

Building a Legal Framework for the Metaverse: Digital Identity, NFT Property Rights, and Global Legal Structures

Zhong CHEN

Fujian Normal University

Abstract

This study explores the construction of a legal framework for the metaverse, analyzing digital identity, NFT property rights, judicial challenges, and the evolution of global legal systems. The paper discusses regulatory trends in major countries, challenges in cross-border legal coordination, and technology-driven legal adaptations. In the future, smart contracts, DAOs, and digital judiciary systems will be key components of metaverse law, ensuring consumer rights and digital asset security. This study highlights the importance of global legal standardization and proposes future research directions to advance legal governance in the metaverse.

Keywords Metaverse; Digital Identity; NFT Property Rights; Judicial Challenges; Legal Framework

1 Introduction

1.1 Background: The Rise of the Metaverse and the Demand for Legal Governance

The metaverse, a collective virtual space created by the convergence of virtually enhanced physical reality and interactive digital environments, has gained significant attention in recent years. With advancements in artificial intelligence, blockchain, and virtual reality, the metaverse has transitioned from a conceptual framework to an emerging digital ecosystem with profound economic, social, and legal implications. The proliferation of digital assets, virtual real estate, and decentralized finance (DeFi) within the metaverse necessitates a robust legal infrastructure that can accommodate new modes of interaction, ownership, and governance.

As digital environments become more immersive, the traditional legal system faces substantial challenges in regulating activities within the metaverse. Unlike the conventional internet, where regulations can be applied to identifiable entities, the decentralized and pseudonymous nature of the metaverse complicates legal oversight. Key concerns such as digital identity authentication, intellectual property (IP) protection, contract enforcement, and dispute resolution require innovative legal solutions. Consequently, there is a growing demand for a legal framework that aligns

with the dynamic nature of virtual interactions and digital economies. Governments and international legal bodies must cooperate to formulate clear and enforceable policies that can effectively regulate digital spaces, ensuring legal security for all stakeholders.

The impact of the metaverse on consumer rights is also significant. Traditional consumer protection laws were designed for physical goods and services, leaving gaps in legal protections for digital transactions. The metaverse introduces new forms of digital commerce, where consumers may face fraudulent schemes, misleading advertisements, and unregulated financial activities. Without strong legal frameworks, users remain vulnerable to exploitation in decentralized environments. Additionally, taxation policies related to virtual assets and transactions require attention. Policymakers need to define the legal status of metaverse-based earnings, including virtual real estate sales and NFT trades, to establish clear tax obligations.

1.2 Legal Challenges in the Metaverse: Digital Identity, NFT Property Rights, and Judicial Adaptation

The metaverse presents an array of legal challenges, particularly in the realms of digital identity, non-fungible token (NFT) property rights, and judicial enforcement. These challenges stem from the fundamental differences between traditional legal systems and the digital-first nature of the metaverse.

Digital identity in the metaverse is one of the most pressing legal concerns. Unlike real-world identities, digital identities are often pseudonymous, decentralized, and controlled by users rather than government entities. While decentralized identity solutions offer enhanced privacy and security, they also create regulatory gaps concerning identity theft, fraud, and accountability. Legal frameworks must address issues such as digital identity verification, rights of virtual personas, and cross-jurisdictional recognition of metaverse-based identities. Furthermore, the integration of biometric authentication and blockchain-based identity management systems raises ethical and privacy concerns. Should metaverse platforms be required to comply with data protection regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA)? How can digital identity disputes be resolved in a decentralized environment? These are critical questions that must be addressed through adaptive legal policies.

NFTs have emerged as a cornerstone of digital ownership in the metaverse, allowing users to buy, sell, and trade unique digital assets. However, the legal recognition of NFT ownership is still in its infancy. Traditional property laws were not designed to accommodate digital assets that exist solely on blockchain networks, leading to ambiguities in ownership rights, transferability, and liability. NFTs also pose significant challenges in intellectual property law. For instance, copyright and trademark disputes have arisen over NFT creations that replicate existing artworks, brand logos, or cultural artifacts. Jurisdictions vary in their interpretation of NFT ownership rights—while some recognize NFTs as legally binding digital assets, others view them as speculative instruments without tangible ownership protections. Additionally, questions arise

concerning the liability of NFT marketplaces and platforms that facilitate the trade of potentially infringing content.

Another critical issue is the enforcement of NFT-related contracts and smart contracts. Although blockchain-based contracts enable automated execution of agreements, they do not always align with legal principles such as consumer protection laws, dispute resolution mechanisms, and enforceability under traditional contract law. Resolving these disparities requires harmonization between emerging blockchain regulations and established legal doctrines. Furthermore, issues such as NFT inheritance and asset protection in the event of a user's death or loss of access pose new legal dilemmas, requiring specialized digital estate laws.

The judicial system must adapt to the complexities of legal disputes in the metaverse, particularly concerning cross-border jurisdiction and digital evidence. Since metaverse transactions occur in a decentralized environment, determining the applicable legal jurisdiction is often challenging. Should disputes be governed by the laws of the user's country of residence, the platform's location, or the jurisdiction of the blockchain network? The use of alternative dispute resolution (ADR) mechanisms, such as decentralized arbitration systems, has been proposed as a means to address metaverse-related conflicts. Platforms like Kleros and Aragon Court leverage blockchain-based dispute resolution processes that rely on decentralized jurors to adjudicate cases. While such systems provide an innovative approach to digital governance, they also raise concerns about fairness, transparency, and enforcement outside of blockchain ecosystems.

Furthermore, evidentiary standards in metaverse litigation require careful consideration. Digital assets, smart contracts, and blockchain records must be legally recognized as admissible evidence in court. The challenge lies in ensuring the authenticity and integrity of digital evidence while balancing privacy and regulatory compliance. Courts may need to establish specialized digital forensic procedures to address these issues effectively. Additionally, metaverse-based criminal activities such as virtual asset theft, cyber harassment, and digital fraud necessitate a re-evaluation of criminal justice frameworks to ensure accountability and user protection.

1.3 Expanding Legal Frameworks for the Metaverse

As legal scholars and regulators explore solutions for metaverse governance, international cooperation is essential to establish consistent legal standards. The metaverse transcends national boundaries, making unilateral regulatory approaches ineffective. Governments must collaborate to develop global frameworks that address digital identity, intellectual property, consumer rights, and dispute resolution within virtual environments.

Furthermore, regulatory sandboxes can serve as testing grounds for emerging legal frameworks, allowing policymakers to experiment with new regulations in controlled virtual settings. These sandboxes can facilitate discussions between lawmakers, technologists, and industry stakeholders to identify best practices for metaverse governance. Additionally, public-private partnerships can play a crucial role in establishing ethical guidelines and security standards for digital

spaces. As the metaverse continues to evolve, legal frameworks must remain flexible to accommodate technological advancements and societal shifts.

This study aims to address the evolving legal challenges in the metaverse by analyzing key issues related to digital identity, NFT property rights, and judicial adaptation. It explores the complexities of digital identity verification, ownership rights, and dispute resolution in decentralized environments. Additionally, it proposes a comprehensive legal framework that balances regulatory oversight with the decentralized nature of metaverse interactions. The research emphasizes the need for international legal collaboration, adaptive policy frameworks, and continuous dialogue between governments, technology providers, and legal experts to ensure that the metaverse develops into a legally sound and user-protective ecosystem.

2 Legal Challenges of Digital Identity

2.1 Digital Identity Definition: Decentralized Identity (DID) and On-Chain Authentication

Digital identity in the metaverse serves as the foundation for user interactions, economic transactions, and governance mechanisms. Unlike traditional identity verification, which relies on centralized authorities such as governments, banks, or corporations, the metaverse increasingly embraces decentralized identity (DID) systems. These systems leverage blockchain technology to provide users with self-sovereign identities (SSI), enabling individuals to maintain control over their credentials without dependence on intermediaries.

Decentralized identity systems utilize cryptographic keys, smart contracts, and distributed ledgers to authenticate users. DID frameworks, such as those developed by the World Wide Web Consortium (W3C) and organizations like Sovrin and uPort, emphasize user-centric identity models where authentication is performed through verifiable credentials stored on a blockchain. This approach enhances security and mitigates risks associated with identity theft, but it also presents regulatory challenges. Many legal frameworks require centralized oversight of identity verification processes to prevent fraud, illicit activities, and financial crimes. The absence of a central authority in DID-based models raises questions regarding liability and legal recognition.

On-chain authentication mechanisms introduce another dimension of complexity. Blockchain records are immutable, meaning identity verification data, once stored, cannot be altered or erased. While this ensures data integrity and prevents unauthorized modifications, it also contradicts legal principles such as the "right to be forgotten" in data protection laws. The interaction between blockchain-based identity solutions and regulatory compliance frameworks necessitates a nuanced approach to reconcile technological advancements with legal obligations.

2.2 Data Privacy and Identity Protection: GDPR, Blockchain, and Identity Management Conflicts

A primary concern surrounding digital identity in the metaverse is the conflict between blockchain technology and existing data privacy regulations. The European Union's General Data Protection Regulation (GDPR), enacted to protect personal data and privacy, imposes strict obligations on data controllers, including the right of individuals to request data deletion. However, blockchain's fundamental design—decentralized, immutable, and tamper-resistant—clashes with these legal requirements.

One of the key areas of contention is the "right to be forgotten." In traditional databases, personal information can be erased upon request. In contrast, blockchain records are permanent, making data removal difficult, if not impossible. This raises concerns about how personal data can be managed within decentralized identity frameworks without violating privacy rights. Some potential solutions involve cryptographic techniques such as zero-knowledge proofs (ZKP) and selective disclosure protocols, which enable identity verification without exposing the full details of a user's credentials. However, these technologies remain in early adoption phases and lack widespread regulatory approval.

Beyond GDPR, other regulatory frameworks such as the California Consumer Privacy Act (CCPA) and China's Personal Information Protection Law (PIPL) impose similar data protection obligations. The challenge for metaverse platforms is ensuring compliance with multiple jurisdictions while maintaining the benefits of decentralized identity solutions. Smart contracts and decentralized autonomous organizations (DAOs) that govern identity verification processes must incorporate mechanisms for legal oversight, consumer rights protection, and dispute resolution.

Another issue related to data privacy is the collection and storage of biometric data. Many metaverse applications integrate facial recognition, fingerprint authentication, and voice analysis for enhanced security. While these biometric authentication methods offer improved user verification, they also increase the risk of data breaches and unauthorized surveillance. Regulators must establish guidelines on how biometric identity data should be processed, stored, and secured within decentralized systems.

A possible regulatory approach involves hybrid identity management models that blend centralized oversight with decentralized authentication. Governments and regulatory bodies could certify trusted issuers of digital identity credentials, allowing users to interact in the metaverse under verified but pseudonymous profiles. This model could strike a balance between privacy, security, and legal compliance.

2.3 Account Ownership and Legal Responsibility: The Legal Status of Virtual Identities

A fundamental legal question in the metaverse is determining the legal status of virtual identities. In traditional legal frameworks, an individual or corporate entity holds legal responsibility for their actions. However, metaverse identities, often represented by avatars, decentralized identi-

fiers, or algorithmically managed accounts, blur the lines of legal responsibility.

One of the most pressing challenges is defining ownership of virtual identities. In centralized platforms, identity ownership is tied to user agreements, meaning that companies ultimately control accounts. In decentralized systems, identity is controlled by private cryptographic keys, meaning that only the key holder can access and manage the identity. If a key is lost, the identity is effectively irretrievable, raising concerns about inheritance, legal claims, and dispute resolution.

Another legal issue is accountability for virtual activities. If a user engages in fraud, defamation, or criminal activities within the metaverse, who should be held liable? Traditional legal principles assign responsibility to individuals or corporate entities, but pseudonymous and decentralized identities complicate attribution. Some legal scholars argue for the establishment of "digital personhood," where metaverse identities could be granted a limited form of legal recognition, similar to corporations. Under this model, digital identities could hold assets, sign contracts, and be subject to legal actions while maintaining pseudonymity.

Disputes over virtual identity theft and impersonation also pose legal challenges. Unlike traditional identity theft, where fraudsters assume real-world identities, metaverse identity theft can involve hacking cryptographic keys or exploiting smart contracts to take control of an avatar. Current legal frameworks do not sufficiently address the consequences of stolen or misused decentralized identities. Courts will need to establish legal precedents for reclaiming stolen virtual identities and compensating victims.

Furthermore, digital identity governance in the metaverse extends to intellectual property rights. Avatars, usernames, and digital personas may be trademarked or subject to copyright protection. For instance, if a well-known public figure's likeness is replicated in the metaverse without consent, should existing intellectual property laws apply? The intersection of digital identity and trademark law is an emerging area that will require judicial interpretation and regulatory adjustments.

The issue of inheritance and succession of virtual identities further complicates legal frameworks. In traditional estates, wills and legal mechanisms dictate asset transfers. In decentralized identity systems, without access to private keys, heirs may be unable to claim digital assets. Some blockchain projects propose "social recovery mechanisms," where trusted contacts can restore access, but legal validation of such mechanisms remains uncertain.

2.4 Conclusion of Digital Identity Challenges

The legal challenges of digital identity in the metaverse are multifaceted, requiring a combination of technological solutions and regulatory adaptations. While decentralized identity (DID) systems offer enhanced security and user control, they conflict with existing legal principles, particularly in data protection and accountability. Resolving these conflicts will necessitate collaboration between blockchain developers, policymakers, and legal professionals.

A hybrid approach that combines the benefits of decentralized identity with regulatory over-

sight appears to be the most viable solution. Governments and international organizations must work towards establishing legal standards that recognize digital identities while ensuring compliance with privacy laws. Furthermore, metaverse platforms should incorporate identity recovery mechanisms, dispute resolution frameworks, and legal safeguards against identity-related crimes.

As the metaverse continues to evolve, the legal recognition of digital identities will be a key determinant in shaping its governance. Establishing a robust legal framework for digital identity will not only enhance user trust but also pave the way for a secure and legally compliant virtual ecosystem.

3 NFT Property Rights: Ownership and Legal Considerations

3.1 NFT Property Rights and Legal Nature: Digital Ownership vs. Traditional Property Rights

The emergence of non-fungible tokens (NFTs) has reshaped the concept of ownership in digital economies. Unlike traditional property rights, which are well-defined under legal frameworks, NFT ownership exists solely on blockchain networks, raising critical questions about its legal recognition, enforceability, and rights associated with digital assets. Traditional property laws are structured around tangible assets or intangible rights, such as copyrights and patents. However, NFTs challenge these distinctions by existing in a hybrid space, where ownership is cryptographically recorded but lacks a universally accepted legal definition.

NFTs are typically minted on blockchain platforms, with ownership determined through smart contract execution and decentralized ledger validation. Unlike fungible cryptocurrencies, NFTs are unique and cannot be exchanged on a one-to-one basis. This uniqueness creates an ownership claim that can be verified on-chain, but it does not inherently confer the same legal protections as traditional property rights. In most jurisdictions, laws governing digital assets remain fragmented, leading to uncertainty about whether NFTs should be classified as personal property, intellectual property, or financial instruments.

One key issue is the extent to which NFT ownership equates to ownership of the underlying asset. For example, purchasing an NFT representing a digital artwork does not necessarily confer copyright ownership or reproduction rights. This discrepancy has led to confusion among buyers and sellers, often resulting in legal disputes over the scope of NFT-based ownership rights. Additionally, unlike physical assets, NFTs do not inherently grant rights such as possession, transferability beyond blockchain ecosystems, or recourse in case of disputes. These limitations necessitate a clearer regulatory framework to define and protect NFT property rights, balancing innovation with legal certainty.

Another consideration is the cross-jurisdictional nature of NFTs. Because NFTs are traded on global marketplaces without geographic limitations, determining the applicable legal jurisdiction for disputes can be challenging. Different countries interpret digital ownership differently,

leading to inconsistencies in NFT enforcement and property protections. For instance, some jurisdictions may treat NFTs as securities, subjecting them to financial regulations, while others classify them as intellectual property or digital collectibles. This lack of uniformity complicates the establishment of a stable legal foundation for NFT property rights.

3.2 Copyright and Smart Contracts: Intellectual Property Protection in NFT Transactions

One of the most contentious legal issues surrounding NFTs is intellectual property (IP) rights. While NFTs provide a means of proving digital ownership, they do not automatically transfer copyright or trademark rights to buyers. This creates a critical distinction between purchasing an NFT and acquiring the legal right to use, reproduce, or distribute the underlying content.

In many cases, NFT creators retain copyright ownership, meaning buyers merely own a blockchain-verified token rather than the associated intellectual property. This discrepancy has led to numerous legal disputes, as buyers may falsely assume they have unrestricted rights to the digital asset. Some NFT platforms have attempted to clarify ownership terms by embedding licensing agreements within smart contracts, but these agreements often lack the enforceability of traditional legal contracts.

Another challenge is the unauthorized minting and sale of copyrighted content as NFTs. Digital artists and brands have reported cases where their works were tokenized and sold without their consent, raising concerns about the enforcement of IP rights in decentralized marketplaces. Unlike traditional copyright infringement cases, where legal recourse is pursued against centralized platforms or individuals, decentralized blockchain environments make enforcement more difficult. Because transactions are immutable, unauthorized NFT sales cannot be reversed, leaving victims with limited options for legal remedies.

Smart contracts play a crucial role in NFT transactions, automating aspects such as royalties, resale conditions, and authentication. However, smart contracts are only as effective as their coding, and they may not align with existing IP laws. For instance, some NFT platforms enable automatic royalty payments to creators upon resale, but enforcing these conditions outside blockchain ecosystems remains a legal gray area. Additionally, smart contracts cannot prevent off-chain infringement, such as unauthorized reproductions or derivative works created outside of blockchain networks.

To address these challenges, legal frameworks must adapt to accommodate blockchain-based transactions while upholding traditional copyright protections. Some potential solutions include developing NFT-specific IP legislation, requiring NFT marketplaces to verify content authenticity before listing, and incorporating digital rights management (DRM) tools into NFT metadata. Furthermore, international cooperation is necessary to establish consistent standards for NFT-related IP rights, ensuring that creators and buyers have clear legal protections regardless of jurisdiction.

3.3 NFT Infringement, Counterfeiting, and Legal Enforcement Challenges

The rapid growth of the NFT market has given rise to significant concerns regarding infringement, counterfeiting, and enforcement difficulties. Due to the decentralized and pseudonymous nature of blockchain transactions, bad actors can exploit NFT marketplaces to create and sell counterfeit tokens, leading to widespread fraud and rights violations.

One of the most prevalent issues is unauthorized NFT minting. Scammers often copy existing digital content, tokenize it as an NFT, and sell it to unsuspecting buyers. Unlike traditional counterfeit goods, which are subject to regulatory oversight and intellectual property enforcement, NFT counterfeiting occurs within decentralized networks where legal interventions are limited. As a result, victims face challenges in proving ownership and seeking recourse.

Additionally, NFT scams involving rug pulls and wash trading have become increasingly common. Rug pulls occur when creators of an NFT project promote and sell assets before abruptly abandoning the project, leaving buyers with worthless tokens. Wash trading involves artificially inflating the value of an NFT through coordinated transactions, deceiving investors about its market demand. These fraudulent activities highlight the need for regulatory mechanisms to enhance transparency and accountability in NFT markets.

From an enforcement perspective, tracking NFT ownership and resolving disputes pose significant hurdles. Blockchain provides a transparent record of ownership transfers, but pseudonymity complicates legal action against infringers. In some cases, NFT marketplace operators have taken steps to delist fraudulent NFTs, but this does not provide restitution to affected parties. Additionally, courts lack established precedents for adjudicating NFT disputes, making legal outcomes uncertain.

To improve enforcement mechanisms, several approaches could be explored. First, NFT marketplaces can implement stricter verification processes, such as requiring proof of authorship before listing tokens. Second, regulatory bodies can establish NFT-specific guidelines that mandate clearer ownership disclosures and anti-fraud measures. Third, smart contract-based escrow systems can be introduced to reduce the risks of fraudulent transactions by ensuring that funds are released only when predefined conditions are met.

The legal complexity surrounding NFTs underscores the importance of evolving regulatory frameworks to protect buyers, creators, and investors. As NFTs continue to gain adoption across various industries, legal institutions must develop tailored solutions that uphold property rights while fostering innovation in digital asset ownership.

3.4 Conclusion on NFT Property Rights and Legal Considerations

The legal landscape of NFT property rights remains in flux, requiring a multidimensional approach to address ownership, intellectual property, and enforcement challenges. While NFTs introduce a novel form of digital ownership, their legal recognition and protections lag behind technological advancements. Establishing clear distinctions between NFT ownership and under-

lying content rights is critical to mitigating disputes and fostering market trust.

Regulatory developments must balance the decentralized nature of blockchain with the need for consumer protection and copyright enforcement. Future legal frameworks should integrate NFT-specific policies, strengthen IP verification processes, and enhance legal recourse for infringement cases. Additionally, collaboration between NFT marketplaces, legal professionals, and policymakers will be essential in shaping a transparent and legally sound NFT ecosystem.

By addressing these legal considerations, the NFT industry can move toward greater legitimacy, ensuring that digital asset ownership is both innovative and legally secure. As blockchain technology evolves, continuous adaptation of legal standards will be necessary to keep pace with the dynamic digital economy.

4 Judicial Challenges in the Metaverse

4.1 Virtual Crimes and Jurisdictional Boundaries in Legal Governance

The metaverse introduces unprecedented challenges in defining and enforcing legal jurisdiction. Traditional legal systems are built on geographic boundaries, but the decentralized and borderless nature of virtual environments complicates the application of existing jurisdictional rules. Virtual crimes, ranging from financial fraud and identity theft to cyber harassment and digital asset theft, pose significant enforcement difficulties when they occur across multiple jurisdictions.

One of the key concerns is determining which legal system has authority over a dispute or criminal act within the metaverse. If a fraudulent NFT transaction occurs between parties residing in different countries, whose laws should apply? Similarly, if a user's digital identity is compromised within a decentralized platform, which court has jurisdiction over the dispute? These questions highlight the need for new legal frameworks capable of addressing cross-border virtual crimes.

Another challenge arises from the anonymity and pseudonymity of metaverse participants. Unlike real-world legal systems, where law enforcement agencies can identify individuals through official documentation, virtual identities often lack verifiable real-world counterparts. This anonymity makes it difficult to track offenders and enforce legal decisions, necessitating new mechanisms for identity verification within judicial processes.

In response, some jurisdictions are considering regulatory approaches that require metaverse platforms to implement identity verification mechanisms, similar to Know Your Customer (KYC) protocols used in financial services. However, such measures raise privacy concerns and may conflict with the decentralized ethos of the metaverse. Striking a balance between law enforcement needs and digital privacy rights will be essential in shaping jurisdictional policies for virtual worlds.

4.2 Dispute Resolution Mechanisms: Decentralized Justice (ODR) and Blockchain Arbitration

The traditional court system is often ill-equipped to handle disputes that arise in decentralized environments. Legal proceedings in conventional courts can be slow, costly, and jurisdictionally complex, making them impractical for resolving many metaverse-related conflicts. As a result, alternative dispute resolution (ADR) methods, such as online dispute resolution (ODR) and blockchain-based arbitration, are gaining attention as potential solutions.

ODR is an emerging approach that leverages digital platforms to facilitate conflict resolution. In the metaverse, ODR mechanisms could provide efficient, scalable, and automated dispute resolution processes. These systems can integrate artificial intelligence (AI) mediators, smart contract-based arbitration, and reputation-based adjudication to streamline legal proceedings without requiring traditional court involvement.

Blockchain arbitration platforms, such as Kleros and Aragon Court, offer decentralized mechanisms for resolving metaverse disputes. These platforms use smart contracts to create impartial and tamper-resistant dispute resolution processes, where community-selected jurors or arbitrators review cases and make binding decisions. Because blockchain arbitration is decentralized, it aligns well with the principles of metaverse governance, allowing disputes to be resolved transparently without reliance on centralized authorities.

However, blockchain arbitration also presents legal challenges. The enforceability of blockchain-based decisions remains uncertain in many jurisdictions. Courts may not recognize smart contract-based rulings as legally binding, leading to difficulties in enforcing judgments outside blockchain ecosystems. Furthermore, decentralized dispute resolution systems must address concerns related to fairness, bias, and security to gain broader legal recognition and adoption.

To bridge the gap between traditional legal frameworks and decentralized dispute resolution, hybrid models are being explored. Some proposals suggest integrating ODR mechanisms with state-recognized arbitration institutions, allowing blockchain rulings to be legally recognized in traditional courts. This hybrid approach could enhance the legitimacy of decentralized justice while maintaining efficiency and transparency in virtual legal processes.

4.3 Evidence Collection and Law Enforcement: Smart Contract Disputes and Digital Forensics

Evidence collection in the metaverse presents unique challenges due to the digital nature of interactions and transactions. Traditional evidentiary standards, such as witness testimony and physical documentation, are often inapplicable in virtual environments. Instead, law enforcement agencies and legal professionals must rely on digital forensics, blockchain analysis, and smart contract audits to gather admissible evidence.

Smart contracts, which automatically execute predefined agreements on blockchain networks, play a crucial role in metaverse transactions. However, disputes can arise due to coding errors,

fraudulent contract terms, or malicious exploitation of smart contract vulnerabilities. Resolving such disputes requires advanced forensic techniques to analyze blockchain transaction records, audit smart contract logic, and trace digital asset transfers. Because smart contracts are immutable, legal professionals must develop expertise in interpreting blockchain evidence to determine liability and enforce contractual obligations.

Another challenge is ensuring the authenticity and integrity of digital evidence. In traditional legal proceedings, courts rely on chain-of-custody protocols to verify the legitimacy of evidence. In the metaverse, similar protocols must be established to prevent tampering, ensure transparency, and maintain trust in digital forensics. Blockchain technology offers a potential solution by providing immutable records of transactions and interactions. Digital timestamps, cryptographic signatures, and decentralized ledgers can serve as verifiable evidence in legal proceedings.

Despite these advantages, legal frameworks for blockchain evidence remain underdeveloped. Courts must determine how to handle digital signatures, cryptographic proofs, and decentralized logs in judicial processes. Additionally, cross-border legal harmonization is necessary to establish global standards for blockchain forensics and smart contract dispute resolution.

To enhance the effectiveness of digital law enforcement, regulatory bodies are exploring collaborative approaches between technology companies, law enforcement agencies, and legal institutions. Establishing dedicated metaverse law enforcement units, training digital forensic experts, and developing legal precedents for blockchain-related cases are critical steps in addressing the judicial challenges posed by virtual environments.

4.4 Conclusion on Judicial Challenges in the Metaverse

The metaverse presents complex judicial challenges that require innovative legal solutions. Issues of jurisdiction, dispute resolution, and digital evidence collection necessitate new approaches to legal governance that balance technological advancements with legal protections. While decentralized dispute resolution mechanisms offer promising alternatives to traditional courts, their legal enforceability remains uncertain, requiring further integration with existing judicial systems.

Legal frameworks must evolve to accommodate the unique characteristics of the metaverse, ensuring that virtual crimes are effectively prosecuted, disputes are fairly resolved, and digital evidence is properly authenticated. Collaborative efforts between governments, technology providers, and legal scholars will be essential in developing metaverse-compatible judicial policies that uphold justice while preserving the decentralized nature of virtual environments.

As the metaverse continues to expand, ongoing legal adaptations and regulatory innovations will be necessary to create a fair, secure, and legally sound digital ecosystem. By addressing these judicial challenges proactively, legal institutions can help shape a metaverse that fosters trust, accountability, and equitable governance.

5 Global Legal Framework Evolution: Regulatory Trends in the Metaverse

5.1 Legislative Landscape in Major Countries and Regions: Policy Analysis of the U.S., EU, and China

As the metaverse continues to evolve, various countries and regions have begun formulating regulatory frameworks to govern digital assets, virtual interactions, and decentralized economies. While there is no universal legal structure governing the metaverse, the regulatory approaches adopted by the United States, the European Union, and China provide insights into global trends and challenges.

The United States has primarily focused on classifying metaverse assets, such as non-fungible tokens (NFTs) and cryptocurrencies, within its existing financial and securities laws. The Securities and Exchange Commission (SEC) has taken an active stance in regulating blockchain-based assets, asserting that certain digital assets fall under securities regulations. The Commodity Futures Trading Commission (CFTC) has also played a role in overseeing digital commodity transactions. However, there is no comprehensive metaverse-specific legislation, leading to uncertainty about the legal status of virtual property, digital identities, and metaverse-based financial activities. Additionally, privacy laws such as the California Consumer Privacy Act (CCPA) impose data protection requirements on platforms operating within the U.S., potentially affecting metaverse service providers.

The European Union has adopted a more structured regulatory approach, emphasizing data protection, digital rights, and financial oversight. The General Data Protection Regulation (GDPR) imposes strict requirements on data processing, raising questions about the compliance of decentralized identity systems and blockchain-based authentication methods. The EU's proposed Markets in Crypto-Assets (MiCA) framework aims to establish clear rules for digital asset issuers, exchanges, and wallet providers, potentially shaping how metaverse transactions are governed. The EU has also focused on digital consumer rights, ensuring transparency in virtual economies and preventing deceptive practices within metaverse platforms.

China has taken a highly centralized and restrictive approach to metaverse regulation. The Chinese government has banned most forms of cryptocurrency transactions, limiting the development of decentralized finance (DeFi) and NFT marketplaces within its jurisdiction. However, China has invested heavily in controlled digital ecosystems, such as the Digital Yuan (e-CNY), which could serve as a state-sanctioned currency for metaverse transactions. The country has also implemented strict content regulations and data localization laws, requiring metaverse platforms operating in China to comply with state censorship policies and cybersecurity frameworks. Unlike the U.S. and EU, China is likely to develop a metaverse regulatory model that prioritizes state control over decentralized governance.

These varying approaches highlight the challenges of harmonizing global metaverse regu-

lations. While some jurisdictions emphasize financial stability and consumer protection, others focus on state control or digital rights. This regulatory fragmentation creates legal uncertainties for businesses and users operating in the metaverse, necessitating greater international cooperation.

5.2 Challenges in Cross-Border Legal Coordination: Data Sovereignty and International Law Enforcement Cooperation

The borderless nature of the metaverse presents significant challenges for cross-border legal coordination. Traditional legal frameworks are based on national sovereignty, but metaverse platforms operate globally, often outside the direct jurisdiction of any single country. This raises concerns about data sovereignty, international enforcement cooperation, and conflicting regulatory requirements.

Data sovereignty is a major issue in metaverse governance, as countries seek to assert control over personal and corporate data generated within their territories. The European Union's GDPR, China's Cybersecurity Law, and various U.S. state-level data privacy laws impose different, and sometimes conflicting, obligations on metaverse service providers. Ensuring compliance with multiple regulatory frameworks is challenging, particularly for decentralized applications (dApps) that lack a central governing entity. Metaverse companies must navigate these legal complexities while avoiding potential conflicts between national laws.

International law enforcement cooperation is another challenge, particularly in cases involving cybercrime, fraud, and intellectual property infringement in the metaverse. Unlike traditional legal disputes, metaverse-related crimes often involve pseudonymous actors, decentralized networks, and transactions that cross multiple jurisdictions. Law enforcement agencies face difficulties in identifying perpetrators, obtaining digital evidence, and enforcing legal decisions across borders.

Efforts to improve international cooperation in metaverse regulation have included initiatives such as the Financial Action Task Force (FATF) guidelines for virtual assets, which aim to combat money laundering and terrorist financing in digital finance. However, these efforts remain limited in scope and do not fully address the complexities of metaverse-related legal disputes. Future regulatory frameworks will need to establish mechanisms for mutual legal assistance, digital evidence-sharing, and joint investigations between nations.

5.3 Technology-Driven Legal Adaptation: AI-Assisted Law Enforcement and Smart Contract Legalization

As the metaverse expands, traditional legal enforcement mechanisms may struggle to keep pace with digital transformations. Emerging technologies such as artificial intelligence (AI) and blockchain are increasingly being explored as tools to assist legal governance, enhance compliance, and automate dispute resolution.

AI-assisted law enforcement offers promising solutions for monitoring virtual activities, detecting fraudulent transactions, and analyzing patterns of criminal behavior within the metaverse. Machine learning algorithms can be deployed to detect suspicious activities in real time, such as money laundering, phishing scams, and unauthorized digital asset transfers. Additionally, AI-driven chatbots and virtual legal assistants could provide metaverse users with legal guidance, helping them understand regulatory requirements and dispute resolution processes.

However, AI-assisted legal enforcement raises ethical and legal concerns, particularly regarding bias, transparency, and accountability. AI models must be trained on diverse datasets to avoid discriminatory enforcement, and their decision-making processes must be explainable to ensure fairness. Furthermore, legal frameworks must establish clear guidelines for the use of AI in metaverse law enforcement, ensuring that automated legal decisions adhere to due process principles.

Another key area of technological legal adaptation is the legalization and formal recognition of smart contracts. Smart contracts—self-executing agreements stored on blockchain networks—have the potential to automate legal transactions, enforce contractual terms, and reduce reliance on intermediaries. In the metaverse, smart contracts could be used for property transactions, employment agreements, and digital rights management. However, their legal enforceability remains a challenge.

Jurisdictions differ in their treatment of smart contracts. While some countries, such as the United States, have recognized certain smart contract terms as legally binding, others require additional legal interpretations to ensure their validity. The enforceability of smart contracts also depends on dispute resolution mechanisms, as errors in coding or unforeseen circumstances may require legal intervention. Establishing international standards for smart contract governance will be crucial in ensuring their widespread legal acceptance.

The intersection of AI, blockchain, and legal governance in the metaverse represents a critical area of research and policy development. Policymakers must balance technological innovation with regulatory oversight, ensuring that AI-driven enforcement and smart contract automation align with legal principles. Collaboration between technology developers, legal scholars, and regulatory authorities will be essential in shaping a metaverse that is both legally robust and technologically advanced.

5.4 Conclusion on Global Legal Frameworks and Metaverse Regulation

The evolution of global legal frameworks for the metaverse is an ongoing process, shaped by the diverse regulatory approaches of different countries, the challenges of cross-border legal coordination, and the impact of emerging technologies on legal enforcement. While the United States, European Union, and China have taken distinct approaches to metaverse regulation, their policies will influence future legal developments in virtual environments.

Achieving global legal harmonization in the metaverse requires addressing data sovereignty issues, strengthening international law enforcement cooperation, and integrating technology-

driven legal solutions. AI-assisted law enforcement and smart contract legalization represent promising avenues for legal adaptation, but they must be implemented with careful consideration of ethical and procedural safeguards.

As the metaverse continues to grow, legal frameworks must remain flexible, allowing for continuous adaptation to new technological and societal developments. A proactive approach to regulation, driven by collaboration between governments, industry stakeholders, and legal experts, will be crucial in ensuring that the metaverse operates as a legally secure and innovation-friendly environment.

6 Future Outlook: Building a Legal Framework for the Metaverse

6.1 Integration of Law and Technology: Smart Contracts, DAOs, and the Digital Judiciary System

The future of legal governance in the metaverse hinges on the seamless integration of law and technology. Emerging digital tools such as smart contracts, decentralized autonomous organizations (DAOs), and blockchain-based judicial mechanisms offer new pathways for legal regulation and dispute resolution in virtual environments.

Smart contracts are self-executing agreements embedded in blockchain networks, ensuring automatic compliance with predetermined terms. In the metaverse, smart contracts can facilitate transactions, enforce property rights, and establish governance protocols for digital communities. However, their legal enforceability remains a subject of debate. While some jurisdictions recognize smart contracts as legally binding, others require additional oversight to align them with traditional contract law. The future legal framework must standardize smart contract regulations, ensuring that automated agreements comply with global legal norms while remaining adaptable to evolving technological advancements.

DAOs represent another innovative approach to governance in the metaverse. As decentralized entities operating through blockchain consensus mechanisms, DAOs offer a model for community-driven decision-making without reliance on centralized authorities. DAOs could govern metaverse economies, manage digital assets, and even serve as alternative judicial systems. However, their legal status remains ambiguous. Many legal systems lack clear guidelines on DAO liability, dispute resolution, and taxation. Future regulatory efforts must establish legal recognition for DAOs, ensuring their compliance with existing laws while preserving their decentralized nature.

Blockchain-based digital judiciary systems could revolutionize dispute resolution in the metaverse. Automated arbitration platforms, such as those powered by artificial intelligence (AI) and blockchain validation, can offer efficient, transparent, and impartial adjudication of virtual disputes. These systems could complement traditional courts by handling cases related to intellectual property infringement, contractual disagreements, and fraud in digital marketplaces. However,

significant challenges remain in harmonizing these technologies with real-world legal principles. Ensuring due process, legal enforceability, and cross-border recognition of blockchain-based judicial decisions will be crucial in shaping the future metaverse legal system.

6.2 Consumer Rights Protection in the Metaverse: Digital Asset Security and Privacy Safeguards

As economic activities expand within the metaverse, consumer protection will become a key focus of legal regulation. Users engaging in digital asset transactions, virtual real estate investments, and NFT trading require robust legal safeguards to protect their rights and interests.

One major concern is the security of digital asset transactions. Unlike traditional financial systems, where regulatory bodies oversee fraud prevention and financial disputes, metaverse marketplaces often operate in decentralized environments with limited consumer protections. Users are vulnerable to scams, hacking incidents, and unauthorized asset transfers. To address these risks, future legal frameworks must establish standardized consumer protection laws tailored to digital transactions. Regulations should mandate transparency in smart contract agreements, require identity verification for high-value transactions, and implement security measures to prevent asset theft.

User privacy is another critical issue in metaverse governance. Virtual platforms collect vast amounts of user data, including behavioral analytics, biometric information, and transaction records. Without adequate legal protections, this data could be exploited for surveillance, targeted advertising, or identity theft. The application of existing data privacy laws, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), to metaverse environments will require significant legal adaptations. Additionally, the development of privacy-enhancing technologies, such as zero-knowledge proofs and decentralized identity management systems, could help balance user privacy with regulatory compliance.

Future consumer protection laws should also address digital identity fraud, unauthorized deepfake content, and unfair trade practices within the metaverse. Establishing clear legal avenues for dispute resolution, fraud prevention, and consumer redress will be essential in fostering a secure and trustworthy digital economy.

6.3 From Experimentation to Standardization: Globalization of Metaverse Law and Future Research Directions

The evolution of metaverse legal systems will require a shift from experimental regulatory approaches to standardized global legal frameworks. As different countries explore metaverse regulations independently, inconsistencies in legal approaches pose challenges for international businesses, users, and developers.

The globalization of metaverse law will necessitate international cooperation among governments, legal institutions, and technology providers. Existing international legal bodies, such as the

United Nations Commission on International Trade Law (UNCITRAL) and the Financial Action Task Force (FATF), could play a role in harmonizing legal standards for digital asset transactions, dispute resolution, and jurisdictional oversight. Collaborative efforts could lead to the establishment of global metaverse regulatory standards, ensuring consistency in legal protections across different virtual environments.

One approach to legal standardization involves the creation of regulatory sandboxes, where governments can test new legal frameworks in controlled virtual settings before full-scale implementation. Regulatory sandboxes allow policymakers to assess the impact of digital asset taxation, intellectual property laws, and decentralized governance models before enacting permanent legislation. These pilot programs can provide valuable insights into the practical challenges of metaverse law, enabling regulators to refine their approaches based on real-world data.

Future research on metaverse law should focus on three key areas: jurisdictional adaptability, technological legal integration, and ethical governance. Jurisdictional adaptability explores how legal systems can manage cross-border virtual interactions, ensuring that metaverse disputes are resolved efficiently and fairly. Technological legal integration examines the role of AI, blockchain, and machine learning in automating legal enforcement and compliance mechanisms. Ethical governance addresses concerns related to digital rights, inclusivity, and equitable access to metaverse resources.

As the metaverse continues to evolve, ongoing interdisciplinary collaboration between legal scholars, technologists, and policymakers will be essential in shaping a comprehensive, forward-thinking legal framework. A successful metaverse legal system must balance innovation with accountability, ensuring that digital societies operate within fair, transparent, and enforceable legal structures.

6.4 Conclusion on the Future of Metaverse Law

The construction of a legal framework for the metaverse represents one of the most complex and dynamic challenges of the digital age. As virtual economies, digital identities, and decentralized governance models gain prominence, legal systems must evolve to accommodate these transformations. The integration of smart contracts, DAOs, and digital judicial systems offers promising avenues for legal innovation, but their practical implementation requires careful regulation.

Consumer protection in the metaverse will be a foundational aspect of future legal frameworks, ensuring that users are safeguarded against fraud, privacy violations, and unfair business practices. Legal harmonization at the international level will be crucial in preventing regulatory fragmentation and ensuring that metaverse governance remains inclusive and globally coherent.

Looking ahead, the transition from experimental legal approaches to standardized metaverse law will depend on continuous research, technological adaptation, and international collaboration. Policymakers must work alongside industry leaders and academic institutions to craft regulations that balance innovation with legal certainty. By proactively addressing these legal challenges,

society can build a metaverse that is not only technologically advanced but also legally sound, ethical, and inclusive for all users.

元宇宙法治体系的构建： 数字身份、NFT 产权与全球法律框架

陈忠

福建师范大学

摘要 本研究探讨了元宇宙法治体系的构建，分析了数字身份、NFT 产权、司法挑战及全球法律框架的演进。文章详细讨论了主要国家的监管趋势，跨国法律协调的挑战，以及技术驱动的法律适应。未来，智能合约、DAO 和数字司法体系将成为元宇宙法律的重要组成部分，确保消费者权益和数字资产交易安全。本研究强调了全球法律标准化的重要性，并提出了未来研究方向，以推动元宇宙的法治发展。

关键词 元宇宙；数字身份；NFT 产权；司法挑战；法律框架

To Cite This Article Zhong CHEN. (2025). Building a Legal Framework for the Metaverse: Digital Identity, NFT Property Rights, and Global Legal Structures. *Digital Society & Virtual Governance*, 1(1), 52-71. <https://doi.org/10.6914/dsvg.010104>

Digital Society & Virtual Governance, ISSN 3079-7624 (print), ISSN 3079-7632 (online), DOI 10.6914/dsvg, a Quarterly, founded on 2025, published by Creative Publishing Co., Limited. Email: wtocom@gmail.com, <https://dsvg.cc>, <https://cpcl.hk>.

Article History Received: November 16, 2024 Accepted: January 22, 2025 Published: February 28, 2025

References

- [1] Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from <https://ethereum.org>
- [2] Wright, A. & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*.
- [3] Zhang, J. (2024). Legal Issues and Solutions in the Metaverse. *Open Journal of Legal Science*, 12(1), 362-369. Retrieved from https://pdf.hanspub.org/ojls20240100000_96069771.pdf
- [4] Zhou, Y. (2025). Research on Legal Responses to Risks in NFT Digital Collectible Transactions. *E-Commerce Letters*, 14(1), 3752-3759. Retrieved from https://pdf.hanspub.org/ecl2025141_4652312996.pdf
- [5] Yang, X. (2023). Legal Challenges and Countermeasures of the Metaverse. *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*. Retrieved from <https://bhxb.buaa.edu.cn/bhsk/cn/article/doi/10.13766/j.bhsk.1008-2204.2021.0959>

- [6] Wang, G. (2024). Research on Copyright Protection of NFT Digital Works. *Open Journal of Legal Science*. Retrieved from https://pdf.hanspub.org/ojls2024127_42922639.pdf
- [7] Li, Y. (2023). Research on the Legal Attributes and Transaction Relationships of NFT Digital Works. *Tsinghua Law Journal*.
- [8] Ruan, S. (2023). On the Property Rights of NFT Digital Assets: A Bundle of Rights Perspective. *Journal of China Social Sciences*.
- [9] Liu, X. (2023). From Metaverse to Law 3.0: Discussing the Genealogy of Artificial Intelligence Law. *Journal of China Social Sciences*.
- [10] Wang, Q. & Zhang, F. (2008). Exploring Civil Law Issues of Online Virtual Property. *Journal of Fujian Normal University (Philosophy and Social Sciences Edition)*, (5), 9.
- [11] Wang, Q. (2023). On the Legal Nature of NFT Digital Art Transactions. *Oriental Law*, (1), 29-33.
- [12] Yang, Y. (2020). On the Legal Nature of Virtual Currency: Focusing on Civil and Financial Law. *Monthly Law Journal*, 301, 54.
- [13] Zhang, Y. & Pan, Y. (2022). Potential Risks and Legal Regulation of Virtual Society under Metaverse Governance. *Yuejiang Academic Journal*, 14(5), 72-79.
- [14] Wu, Y. (2023). Metaverse: Legal Mapping and Normative Logic. Beijing: *China Renmin University Press*, 41, 142.
- [15] Gangdao, Y. (2023). Illustrated Metaverse: Future Business Opportunities. Beijing: *Machinery Industry Press*, 80-81.

Editor Sophia LI wtoecom@gmail.com