
Challenges to Contract Certainty and Dispute Resolution in the Digital Economy

Elsa Puspita Bunga Sari^{1*}, Agnesia Kurmaliasari², Rina Arum Prastyanti³

^{1,2,3}Duta Bangsa University, Jl. Bhayangkara No.55, Tipes, Kec. Serengan, Kota Surakarta, Jawa Tengah 57154, Indonesia

Keywords

Contract Certainty; Digital Economy; E-Commerce; Online Dispute Resolution (ODR); Legal Framework

***Correspondence Email:**

elsabunga594@gmail.com

Abstract

The rapid development of the digital economy has transformed traditional contract formation and dispute resolution processes, creating both opportunities and challenges for legal certainty. In online transactions, the absence of physical presence, cross-border interactions, and reliance on automated systems complicate the determination of valid consent, evidence authenticity, and jurisdiction. This paper aims to examine the challenges to achieving contract certainty and effective dispute resolution in digital commerce, focusing on how digitalization affects contractual obligations, enforcement mechanisms, and consumer protection. Using a qualitative normative legal research method, this study analyzes legal frameworks, scholarly literature, and case precedents concerning electronic contracts and online dispute resolution (ODR). The findings indicate that ambiguity in digital contract terms, lack of uniform international standards, and limited consumer awareness remain major barriers to legal certainty. Furthermore, while ODR platforms offer efficiency and accessibility, they still face issues regarding data integrity, fairness, and enforcement of decisions across jurisdictions. The study concludes that strengthening digital signature legislation, harmonizing cross-border e-commerce regulations, and integrating artificial intelligence into dispute management systems can enhance contractual reliability and fairness. Practically, this research implies that policymakers and technology providers must collaborate to establish transparent and interoperable digital legal infrastructures that balance innovation with legal accountability.

1. Introduction

The digital economy is rapidly changing the landscape of modern commerce, law, and social interaction. Digital platforms such as e-commerce marketplaces, virtual service providers, and the growing use of automated systems are reshaping the way agreements are made, documented, and enforced. While technological advancements offer significant benefits such as instant communication, broader accessibility, and streamlined business processes they also introduce complex legal challenges. These include uncertainty in contract formation, the verification of consent, and the proper protection of

consumer rights in the absence of physical interactions.

Compared to traditional methods, digital transactions are characterized by high speed and low barriers to entry, allowing individuals and businesses from around the globe to connect effortlessly (Cantemir et al., 2023). However, rapid development can outpace regulatory adaptation, leaving gaps that may jeopardize key legal principles such as certainty, justice, and equal protection. This paper explores such challenges by analyzing how digitalization affects core aspects of contract law, focusing on the ongoing efforts to establish clear obligations, ensure consent is genuine, and safeguard consumers in an ever-evolving digital environment.

1.1 Literature Review

1.1.1 Contract Formation in the Digital Age

- **Absence of Physical Presence**

Traditionally, contract formation relied on tangible elements: parties would meet in person, exchange paper documents, and sign agreements by hand. These processes provided clarity about the intentions of each party and created physical evidence of the transaction. In the digital context, most contracts are formed electronically using emails, online forms, mobile apps, or even algorithmic bots with participants often located in different countries or continents.

The absence of face-to-face interaction brings new questions about the authenticity of a party's identity and intent. For instance, digital transactions can be automated or handled by intermediaries, clouding the line between willful agreement and automated response (Tejomurti, 2025). This raises legitimate concerns on whether all parties genuinely understood and assented to the same contract terms. As highlighted in recent literature, doubts about participant identity and intent are especially prevalent in cross-border arrangements, where fraud and impersonation risks can be higher. In such scenarios, traditional, manual verification mechanisms are often insufficient, necessitating the adoption of robust digital identity checks and multi-factor authentication methods.

- **Validity and Authenticity**

The legal recognition of digital contract elements remains inconsistent across jurisdictions. Elements such as electronic signatures or digital certificates are legally binding in some countries but only valid in others if certain additional criteria are met such as government accreditation of the signature mechanism or third-party digital verification services. Complicating matters further, some regulatory systems still require a handwritten, or “wet,” signature for particular types of transactions (e.g., land sales or wills), contributing to greater uncertainty for international operators.

The lack of harmonized international standards means that businesses and individuals must navigate a confusing patchwork of requirements. For example, an agreement considered valid in

Indonesia may not be enforceable in the European Union or vice versa, if the appropriate digital protocols or accreditations are not met. This environment creates both legal and business risks, particularly in high-value, cross-jurisdictional transactions where the authenticity and enforceability of digital contracts are paramount.

- **Automated Contracts and Smart Contracts**

Emerging technologies such as smart contracts blockchain-based, self-executing digital contracts—embody both the promise and the challenge of digital contracting. Theoretically, smart contracts provide greater certainty by ensuring transactions execute automatically once coded criteria are satisfied, with no need for human intervention. This can reduce disputes by minimizing ambiguity: once the contract is on the blockchain, its code determines the outcome.

However, this automation comes at a price. The inherent rigidity of smart contracts means they can struggle to accommodate unforeseen circumstances such as force majeure, changes in regulatory environments, or simple human error. If one party needs to adjust or renegotiate terms, the coded contract may actually prevent adaptation even when fairness, market realities, or legal developments warrant a change. In short, the efficiency of smart contracts may sacrifice the flexibility and negotiation options present in traditional agreements, creating new avenues for disputes and requiring new forms of legal recourse. Addressing these challenges requires not just technological solutions, but thoughtful regulatory frameworks that combine predictability with sufficient adaptability (Mediawati et al., 2025).

1.1.2 Dispute Resolution Mechanisms

- **Online Dispute Resolution Systems**

Online Dispute Resolution (ODR) platforms have grown in popularity as effective solutions for settling disagreements that arise from digital transactions (Kurniawan et al., 2024). ODR includes a range of processes, from automated negotiation tools and digital mediation forums to full-fledged online arbitration systems. These platforms allow parties from any location to submit evidence, present arguments, and reach decisions quickly often at a fraction of the cost and time required for traditional court proceedings.

Despite these advantages, ODR brings its own set of challenges. Questions arise about the impartiality of digital mediators or arbitrators, the transparency of the dispute resolution process, and the reliability of the technology itself (Sulistianingsih et al., 2023). For example, technical issues such as software bugs or data corruption can undermine confidence in the platform's outcomes. Moreover, many users (especially those less familiar with legal or technological language) may find digital proceedings confusing or intimidating. Thus, ensuring accessibility and fairness within ODR systems remains a major focus of ongoing legal and technological reforms.

- **Jurisdictional Complexity**

A recurring issue in digital disputes is the confusion over applicable law and jurisdiction. When parties operate in different countries, it can be challenging to agree on which nation's law governs the contract or whether an ODR platform's decision is enforceable in the courts of either country. This can lead to situations where, despite a valid decision issued digitally, the losing party refuses to comply, knowing that legal remedies may be difficult to enforce across borders (Danesh et al., 2023).

Such complexity demands clear contract clauses specifying governing law and chosen dispute resolution methods (forum selection). However, with the fast-paced nature of online commerce, such clauses are often overlooked or buried in lengthy electronic terms and conditions. As a result, disputes frequently escalate with little hope of practical resolution, highlighting the vital need for clearer international norms and technical provisions that support cross-jurisdictional enforcement (OECD, 2024).

- **Data Security and Integrity**

Effective dispute resolution in the digital age relies heavily on the security and integrity of digital evidence. Digital documents, transaction logs, and communication records can all be manipulated, lost, or even fabricated if adequate controls are not in place. With cyber-attacks and data breaches on the rise globally, questions of data authenticity and tampering are at the forefront of any ODR process.

Technologies such as blockchain and digital signatures offer promising solutions: blockchain records are typically immutable and provide clear audit trails, while advanced digital signatures verify identities and document validity (Azizah et al., 2023). Nevertheless, challenges remain. Many countries lack robust legal frameworks or technical capacity to fully leverage these advances, and incompatibility between systems can create loopholes or "legal vacuums" where evidence or decisions lose their power. Building truly reliable systems for cross-border digital dispute resolution will require ongoing investment in infrastructure, regulation, and education for all parties involved (Rizkiana, 2021).

1.1.3 Consumer Protection Issues

- **Low Digital Literacy**

One of the most significant hurdles to effective consumer protection in the digital economy is low digital literacy among customers. Many users have not developed sufficient capability to understand the terms, risks, or even basic navigation of digital contracts, platforms, and online dispute processes. This limitation fosters greater susceptibility to fraud, manipulation, and exploitation especially in global transactions where cultural and legal norms diverge (Yulianti, 2025).

In practical terms, digital literacy entails much more than the ability to operate applications. It refers to a broader capacity: understanding how to verify information sources, differentiate authentic from deceptive online practices, and recognize legitimate contract consent mechanisms. As digital commerce becomes more complex, the gap between informed and uninformed consumers deepens, exposing less

literate individuals to unfair practices and making it harder for them to seek recourse or assert their rights (Keck et al., 2021).

Global consumer agencies, such as Indonesia's National Consumer Protection Agency (BPKN), have observed that the bulk of complaints in recent years stem from misunderstandings or lack of information about digital rights and procedures. Raising digital literacy through education, platform guidance, and public campaigns is now seen as a regulatory imperative not just a social responsibility.

- **Regulatory Gaps**

The fragmented nature of consumer protection laws at the international level has accentuated the risks for consumers in the digital economy (Safrida, 2023). Different jurisdictions impose varying requirements for digital contract validity, the recognition of e-signatures, consumer privacy protections, and available remedies for complaints. Businesses operating across borders often default to minimal regulatory standards, which may fall short of robust, consumer-friendly protections.

This situation is particularly worrisome when disputes arise. Enforcement of national consumer rules is often ineffective, especially if the seller or service provider is based in another country and does not maintain a legal presence or assets in the consumer's jurisdiction. Consequently, consumers can find themselves without clear pathways to obtain redress or compensation when their rights are violated.

Adaptive legal frameworks are needed to bridge these regulatory gaps. Policymakers and international organizations should strive for harmonization of basic standards such as transparency, fair business practices, and enforceable consumer rights while allowing flexibility for local contexts (Fawwaz & Mustomi, 2025).

- **Redress and Support Mechanisms**

Even when technological platforms offer online dispute resolution or helpdesk services, consumers with low digital literacy or limited experience frequently experience difficulties initiating claims or presenting evidence. Complex interface designs, legal jargon, and multi-step procedures can dissuade users from pursuing remedy for losses or grievances.

To rectify these challenges, user interface improvements, clear step-by-step support, and integrated education modules must be prioritized by platform operators and regulators (Gurung, 2025). Platforms should offer tutorials, warning systems, and simplified complaint mechanisms to empower consumers to engage actively and knowledgeably with their own protection options.

1.1.4 Legal Frameworks and Case Examples

- **National Regulation**

Governments worldwide are modernizing contract and commerce laws to adapt to digital transformation. Many have legally recognized digital evidence, electronic signatures, and automated

contracts, expanding opportunities for innovation and efficiency. However, the scope of these reforms varies widely. While some countries embrace blockchain and smart contracts, others hesitate due to uncertainties about enforceability, auditability, or risk management in these technologies

An example is Indonesia, which has initiated efforts to formally recognize electronic documents and digital identities. Despite these advancements, practical enforcement and oversight mechanisms especially for disputes involving foreign sellers or complex smart contracts are still developing. This highlights the need for a robust legal framework that can effectively address the challenges posed by digital commerce.

- **International Norms**

Cross-border digital commerce presents unique legal obstacles. Organizations such as the United Nations Commission on International Trade Law (UNCITRAL) and the Organisation for Economic Co-operation and Development (OECD) have taken steps toward developing harmonized standards for the validity, execution, and dispute resolution of digital contracts. However, consensus remains slow, and coverage is incomplete. This absence of overarching international norms forces businesses and consumers to navigate a “patchwork” of local rules and uncertainties, often resulting in confusion, inconsistent outcomes, and limitations on access to effective remedies.

For instance, the OECD addresses various aspects related to e-commerce, including consumer protection, privacy and data protection, and digital signatures. Its involvement in e-commerce issues started with the 1998 Action Plan for Electronic Commerce, structured around building trust for users and consumers, establishing ground rules for the digital marketplace, enhancing the information infrastructure for electronic commerce, and maximizing its benefits. Such issues have since been approached in OECD recommendations and guidelines

- **Indonesian Context**

In Indonesia, digitalization of commerce has yielded efficiency gains and widened economic participation, but has also introduced new risks: cyber attacks, privacy breaches, and uneven access to technology infrastructure. While national regulations now facilitate the use of smart contracts and blockchain-based verification (Noeri et al., 2025), they still lag behind in providing comprehensive dispute resolution procedures and specialized oversight agencies for digital commerce cases.

Experts highlight the need for targeted reforms, including stronger cybersecurity governance, greater public outreach about digital rights and risks (Berliana et al., 2025), and the establishment of dedicated channels for handling digital commerce disputes especially as the country accelerates its involvement in the global digital economy.

2. Research Methods

This study employs a normative legal research method, focusing on the analysis of legal norms,

doctrines, and regulatory frameworks governing digital contracts and consumer protection in the digital economy. The research adopts a qualitative and descriptive-analytical approach to examine the evolution of contract formation, dispute resolution mechanisms, and consumer protection challenges in digital transactions. The research utilizes a conceptual approach to analyze legal concepts related to electronic contracts, smart contracts, online dispute resolution, and digital consumer rights, as developed in scholarly literature. In addition, a statutory approach is applied to examine national and international legal instruments, including laws, regulations, and policy frameworks governing digital contracts, electronic signatures, and cross-border e-commerce.

To enrich the analysis, a comparative approach is employed by reviewing regulatory practices and legal standards across different jurisdictions, including Indonesia and selected international frameworks such as those developed by the OECD and UNCITRAL. This approach enables the identification of regulatory gaps, inconsistencies, and best practices relevant to digital contract enforcement and consumer protection. The legal materials used in this research consist of primary legal materials, including statutes, international guidelines, and official regulatory documents, as well as secondary legal materials, such as journal articles, books, policy reports, and previous studies related to digital contracts and online dispute resolution. Data collection is conducted through document-based research, and the collected materials are analyzed using qualitative legal analysis, involving interpretation, classification, and systematic comparison of legal norms. The results of the analysis are presented descriptively to formulate recommendations aimed at strengthening digital contract regulation, improving consumer protection mechanisms, and enhancing cross-border dispute resolution frameworks in the digital economy.

3. Result and Discussion

3.1 Digital Signature Laws

Policymakers must bolster both the legal status and technical reliability of digital signatures and certificates to efficiently authenticate online contracts and minimize fraud. Such reforms should clarify which forms of electronic identification are valid, standardized, and robust across platforms and jurisdictions. The Electronic Signatures in Global and National Commerce (E-Sign) Act in the United States serves as an example, allowing the use of electronic records to satisfy any statute, regulation, or rule of law requiring that such information be provided in writing, provided the consumer has affirmatively consented to such use and has not withdrawn such consent

3.2 Harmonization of Cross-Border E-Commerce Regulation

Building truly trustworthy and effective consumer protection requires international cooperation. Global organizations, national governments, and major platforms need to work together to formulate core standards for contract formation, consumer privacy, complaint procedures, and dispute resolution that apply consistently across borders (Shoukat et al., 2025). Regional agreements, model laws, or mutual recognition arrangements can help close regulatory gaps.

3.3 Integration of Artificial Intelligence

Artificial intelligence offers powerful new tools for resolving digital disputes. AI can assist with early identification of problematic transactions, triage cases for escalation, and even provide preliminary recommendations for settlement improving the speed and fairness of digital dispute processes. However, careful design, oversight, and human review must complement AI deployment to preserve transparency and equitable outcomes.

3.4 Capacity Building and Legal Education

Lasting progress in digital consumer protection will depend on long-term investment in education and professional capacity-building. Governments must expand digital literacy campaigns for the public, update law curricula to include digital contracts and technology regulations, and invest in ongoing training for legal professionals (Bouke et al., 2023). Platform operators share responsibility for providing accessible educational resources and practical support modules for users.

The International Institute for Sustainable Development (IISD) emphasizes the evolving nature of e-commerce due to technological developments and online business innovations, requiring better consumer protection frameworks and substantial investments in technical and institutional capacity building (Development, 2025)

4. Conclusion

The surge of the digital economy has fundamentally shifted the realities of consumer protection, contract law, and dispute resolution. Stakeholders ranging from regulators and platform developers to consumers themselves face unprecedented opportunities and genuine risks in a rapidly changing global marketplace. Addressing the inherent ambiguities, jurisdictional complexities, and gaps in consumer support requires proactive, sustained collaboration across all sectors. By strengthening legal frameworks, embracing innovative technologies, improving digital literacy, and harmonizing cross-border standards, society can build a digital marketplace that is more robust, equitable, and trustworthy. Only through collective effort will justice, transparency, and sustainable innovation thrive in the digital era.

5. References

- Azizah, Ilmiah, F., Hadiwinata, K., & Waeno, M. (2023). *DIGITALIZATION OF ALTERNATIVE DISPUTE RESOLUTION: REALIZING BUSINESS FAIR PRINCIPLES*. 23(2). <https://doi.org/10.20884/1.jdh.2023.23.2.3667>
- Berliana, D., Rotua, B., Dewantara, R., & Widyanti, Y. E. (2025). *Can Smart Contracts Have a Legality Valid in Indonesia?* 6(1), 895–911.
- Bouke, M. A., Alshatebi, S. H., Abdullah, A., Cengiz, K., & Atigh, H. El. (2023). *African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions*. 1–15.
- Cantemir, M., Pitic, A., & Bayraktar, D. (2023). *DRIVERS OF DIGITAL TRANSFORMATION AND THEIR IMPACT ON ORGANIZATIONAL MANAGEMENT*. 18(18), 149–170. <https://doi.org/10.2478/sbe-2023-0009>

- Danesh, P., Law, C., & Chamran, S. (2023). *The Future of Online Dispute Resolution: Legal Frameworks for Managing Digital Disputes in E-Commerce, Intellectual Property, and Consumer Protection*. 2(2), 37–48.
- Development, I. I. for S. (2025). *Consumer Protection and E Commerce* (Issue 1).
- Fawwaz, S. M., & Mustomi, O. (2025). *Legal Protection for Consumers in Electronic Transactions*. 06(01), 26–39.
- Gurung, S. (2025). SAFEGUARDING CONSUMERS IN THE DIGITAL AGE: THE ROLE OF ONLINE DISPUTE RESOLUTION IN RAPIDLY. *Indian Journal of Integrated Research in Law, IV(V)*, 1039–1047.
- Keck, M., Gillani, S., Dermish, A., Grossman, J., & Accelerator, P. (2021). The Role of Consumer Protection in the Digital Economy. In *Unlocking Public and Private Finance for the Poor*.
- Kurniawan, R., Putra, C., & Djajaputra, G. (2024). *Legal Remedies for Breach of Contract in Digital Service Agreements*. 5(2), 1000–1007.
- Mediawati, N. F., Kurniawan, F., Aulia, M. Z., Purwaningsih, S. B., Rosnawati, E., & Abadi, T. W. (2025). *Indonesian Journal of Law and Economics*. 20(4), 1–12.
- Noeri, I., Nur, S., & Hermendasari, R. (2025). *Regulatory Compliance of Indonesian Smart Contracts*. 1(1), 15–25.
- OECD. (2024). *OECD Online Dispute Resolution Framework*. 1–44.
- Rizkiana, R. E. (2021). *THE FUTURE OF ONLINE DISPUTE RESOLUTION: BUILDING A FRAMEWORK FOR E-COMMERCE DISPUTE RESOLUTION IN INDONESIA*. 1(2), 114–138.
- Safrida. (2023). *Dynamics Of Consumer Protection Law In The Digital Era: Case Study On E-Commerce In Indonesia*. 19, 49–59.
- Shoukat, D., Dar, M. H., Amjad, I., Zia, Q., Shah, U., Salman, F., & Nadeem, H. (2025). *AI-MEDIATION IN CROSS-BORDER E-COMMERCE: BRIDGING LAW, TECHNOLOGY AND ETHICS IN EU REGULATORY FRAMEWORKS*. 3(6).
- Sulistianingsih, D., Anggita, A., Lembang, R., & Adhi, Y. P. (2023). Online dispute resolution: Does the system actually enhance the mediation framework? Online dispute resolution: Does the system actually enhance the mediation framework? *Cogent Social Sciences*. 9(1).
<https://doi.org/10.1080/23311886.2023.2206348>
- Tejomurti, K. (2025). *Legal Challenges and Reform Proposals for Algorithmic Contracts under Indonesia's Information and Electronic Transactions Law*. 7(02), 559–582.
- Yulianti, Y. (2025). *Gudang Jurnal Multidisiplin Ilmu Consumer Protection in Live Streaming-Based Commercial Transactions*. 3(2022), 124–130.