DIGITAL CONTRACTS AND ITS LEGAL VALIDITY IN INTERNATIONAL TRADE: AN ANALYSIS

- Ramsha Haque*

Abstract

This paper delves into the legal validity of digital contracts within the framework of international trade, presenting a comparative analysis of the legislative environments in India, the United States, the United Kingdom, and the European Union. As businesses increasingly adopt digital platforms for their transactions, understanding the legal recognition and enforceability of electronic agreements becomes paramount. The study scrutinises pivotal regulations, including the Indian Contract Act, the Electronic Signatures in Global and National Commerce Act (ESIGN), the Uniform Electronic Transactions Act (UETA), and the EU's Data Act. It explores the ramifications of electronic signatures and smart contracts, addressing the complexities introduced by technological advancements, such as discrepancies in interpretation and potential liability concerns. Furthermore, this analysis evaluates the strengths and limitations of existing legal frameworks, identifying best practices and areas that require enhancement. By emphasising the importance of harmonisation and adaptability in legal approaches, the findings contribute to the development of a more coherent and effective international legal environment for digital transactions. This work ultimately aims to facilitate smoother cross-border trade in an increasingly digital economy, providing valuable insights for policymakers, legal practitioners, and businesses navigating this evolving landscape.

Keywords: *Digital Contracts, Comparative Analysis, Electronic Signature, Cross- Border Trade, Digital Economy.*

* LL.M. Student @ West Bengal National University of Juridical Sciences, Kolkata

INTRODUCTION

Just as vending machines have supplanted human vendors, smart contracts possess the potential to render intermediaries obsolete across various sectors, as articulated by Nick Szabo.[1] An American computer scientist and the creator of the digital currency Bit Gold, Szabo defined "smart contracts" in 1998 as "computerised transaction protocols that execute the terms of a contract."[2] Smart contracts are digital agreements capable of autonomous execution, enabling parties to transfer digital and physical assets, or any item of value, between themselves in a transparent and conflict-free manner[3]. They implement the necessary logic to deliver complex services in response to customer demands, encompassing functions such as state management, governance enforcement, and identity verification. Furthermore, smart contracts facilitate the storage and retrieval of data from blockchain systems without requiring extensive searches; instead, they provide a computational interface to access the underlying blockchain storage structures[4].

A smart contract can be said to be a set of computer code that autonomously executes all or part of an agreement stored on a blockchain platform. It exists along a continuum, ranging from fully encoded digital agreements to the automated execution of traditional paper contracts. These contracts are designed to minimise the transaction costs effectively. Thus, breaching the agreement is both challenging and costly for the involved parties. As a result, there is a growing interest among businesses in utilizing smart contracts to enhance efficiency in international trade. Many experts have started to examine the potential of smart contracts to reduce transaction costs in this domain. Ramesh Gopinath, IBM's Vice President of Blockchain Solutions, has pointed out the inefficiencies inherent in the current supply chain system, which relies heavily on the physical movement of a multitude of paper documents for shipping transactions.[5] He emphasises that this system is particularly vulnerable to fraud, human error, and inadvertent delays. Wolfgang Lehmacher, Head of Supply Chain and Transport Industries at the World

[1] Tharika Dishani Lamappulage Donn, "Smart Contracts and International Trade: European Legal Strategies for Managing Challenges", 1 (4) *Journal of Digital Technologies and Law* 1042-1057 (2023), *available at*: https://doi.org/10.21202/jdtl.2023.41 (last visited on: 28.12.2024)

[2] *Ibid.*

[3] IBM, "What are smart contracts on blockchain?" *available at*: https://www.ibm.com/topics/smart-contracts (last visited on: 08.01.2025)

[4] Nanayakkara, Samudaya, Srinath Perera, Sepani Senaratne, Geeganage Thilini Weerasuriya, & Herath Mudiyanselage Nelanga Dilum Bandara, "Blockchain and Smart Contracts: A Solution for Payment Issues in Construction Supply Chains" 8 (2) *Informatics* 36, *available at*: https://doi.org/10.3390/informatics8020036

[5] Anna Duke, "What Does the CISG Have to Say About Smart Contracts? A Legal Analysis", 20 (1) *Chicago Journal of International Law* 141 (2019), *available at*: https://chicagounbound.uchicago.edu/cjil/vol20/iss1/4 (28.12.2024)

Economic Forum, had viewed blockchain technology and smart contracts as solutions to these transaction costs, offering the promise of more straightforward and transparent payments and collaborations among traders.[6] Additionally, Emmanuelle Ganne, a former advisor to the Director General of the World Trade Organization, has published a report outlining the revolutionary potential of blockchain and smart contracts in reshaping international trade.[7]

Despite all the buzz surrounding the advantages of blockchain and cross-border smart contracts, it is essential to recognize that some of this enthusiasm may be driven by hype from an increasing number of startups in the blockchain sector. As noted by industry insiders, realising the full benefits of smart contracts in international trade will require considerable time, given the entrenched nature of existing financial infrastructures and the difficulty in achieving cooperation among competing institutions. Nevertheless, the legal and business sectors have begun to engage with this discourse, seeking to capitalise on its potential. For example, IBM and Maersk have made joint investments aimed at integrating blockchain technology into the shipping industry[8]; however, they face challenges in securing participation from carriers, many of whom remain hesitant due to the unprecedented nature of the blockchain initiative. Furthermore, Legal Zoom has partnered with a blockchain firm to implement smart contracts in the creation of legal documents encompassing a range of products, from wills and trusts to trademarks and copyrights. However, the application of smart contracts in business agreements has raised some critical questions regarding their legal validity, which remain largely unanswered in existing case law and relevant international legal texts. The diversity of smart contracts necessitates an exploration of their various forms; at one end of the spectrum, a smart contract may encompass all contractual terms in coded form, functioning as a complete agreement in execution. Conversely, on the other hand, a smart contract may simply automate basic actions, such as payment, in conjunction with an associated traditional contract. Given the broad range of smart contract configurations, the determination of when a smart contract becomes legally binding is often contingent upon the applicable legal framework and the specific circumstances surrounding each case.

DIGITALIZATION OF CONTRACTS IN INTERNATIONAL TRADE

[6] Wolfgang Lehmacher, "Why blockchain should be global trade's next portal of call", World Economic Forum, *available at*: https://www.weforum.org/stories/2017/05/blockchain-ports-global-trades/ (last visited on: 28.12.2024)

[7] *Supra* note 5.

[8] *Supra* note 5.

On average, a cross-border transaction necessitates the exchange of 36 documents and 240 copies. For example, a shipment of roses from Kenya to Rotterdam can generate a stack of paperwork measuring 25 cm in height, with the associated handling costs often exceeding those of transporting the containers themselves. According to Maersk (Maersk is a Danish shipping and logistics company that offers supply chain and logistics services for businesses of all sizes), the cost of processing trade documents can account for up to 20 percent of the physical transportation expenses for a shipment.[9]

The COVID-19 pandemic has underscored the vulnerabilities of supply chains that rely on physical documentation.[10] Lockdowns, health protocols, and teleworking measures significantly affected the ability of traders to import and export goods within traditional paper-based systems.[11] Furthermore, paper documents are prone to forgery, and while trust services that ensure the authenticity and integrity of these documents as notary services exist, they often lack time and cost efficiency[12]. Transitioning from paper to digital formats offers numerous advantages. Firstly, it significantly reduces processing times and enables companies to leverage data more effectively. Artificial intelligence can be employed to automatically detect faulty patterns and fight trade-based money laundering. Additionally, the pandemic has highlighted the health benefits of digitalisation, which minimizes physical contact among stakeholders. Moreover, digital systems allow supply chain participants to access consistent and real-time information. Technologies such as blockchain and distributed ledger technology (DLT) ensure the integrity and authenticity of data exchanged on these platforms, thereby enhancing trust among supply chain stakeholders and addressing the double-spending problem that has contributed to various fraud scandals.[13] To foster the global adoption of electronic transactions and documents in international trade, governments have a critical role in developing comprehensive legal frameworks that explicitly recognise the validity and enforceability of these

[9] WTO, *The promise of TradeTech*, 28-39 (World Trade Organisation, February 2022), *available at*: https://doi.org/10.30875/9789287071026c005 (last visited on: 28.12.2024)

[10] Suriyan Jomthanachai, Wai-Peng Wong, Kend-Lin Soh & Chee-Peng Lim, "A global trade supply chain vulnerability in COVID-19 pandemic: An assessment metric of risk and resilience-based efficiency of CoDEA method" 93 Research in Transportation Economics (2022), *available at*: https://doi.org/10.1016/j.retrec.2021.101166 (last visited on: 08.01.2025)

[11] Enrico Battisti, Simona Alfiero & Erasmia Leonidou, "Remote working and digital transformation during the COVID-19 pandemic: Economic–financial impacts and psychological drivers for employees" 150 *Journal of Business Research* 38-50 (2022), *available at*: https://doi.org/10.1016/j.jbusres.2022.06.010 (last visited on: 08.01.2025)

[12] *Supra* note 9, *available at*: https://www.wto.org/english/res_e/booksp_e/tradtechpolicyharddigit0422_e.pdf (last visited on: 28.12.2024)

[13] Scott Nevil, "Distributed Ledger Technology (DLT): Definition and How It Works", *available at*: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp (last visited on: 28.12.2024)

digital mechanisms within their jurisdictions[14]. Establishing such frameworks is essential for ensuring that electronic transactions are treated with the same legal standing as traditional paper-based transactions. This recognition is vital for businesses and individuals engaged in electronic commerce, as it provides them with the assurance that their digital agreements and documents can be legally upheld. Key elements of these legal frameworks should include specific provisions for electronic transferable documents and trust services, such as electronic signatures. Electronic transferable documents facilitate the exchange of ownership and rights in a digital format, which is crucial for streamlining transactions and enhancing efficiency in trade. Trust services, including e-signatures, provide a means to authenticate and verify the identity of parties involved in electronic transactions, thereby enhancing security and trust in digital interactions. By incorporating these provisions, governments can create a more enabling environment for electronic trade, encouraging businesses to adopt digital solutions.

Moreover, it is imperative that these legal frameworks align with international standards. Doing so will facilitate cross-border recognition and utilisation of electronic transactions and documents, allowing businesses to operate seamlessly across different jurisdictions. This alignment helps mitigate legal uncertainties that can arise when dealing with electronic transactions in various countries, ultimately promoting confidence among international trading partners. For instance, aligning national laws with standards set by international organisations, such as the United Nations Commission on International Trade Law (UNCITRAL) or the International Organization for Standardization (ISO), can provide a consistent legal foundation that supports the growth of global electronic commerce[15]. In addition to legal recognition, governments must take a coordinated approach to address the legal implications of various algorithms and technologies increasingly utilised alongside TradeTech. The rapid advancement of technology, including artificial intelligence and blockchain, introduces new complexities in legal interpretation and regulation.[16] Without a cohesive strategy, there is a risk of regulatory fragmentation, where different jurisdictions may adopt conflicting regulations that could hinder the effectiveness and efficiency of electronic transactions. By proactively engaging with stakeholders, including businesses, technologists, and legal experts, governments can develop a

[14] Liliyana Daza Jaller, Simon Gaillard & Martin Molinuevo, *The Regulation of Digital Trade: Key Policies and International Trends"* (World Bank Group, 2021)," *available at*: https://documents1.worldbank.org/curated/en/998881578289921641/pdf/The-Regulation-of-Digital-Trade-Key-Policies-and-International-Trends.pdf (last visited on: 28.12.2024)

[15] United Nations, "United Nations Commission on International Trade Law", UNCITRAL, available at: https://uncitral.un.org/ (last visited on: 08.01.2025)

[16] The World Bank, "Transformative technologies (AI) challenges and principles of regulation", *available at:* https://digitalregulation.org/3004297-2/(last visited on: 09.01.2025)

unified regulatory framework that supports innovation while protecting the interests of all parties involved. Furthermore, it is essential for governments to foster collaboration between public and private sectors in the development and implementation of these frameworks. Engaging industry stakeholders in the legislative process can provide valuable insights into the practical challenges and opportunities associated with electronic transactions. This collaborative approach can lead to more effective regulations that not only enhance legal certainty but also promote innovation and competitiveness in the digital economy.

In summary, to promote the global adoption of electronic transactions and documents in international trade, governments must develop robust legal frameworks that recognise and validate these digital mechanisms. By ensuring alignment with international standards, addressing technological implications, and fostering public-private collaboration, governments can create a conducive environment for electronic commerce. This comprehensive strategy will ultimately enhance the efficiency and security of international trade, benefiting businesses and consumers alike in the increasingly interconnected digital marketplace.

INTERNATIONAL PERSPECTIVE

1. UK

The Thirteenth Programme of Law Reform directed the Law Commission to conduct research and analysis on smart legal contracts at the request of the Lord Chancellor[17]. In November 2019, the UK Jurisdiction Taskforce (UKJT) published a legal statement addressing crypto assets and smart contracts, establishing that these contracts can create legally binding obligations.[18] Following this, the Ministry of Justice placed an order to the Law Commission to undertake a comprehensive review of the existing legal framework surrounding smart legal contracts. In response, the commission has sought to clarify ambiguities and identify deficiencies in current legislation while assessing the need for further research, both immediate and future[19]. In instances of contractual disputes, courts will refer to a specific publication that offers guidance on interpreting the contracts in question. This publication advises that courts evaluate the meaning of the programming language from the perspective of a reasonable programmer, considering all relevant contextual information available to the parties at the time the contract was created. The Law Commission emphasised the necessity of interpreting smart contracts,

[17] Lord Chancellor and Secretary of State for Justice, "Smart legal contracts (Advice to Government), Law Commission 2021", *available at:* https://lawcom.gov.uk/project/smart-contracts/ (last visited on: 09.01.2025)
[18] *Supra* note 1.
[19] *Supra* note 17.

even those composed entirely in code, due to the potential difference between the intended meaning of the code and its actual execution. This distinction highlights the difference between the semantic interpretation of the code and its practical implementation, which may lead to interpretive challenges.

The Law Commission recommends adopting a modified version of conventional interpretive tests, wherein the understanding of coded terms is informed by the expertise of individuals knowledgeable in the relevant field. This approach aligns with established methods of contract interpretation. The significance of legal certainty in this context cannot be exaggerated. English law is recognised as capable of accommodating smart contracts, providing assurance to parties engaged in computerised global trade agreements governed by English law. Furthermore, the Law Commission's report identifies key considerations for contracting parties, particularly those operating within the realm of Decentralized Finance.[20]

2. EU

On March 14, 2023, the European Parliament adopted legislation regarding smart contracts and the Internet of Things as part of the Data Act[21]. This legislation received broad support, passing with 500 votes in favour and only 23 against, with the aim of fostering innovative business models that can lead to the development of new industries and job opportunities[22]. Article 30 of the Data Act outlines essential requirements for smart contracts related to data sharing[23]. The successful implementation of the Data Act requires the development of mechanisms to halt ongoing transactions effectively. These mechanisms might include internal features that allow for the resetting or termination of a smart contract. It is crucial to clearly define the conditions under which a smart contract should be reset or terminated. In the field of information technology, the "kill switch" mechanism is often employed to disable a device, network, or software in response to security threats. In the context of smart contracts, a kill switch can either

[20] *Supra* note 1.

[21] European Parliament, "Proposal for a regulation of the European Parliament and of the Council on harmoised rules on fair access to and use of data (Data Act)", *available at:* https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.html#:~:text=It%20imposes%20the%20obligation%20on,and%20in%20a%20transparent%20manner (last visited on: 09.01.2025)

[22] Assad Jafri, "EU Passes Data Act including Smart Contract Regulation", CryptoSlate, *available at*: https://cryptoslate.com/eu-passes-data-act-including-smart-contract-regulation/(last visited on: 09.01.2025)

[23] European Union Cybersecurity Agency, "Draft Article 30 of the Data Act: Implications for DLT and Smart Contracts in the EU", *available at*: https://eu.ci/data-act-position-paper-euci/ (last visited on: 09.01.2025)

terminate the contract or trigger a pause, repair, and subsequent reissue of the contract in the event of a significant vulnerability or breach[24].

The Data Act is a pivotal initiative aimed at improving data accessibility in line with EU principles and regulations. It is a fundamental element of the European data strategy, contributing significantly to the digital transformation goals outlined in the Digital Decade initiative. Compliance with the essential requirements will be evaluated by the smart contract provider, who will be responsible for issuing a declaration of conformity and ensuring adherence to the necessary standards. However, the term "responsible" remains ambiguous in this context, raising questions about whether users of the smart contract could face civil liability. If a supplier fails to provide a compliant smart contract, the consequences will be determined according to the laws of the relevant EU member state.

3. USA

In the United States, two key regulations govern the use of electronic contracts in e-commerce and digital transactions:

1. **The Electronic Signatures in Global and National Commerce Act (ESIGN)**: Enacted by the U.S. Congress in June 2000, the ESIGN Act was made to facilitate and validate electronic transactions by establishing the legal status of electronic signatures and records[25]. This legislation specifically addresses both the interstate and the international contexts, ensuring that electronic signatures are recognised as having the same legal authority as traditional handwritten signatures. By doing so, the ESIGN Act promotes confidence in electronic commerce, allowing businesses and consumers to enter into binding agreements without the need for physical documentation. This federal statute not only underscores the importance of technological advancements in commerce but also aims to enhance the efficiency of transactions in an increasingly digital marketplace.
2. **The Uniform Electronic Transactions Act (UETA)**: The UETA serves as a complementary framework to the ESIGN Act, providing a comprehensive legal structure

[24] Fabio Bassan & Maddalena Rabitti, "From smart legal contracts to contracts on blockchain: An empirical investigation", 55 *Computer Law & Security Review* 106035 (2024), *available at*: https://doi.org/10.1016/j.clsr.2024.106035 (last visited on: 09.01.2025)

[25] Federal Deposit Insurance Corporation Consumer Compliance Examination Manual - January 2014: X-3.1, "Electronic Signatures in Global and National Commerce act (E- Sign Act)", *available at:* https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf (last visited on: 09.01.2025)

for electronic transactions across the United States. Developed by the National Conference of Commissioners on Uniform State Laws in 1999, the UETA seeks to standardise the use of electronic signatures and records in various contexts, including governmental and commercial transactions. This act affirms that electronic records and signatures hold the same legal validity as their paper-based counterparts, thereby simplifying the process for parties engaged in electronic dealings. The widespread adoption of UETA by most U.S. states marks a pivotal development in establishing a cohesive legal environment for electronic transactions, paving the way for enhanced interoperability and consistency in the enforcement of electronic contracts[26].

Together, these regulations reflect the United States' commitment to embracing digital innovation in commerce while ensuring that legal frameworks evolve to meet the demands of a rapidly changing economic landscape. By facilitating electronic transactions, the ESIGN Act and UETA foster a more efficient and accessible marketplace, enabling businesses and consumers alike to engage in seamless, legally binding agreements in an increasingly digital world.[27]

4. INDIA'S PERSPECTIVE

In India, the framework governing all agreements and contracts, including electronic contracts, is primarily outlined in the Indian Contract Act of 1872.[28] This Act establishes the legal foundation for contractual relationships in the country by defining what constitutes a valid contract and setting forth the essential elements required for enforceability under the law. A contract is fundamentally defined as an agreement that can be enforced by law, meaning that the parties involved have legal recourse in the event of a breach.[29] Section 10 of the Act enumerates the essential requirements for a contract to be valid, beginning with the necessity of an offer made by one party and acceptance by another. This principle of mutual consent is crucial; it indicates that both parties agree to the terms and conditions of the contract, thus forming the basis of their legal obligations.[30]

---

[26] "ESIGN Act and UETA", *available at*: https://www.docusign.com/learn/esign-act-ueta (last visited on: 09.01.2025)

[27] "E-Signatures and E-Contracts for cross boundary transactions- Are they legally valid?", *available at*: https://signdesk.com/in/esign/esignature-and-electronic-contracts-for-cross-boundary-transactions (last visited on: 09.01.2025)

[28] Indian Contract Act 1872, sec. 10.

[29] Ironclad Journal "Contract Law: Know the fundamentals", *available at:* https://ironcladapp.com/journal/contracts/contract-law/ (last visited on: 09.01.2025)

[30] Abhay Pandey & Aksshay Sharma, "Essentials of a Valid Contract", *available at*: https://blog.ipleaders.in/essentials-of-a-valid-contract/ (last visited on: 09.01.2025)

The intention to create legal relations is another critical element specified in the Act. This requirement ensures that the parties involved genuinely intend to enter into a legally binding agreement rather than a mere social arrangement or informal understanding. It highlights the need for a clear purpose behind the agreement, reinforcing the legal implications of their actions. Legal capacity is also a fundamental requirement. The parties to the contract must possess the capacity to enter into a binding agreement, which includes being over 18 years of age, of sound mind, and solvent. This provision protects individuals who may be vulnerable, such as minors or those with mental incapacities, ensuring that they cannot be bound by agreements that they do not fully understand or that exploit their situation. Additionally, the object of the contract must be legal. This means that the agreement cannot involve illegal activities or contravene public policy. For example, an agreement to sell prohibited drugs or engage in illegal gambling would be deemed invalid. This requirement serves to uphold societal norms and legal standards, ensuring that contracts promote lawful behaviour. Consideration is another vital aspect of a valid contract, referring to the value exchanged between the parties. This can take the form of money or other benefits, but it must be something of value that each party agrees to provide. Without consideration, a contract may be considered a mere gift, lacking the necessary enforceability. The agreement must also be capable of performance, meaning that the terms set forth in the contract should be feasible and realistic. If the obligations outlined in the contract cannot be performed, the contract may be rendered void. Lastly, the terms of the contract must be clear and certain. Ambiguities in the agreement can lead to disputes and uncertainty, making it difficult to enforce the contract. Therefore, it is essential that the rights and obligations of each party are defined explicitly to avoid any misunderstandings.

In summary, for a contract to be valid under the Indian Contract, it must satisfy a comprehensive set of criteria, including mutual consent, intention to create legal relations, the legal capacity of the parties, a lawful object, consideration, capability of performance, and clarity of terms. Only when all these elements are present can a contract be deemed valid and enforceable, ensuring that the legal framework supports fair and just contractual relationships in the realm of both traditional and electronic commerce. Electronic contracts are recognised as legitimate and enforceable in India under the Information Technology Act; section 10-A of the act talks about it. To validate an electronic contract, compliance with the relevant requirements established in the Indian Contract Act is essential. Furthermore, the Indian Evidence Act also recognises electronic contracts as admissible evidence of contractual consent in court

proceedings.[31] Section 10-A of the Information Technology Act[32] specifically affirms the legal validity of contracts formed through electronic means, stating: "*Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals, and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.*"

INTERNATIONAL LAWS FOR ELECTRONIC AUTHENTICATION

International laws for electronic authentication primarily focus on establishing a legal framework for recognising electronic signatures and ensuring secure electronic transactions. It aims to create a secure and reliable environment for electronic transactions. By establishing legal recognition for electronic signatures and promoting best practices, these frameworks facilitate global commerce and build trust in digital interactions. The following international laws and frameworks collectively establish a robust legal environment for digital authentication in international trade. By ensuring the legal validity and reliability of electronic transactions, they facilitate a more secure and efficient global trading system. As digital trade continues to expand, these laws will play a crucial role in promoting confidence and enabling seamless cross-border transactions. Through ongoing collaboration and adaptation of these frameworks, countries can enhance their participation in the increasingly digital global marketplace.

1. UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS (2005)

The United Nations Convention on the Use of Electronic Communications in International Contracts, adopted in 2005, seeks to promote international trade by establishing a comprehensive and uniform legal framework governing electronic communications in the context of contract formation.[33] This convention is particularly significant in an era where digital transactions are increasingly prevalent, as it recognises that electronic communications should not be denied legal effect, validity, or enforceability solely due to their electronic nature. This

[31] AZB & Partners, "At a glance: Electronic contracts in India", *available at:* https://www.lexology.com/library/detail.aspx?g=299292f4-aed9-4e09-990d-a3169e02c48d#:~:text=Additionally%2C%20the%20Indian%20Evidence%20Act,of%20proof%20and%20will%20be (last visited on: 09.01.2025)

[32] Information Technology Act, 2000, sec. 10-A

[33] United Nations Commission on International Trade Law, "United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)", *available at:* https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications#:~:text=The%20Electronic%20Communications%20Convention%20aims,their%20traditional%20paper%2Dbased%20equivalents (last visited on: 09.01.2025)

principle is essential in ensuring that digital contracts can be executed with the same legal standing as traditional paper contracts, thereby facilitating smoother transactions in the global marketplace. A critical component of the convention is Article 9, which underscores the necessity of mutual consent among contracting parties regarding the use of electronic communications. This provision aligns with fundamental contractual principles, affirming that parties have the freedom to determine the terms of their agreements, including the method of communication. By explicitly requiring consent, the convention reinforces the importance of autonomy in contractual relations, ensuring that all parties are fully aware and agreeable to the electronic processes involved.[34]

Article 10 further addresses the issue of authenticity in electronic communications. It stipulates that a message should be considered authentic if it can be reliably attributed to the sender. This provision is vital in establishing trust in electronic transactions, as it provides a legal basis for verifying the identity of the parties involved and the integrity of the communications exchanged. Consumer protection is another critical aspect of the convention. It includes provisions designed to safeguard consumers by ensuring they are adequately informed about the terms of the contract and that they can provide consent electronically. This emphasis on consumer rights is particularly important in the realm of e-commerce, where consumers must feel confident that their rights are protected when engaging in online transactions. To facilitate the widespread adoption of these principles, the convention encourages member states to harmonise their domestic laws with its provisions. This alignment is intended to reduce legal uncertainties and discrepancies in cross-border transactions, making it easier for businesses to operate internationally and enhancing the overall efficiency of global trade.

In summary, the United Nations Convention on the Use of Electronic Communications in International Contracts establishes a robust framework that not only legitimises electronic communications in contract formation but also prioritises mutual consent, authenticity, and consumer protection. By encouraging the harmonisation of laws among member states, the convention aims to foster a more coherent and reliable legal environment for international trade in an increasingly digital world.

[34] "United Nations Convention on the Use of Electronic Communications in International Contracts", *available at*: https://wipolex-res.wipo.int/edocs/lexdocs/treaties/en/uncitral-uecic/trt_uncitral_uecic.pdf (last visited on: 09.01.2025)

2. UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE (1996)

The UNCITRAL Model Law on Electronic Commerce, adopted in 1996, plays a critical role in establishing a legal framework that recognises and regulates electronic transactions. Its primary aim is to facilitate international trade by promoting legal certainty and consistency in electronic communications, which is increasingly vital in today's digital economy[35].

One of the cornerstone principles of the Model Law is the legal recognition of electronic records. It explicitly affirms that electronic records are valid and enforceable as long as they meet specified criteria. This provision is essential because it assures businesses that electronic communications, such as emails, digital contracts, and electronic signatures, hold the same legal standing as traditional paper documents. By removing legal ambiguities surrounding electronic transactions, the Model Law encourages businesses to adopt digital methods without the apprehension of potential legal challenges[36]. Another significant aspect of the Model Law is the principle of functional equivalence. This principle states that electronic communications should be treated equivalently to traditional ones if they perform the same functions. For example, a signed electronic document should be considered equivalent to a signed paper document, provided it meets certain standards of reliability. This principle is foundational for developing other legal frameworks governing electronic transactions, as it reinforces the idea that the medium of communication should not diminish the validity or enforceability of the content. The adaptability of the Model Law is also noteworthy. It is crafted to be flexible, allowing countries to tailor their laws according to their unique legal environments while still conforming to the overarching principles set forth by UNCITRAL. This adaptability is crucial in accommodating the diverse legal systems and cultural contexts of different jurisdictions, enabling nations to integrate the Model Law into their domestic legislation effectively. Global adoption of the Model Law has been substantial, with numerous countries incorporating its principles into their national laws. This widespread acceptance is vital for the harmonisation of laws related to electronic commerce, as it creates a more consistent legal landscape for businesses that operate across borders. By reducing legal disparities and uncertainties in different jurisdictions, the Model Law enhances the ability of companies to engage in international trade and fosters greater confidence in electronic transactions. Additionally, the Model Law addresses issues such as the integrity and authenticity of electronic messages, further reinforcing trust in electronic commerce. By

[35] United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998", *available at:* https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce (last visited on: 09.01.2025)

[36] *Ibid.*

establishing guidelines for verifying the sender's identity and ensuring the integrity of the message, the Model Law contributes to a secure and reliable framework for electronic transactions.

In summary, the UNCITRAL Model Law on Electronic Commerce represents a significant advancement in the legal recognition of electronic transactions. Through its principles of legal recognition, functional equivalence, adaptability, and global adoption, the Model Law not only facilitates international trade but also lays the groundwork for a robust legal environment that supports the continued growth and evolution of electronic commerce in a rapidly digitising world.

3. UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

The UNCITRAL Model Law on Electronic Signatures, adopted in 2001, is an important legislative framework that complements the Model Law on Electronic Commerce by specifically addressing the legal status and validity of electronic signatures[37]. As the use of electronic signatures becomes increasingly prevalent in commercial transactions, this Model Law plays a crucial role in ensuring that these signatures are recognized as legally binding, thus providing a foundation for the enforceability of digital contracts. One of the key aspects of the Model Law is its explicit recognition of electronic signatures as valid and legally binding, provided they satisfy certain criteria. These criteria include reliability, security, and the intent of the parties to authenticate the signature[38]. This legal acknowledgement is essential because it provides the necessary assurance for individuals and businesses to engage in electronic transactions with confidence, knowing that their digital agreements will hold up in a legal context.

The principle of technological neutrality is another significant feature of the Model Law. By adopting a stance of neutrality, the Model Law does not favour any specific technology or method of creating electronic signatures. Instead, it allows for a wide range of electronic signature technologies, ensuring that the law remains relevant and adaptable as technological advancements occur. This flexibility is crucial in a rapidly evolving digital environment, as it enables businesses to choose the electronic signature solutions that best fit their needs without

[37] United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Signatures (2001)", *available at:* https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures#:~:text=The%20MLES%20establishes%20criteria%20of,parties%20intervening%20in%20the%20signature (last visited on: 09.01.2025)

[38] United Nations, "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001", (20) United Nations Publication, *available at:* https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf (last visited on: 09.01.2025)

being constrained by outdated legal frameworks. Moreover, the Model Law promotes cross-border applicability by encouraging countries to adopt similar legislative provisions regarding electronic signatures. This harmonisation is particularly beneficial for businesses engaged in international trade, as it facilitates the mutual recognition of electronic signatures across different jurisdictions. By minimising discrepancies in legal standards related to electronic signatures, the Model Law helps reduce the risk of legal disputes that can arise from differing interpretations of signature validity in cross-border transactions. In addition to establishing legal recognition and technological neutrality, the Model Law provides valuable guidance on best practices for the implementation of electronic signature systems. This guidance emphasises the importance of security measures to protect the integrity and authenticity of electronic signatures[39]. By outlining best practices, the Model Law fosters confidence among users and encourages the adoption of secure electronic transaction methods. Furthermore, the Model Law addresses the need for accountability and traceability in electronic signatures, thereby reinforcing the legitimacy of electronic transactions[40]. It emphasises that an electronic signature must be linked to the signatory in a manner that allows for the verification of the signatory's identity. This aspect is critical in preventing fraud and ensuring that the parties to a transaction can trust the authenticity of the signatures involved.

In summary, the UNCITRAL Model Law on Electronic Signatures provides a comprehensive and forward-looking framework that addresses the complexities of electronic signatures in today's digital economy. By recognising the legal validity of electronic signatures, maintaining technological neutrality, promoting cross-border applicability, and offering guidance on best practices, the Model Law plays a vital role in enhancing the reliability and acceptance of electronic transactions. It ultimately contributes to a more secure and efficient framework for conducting business in a global marketplace, ensuring that electronic signatures are upheld and recognised in legal contexts worldwide.

4. EUROPEAN UNION ELECTRONIC IDENTIFICATION AND TRUST SERVICES REGULATION (EIDAS)

The European Union Electronic Identification and Trust Services Regulation (eIDAS), adopted in 2014, provides a robust framework aimed at facilitating secure electronic transactions across

[39] *Ibid.*

[40] Carmen Maria Ramirez Ortiz & Luca Castellani, "Driving Digitalization in Global Trade: UNCITRAL Model Law on Electronic Transferable Records", *available at*: https://www.adb.org/sites/default/files/publication/932456/adb-brief-280-driving-digitalization-global-trade.pdf (last visited on: 09.01.2025)

EU member states[41]. This regulation is a significant step towards creating a unified digital market within the EU, enhancing the legal certainty of electronic identification and trust services. A central feature of the eIDAS Regulation is the categorisation of electronic signatures into three distinct types: simple, advanced, and qualified. Simple electronic signatures, while valid, do not provide the same level of security or legal assurance as the other two types. Advanced electronic signatures offer a higher degree of security by ensuring that the signature is uniquely linked to the signatory and that any subsequent changes to the signed data are detectable[42]. However, it is the qualified electronic signature that carries the highest level of security and legal standing, making it equivalent to a handwritten signature under EU law. This equivalence is vital as it allows for a reliable and legally binding means of conducting transactions electronically, particularly in sensitive areas such as finance, legal agreements, and governmental processes[43]. The eIDAS Regulation also emphasises interoperability among electronic identification systems within the EU. By promoting interoperability, the regulation allows for seamless recognition of electronic signatures and identities across member states, thereby eliminating legal uncertainties that could arise in cross-border transactions. This uniformity is crucial for businesses that operate in multiple jurisdictions, as it fosters confidence in the use of electronic signatures and streamlines the process of conducting international business.

In addition to electronic signatures, eIDAS outlines a range of standards for trust services. These services include electronic seals, which ensure the authenticity of documents; time-stamping, which provides a reliable date and time for the signing of documents; and website authentication, which confirms the identity of the entity behind a website. Together, these trust services enhance the overall security of digital transactions and are designed to build consumer trust in the electronic marketplace. Moreover, the regulation imposes specific compliance requirements on service providers, mandating that they adhere to the established standards for electronic identification and trust services. This accountability is essential in maintaining the integrity and reliability of electronic transactions. Service providers are required to implement measures that ensure the security of their systems and the confidentiality of user data. This level of oversight fosters trust among users, as they can be assured that the services they are using comply with

41 "eIDAS Regulation", *available at:* https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation#:~:text=The%20eIDAS%20regulation%20facilitates%20secure,digital%20services%20in%20the%20EU (last visited on: 09.01.2025)

42 "Types of Digital Signatures: AES, QES, SES Explained", *available at:* https://www.docusign.com/en-gb/blog/types-digital-signature-aes-qes-ses-explained (last visited on: 09.01.2025)

43 "What is qualified electronic signatures", *available at:* https://www.agrello.io/digital-signing/what-is-a-qualified-electronic-signature (last visited on: 09.01.2025)

stringent EU standards. The eIDAS Regulation also plays a crucial role in supporting innovation within the digital economy. By providing a clear legal framework, it encourages the development and adoption of new technologies related to electronic identification and trust services. This adaptability is essential in a rapidly changing technological landscape, where emerging technologies like blockchain and biometric identification are becoming increasingly relevant.

In summary, the eIDAS Regulation represents a comprehensive and forward-thinking approach to electronic identification and trust services within the European Union. By categorising electronic signatures, promoting interoperability, establishing standards for trust services, and ensuring compliance and accountability among service providers, eIDAS significantly enhances the security and reliability of electronic transactions. This regulation not only facilitates smoother cross-border business operations but also fosters greater trust among consumers and businesses in the digital economy, paving the way for a more integrated and secure European digital market.

5. GENERAL AGREEMENT ON TARIFFS AND TRADE (GATT)

The General Agreement on Tariffs and Trade (GATT), established in 1947, is a foundational international treaty aimed at promoting and facilitating global trade by reducing barriers such as tariffs and quotas[44]. While GATT is not specifically focused on digital authentication, its principles are increasingly relevant in the context of digital trade, which has grown significantly in the age of globalisation and technological advancement[45]. One of the core tenets of GATT is the principle of non-discrimination, which encompasses the most-favoured-nation (MFN) treatment. This principle ensures that any favourable trading conditions granted by one member country to another must also be extended to all other GATT member countries. This creates an equitable trading environment where nations are treated equally in their trade relations, including those that involve digital goods and services. By applying this principle, GATT helps to prevent discriminatory practices that could hinder access to digital markets, thus promoting fairness and competition in international trade[46]. Transparency is another fundamental principle emphasised by GATT. The agreement underscores the necessity for member countries to provide clear and

[44] Christine Majaski, "What is the General Agreement on Tariffs and Trade (GATT)?", by Christine Majaski, *available at:* https://www.investopedia.com/terms/g/gatt.asp#:~:text=The%20General%20Agreement%20on%20Tariffs%20and%20Trade%20(GATT)%20was%20signed,aspects%20of%20the%20prewar%20period (last visited on: 09.01.2025)

[45] The International Monetary Fund, "Digital Trade for Development", World Trade Organization, *available at:* https://www.wto.org/english/res_e/booksp_e/dtd2023_e.pdf (last visited on: 09.01.2025)

[46] "Most-favoured-nation Treatment Principle", *available at:* https://www.meti.go.jp/english/report/data/2015WTO/02_01.pdf (last visited on: 09.01.2025)

accessible information regarding their trade regulations and policies. This transparency is vital in fostering trust among trading partners, particularly in the realm of digital transactions where parties may be located in different jurisdictions. By making regulations known and understandable, GATT helps stakeholders—such as businesses and consumers—navigate the complexities of international trade, enhancing their confidence in engaging in electronic commerce.

As the global economy evolves with the rapid digitisation of trade, the principles outlined in GATT may need to be adapted to address the unique challenges posed by electronic transactions. One significant challenge is the legal recognition of digital contracts. In traditional commerce, contracts are often documented on paper, making them straightforward to authenticate and enforce. However, digital contracts require specific mechanisms for verification and authentication to ensure their legitimacy in a legal context. The adaptation of GATT principles to encompass these new realities is essential for providing a robust framework that can support the growth of digital trade. Moreover, as businesses increasingly rely on electronic means for transactions, issues surrounding data security, privacy, and the integrity of digital communications become paramount. GATT's principles can guide the development of international norms and regulations that address these concerns, promoting secure and reliable digital transactions. For instance, member countries might collaborate on establishing standards for electronic signatures, data protection, and dispute resolution in the context of digital trade. Furthermore, the integration of GATT principles with other international agreements focused on digital trade, such as the World Trade Organization's Trade Facilitation Agreement and the recently established Digital Economy Partnership Agreement, can provide a more comprehensive approach to addressing the complexities of electronic commerce. By aligning various trade frameworks, countries can create a cohesive legal environment that facilitates cross-border digital transactions while upholding the values of fairness, transparency, and non-discrimination.

In summary, while the GATT is not specifically centred on digital authentication, its principles of non-discrimination and transparency are crucial for the development of a fair and trustworthy environment for digital trade. As international trade continues to adapt to the challenges and opportunities presented by digitalisation, the principles established by GATT can serve as a foundational framework that promotes equitable practices, fosters trust and encourages cooperation among nations in the increasingly interconnected digital economy.

6. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) GUIDELINES

The Organization for Economic Co-operation and Development (OECD) Guidelines are a set of comprehensive recommendations designed to enhance electronic commerce among member countries[47]. These guidelines play a pivotal role in shaping policies and practices that support the growth of digital transactions and foster a secure, trustworthy environment for users[48]. A focus of the OECD Guidelines is the cultivation of user confidence in digital transactions. This aspect is critically important, as user trust is foundational to the adoption and success of electronic commerce[49]. The guidelines emphasise that effective digital authentication mechanisms are essential for building this trust. By implementing reliable authentication processes, countries can ensure that users feel secure when engaging in online transactions, thereby encouraging broader participation in the digital economy. User confidence is bolstered by measures that protect personal data and enhance the overall integrity of digital interactions. In addition to fostering user confidence, the OECD Guidelines advocate for the development of robust legal frameworks that support electronic commerce. Such frameworks are vital for creating a conducive environment for international trade and facilitating seamless digital transactions. The guidelines encourage countries to establish clear laws that address the validity of electronic contracts, the use of electronic signatures, and the protection of consumer rights. By harmonising legal standards across jurisdictions, countries can reduce barriers to trade and create a more cohesive digital marketplace. This legal clarity is especially important in cross-border transactions, where differing regulations can lead to confusion and disputes[50].

Moreover, the OECD Guidelines outline best practices for ensuring security, privacy, and consumer protection in electronic commerce. These practices are designed to help businesses and governments create systems that safeguard sensitive information and protect consumers

[47] OECD Legal Instrument, "Recommendation of the Council on Consumer Protection in E-commerce", OECD/LEGAL/0422, *available at:* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422 (last visited on: 09.01.2025)

[48] OECD, "Digital", *available at:* https://www.oecd.org/en/topics/policy-areas/digital.html (last visited on: 09.01.2025)

[49] *Supra* note 47.

[50] "A global Action Plan for Electronic Commerce: Prepared by Business with Recommendations for Governments", OECD Digital Economy Papers No. 44, *available at*: https://www.oecd.org/content/dam/oecd/en/publications/reports/1999/10/a-global-action-plan-for-electronic-commerce_g17a1b50/236544834564.pdf (last visited on: 09.01.2025)

from fraud and abuse. The guidelines recommend implementing strong data protection measures, conducting regular security assessments, and fostering transparency in data handling practices. By prioritising security and privacy, countries can enhance user trust and promote the widespread adoption of digital contracts. The guidelines also emphasise the importance of stakeholder collaboration in advancing electronic commerce. They encourage governments, businesses, and civil society to work together to address the challenges and opportunities presented by the digital economy. By fostering partnerships among these groups, countries can develop innovative solutions that enhance the digital landscape and promote sustainable growth.

In conclusion, the OECD Guidelines serve as a vital framework for member countries seeking to enhance electronic commerce. By focusing on user confidence, advocating for robust legal frameworks, and promoting best practices for security and privacy, the guidelines contribute to the creation of a secure and trustworthy digital environment[51]. This, in turn, supports the growth of electronic commerce and facilitates international trade, ensuring that the benefits of the digital economy can be realised by all stakeholders.

7. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) STANDARDS

The International Organization for Standardization (ISO) plays a significant role in establishing secure digital authentication processes through its various standards. These standards provide frameworks and guidelines that organisations can adopt to enhance their security measures, ensure compliance with legal requirements, and build consumer trust in digital transactions[52]. One of the most prominent standards is ISO/IEC 27001, which focuses on information security management systems (ISMS)[53]. This standard outlines comprehensive requirements for establishing, implementing, maintaining, and continually improving an organisation's information security management system. For organisations involved in international trade, compliance with ISO/IEC 27001 is vital, as it helps them manage sensitive information effectively and secure transactions against various threats.[54] The standard requires organisations to assess risks,

[51] OECD, "Privacy and Data Protection", *available at:* https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html (last visited on: 09.01.2025)

[52] eMudhra Limited, Feb. 24, 2024 "ISO Standards in Digital Security Setting the Global Benchmark", *available at:* https://emudhra.com/blog/iso-standards-in-digital-security-setting-the-global-benchmark (last visited on: 09.01.2025)

[53] "Information Security, cybersecurity and privacy protection- Information security management Systems - Requirements", ISO/IEC 27001:2022, *available at:* https://www.iso.org/standard/27001 (last visited on: 09.01.2025)

[54] Mark Sharron, "ISO 27001 Certification, Simplified", *available at*: https://www.isms.online/iso-27001/certification/ (last visited on: 09.01.2025)

implement security controls, and conduct regular audits, thereby ensuring that their information security practices are robust and up to date. By adhering to this standard, organisations not only enhance their security posture but also demonstrate their commitment to safeguarding sensitive data, which is crucial for maintaining the trust of customers and partners. Another important ISO standard is *ISO/IEC 29100*, which provides a privacy framework designed to guide organisations in protecting personal data during digital transactions[55]. This framework outlines key concepts and principles for managing privacy risks, emphasising the need for organisations to adopt a proactive approach to data protection. In the context of digital authentication, implementing the guidelines of ISO/IEC 29100 is essential, as it helps organisations create mechanisms for obtaining consent, informing users about data handling practices, and ensuring that personal data is processed transparently[56]. By following these guidelines, organisations can significantly enhance consumer trust, which is critical in encouraging individuals to engage in electronic transactions. Additionally, ISO/IEC 29151 specifically addresses the protection of personal information, providing further clarity and direction for organisations looking to strengthen their privacy practices[57]. This standard builds on the principles outlined in ISO/IEC 29100 and provides detailed guidance on best practices for handling personal data. It focuses on the confidentiality, integrity, and availability of personal information, encouraging organisations to implement strong data protection measures. By adhering to ISO/IEC 29151, organisations can enhance their compliance with privacy regulations and demonstrate their commitment to protecting user information, thus fostering greater trust among users[58].

In summary, the ISO standards related to digital authentication provide a comprehensive framework that organisations can leverage to enhance their security and privacy practices. By implementing ISO/IEC 27001, organisations can establish effective information security management systems, while ISO/IEC 29100 and ISO/IEC 29151 guide them in protecting

[55] "Information Technology - Security Techniques - Privacy Framework", ISO/IEC 29100:2024 (en), *available at:* https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-2:v1:en (last visited on: 09.01.2025)

[56] Privacy Engine, "ISO 29100 Information Security Standard", *available at*: https://www.privacyengine.io/resources/glossary/iso-29100-information-security-standard/ (last visited on: 09.01.2025)

[57] Privacy Engine, "ISO 29151 Information Security Standard", *available at:* https://www.privacyengine.io/resources/glossary/iso-29151-information-security-standard/#:~:text=The%20primary%20focus%20of%20ISO,the%20protection%20of%20personal%20data (last visited on: 09.01.2025)

[58] "Information technology- Security Techniques- Code of practice for personally identifiable information protection", IS0/IEC 29151:2017, *available at*: https://www.iso.org/standard/62726.html (last visited on: 09.01.2025)

personal data and ensuring compliance with privacy requirements[59]. Collectively, these standards play a critical role in establishing secure and reliable digital authentication processes, ultimately contributing to a safer and more trustworthy digital economy. Through adherence to these internationally recognised standards, organisations can not only mitigate risks but also build lasting trust with consumers, which is essential for the continued growth and success of digital commerce.

CONCLUSION

The emergence of digital contracts signifies a transformative development in international trade, propelled by the necessity for enhanced efficiency, security, and adaptability in an increasingly globalised marketplace. This analysis underscores the vital legal frameworks that govern electronic authentication, including key instruments such as the United Nations Convention on the Use of Electronic Communications in International Contracts, the UNCITRAL Model Law on Electronic Commerce, and the eIDAS Regulation within the European Union. These regulations establish a solid foundation for recognising the validity of digital contracts, ensuring they hold the same legal authority as traditional paper agreements.

Across these jurisdictions, there is a common recognition of the importance of digitalisation in contracts and the need for robust legal frameworks to support their validity. Each country has unique regulatory environments and challenges, but all are moving towards enhancing the legal recognition and enforcement of digital and smart contracts in international trade. This shift aims to foster innovation, improve efficiency, and promote consumer protection in the digital economy.

From the Indian perspective, the legal landscape is guided by the Indian Contract Act of 1872 and the Information Technology Act of 2000, which collectively facilitate the recognition and enforcement of electronic contracts. India's efforts to align its legal framework with international standards demonstrate its acknowledgement of the significance of digitalisation in fostering trade and commerce.

Across India, the USA, the UK, and the EU, there is a clear trend toward recognising the validity of digital contracts, driven by the need for efficiency in international trade. While each jurisdiction has developed its legal framework, common themes include the emphasis on

[59] Mark Sharron, "ISO 27701- The Standard for Privacy Information Management", *available at:* https://www.isms.online/iso-27701/ (last visited on: 09.01.2025)

electronic signatures, the recognition of smart contracts, and the ongoing challenges related to interpretation and liability. This comparative study highlights the importance of aligning legal frameworks to facilitate smoother cross-border transactions and address the complexities arising from digitalisation. Continued collaboration and adaptation will be essential as the landscape of international trade evolves in the digital age.

In summary, the interaction between international laws and national regulations creates a comprehensive framework for the adoption of digital contracts in global trade. As nations continue to navigate the digital era, ongoing collaboration and harmonisation of legal standards will be essential for building trust and reliability in digital transactions. This evolution will not only enhance efficiency in international trade but also encourage the development of innovative business models, ultimately contributing to economic growth and prosperity across borders.