Volume 3 Issue 1 (2026) 34-53
E-ISSN 2988-6740 | © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v3i1.43
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

Legal Analysis of Transaction Security in The Metaverse: Consumer Protection Challenges in The Virtual World

Lufiano Tilman Martins[1*], Lala Hucadinota Ainul Amri[2], Darma Setiawan Putra[3]
[1]Instituto Superior Cristal, Timor Leste
[2]Politeknik Negeri Madiun, Indonesia
[3]Politeknik Aceh Selatan, Indonesia
Corresponding Author: lufianotilman@gmail.com

ABSTRACT

The development of the metaverse as a space for digital interaction and transactions presents both new economic opportunities and complex legal risks, particularly regarding transaction security and consumer protection in the virtual world. The immersive, cross-border, and digital asset- and smart-contract-based characteristics of the metaverse pose serious challenges to existing conventional legal frameworks. This study aims to analyze legal protection for transaction security in the metaverse and identify consumer protection challenges in virtual transaction practices. The research method used is a normative juridical approach with a qualitative approach, using a statute approach to examine relevant laws and regulations, a conceptual approach to examine legal concepts regarding digital assets, smart contracts, and cybersecurity, and a comparative approach by comparing consumer protection regulations in several countries. The results show that national regulations provide basic protection for consumers, but have not fully addressed the unique risks of transactions in the metaverse, such as digital fraud, system hacking, uncertainty about the legal status of digital assets, and smart contract-based disputes. Key challenges include cross-border jurisdiction, immersive data security, and limited digital dispute resolution mechanisms. This study concludes that adaptive regulatory updates, strengthening transaction security standards, and cross-jurisdictional cooperation are needed to enhance consumer protection in the metaverse ecosystem.

Keywords: metaverse, cyber law, consumer protection, digital transactions, smart contracts

Article received on 20-07-2025 — Final revised on 06-09-2025 — Approved on 19-12-2025

Introduction

The development of digital technology over the past two decades has fundamentally changed the way humans interact, communicate, and conduct economic transactions. One rapidly developing innovation is the metaverse, a three-dimensional virtual environment that allows users to interact and conduct transactions in real time through digital avatars. The metaverse serves not only as an entertainment and social space but has also evolved into a complex digital economic ecosystem, where various forms of digital assets are traded,

transactions are conducted using cryptocurrencies, and legal relationships are facilitated through automatically executed smart contracts. The immersive, interactive, and cross-jurisdictional characteristics of the metaverse mark the birth of a new paradigm in the digital economy and also present new legal challenges, particularly related to transaction security and consumer protection, which have not been fully anticipated by conventional legal systems (Vidal-Tomás, 2022).

In the context of Indonesian law, regulations regarding electronic transactions and consumer protection are essentially regulated by Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, Law Number 8 of 1999 concerning Consumer Protection, and Law Number 27 of 2022 concerning Personal Data Protection. Furthermore, cybersecurity aspects are regulated through various national policies and technical regulations, while crypto assets are classified as commodities under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti). However, these regulations are still oriented towards conventional electronic transactions and do not explicitly address the unique characteristics of transactions in the metaverse, such as the legal status of virtual assets, the legal responsibilities of metaverse platform operators, and the protection of immersive data generated from user activity in virtual spaces (Huang et al., 2022).

These regulatory limitations pose various legal risks for consumers, including digital fraud, account and wallet hacking, misuse of personal data, and legal disputes related to the automated and difficult-to-revoke execution of smart contracts. Furthermore, the cross-jurisdictional nature of the metaverse also creates legal uncertainty regarding applicable law, court jurisdiction, and effective dispute resolution mechanisms for Indonesian consumers. Therefore, a systematic legal analysis is needed through a normative juridical approach, combining statutory, conceptual, and comparative approaches to assess the adequacy of the national legal framework and compare it with international best practices. This approach is expected to formulate adaptive legal policy recommendations, responsive to technological developments, and oriented toward strengthening transaction security and consumer protection in the ever-evolving metaverse ecosystem (Bhattacharya et al., 2022).

Based on this background, this study focuses on the following issues: (1) how cyber legal authorities can protect metaverse users from transaction risks, including digital fraud, hacking, and misuse of personal data; (2) the extent to which existing regulations are effective in guaranteeing transaction security in the metaverse; (3) legal challenges arising from the unique characteristics of the metaverse, including the use of digital assets, smart contracts, and virtual environments that are cross-jurisdictional; and (4) the preparation of legal policy recommendations to strengthen consumer protection and transaction security in the metaverse (Y. Ren et al., 2024).

Various literature shows that digital transaction security and consumer protection are central issues in technology-based economic ecosystems, especially with the increasing use of virtual platforms such as the metaverse. (Kimotho, 2022) emphasized that transaction automation through blockchain technology and smart contracts does increase efficiency and speed, but simultaneously also expands the spectrum of legal risks, such as digital fraud, system hacking, and digital asset manipulation. Similarly, (Aprilya, S., & Misbach, 2024) emphasized the importance of implementing Good Corporate Governance (GCG) principles in digital services as an instrument to ensure transparency, accountability, and protection of user rights. However, most of these studies still view transaction security from a technical and corporate governance perspective, without deeply linking it to consumer protection in the context of immersive and automated virtual transactions such as the metaverse (Momtaz, 2022).

International literature also shows that several jurisdictions have begun developing more progressive regulatory frameworks to address the challenges of digital transactions in virtual environments. The European Union, for example, has made the General Data Protection Regulation (GDPR) the primary foundation for personal data protection, including in virtual interactions, while the United States regulates digital transaction security and platform liability through a combination of federal and state regulations. However, the primary focus of these studies remains limited to issues of personal data protection, cybersecurity, and digital platform compliance, thus failing to fully address the complexities of metaverse transactions involving digital asset ownership, automated smart contract execution, and cross-jurisdictional legal relationships. Therefore, the cross-jurisdictional approaches discussed in the literature remain partial and do not provide a comprehensive legal framework for consumer protection in the metaverse as a global ecosystem (Ersoy & Gürfidan, 2023).

On the other hand, previous research in Indonesia has generally focused on regulating conventional electronic transactions, general consumer protection, and increasing public legal awareness in addressing the risks of digital transactions. (Soekanto, 2019), for example, emphasized the importance of legal awareness and legal education as preventive instruments against fraud and misuse of personal data. However, this approach still focuses on user behaviour and general normative aspects, without specifically examining the characteristics of transactions in the metaverse, which are three-dimensional, immersive, cross-platform, and based on digital assets and smart contracts. As a result, national legal studies have not been able to adequately address issues regarding the legal status of virtual assets, the legal responsibilities of metaverse platform operators, and effective consumer protection mechanisms in a virtual environment that recognizes no geographical boundaries (Rafique & Qadir, 2024).

Based on this description, there is a significant literature gap, both at the international and national levels. The existing literature remains fragmented between technical studies of cybersecurity, personal data protection, digital platform governance, and conventional electronic transactions, without a complete integration of the unique characteristics of the metaverse. There is no legal study that comprehensively links Indonesian national regulations, the technical and social dynamics of the metaverse, and international best practices within a single normative analytical framework. Therefore, this research is crucial to fill this gap by conducting a systematic legal analysis of transaction security in the metaverse and consumer protection challenges, in order to formulate legal policy recommendations that are adaptive, contextual, and responsive to developments in the virtual world (Wu & Liu, 2022).

This research employs a normative juridical method with a qualitative approach, as the primary focus is on legal review and regulatory analysis, rather than quantitative data collection or field experiments. Within this framework, three main approaches are employed. First, the Statute Approach, which examines Indonesian regulations related to digital transactions, such as the ITE Law, the Consumer Protection Law, and cybersecurity regulations, to evaluate the extent to which cyberlaw authorities can protect users from the risks of transactions in the metaverse and anticipate the unique challenges posed by virtual interactions. Second, the Conceptual Approach, which focuses on examining the legal principles underlying digital consumer protection, transaction security, smart contracts, and digital assets, allows for an in-depth analysis of the relevance and limitations of existing regulations in the context of cross-jurisdictional transactions. Third, the Comparative Approach, which compares consumer protection and transaction security practices in the metaverse in other countries, such as the European Union and the United States, which have already developed virtual world regulations. This comparative finding can serve as a

reference for formulating more adaptive, comprehensive, and effective national legal policy recommendations to address the dynamics of digital transactions in the metaverse (Guo et al., 2023).

This research has significant theoretical and practical implications for the development of cyber law and consumer protection in the era of the virtual economy. Theoretically, this research expands the study of electronic transaction law by incorporating the unique characteristics of the metaverse: immersive, automated, and cross-jurisdictional, thereby enriching the legal discourse related to digital assets, smart contracts, and virtual transaction security. Practically, the findings of this research are expected to serve as a reference for policymakers, regulators, and digital platform operators in formulating transaction security standards, consumer protection mechanisms, and digital dispute resolution models that are more adaptive and responsive to transaction risks in the metaverse. These implications are crucial for increasing legal certainty, consumer trust, and the sustainability of the virtual economy ecosystem in Indonesia.

The novelty of this research lies in its integrative and contextual legal analysis approach to transactions in the metaverse. Unlike previous research, which generally focused on cybersecurity, personal data protection, or conventional electronic transactions separately, this study examines the security of metaverse transactions as a unified legal ecosystem involving digital assets, smart contracts, the role of platform providers, and cross-jurisdictional legal relationships. Furthermore, this research specifically places consumer protection as a primary focus in metaverse transactions, linking Indonesia's national legal framework with international best practices, resulting in a new, more comprehensive and applicable perspective in the context of the virtual world.

The research gap that underpins this study is the lack of a legal review that systematically integrates Indonesian national regulations, the technical and social characteristics of the metaverse, and a cross-jurisdictional comparative approach within a single normative analytical framework. The existing literature remains fragmentary and fails to fully address issues regarding the legal certainty of digital assets, the legal liability of metaverse platforms, and the effectiveness of consumer protection and digital dispute resolution mechanisms. Therefore, this study seeks to address this gap by providing a comprehensive legal analysis and adaptive policy recommendations to bridge the development of metaverse technology with the need for consumer legal protection in Indonesia.

This research aims to analyze legal protection for transaction security in the metaverse, identify emerging legal challenges, and formulate policy recommendations that strengthen consumer rights and transaction security. The research is expected to contribute academically to the development of cyber law in Indonesia, provide a basis for policymakers in developing metaverse regulations, and raise public awareness of the risks and rights associated with virtual transactions.

Research Method

This research uses a normative legal research method with a qualitative approach. This method was chosen because the focus of this research is analyzing legal provisions governing transactions in the metaverse and consumer protection in virtual environments. This approach allows researchers to examine relevant laws and regulations, legal literature, official documents, and legal principles without conducting experiments or quantitative surveys (R. Li et al., 2024).

This research also applies three main approaches to strengthen the legal analysis related to transactions in the metaverse. First, the Statute Approach, which examines applicable regulations in Indonesia, including the ITE Law, the Consumer Protection Law,

government regulations, and regulations related to information technology, with the aim of evaluating the extent to which these legal provisions can protect users from transaction risks such as digital fraud, hacking, and misuse of personal data. Second, the Conceptual Approach, which focuses on the study of legal principles and concepts underlying digital consumer protection, transaction security, digital assets, smart contracts, and cross-jurisdictional transactions, thus enabling an in-depth understanding of the relevance and limitations of existing regulations in addressing the unique characteristics of transactions in the virtual world. Third, the Comparative Approach, which compares consumer protection and transaction security practices in the metaverse in countries that have already regulated legal aspects of the virtual world, such as the European Union and the United States. The results of this analysis serve as the basis for formulating recommendations for more adaptive, comprehensive, and effective national legal policies in addressing the dynamics of digital transactions in the metaverse (Kou et al., 2023).

This study uses secondary data obtained through library research on various official and scientific sources relevant to transaction security in the metaverse and consumer protection. Primary legal sources include Indonesian laws and regulations directly related to electronic transactions, cybersecurity, and consumer protection, such as Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, Law Number 8 of 1999 concerning Consumer Protection, Law Number 27 of 2022 concerning Personal Data Protection, government regulations and implementing regulations related to electronic systems and transactions, and technical regulations from authorized institutions governing digital assets and cybersecurity. Secondary legal sources include legal textbooks, national and international scientific journal articles, research reports, and academic publications specifically discussing cyber law, smart contracts, digital assets, the metaverse, and digital consumer protection, selected based on criteria such as substantive relevance, author or publisher authority, novelty of the study, and its relevance to the research focus. Tertiary legal sources in the form of legal dictionaries, encyclopedias, and other conceptual references are used selectively to clarify the definitions, concepts, and legal terminology being analyzed, so that all data sources used support legal analysis that is systematic, valid, and academically accountable (Kaur et al., 2023).

The data in this study was collected through library research using several systematic steps. First, national and international regulations relevant to transactions in the metaverse were identified. Next, legal documents and academic literature were reviewed to understand the concepts of consumer protection, transaction security, and the unique characteristics of the metaverse. The next step involved analyzing comparative documents from other countries using a comparative approach, with the aim of assessing best practices in protecting virtual transactions. Finally, all data obtained was classified and categorized according to the research focus: cyber law authority, regulatory effectiveness, legal challenges, and the development of adaptive and comprehensive legal policy recommendations for transactions in the virtual world (Nakavachara & Saengchote, 2022).

The data obtained was analyzed using a qualitative-descriptive approach with several stages. First, data reduction was performed, namely sorting legal documents and literature to highlight aspects relevant to the research focus. Next, the data was categorized based on the research focus, including cyber law authority, regulatory effectiveness, legal challenges in the metaverse, and the development of legal policy recommendations. The next stage was interpretation, which included interpreting regulations, legal concepts, and international practices to assess the extent to which consumer protection and transaction security can be realized in virtual transactions in the metaverse. Finally, synthesis was performed, namely compiling the analysis results into comprehensive legal conclusions and recommendations, which refer to national legal principles and best international practices to ensure that legal

regulations and policies are adaptive and effective in facing developments in digital technology (F.-Y. Wang, 2022).

To ensure data validity, this study employed source triangulation, comparing information obtained from various primary, secondary, and tertiary legal sources to ensure consistency and accuracy. Furthermore, the literature used was verified through official documents and relevant academic publications, ensuring that each finding has a strong foundation. The study also examined the alignment between national regulations and international practices as part of an effort to support the formulation of realistic and applicable legal recommendations. By applying this method, the study is expected to produce an in-depth, systematic, and comprehensive legal analysis, while also providing a basis for effective policy recommendations to strengthen consumer protection and transaction security in the virtual, cross-platform, and cross-jurisdictional metaverse ecosystem (Z. Zheng et al., 2022).

This study has several limitations that require attention. First, the study uses a normative juridical approach with secondary data sources. Therefore, the resulting analysis focuses on the study of legislation, legal doctrine, and academic literature, without involving empirical data on transaction practices and direct consumer experiences on metaverse platforms. Second, the rapidly evolving dynamics of metaverse technology have the potential to lead to changes in regulations, platform policies, and international practices that have not been fully accommodated in this study. Third, the comparative analysis is limited to practices and regulations in certain jurisdictions considered representative, thus not comprehensively encompassing the entire global legal approach. Therefore, the findings of this study place greater emphasis on the conceptual and normative framework and open up space for further empirical and multidisciplinary research to deepen understanding of transaction security and consumer protection in the metaverse.

Result and Discussion

Tabel 1. An Analysis of Cyber Law's Authority in Protecting Metaverse Users

No	Analysis Aspects	Findings
1	Cyber law authority	Indonesia's cyber legal framework, through Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 (the ITE Law), provides a legal basis for prosecuting digital fraud, system hacking, and illegal access to electronic data. The provisions of Article 28 paragraph (1) of the ITE Law, for example, can be used to prosecute perpetrators of digital transaction-based fraud. However, in the context of the metaverse, this provision does not explicitly regulate virtual asset-based transactions such as NFTs or digital items within metaverse platforms. Examples of NFT fraud cases on various global platforms demonstrate that consumer losses are often difficult to qualify as "electronic consumer losses" in the conventional sense of the ITE Law.
2	Personal data protection	Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides protection for users' personal data, including the obligation of data controllers to maintain data security and confidentiality. However, the PDP Law does not specifically regulate immersive data generated in the metaverse, such as avatar biometric data, body movement patterns, virtual facial expressions, and real-time interaction recordings. International practice has seen cases of avatar data misuse and digital identity theft on virtual platforms, demonstrating that this type of data is highly sensitive but has not been clearly classified under Indonesia's data protection regime.

No	Analysis Aspects	Findings
3	Law enforcement mechanisms	Cyber law enforcement in Indonesia involves various institutions, such as the Ministry of Communication and Informatics (Kominfo), the Indonesian National Police, and, in certain contexts, the Financial Services Authority (OJK) or Bappebti for crypto asset transactions. However, in metaverse transactions that are cross-jurisdictional and executed through smart contracts, law enforcement officials face significant challenges. For example, in cases of crypto wallet hacking or exploiting smart contract vulnerabilities, determining the locus of crime and the perpetrator responsible is difficult, especially when the server, platform, and perpetrator are located in different countries.

Indonesia's cyber law authority has essentially provided a normative foundation to protect users from various digital transaction risks. However, the provisions of the ITE Law, the Consumer Protection Law, and the PDP Law are still designed for conventional electronic transactions, thus not fully addressing the complexities of transactions in the metaverse. The absence of specific regulations regarding the legal status of virtual assets, the responsibilities of metaverse platform operators, and the execution and cancellation of smart contracts results in suboptimal consumer protection. Furthermore, technical challenges in law enforcement, such as difficulties in identifying perpetrators, cross-border digital evidence, and coordination between authorities, reinforce the need for more adaptive regulations and law enforcement mechanisms that are appropriate to the characteristics of the virtual world.

Tabel 2. Evaluating the Effectiveness of Existing Regulations in Providing Transaction Security Guarantees in the Metaverse

No	Analytical Aspect	Findings
1	EIT Law and Consumer Protection	Indonesia's Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 19 of 2016) and the Consumer Protection Law (Law No. 8 of 1999) provide a basic legal framework to protect users in digital transactions, including provisions on consumer rights, prohibited conduct, and sanctions for fraud. For instance, Article 28(1) of the EIT Law may be applied to digital fraud cases involving misleading information. However, these provisions were designed for conventional electronic transactions and do not explicitly address immersive virtual transactions in the metaverse, such as the sale of virtual land or digital assets. As seen in several international cases involving virtual land fraud and misleading NFT sales, consumers often face difficulties in asserting their rights due to the lack of legal clarity regarding the nature of virtual goods and platform liability.
2	Regulation of digital assets and smart contracts	At the national level, Indonesia does not yet have specific regulations governing non-fungible tokens (NFTs), virtual assets used in metaverse platforms, or the legal validity and enforceability of smart contracts as autonomous transaction mechanisms. While crypto assets are regulated as commodities under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti), this regime does not extend to virtual assets used solely within metaverse ecosystems. In practice, disputes arising from smart contract failures—such as coding errors or unauthorized exploitation—often lack clear legal remedies, as existing contract law frameworks presuppose human intent and intervention.
3	Implementation of transaction security guarantees	In practice, regulatory authorities and digital platform operators have not yet established specific security standards tailored to metaverse transactions. Unlike the financial sector, which is subject to strict

No	Analytical Aspect	Findings
		cybersecurity and consumer protection standards, metaverse platforms operate with varying levels of internal security governance. Several reported cases of hacked digital wallets and stolen virtual assets illustrate the absence of mandatory security protocols, consumer compensation mechanisms, and platform accountability. This regulatory gap increases the risk of financial loss, identity theft, and transactional fraud for users participating in metaverse-based commerce.

These findings demonstrate that the effectiveness of existing regulations in ensuring transaction security in the metaverse remains limited. Although current laws provide foundational consumer protection in digital environments, they are not sufficiently equipped to address the unique risks posed by metaverse transactions, particularly those involving virtual assets and automated smart contracts. The absence of explicit legal recognition of metaverse assets, combined with the lack of standardized security obligations for platform providers, significantly weakens consumer protection. Consequently, these conditions highlight the urgent need for regulatory reform, the development of specialized transaction security standards, and clearer rules on platform responsibility to ensure legal certainty and effective consumer protection in the metaverse ecosystem.

Tabel 3. Identifying Legal Challenges Emerging from the Unique Characteristics of the Metaverse

No	Analytical Aspect	Findings
1	Cross-jurisdictional transactions	The metaverse operates as a global digital environment in which transactions frequently involve users, platform providers, and servers located in different countries. This creates significant legal challenges related to jurisdiction, applicable law, and cross-border law enforcement. For example, cases involving fraud in virtual land sales on global metaverse platforms have demonstrated difficulties in determining the competent court and the applicable legal regime when victims and perpetrators reside in different jurisdictions. Under Indonesian law, existing jurisdictional principles in the Electronic Information and Transactions Law (EIT Law) provide only limited guidance for addressing transnational virtual disputes, particularly when platform operators are incorporated overseas.
2	Digital assets and smart contracts	Transactions in the metaverse commonly involve digital assets such as non-fungible tokens (NFTs), virtual goods, and automated smart contracts executed on blockchain networks. However, Indonesian contract law and electronic transaction regulations do not explicitly recognize the legal status of NFTs or smart contracts as self-executing agreements. International incidents involving smart contract exploits—where vulnerabilities in code were used to divert digital assets—illustrate the legal uncertainty surrounding liability, contract validity, and remedies. The absence of specific provisions governing digital asset ownership and smart contract enforceability increases the risk of unresolved disputes and weak consumer protection.
3	Data security and privacy protection	Metaverse platforms collect and process extensive amounts of personal and immersive data, including biometric identifiers, behavioral patterns, and real-time avatar interactions. While Indonesia's Personal Data Protection Law (Law No. 27 of 2022) establishes general obligations for data controllers, it does not explicitly address immersive data or cross-platform data sharing in virtual environments. International cases of avatar identity theft and unauthorized use of biometric data in virtual platforms highlight the heightened risks faced by users. These gaps demonstrate that existing data protection frameworks are not

No	Analytical Aspect	Findings
		yet fully equipped to safeguard users in immersive and interconnected metaverse ecosystems.

The findings indicate that legal challenges in the metaverse are complex and multidimensional, extending beyond technical risks to include unresolved legal issues related to jurisdiction, the legal status of digital assets, and the protection of immersive personal data. Current regulatory frameworks, including the EIT Law and the Personal Data Protection Law, provide only a partial response to these challenges and remain oriented toward conventional digital environments. Consequently, these conditions underscore the need for adaptive legal frameworks that explicitly address the unique characteristics of metaverse transactions, establish clear rules on digital asset ownership and smart contract liability, and strengthen cross-jurisdictional enforcement mechanisms to ensure effective consumer protection in virtual worlds.

Tabel 4. Drafting Legal Policy Recommendations to Strengthen Consumer Protection

No	Analytical Aspect	Findings
1	Regulatory reform	It is recommended that Indonesia develop specific regulations governing metaverse transactions, explicitly addressing the legal status of virtual assets, non-fungible tokens (NFTs), and the enforceability of smart contracts. International cases involving disputes over virtual land ownership and fraudulent NFT offerings illustrate the limitations of applying conventional electronic transaction laws to immersive virtual environments. A dedicated regulatory framework would provide legal certainty regarding consumer rights, platform obligations, and liability allocation in metaverse-based transactions.
2	Transaction security standards	The establishment of mandatory security standards tailored to metaverse transactions is essential. These standards should include transaction verification mechanisms, regular smart contract audits, cybersecurity risk assessments, and enhanced user authentication protocols. Several high-profile incidents of smart contract exploits and hacked digital wallets demonstrate that the absence of standardized security obligations exposes consumers to significant financial loss. Clear regulatory requirements would help ensure that platform providers implement adequate safeguards and consumer compensation mechanisms.
3	Cross-jurisdictional cooperation	Given the inherently global nature of the metaverse, effective consumer protection requires strengthened international cooperation. Cross-border fraud cases involving metaverse platforms have shown that national enforcement mechanisms alone are insufficient when perpetrators and infrastructure are located in multiple jurisdictions. Legal policy should therefore promote cooperation through mutual legal assistance, information sharing between regulators, and alignment with international best practices on digital consumer protection and cyber enforcement.

Based on these findings, this study recommends comprehensive regulatory reform combined with the implementation of specialized transaction security standards for metaverse environments. Furthermore, enhanced cross-jurisdictional cooperation is crucial to addressing legal uncertainty and enforcement challenges arising from transnational virtual transactions. By adopting these measures, consumer rights can be more effectively safeguarded, transaction risks minimized, and the overall security and sustainability of the metaverse ecosystem significantly strengthened.

Table 5. Comparative Analysis of International Practices in Consumer Protection and Transaction Security in the Metaverse

No	Jurisdiction Group	Key Legal Frameworks	Practices and Case Examples	Analytical Findings
1	European Union & United Kingdom	GDPR / UK GDPR; Digital Services Act (DSA); Digital Markets Act (DMA); Online Safety Act; Consumer Rights Act	Enforcement actions related to unauthorized tracking of avatar behavior, misuse of personal data, and disputes over virtual goods highlight strong data protection and platform accountability obligations. The DSA and Online Safety Act impose transparency, risk assessment, and due-diligence duties on large platforms operating virtual environments.	This group prioritizes data protection and platform responsibility as the foundation of consumer protection. However, regulation of virtual assets and smart contracts remains fragmented, and transaction security in metaverse environments is not governed by a dedicated legal regime.
2	United States	Federal Trade Commission Act; Computer Fraud and Abuse Act; State Consumer Protection Laws	Cases involving misleading NFT sales, virtual land fraud, and deceptive digital asset schemes are addressed through unfair or deceptive trade practice enforcement by the FTC, relying primarily on ex post remedies.	The U.S. adopts an enforcement-driven and sectoral approach, offering regulatory flexibility but limited ex ante legal certainty due to the absence of specific rules governing metaverse transactions, smart contracts, and platform security obligations.
3	Japan & South Korea	APPI (Japan); Financial Instruments and Exchange Act; Personal Information Protection Act (PIPA); National Metaverse Strategy	High-profile digital asset theft and data breach incidents prompted stricter cybersecurity requirements, mandatory security audits, and enhanced consumer disclosure obligations. South Korea has introduced a national policy roadmap specifically addressing metaverse governance.	These jurisdictions emphasize preventive regulation and technical standards, integrating data protection, cybersecurity, and platform governance. Nonetheless, the legal recognition of smart contracts and consumer remedies in immersive virtual environments remains underdeveloped.

These comparative findings indicate that international approaches to consumer protection in the metaverse generally emphasize three key dimensions: robust personal data protection, enhanced platform responsibility, and strengthened digital transaction security standards. Jurisdictions such as the European Union and South Korea adopt more proactive and preventive regulatory strategies, while the United States and the United Kingdom rely more heavily on enforcement mechanisms and general consumer law principles. Nevertheless, a common challenge across jurisdictions is the absence of a comprehensive legal framework specifically tailored to metaverse transactions, particularly regarding the legal status of virtual assets and smart contracts. These findings suggest that Indonesia may benefit from adopting a hybrid regulatory model that integrates strong data protection, explicit platform obligations, and dedicated transaction security standards, while remaining consistent with national legal principles.

An Analysis of Cyber Law's Authority in Protecting Metaverse Users

Indonesia's cyber legal authority, through the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), has normatively established a basic framework for user protection in digital transactions. These regulations provide legitimacy for law enforcement officials to prosecute cybercrimes such as online fraud, hacking, and misuse of personal data. Consistent with (Soekanto, 2019) findings, the existence of clear legal authority plays a crucial role in raising legal awareness and providing certainty for the digital community. However, in the context of the metaverse, this authority faces more

complex implementation challenges because the risks faced by users are no longer limited to conventional electronic transactions but also encompass high-value digital assets, automated smart contracts, and immersive cross-jurisdictional interactions (Fang et al., 2024).

From the perspective of regulators and law enforcement officials, the main implementation challenge lies in the limitations of generic regulations (T. Li et al., 2023). Research by (Aprilya, S., & Misbach, 2024) shows that digital regulations in Indonesia have not been designed to accommodate the unique characteristics of the metaverse, such as the execution of transactions without intermediaries through smart contracts and the use of intangible digital assets. As a result, law enforcement officials often struggle to determine the legal basis, responsible legal entities, and appropriate enforcement mechanisms. This is exacerbated by the lack of optimal technical capabilities, such as blockchain forensics and digital transaction tracking, which are crucial for handling disputes and crimes in virtual environments (Lazaroiu et al., 2024).

From a consumer perspective, the challenges of implementing cyber law are also related to low legal and technological literacy in understanding the risks of transactions in the metaverse. As (Rizal, 2021) noted, existing personal data protection systems still do not fully cover new types of data emerging in virtual environments, such as biometric data, avatar identities, and immersive interaction histories. This situation increases consumers' vulnerability to identity theft, avatar manipulation, and misuse of digital assets. Furthermore, metaverse platform operators face a dilemma between technological innovation and legal compliance, as the lack of clear regulatory standards potentially raises the risk of legal liability in the event of security breaches or consumer disputes (W. Zheng et al., 2023).

To address these limitations, legal solutions need to be combined with technological solutions. From a legal perspective, as suggested by (Nakamoto, 2020), specific regulations are needed that recognize smart contracts as legal instruments and define the responsibilities of platform operators and code developers (Han et al., 2023). From a technological perspective, the implementation of smart contract audits, digital identity verification mechanisms, blockchain-based traceability systems, and metaverse-specific cybersecurity standards can serve as preventative instruments that support effective law enforcement. This approach demonstrates that consumer protection in the metaverse cannot rely solely on a repressive approach but must be preventative and based on system design (security and compliance by design) (Pandey & Gilmour, 2024).

Furthermore, the effectiveness of cyber law enforcement is also significantly influenced by the perspectives and involvement of cross-border stakeholders. Kimotho (2022) emphasized that the anonymity and cross-jurisdictional nature of virtual transactions are global challenges that cannot be resolved unilaterally. The European Union's experience in implementing GDPR principles demonstrates that a combination of strict regulation, digital platform obligations, and cross-jurisdictional cooperation can enhance digital consumer protection (Zhang, 2022). By adopting these best international practices and adapting them to the national context, Indonesia can develop a more adaptive and holistic cyber law enforcement. This approach not only strengthens legal certainty but also builds public trust and creates a safe, transparent, and sustainable metaverse ecosystem (Sihare & Khang, 2023).

Evaluation of the Effectiveness of Existing Regulations in Providing Transaction Security Guarantees

An evaluation of existing regulations shows that the Electronic Information and Transactions Law (ITE Law) and the Consumer Protection Law provide a strong normative foundation for protecting consumers in conventional digital transactions (Khaliq & Manda, 2023). These regulations address consumer rights to security, information transparency, and

complaint and redress mechanisms. Consistent with (Rahman, 2021) findings, these provisions are relatively effective when applied to electronic transactions that are linear in nature and easily identifiable by the parties. However, this effectiveness decreases significantly when the same regulations are applied to the immersive, decentralized metaverse ecosystem, involving intangible digital assets and automatically executed smart contracts, creating implementation challenges not fully addressed by existing regulations (Doe et al., 2023).

From the perspective of consumers and regulators, the main implementation challenge lies in the lack of specific regulations regarding digital assets, NFTs, and smart contracts. (Nakamoto, 2020) research confirms that while smart contracts improve transaction efficiency and speed, their self-executing and code-based nature creates new legal risks, particularly when programming errors, system bugs, or manipulation by certain parties occur. In the Indonesian context, the lack of clarity regarding the legal entity responsible—whether the code developer, the platform provider, or the user—makes it difficult for consumers to effectively seek legal protection. This indicates that existing regulations have not been able to bridge the gap between technological innovation and legal certainty, necessitating specific regulations that integrate contractual legal aspects with the technical characteristics of smart contracts (Gai et al., 2023).

Furthermore, regulatory effectiveness is also influenced by differences in security standards implemented by metaverse platform operators. (Kimotho, 2022) points out that disparities in security systems—from encryption and digital identity verification to blockchain-based asset protection—lead to varying levels of risk for consumers. From the perspective of platform operators, the lack of clear technical standards creates uncertainty regarding legal compliance, while for consumers, this situation complicates transaction risk assessment (Cui, 2022). Therefore, legal solutions need to be complemented by technological solutions, such as establishing minimum security standards, mandating smart contract audits, implementing blockchain-based traceability systems, and proportional digital identity verification mechanisms, to strengthen the effectiveness of preventative consumer protection (Dubey et al., 2023).

In the context of consumer protection, the Consumer Protection Law (UU PPA) normatively guarantees the right to security and compensation, but its implementation in the metaverse faces serious obstacles. (Aprilya, S., & Misbach, 2024) highlight that the cross-jurisdictional, intangible asset-based, and automated nature of transactions complicates proving losses and enforcing legal liability. Law enforcement officials also point to limited technical capacity in conducting blockchain audits, digital forensics, and monitoring virtual transactions (Sutanto, 2022). This situation emphasizes that regulatory effectiveness is determined not only by legal norms but also by institutional readiness, technological literacy of officials, and inter-agency synergy in overseeing digital transactions in the metaverse (S. Wang & Wang, 2023).

International experience, particularly from the European Union, demonstrates that regulatory effectiveness can be enhanced through an adaptive approach that combines law and technology. The implementation of the GDPR and the digital asset regulatory framework in Europe establish data protection standards, security audits, and digital dispute resolution mechanisms that are more responsive to new technologies (European Digital Rights, 2021). This model is relevant for Indonesia as a reference in strengthening metaverse regulation, particularly in establishing transaction security standards, digital-based dispute resolution mechanisms, and cross-jurisdictional cooperation (Oh et al., 2023). By integrating regulatory updates, strengthening technical capacity, and adopting international best practices, the effectiveness of national regulations can be enhanced, thereby ensuring transaction security

and more comprehensive consumer protection in the metaverse ecosystem (Casale-Brunet et al., 2023).

Identifying Legal Challenges Emerging from the Unique Characteristics of the Metaverse

The cross-jurisdictional nature of the metaverse poses a major implementation challenge to consumer protection, as transactions can involve users, platform providers, technology developers, and server infrastructure located in multiple countries simultaneously. (Kimotho, 2022) emphasized that differences in legal systems and consumer protection standards across countries create legal uncertainty in enforcing responsibilities and resolving disputes (Dong & Wang, 2023). From a regulator's perspective, this situation limits national oversight authority, while from a consumer perspective, it increases the risk of unclear rights and redress mechanisms. Therefore, in addition to harmonizing international regulations, technological solutions such as cross-border compliance tools, jurisdictional tagging, and blockchain-based platform-level dispute resolution systems need to be developed to support the effective implementation of cross-border laws (Singh et al., 2025).

Digital assets and smart contracts also pose serious challenges to consumer protection practices due to their automated nature, immutability, and often lack of legal correction mechanisms. (Nakamoto, 2020) points out that coding errors or manipulation in smart contracts can lead to consumer losses without clear redress. From the consumer perspective, this risk weakens their bargaining position, while from the perspective of businesses and platform developers, regulatory ambiguity creates uncertainty regarding legal compliance. Therefore, legal solutions in the form of legal recognition of smart contracts need to be integrated with technological solutions, such as mandatory smart contract audits, kill-switch mechanisms, and human-in-the-loop governance, so that consumer protection is not only normative but also operational (Mohamed & Faisal, 2024).

Data security and user privacy in the metaverse face more complex implementation challenges than conventional digital transactions, as the data processed includes biometrics, virtual behavior, and immersive interactions. (Aprilya, S., & Misbach, 2024) emphasize that regulations such as the PDP Law and the ITE Law are not yet fully capable of addressing the dynamic and cross-platform nature of data (Rajawat et al., 2023). From a consumer perspective, the risk of data leakage and misuse increases, while for platform operators, implementing data protection standards often faces challenges such as cost and technical complexity. Therefore, in addition to strengthening regulations, technological solutions such as privacy-by-design, decentralized identity (DID), and zero-knowledge proofs are crucial to ensuring effective and practical data protection in the metaverse ecosystem (Xiao et al., 2023).

Implementation challenges also arise in the oversight and law enforcement of global metaverse platforms. (Sutanto, 2022) points out that limited technical capacity among law enforcement officials hinders the oversight of blockchain-based transactions, NFTs, and smart contracts. From a regulator's perspective, these limitations weaken the effectiveness of regulations, while for consumers, they reduce the level of actual legal protection. Therefore, the necessary solution is not only regulatory reform but also increased institutional capacity through technical training, the use of regulatory technology (RegTech), and collaboration between the government, digital platforms, and the technology community to create a transparent and real-time transaction monitoring system (Xiao et al., 2023).

Overall, previous research shows that legal challenges in the metaverse are multidimensional and cannot be resolved solely through conventional legal approaches. European Digital Rights (2021) emphasizes the importance of digital dispute resolution mechanisms that adapt to the nature of blockchain and virtual transactions. Therefore, strengthening consumer protection in the metaverse requires an integrated approach that combines regulatory reform, international harmonization, transaction security technology

solutions, and the active involvement of all stakeholders—regulators, businesses, technology developers, and consumers (Kliestik et al., 2024). With this approach, consumer protection is not merely reactive, but also preventive and sustainable, so that the metaverse can develop as a safe, transparent, and trustworthy digital economic ecosystem (Tao et al., 2023).

Drafting Legal Policy Recommendations to Strengthen Consumer Protection

Developing legal policy recommendations to strengthen consumer protection in the metaverse must begin with updating and expanding national regulations to align with the unique characteristics of virtual transactions. The Electronic Information and Transactions Law (ITE) and the Consumer Protection Law currently provide the legal foundation for electronic transactions, but they do not specifically regulate digital assets, smart contracts, and cross-platform and cross-jurisdictional transactions, which are key characteristics of the metaverse. (Kimotho, 2022) emphasized that general regulations tend to be difficult to implement effectively for complex new technologies. From a regulator's perspective, regulatory updates face challenges in cross-sector harmonization, while from the business perspective, there are concerns about the burden of compliance. Therefore, regulations need to be designed adaptively and risk-based, supported by technological solutions such as regulatory sandboxes and compliance-by-design to ensure they can be implemented realistically without stifling innovation (Xie et al., 2024).

Beyond normative aspects, establishing transaction security standards is a crucial implementation challenge in metaverse consumer protection. These standards encompass digital identity verification, smart contract audits, and the protection of users' personal and biometric data. (Aprilya, S., & Misbach, 2024) emphasize the importance of collaboration between regulators, platform providers, and technology developers in formulating consistent and applicable standards across platforms. From a consumer perspective, clear standards enhance security, while for platforms, they serve as operational technical guidelines (Chatterjee et al., 2024). Technological solutions such as smart contract auditing tools, multi-factor authentication, and privacy-by-design architecture need to be integrated with legal obligations so that consumer protection is not merely declarative but also operational and measurable (X. Ren et al., 2024).

Cross-jurisdictional collaboration is an integral policy recommendation of the global nature of the metaverse. European Digital Rights (2021) points out that without international cooperation, law enforcement of cross-border transactions will face serious obstacles, both in determining jurisdiction and executing judgments. From a state perspective, this cooperation requires preparedness in legal diplomacy and harmonization of standards, while for consumers, cross-jurisdictional mechanisms provide greater certainty of protection. The implementation of this collaboration can be strengthened by technological solutions such as cross-border data sharing frameworks, blockchain-based evidence systems, and internationally recognized online dispute resolution (ODR) to support the effectiveness of global consumer protection (Chu, 2023).

Policy recommendations should also address the role of legal education and institutional capacity building, often overlooked implementation challenges. Soekanto (2019) emphasized that consumer legal literacy is an effective preventive tool in reducing the risk of fraud and abuse in digital transactions. From a consumer perspective, understanding rights, risks, and complaint mechanisms improves bargaining power, while for law enforcement officials, improving technical capacity is a key prerequisite for regulatory effectiveness. (Sutanto, 2022) points out that limited understanding of technologies such as blockchain and smart contracts hinders law enforcement. Therefore, legal policies need to be accompanied by technical training, the use of regulatory technology (RegTech), and strengthened cross-agency coordination to ensure optimal implementation of consumer protection (Zaman et al., 2023).

Overall, previous research indicates that legal policy recommendations for metaverse transactions must be holistic and multidimensional (Zahid et al., 2025). Regulatory reform, establishing security standards, international collaboration, consumer education, increasing the capacity of law enforcement, and developing digital dispute resolution mechanisms are interrelated and cannot stand alone (Zahid et al., 2025). European Digital Rights (2021) emphasizes that adaptive digital dispute resolution mechanisms, supported by blockchain technology and automated claims systems, can increase legal certainty and consumer confidence. By combining legal and technological solutions and involving all stakeholders—government, businesses, technology developers, and consumers—Indonesia can build an effective, adaptive, and sustainable metaverse consumer protection framework, in line with developments in the global digital economy (Balaji et al., 2023).

International Practices in Consumer Protection and Transaction Security in the Metaverse

International practice shows that consumer protection and transaction security in the metaverse tend to be developed through an adaptive and risk-based regulatory approach. The European Union, for example, has implemented the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) as the foundation for digital consumer protection, including in virtual ecosystems. Research by European Digital Rights (2021) shows that this approach is effective in increasing transparency, platform accountability, and consumer control over their personal data. However, implementation challenges arise when stringent regulations confront rapid technological innovation, leaving platform operators facing a high compliance burden, while regulators must continually adapt their oversight instruments. From a consumer perspective, these regulations enhance security, but from a business perspective, technological solutions such as automated compliance systems are needed to ensure efficient legal compliance without stifling innovation.

In the United States, the consumer protection approach in virtual spaces places greater emphasis on ex-post regulation and business actor responsibility through the principle of self-regulation and enforcement by agencies such as the Federal Trade Commission (FTC). (Kimotho, 2022) research notes that this model provides significant flexibility for metaverse platform innovation, but poses implementation challenges in the form of unequal consumer protection, particularly in the event of digital asset fraud or smart contract failure. From a regulator's perspective, this approach requires strong law enforcement capacity, while from a consumer perspective, there is a risk of delays in protection. To address this, technological solutions such as real-time transaction monitoring, smart contract auditing, and consumer redress automation are being developed to complement conventional legal instruments.

A comparative approach is also seen in Asian regions, such as Japan and South Korea, which have adopted a hybrid model of state regulation and industry collaboration. Research by (Aprilya, S., & Misbach, 2024) shows that governments in these countries are encouraging the development of technical standards for metaverse transaction security through collaboration with technology developers and industry players. Implementation challenges arise from cross-sector coordination and differing levels of technological readiness between platforms. From a business perspective, clear standards provide legal certainty, while for consumers, they increase protection against the risks of hacking and transaction manipulation. Technological solutions such as certification schemes, security-by-design frameworks, and interoperable identity systems are used to ensure consistent operationalization of legal standards.

Cross-jurisdictional issues are a major challenge in the international practice of metaverse consumer protection, as virtual transactions often involve entities from multiple countries with differing legal regimes. European Digital Rights (2021) asserts that without an international coordination mechanism, consumer protection will be fragmented and difficult

to enforce. From a state perspective, the implementation challenge lies in harmonizing laws and recognizing decisions across jurisdictions, while for consumers, this uncertainty increases the risk of losing their rights. Some international practices are beginning to integrate legal solutions in the form of multilateral agreements and technological solutions such as blockchain-based evidence systems and online dispute resolution (ODR) to support more effective and transparent cross-border law enforcement.

Overall, the comparative analysis shows that international practice emphasizes the importance of integrating adaptive regulation, stakeholder collaboration, and the use of technology as instruments for consumer protection in the metaverse. Previous research, such as (Kimotho, 2022) and European Digital Rights (2021), emphasizes that regulation alone is insufficient without the support of technical solutions that enable effective implementation. Lessons learned from the European Union, the United States, and Asia demonstrate that optimal consumer protection requires a balance between legal certainty, innovation flexibility, and technological security. These findings are relevant for Indonesia in formulating metaverse legal policies that are not only normative but also applicable, by simultaneously involving regulators, business actors, technology developers, and consumers to build a safe, fair, and sustainable virtual transaction ecosystem.

Conclusions

This study concludes that Indonesia's cyber legal framework, through the ITE Law, the Consumer Protection Law, and the Personal Data Protection Law, has provided a normative basis for protecting consumers from the risks of digital transactions in the metaverse, such as fraud, hacking, and data misuse. However, its effectiveness remains limited because it does not explicitly regulate the unique characteristics of the metaverse, including digital assets, smart contracts, user anonymity, and cross-jurisdictional transactions. Existing regulations have proven adequate for conventional digital transactions, but are unable to guarantee the security of virtual transactions that are automated, immersive, and global. Therefore, this study recommends priority short-term (1–2 years) measures in the form of issuing derivative regulations or technical guidelines that establish minimum standards for metaverse transaction security, smart contract audit obligations, and immersive data protection; medium-term (3–5 years) measures in the form of updating laws to regulate the legal status of digital assets, platform liability, and the establishment of a dedicated digital dispute resolution mechanism; and long-term (more than 5 years) measures in the form of harmonizing cross-jurisdictional regulations and adopting international best practices to address global-scale metaverse transactions. With this phased approach, supported by increased technical capacity of law enforcement officials and consumer legal education, the findings of this study can be realistically implemented to strengthen consumer protection, increase legal certainty, and build a safe, transparent, and sustainable metaverse transaction ecosystem in Indonesia.

Acknowledgement

The author expresses sincere gratitude to all individuals and institutions who contributed to the completion of this study. Appreciation is extended to legal scholars, digital technology experts, and consumer protection practitioners who provided valuable insights regarding transaction security in the metaverse. The author also thanks academic advisors and colleagues for their guidance and constructive feedback. It is hoped that this research contributes to strengthening consumer protection frameworks in the virtual world.

References

Aprilya, S., & Misbach, I. (2024). Good corporate governance in digital platforms: Strengthening consumer protection in automated transactions. *Journal of Digital Law and Governance*, *6(1)*, 45–62.

Balaji, A. C., K., P., & Anuradha, S. (2023). The Non-Fungible Token (NFT) Marketplace : Technological Innovation and Opportunities for Creators. *Indian Journal of Marketing*, *53*(8), 8. https://doi.org/10.17010/ijom/2023/v53/i8/172973

Bhattacharya, P., Obaidat, M. S., Savaliya, D., Sanghavi, S., Tanwar, S., & Sadaun, B. (2022). Metaverse assisted Telesurgery in Healthcare 5.0: An interplay of Blockchain and Explainable AI. *2022 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 1–5. https://doi.org/10.1109/CITS55221.2022.9832978

Casale-Brunet, S., Mattavelli, M., & Chiariglione, L. (2023). Exploring blockchain-based metaverses: Data collection and valuation of virtual lands using machine learning techniques. *Digital Business*, *3*(2), 100068. https://doi.org/10.1016/j.digbus.2023.100068

Chatterjee, P., Das, D., Rawat, D. B., Ghosh, U., Banerjee, S., & Al-Numay, M. S. (2024). Digital Twins and Blockchain Fusion for Security in Metaverse-Driven Consumer Supply Chains. *IEEE Transactions on Consumer Electronics*, *70*(3), 5688–5697. https://doi.org/10.1109/TCE.2024.3477297

Chu, C.-H. (2023). Deep resource allocation for a massively multiplayer online finance of tourism gamification in metaverse. *Information Technology & Tourism*, *25*(4), 565–583. https://doi.org/10.1007/s40558-023-00267-8

Cui, Y. (2022). A Cross-Chain Protocol based on Quantum Teleportation for Underlying Architecture of Metaverse. *2022 7th International Conference on Computer and Communication Systems (ICCCS)*, 508–512. https://doi.org/10.1109/ICCCS55155.2022.9845967

Doe, D. M., Li, J., Dusit, N., Gao, Z., Li, J., & Han, Z. (2023). Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse Through Diversified Incentive Mechanism Design. *IEEE Open Journal of the Computer Society*, *4*, 171–184. https://doi.org/10.1109/OJCS.2023.3260829

Dong, Y., & Wang, C. (2023). Copyright protection on NFT digital works in the Metaverse. *Security and Safety*, *2*, 2023013. https://doi.org/10.1051/sands/2023013

Dubey, A., Bhardwaj, N., Upadhyay, A., & Ramnani, R. (2023). AI for Immersive Metaverse Experience. *Proceedings of the 6th Joint International Conference on Data Science & Management of Data (10th ACM IKDD CODS and 28th COMAD)*, 316–319. https://doi.org/10.1145/3570991.3571045

Ersoy, M., & Gürfidan, R. (2023). Blockchain-based asset storage and service mechanism to metaverse universe: Metarepo. *Transactions on Emerging Telecommunications Technologies*, *34*(1). https://doi.org/10.1002/ett.4658

Fang, G., Sun, Y., Almutiq, M., Zhou, W., Zhao, Y., & Ren, Y. (2024). Distributed Medical Data Storage Mechanism Based on Proof of Retrievability and Vector Commitment for Metaverse Services. *IEEE Journal of Biomedical and Health Informatics*, *28*(11), 6298–6307. https://doi.org/10.1109/JBHI.2023.3272021

Gai, K., Wang, S., Zhao, H., She, Y., Zhang, Z., & Zhu, L. (2023). Blockchain-Based Multisignature Lock for UAC in Metaverse. *IEEE Transactions on Computational Social Systems*, *10*(5), 2201–2213. https://doi.org/10.1109/TCSS.2022.3226717

Guo, C., Dou, Y., Bai, T., Dai, X., Wang, C., & Wen, Y. (2023). ArtVerse: A Paradigm for Parallel Human–Machine Collaborative Painting Creation in Metaverses. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2200–2208.

https://doi.org/10.1109/TSMC.2022.3230406

Han, D., Ryu, J., Kim, S., Kim, S., & Yoo, H.-J. (2023). 2.7 MetaVRain: A 133mW Real-Time Hyper-Realistic 3D-NeRF Processor with 1D-2D Hybrid-Neural Engines for Metaverse on Mobile Devices. *2023 IEEE International Solid- State Circuits Conference (ISSCC)*, 50–52. https://doi.org/10.1109/ISSCC42615.2023.10067447

Huang, H., Zeng, X., Zhao, L., Qiu, C., Wu, H., & Fan, L. (2022). Fusion of Building Information Modeling and Blockchain for Metaverse: A Survey. *IEEE Open Journal of the Computer Society*, *3*, 195–207. https://doi.org/10.1109/OJCS.2022.3206494

Kaur, D., Singh, B., & Rani, S. (2023). *Cyber Security in the Metaverse* (pp. 418–435). https://doi.org/10.4018/978-1-6684-8851-5.ch023

Khaliq, L. N., & Manda, V. K. (2023). *Customer Experience in the Web 3.0 Era* (pp. 258–274). https://doi.org/10.4018/978-1-6684-7649-9.ch015

Kimotho, J. M. (2022). Legal risks of blockchain-based transactions and smart contracts in virtual environments. *International Journal of Law and Information Technology*, *30(3)*, 215–233.

Kliestik, T., Dragomir, R., Băluță, A. V., Grecu, I., Durana, P., Karabolevski, O. L., Kral, P., Balica, R., Suler, P., Bușu, O. V., Bugaj, M., Voinea, D.-V., Vrbka, J., Cocoșatu, M., Grupac, M., Pera, A., & Gajdosikova, D. (2024). Enterprise generative artificial intelligence technologies, Internet of Things and blockchain-based fintech management, and digital twin industrial metaverse in the cognitive algorithmic economy. *Oeconomia Copernicana*, *15*(4), 1183–1221. https://doi.org/10.24136/oc.3109

Kou, G., Yüksel, S., & Dinçer, H. (2023). A facial expression and expert recommendation fuzzy decision-making approach for sustainable business investments within the metaverse world. *Applied Soft Computing*, *148*, 110849. https://doi.org/10.1016/j.asoc.2023.110849

Lazaroiu, G., Gedeon, T., Rogalska, E., Valaskova, K., Nagy, M., Musa, H., Zvarikova, K., Poliak, M., Horak, J., Crețoiu, R. I., Krulicky, T., Ionescu, L., Popa, C., Hurloiu, L. R., Nistor, F., Avram, L. G., & Braga, V. (2024). Digital twin-based cyber-physical manufacturing systems, extended reality metaverse enterprise and production management algorithms, and Internet of Things financial and labor market technologies in generative artificial intelligence economics. *Oeconomia Copernicana*, *15*(3), 837–870. https://doi.org/10.24136/oc.3183

Li, R., Wang, Z., Fang, L., Peng, C., Wang, W., & Xiong, H. (2024). Efficient Blockchain-Assisted Distributed Identity-Based Signature Scheme for Integrating Consumer Electronics in Metaverse. *IEEE Transactions on Consumer Electronics*, *70*(1), 3770–3780. https://doi.org/10.1109/TCE.2024.3372506

Li, T., Yang, C., Yang, Q., Lan, S., Zhou, S., Luo, X., Huang, H., & Zheng, Z. (2023). Metaopera: A Cross-Metaverse Interoperability Protocol. *IEEE Wireless Communications*, *30*(5), 136–143. https://doi.org/10.1109/MWC.011.2300042

Mohamed, A., & Faisal, R. (2024). Exploring metaverse-enabled innovation in banking: Leveraging NFTS, blockchain, and smart contracts for transformative business opportunities. *International Journal of Data and Network Science*, *8*(1), 35–44. https://doi.org/10.5267/j.ijdns.2023.10.020

Momtaz, P. P. (2022). Some Very Simple Economics of Web3 and the Metaverse. *FinTech*, *1*(3), 225–234. https://doi.org/10.3390/fintech1030018

Nakamoto, S. (2020). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.org.

Nakavachara, V., & Saengchote, K. (2022). Does unit of account affect willingness to pay? Evidence from metaverse LAND transactions. *Finance Research Letters*, *49*, 103089. https://doi.org/10.1016/j.frl.2022.103089

Oh, J., Kim, M., Park, Y., & Park, Y. (2023). A Secure Content Trading for Cross-Platform in the Metaverse With Blockchain and Searchable Encryption. *IEEE Access*, *11*, 120680–

120693. https://doi.org/10.1109/ACCESS.2023.3328232
Pandey, D., & Gilmour, P. (2024). Accounting meets metaverse: navigating the intersection between the real and virtual worlds. *Journal of Financial Reporting and Accounting*, *22*(2), 211–226. https://doi.org/10.1108/JFRA-03-2023-0157
Rafique, W., & Qadir, J. (2024). Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain. *Computer Science Review*, *54*, 100678. https://doi.org/10.1016/j.cosrev.2024.100678
Rahman, F. (2021). Perlindungan konsumen dalam transaksi elektronik di Indonesia: Evaluasi terhadap efektivitas Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Hukum & Pembangunan*, *51(2)*, 356–378.
Rajawat, A. S., Goyal, S. B., Solanki, R., Raboaca, M. S., Mihaltan, T. C., Illés, Z., & Verma, C. (2023). Blockchain-based Security Framework for Metaverse: A Decentralized Approach. *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 01–06. https://doi.org/10.1109/ECAI58194.2023.10193962
Ren, X., Du, H., Qiu, C., Luo, T., Liu, Z., Wang, X., & Niyato, D. (2024). Dual-Level Resource Provisioning and Heterogeneous Auction for Mobile Metaverse. *IEEE Transactions on Mobile Computing*, *23*(11), 10329–10343. https://doi.org/10.1109/TMC.2024.3377211
Ren, Y., Lv, Z., Xiong, N. N., & Wang, J. (2024). HCNCT: A Cross-chain Interaction Scheme for the Blockchain-based Metaverse. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *20*(7), 1–23. https://doi.org/10.1145/3594542
Rizal, M. (2021). Perlindungan data pribadi dalam perkembangan ekonomi digital di Indonesia. *Jurnal Hukum IUS QUIA IUSTUM*, *28(3)*, 567–589.
Sihare, S., & Khang, A. (2023). *Effects of Quantum Technology on the Metaverse* (pp. 174–203). https://doi.org/10.4018/978-1-6684-8851-5.ch009
Singh, A., Luthra, A., Garg, S., Pancholi, N., & Sharma, V. (2025). Banking transformation in PSU banks through the adoption of Metaverse: Indian context. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-024-02611-5
Soekanto, S. (2019). *Faktor-faktor yang mempengaruhi penegakan hukum*. RajaGrafindo Persada.
Sutanto, A. (2022). Penegakan hukum siber di Indonesia: Tantangan kapasitas teknis aparat dan pengawasan transaksi digital. *Jurnal Legislasi Indonesia*, *19(3)*, 421–440.
Tao, B., Dai, H.-N., Xie, H., & Wang, F. L. (2023). Structural Identity Representation Learning for Blockchain-Enabled Metaverse Based on Complex Network Analysis. *IEEE Transactions on Computational Social Systems*, *10*(5), 2214–2225. https://doi.org/10.1109/TCSS.2022.3233059
Vidal-Tomás, D. (2022). The new crypto niche: NFTs, play-to-earn, and metaverse tokens. *Finance Research Letters*, *47*, 102742. https://doi.org/10.1016/j.frl.2022.102742
Wang, F.-Y. (2022). The Metaverse of Mind: Perspectives on DeSci for DeEco and DeSoc. *IEEE/CAA Journal of Automatica Sinica*, *9*(12), 2043–2046. https://doi.org/10.1109/JAS.2022.106106
Wang, S., & Wang, W. (2023). A review of the application of digital identity in the Metaverse. *Security and Safety*, *2*, 2023009. https://doi.org/10.1051/sands/2023009
Wu, C.-H., & Liu, C.-Y. (2022). Educational Applications of Non-Fungible Token (NFT). *Sustainability*, *15*(1), 7. https://doi.org/10.3390/su15010007
Xiao, Y., Xu, L., Zhang, C., Zhu, L., & Zhang, Y. (2023). Blockchain-Empowered Privacy-Preserving Digital Object Trading in the Metaverse. *IEEE MultiMedia*, *30*(2), 81–90. https://doi.org/10.1109/MMUL.2023.3246528
Xie, T., Gai, K., Zhu, L., Wang, S., & Zhang, Z. (2024). RAC-Chain: An Asynchronous Consensus-based Cross-chain Approach to Scalable Blockchain for Metaverse. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *20*(7), 1–24.

https://doi.org/10.1145/3586011

Zahid, H., Zulfiqar, A., Adnan, M., Iqbal, M. S., Shah, A., Abbasi, U., & Mohamed, S. E. G. (2025). Transforming nano grids to smart grid 3.0: AI, digital twins, blockchain, and the metaverse revolutionizing the energy ecosystem. *Results in Engineering*, *27*, 105850. https://doi.org/10.1016/j.rineng.2025.105850

Zaman, S., Dantu, R., Badruddoja, S., Talapuru, S., & Upadhyay, K. (2023). Layerwise Interoperability in Metaverse: Key to Next-Generation Electronic Commerce. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 9–16. https://doi.org/10.1109/MetaCom57706.2023.00018

Zhang, L.-J. (2022). *MRA: Metaverse Reference Architecture* (pp. 102–120). https://doi.org/10.1007/978-3-030-96068-1_8

Zheng, W., Yan, L., Zhang, W., Ouyang, L., & Wen, D. (2023). D→K→I: Data-Knowledge-Driven Group Intelligence Framework for Smart Service in Education Metaverse. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2056–2061. https://doi.org/10.1109/TSMC.2022.3228849

Zheng, Z., Li, T., Li, B., Chai, X., Song, W., Chen, N., Zhou, Y., Lin, Y., & Li, R. (2022). *Industrial Metaverse: Connotation, Features, Technologies, Applications and Challenges* (pp. 239–263). https://doi.org/10.1007/978-981-19-9198-1_19