Second) of Conflict of Laws. St. Paul, MN*. American Law Institute Publishers.

Restatement (Second) of Torts (1965). *Restatement (Second) of Torts § 402A. St. Paul, MN*. American Law Institute Publishers.

Rodrigues, U. R. (2019). Law and the blockchain. *Iowa Law Rev.*, 679–729.

Rosenberg, L. B. (2022). "Regulating the metaverse: a blueprint for the future," in *Metaverse perspectives* (Springer), 263–272. doi:10.1007/978-3-031-15546-8_23

Rules of Court (2021). *Rules of Court 2021, Order 10, in force since April 1, 2022*. Publisher: Government of Singapore.

Santana, C., and Albareda, L. (2022). Blockchain and the emergence of decentralized autonomous organizations (DAOs): an integrative model and research agenda. *Technol. Forecast. Soc. Change* 182, 121806. doi:10.1016/j.techfore.2022.121806

Sayeed, S., Marco-Gisbert, H., and Caira, T. (2020). Smart contract: attacks and protections. *IEEE Access* 8, 24416–24427. doi:10.1109/ACCESS.2020.2970495

Shivare, S., and Park, K.B. (2025). South Korea's new AI Framework Act: a balancing act between innovation and regulation. *Future of Privacy Forum* Available online at: https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/ (Accessed October 7, 2025).

Smith, O. (2024). Decentraland's active users at an all time low. *NFT Evening*, Available online at: https://nftevening.com/decentralands-active-users-at-an-all-time-low/ (Accessed October 7, 2025).

Supreme People's Court of the People's Republic of China (2022). Opinions on providing judicial services and guarantees for accelerating the construction of a unified national market. *CLI.3.5131435(EN)* Available online at: https://www.lawinfochina.com/display.aspx?id=39157&lib=law (Accessed October 7, 2025).

Pacific Recreation Pte Ltd (2008). Pacific Recreation Pte Ltd v. S Y Technology Inc, SGCA 1.

Uniform Commercial Code (1977). *Uniform Commercial Code § 1-301, Territorial Applicability; Parties' Power to Choose Applicable Law, 1977*. Publisher: National Conference of Commissioners on Uniform State Laws.

Uniform Commercial Code (1951). *Uniform Commercial Code, Article 2 – Sales, 15 U.L.A. § 2-101 et seq. (1951)*. Publisher: National Conference of Commissioners on Uniform State Laws.

United States Congress Senate Committee on the Judiciary (1998).

Weber, R. H. (2020). "Blockchain technology, smart contracts and virtual currencies," in *Digital revolution – new challenges for law*. Editor Franceschi A., Schulze R., Graziadei M., Pollicino O., Riente F., Sica S. and Sirena P. (Munich: Verlag C.H. Beck), 299–312.

Wilson, T., and Howcroft, E. (2022). Blockchain project Ronin hit by $615 million crypto heist, *Reuters*. Available online at: https://www.reuters.com/technology/blockchain-company-ronin-hit-by-615-million-crypto-heist-2022-03-29/ (Accessed October 7, 2025).

Woon, W. (1999). "The applicability of English law in Singapore," in *The Singapore legal system*. Editor K. Y. L. Tan (Singapore: Singapore University Press), 230–247.

Yadav, A. B. (2024). Protecting privacy in the digital marketplace: a comparative study of legal mechanisms for consumer rights in the metaverse. *J. Data Prot. and Priv.* 6 (4), 355. doi:10.69554/FHZJ9408

Yuga Labs, Inc. (2023). Yuga Labs, Inc. v. Ripps, No. CV22-4355, 2023 WL 3316748 (C.D. Cal. Apr. 21, 2023).

Zafar, A. (2025). Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. *J. Cybersecurity* 11, tyaf002–tyaf020. doi:10.1093/cybsec/tyaf002

Zetzsche, D. A., Buckley, R. P., and Arner, D. W. (2017). "The distributed liability of distributed ledgers: legal risks of blockchain," in *European banking institute working paper no. 14*. doi:10.2139/ssrn.3018214

Zhou, L., Diro, A., Saini, A., Kaisar, S., and Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: a survey of advancements, challenges and opportunities. *J. Inf. Secur. Appl.* 80, 103678. doi:10.1016/j.jisa.2023.103678