



DOI: <https://doi.org/10.38035/sijal.v4i1>
<https://creativecommons.org/licenses/by/4.0/>

Received: 26-08-2026 | Revised: 16-09-2026 | Accepted: 21-09-2026

The Urgency of Regulating Blockchain-Based Smart Contracts in International Business Law: Legal Certainty and Global Regulatory Harmonization

Leni Indrawati¹, Dhaniswara K. Harjono², Adi Nur Rohman³, Elly Rachman⁴

¹Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, leniindrawati.pangestu@gmail.com

²Universitas Kristen Indonesia, Jakarta, Indonesia, dhaniswara.harjono@uki.ac.id

³Universitas Bhayangkara Jakarta Raya, Indonesia, adi.nur@dsn.ubharajaya.ac.id

⁴Temple University Japan, Japan, ellyrch@gmail.com

Corresponding Author: leniindrawati.pangestu@gmail.com¹

Abstract: Blockchain-based smart contracts automate cross-border commercial performance, yet their finality does not by itself resolve questions of consent, validity, liability, applicable law, jurisdiction, evidence, remedies, and enforcement. Existing scholarship generally examines domestic contractual validity or sector-specific digital-asset regulation, leaving insufficient analysis of an integrated transnational framework. This study analyzes the legal status and regulatory urgency of smart contracts in international business law and formulates a harmonization model capable of reconciling code-based execution with legal certainty. It employs normative legal research using statutory, conceptual, comparative, and international-law approaches. Legal instruments and regulatory developments in Indonesia, the United States, the European Union, Singapore, UNCITRAL, and UNIDROIT are analyzed qualitatively. The study finds that functional equivalence and technological neutrality support legal recognition, but fragmented national rules remain inadequate for algorithmic error, oracle failure, code auditing, consumer protection, dispute resolution, and cross-border enforcement. The article proposes Transnational Smart Contract Regulation, an UNCITRAL-oriented model organized around legal recognition, blockchain evidence, electronic signatures, party autonomy, jurisdiction, code auditing, cybersecurity, digital consumer protection, online dispute resolution, and enforcement. Its novelty lies in integrating legal certainty, harmonization, and law-and-technology theories into a risk-based regulatory architecture that preserves innovation while ensuring intelligible consent, accountability, corrective intervention, and interoperable remedies.

Keywords: smart contracts, blockchain, international business law, legal certainty, regulatory harmonization.

INTRODUCTION

The Fourth Industrial Revolution has transformed the pattern of global economic relations through the digitalization of international commercial activities. One of the most significant technological developments is the emergence of blockchain as a decentralized digital ledger system that enables the secure exchange of data and value without the involvement of intermediaries.

The development of blockchain technology has given rise to a new legal and commercial instrument known as the smart contract. The concept of smart contracts was first introduced by Nick Szabo in 1996 as a digital transaction protocol capable of automatically executing contractual terms through computer algorithms (Szabo, 1996).

In practice, smart contracts are utilized across various sectors, including international trade, financial services, logistics, insurance, digital investment, global supply chains, and cryptocurrency transactions. Their principal advantage lies in their ability to function as self-executing agreements, thereby reducing transaction costs, accelerating business processes, enhancing administrative efficiency, and minimizing the risk of contractual breach (De Filippi & Wright, 2018).

Nevertheless, the development of smart contracts has generated a range of novel legal issues. Traditional contract law is founded upon the parties' intent, the principle of consensualism, good faith, and dispute resolution mechanisms administered through courts or arbitration. In contrast, smart contracts operate through automated computer code, raising significant questions regarding legal validity, liability, and dispute resolution (Raskin, 2017).

These issues become even more complex because blockchain technology is inherently borderless. Contracting parties may be located in different jurisdictions, while transaction data is distributed across a global network that is not subject to any single legal system. This situation gives rise to challenges concerning the applicable law (choice of law), judicial jurisdiction, the recognition of electronic evidence, and the cross-border enforcement of judicial decisions and arbitral awards (Reed, 2012).

Recent studies indicate that most jurisdictions, including Indonesia, have yet to enact comprehensive regulations governing the validity of smart contracts, automated execution mechanisms, code auditing standards, and legal accountability arising from their operation. Consequently, legal uncertainty remains one of the principal obstacles to the development of blockchain-based global digital transactions.

Based on the foregoing background, this research examines the urgency of regulating smart contracts within the framework of international business law and proposes a model of regulatory harmonization capable of ensuring legal certainty in cross-border digital transactions.

Research Novelty

The novelty of this research lies in several aspects that distinguish it from previous studies. Integration of the Theory of Legal Certainty, the Theory of Legal Harmonization, and the Theory of Law and Technology

This research does not merely examine smart contracts from the perspective of contract law. Instead, it integrates the Theory of Legal Certainty, the Theory of Legal Harmonization, and the Theory of Law and Technology into a comprehensive analytical framework (Radbruch, 1932). Such an approach enables a more in-depth examination of legal certainty, the necessity for international regulatory harmonization, (UNCITRAL, 1996) and the adaptation of legal systems to the rapid development of blockchain technology (Lessig, 1999). Comparative Analysis of Smart Contract Regulation in the United States, the European Union, Singapore, and Indonesia.

This research undertakes an integrated comparative legal analysis of the regulatory frameworks governing smart contracts in the United States, the European Union, Singapore,

and Indonesia (De Cruz, 2016). The analysis seeks to identify the similarities, differences, strengths, and weaknesses of each legal system, thereby providing a foundation for the development of a more effective and responsive regulatory framework in Indonesia. Furthermore, the comparative approach is supported by international standards concerning electronic commerce and digital transactions (UNCITRAL, 1996).

Formulation of a Blockchain-Based International Legal Harmonization Model

A further novelty of this research lies in the formulation of an international legal harmonization model specifically designed to accommodate the use of blockchain technology in global business transactions. The proposed model integrates technological developments with the fundamental principles of modern contract law in order to enhance legal certainty, facilitate cross-border commercial transactions, and promote greater consistency in the regulation and enforcement of smart contracts at the international level (Reed, 2012). This model also draws upon scholarly discussions concerning the legal nature and enforceability of smart contracts within contemporary legal systems (Raskin, 2017).

Development of the Concept of Transnational Smart Contract Regulation.

This research proposes the concept of Transnational Smart Contract Regulation as a prospective legal framework designed to address legal challenges arising from cross-border smart contract transactions, particularly those relating to jurisdiction, choice of law, and dispute resolution mechanisms. The concept seeks to establish a legal framework capable of accommodating the transnational nature of blockchain-based transactions, which frequently transcend the territorial boundaries of individual states and legal systems (De Filippi & Wright, 2018).

The proposed framework is grounded in the principle that the regulation of smart contracts should not be confined solely to domestic legal systems. Rather, it should incorporate internationally harmonized legal standards that facilitate legal certainty, predictability, and enforceability in cross-border digital transactions (UNCITRAL, 1996). In this regard, the concept of Transnational Smart Contract Regulation is intended to serve as a normative foundation for the development of a more coherent and responsive international regulatory regime capable of adapting to rapid technological advancements and the evolving digital economy (Reed, 2012).

Furthermore, this concept aims to promote legal harmonization among jurisdictions by integrating existing principles of international commercial law, electronic commerce regulations, and emerging blockchain governance standards. Through such harmonization, it is anticipated that legal conflicts arising from divergent national regulations can be minimized, thereby enhancing confidence among international business actors engaging in smart contract-based transactions (Hildebrandt, 2015).

Accordingly, the development of the concept of Transnational Smart Contract Regulation represents one of the principal contributions and novelties of this research, offering a theoretical and practical framework for future international legal reform in the field of digital commerce and blockchain technology (UNIDROIT, 2016).

Against this background, the study addresses four connected questions: the legal status of blockchain-based smart contracts in international business law; the comparative direction of regulation in the United States, the European Union, Singapore, and Indonesia; the reasons harmonization is required; and the design of a Transnational Smart Contract Regulation model capable of supplying legal certainty in cross-border transactions. These questions structure the discussion and are answered in the conclusion.

METHODS

This study employs a normative legal research method, focusing on the analysis of legal norms, principles, doctrines, and regulatory frameworks governing smart contracts and

blockchain-based transactions in international business law. The research applies the following approaches:

Statutory Approach, through the examination of relevant national and international legal instruments governing electronic transactions, digital contracts, and blockchain technology;

Conceptual Approach, by analyzing legal doctrines and theoretical frameworks concerning legal certainty, legal harmonization, and the interaction between law and technological innovation;

Comparative Approach, through a comparative assessment of legal frameworks adopted in different jurisdictions regarding the recognition and regulation of smart contracts;

International Legal Approach, by examining international model laws, soft-law instruments, and transnational regulatory initiatives relevant to blockchain technology and digital commerce. The primary legal materials consist of:

- UNCITRAL Model Law on Electronic Commerce 1996; (UNCITRAL, 1996)
- UNCITRAL Model Law on Electronic Transferable Records 2017; (UNCITRAL, 2017b)
- Singapore Electronic Transactions Act; (Singapore, 2010)
- European Union Markets in Crypto-Assets Regulation (MiCA); (European Union, 2023a)
- Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024 (Indonesia, 2024).

The collected legal materials are analyzed qualitatively through legal interpretation and comparative legal analysis. Previous studies have generally focused on the validity of smart contracts under domestic contract law or the implementation of blockchain technology in digital financial services. However, limited scholarship has simultaneously examined the interrelationship between legal certainty, international regulatory harmonization, and the development of a transnational model of smart contract regulation within the framework of international business law. Accordingly, this research seeks to address this gap by employing a comparative legal approach and proposing a blockchain-based legal harmonization model capable of supporting cross-border commercial transactions.

The analysis applies grammatical, systematic, and teleological interpretation to determine how conventional contract-law requirements operate when formation or performance is automated. Comparative functional analysis is used to identify regulatory equivalents rather than merely contrasting statutory labels. The proposed model is then evaluated against legal certainty, technological neutrality, party autonomy, accountability, and cross-border enforceability. The study does not treat the illustrative Company A–Company B scenario as an empirical case; it is a normative problem scenario used to test whether the proposed rules produce determinate legal consequences.

RESULTS AND DISCUSSION

Theory of Legal Certainty

The legal validity and enforceability of digital contracts; The certainty and verifiability of the identities of contracting parties; The theory of legal certainty is principally associated with Gustav Radbruch, who argued that law should embody three fundamental values: legal certainty (Rechtssicherheit), justice (Gerechtigkeit), and expediency or utility (Zweckmäßigkeit) (Radbruch, 1932). Legal certainty serves as a foundational requirement of the rule of law because it enables individuals and business actors to predict the legal consequences of their actions and transactions.

Within blockchain-based transactions and smart contract environments, legal certainty is essential to ensure:

The legal validity and enforceability of digital contracts;

3. The certainty and verifiability of the identities of contracting parties;

4. The certainty of automated contractual execution through self-executing code;
5. The availability of clear mechanisms for dispute resolution; and
6. The effectiveness of legal enforcement across jurisdictions.

The absence of specific and harmonized regulations governing smart contracts has generated legal uncertainty regarding their status, enforceability, and recognition in various jurisdictions. Such uncertainty may hinder cross-border digital commerce, increase transaction costs, and create obstacles to the widespread adoption of blockchain technology in international business transactions. Therefore, the establishment of coherent legal frameworks capable of accommodating technological developments while maintaining legal certainty remains a significant challenge for contemporary legal systems.

Theory of Legal Harmonization

The Theory of Legal Harmonization explains that globalization necessitates the alignment of legal norms among states in order to minimize legal conflicts and enhance certainty in international transactions (Glenn, 2014).

Smart contracts, which operate through global blockchain networks, require uniform international legal standards to ensure legal certainty, consistency, and enforceability across jurisdictions (Reed, 2012).

Law and Technology Theory

Lawrence Lessig introduced the concept of “Code is Law.” (Lessig, 1999) This concept explains that computer code may function as a mechanism for regulating behavior in a manner similar to legal rules and regulations (Lessig, 1999). Within the context of smart contracts, the performance of contractual obligations is no longer carried out by human intervention but rather by computer algorithms that automatically execute predetermined instructions based on digital code (De Filippi & Wright, 2018).

The Concept of Smart Contracts in International Business Law

A smart contract is a digital agreement that is automatically executed through computer code deployed on a blockchain network (Szabo, 1996). Unlike conventional contracts, smart contracts possess several distinctive characteristics: (Raskin, 2017)

1. Self-executing;
2. Immutable;
3. Decentralized;
4. Transparent;
5. Cryptographically secured.

This technology enables international transactions to be conducted rapidly and efficiently without the involvement of intermediaries, thereby reducing transaction costs and enhancing operational effectiveness in cross-border commercial activities (De Filippi & Wright, 2018).

Legal Issues Concerning Smart Contracts

Validity of Smart Contracts

The first legal issue concerns the fulfillment of the essential requirements for a valid contract as stipulated under Article 1320 of the Indonesian Civil Code (KUHPerdata) (Indonesia, Civil Code, art. 1320).

A fundamental question arises as to whether computer code may be regarded as a valid expression of the parties' intention and consent. Contemporary legal scholarship suggests that smart contracts may be classified as electronic contracts; however, not all legal systems recognize computer code as a complete and sufficient representation of legally binding

agreement (Raskin, 2017). Consequently, uncertainties remain regarding the legal validity and enforceability of smart contracts in various jurisdictions (Werbach & Cornell, 2017).

1. Jurisdiction and Choice of Law.

Blockchain technology operates through decentralized networks that lack a specific geographical location (De Filippi & Wright, 2018). As a result, significant challenges arise in determining:

2. the competent forum for dispute resolution;
3. the applicable law governing the transaction; and
4. the authority responsible for legal enforcement.

These issues constitute one of the most significant challenges in contemporary international business law (Reed, 2012).

5. Legal Liability

Smart contracts may be affected by:

6. system bugs;
7. coding errors;
8. cyberattacks; and
9. oracle failures.

At present, no universally accepted international standard exists regarding the allocation of legal responsibility when losses result from algorithmic errors or technological failures within blockchain-based transactions (Levy, 2017).

10. Dispute Resolution.

The self-executing nature of smart contracts often limits the ability of courts and arbitral tribunals to intervene once contractual performance has been automatically executed (Werbach & Cornell, 2017).

Accordingly, several innovative dispute resolution mechanisms have emerged, including:

11. Online Dispute Resolution (ODR);
12. Blockchain Arbitration; and
13. Smart Legal Contract Frameworks (Allen, 2018).

Comparative Regulatory Approaches

United States

Several U.S. states, including Arizona, Tennessee, and Nevada, have expressly recognized the legal validity and enforceability of smart contracts (Arizona Revised Statutes, 2017; Nevada Revised Statutes, 2017; Tennessee Code, 2018). The United States generally adopts a market-oriented and innovation-driven regulatory approach that emphasizes technological development and commercial efficiency (Reyes, 2018).

European Union

The European Union has developed a comprehensive digital regulatory framework through:

1. the Markets in Crypto-Assets Regulation (MiCA);
2. the Digital Services Act (DSA); and
3. the Digital Markets Act (DMA) (European Union, 2022a, 2022b, 2023a).

The EU approach places greater emphasis on consumer protection, digital security, and regulatory oversight (European Commission, 2023).

Singapore

Singapore has adopted a pro-innovation regulatory strategy through:

1. the Electronic Transactions Act (ETA); and
2. the Payment Services Act (PSA) (Singapore, 2010, 2019).

As a result, Singapore has become one of Asia's leading fintech and blockchain hubs (Monetary Authority of Singapore, 2024).

Indonesia

Indonesia has not yet enacted a specific legal framework governing smart contracts (Indonesia, 2024).

Existing regulations are dispersed across several legal instruments, including:

1. the Indonesian Civil Code (KUHPerdata);
2. Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016;
3. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions; and
4. Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector.
5. This fragmented regulatory framework creates legal gaps concerning code auditing, algorithmic validity, and digital legal liability (Pramono, 2021).

Table 1. Comparative orientation of smart contract regulation

Jurisdiction	Legal recognition	Regulatory emphasis	Principal gap
United States	Express in several states	Innovation and enforceability	Fragmented state-level rules
European Union	Indirect and sectoral	Data, digital assets, consumers	No unitary contract regime
Singapore	Automated contracting recognized	Technology-neutral facilitation	Limited smart-contract-specific liability
Indonesia	General electronic-contract rules	Electronic systems and digital finance	No integrated code-risk framework

Source: Authors' analysis, 2026.

The Urgency of International Legal Harmonization

International legal harmonization is necessary because:

1. blockchain networks operate globally;
2. transactions frequently involve multiple jurisdictions;
3. no comprehensive international standard currently exists;
4. the risk of legal conflicts is substantial; and
5. legal certainty is essential for investors and business actors (Dickinson, 2010).

Recent studies indicate that existing smart contract regulations remain fragmented and sectoral in nature. Consequently, there is a pressing need for a new international legal instrument capable of integrating contract law, blockchain technology, data protection, and digital dispute resolution into a coherent regulatory framework (UNCTAD, 2024).

An Ideal Regulatory Model for Smart Contracts

This research proposes the establishment of a UNCITRAL Model Law on Smart Contracts, which would provide for:

1. International Recognition of Smart Contracts

Smart contracts should receive explicit legal recognition as valid and enforceable contractual instruments in international commercial transactions. Legal recognition is essential because smart contracts may be formed and performed through automated computer systems and blockchain technology, which may create uncertainty regarding whether code-based agreements satisfy traditional requirements relating to contract formation, consent, validity, and enforceability. An international framework should therefore establish that a smart contract should not be denied legal effect, validity, or enforceability merely because contractual rights and obligations are expressed or performed through automated systems or distributed ledger

technology, provided that the fundamental requirements of applicable contract law are satisfied (UNCITRAL, 1996, 2005).

This approach is consistent with the fundamental principles of non-discrimination, technological neutrality, and functional equivalence developed in UNCITRAL's electronic commerce instruments. In particular, the UNCITRAL Model Law on Automated Contracting, adopted in 2024, expressly seeks to facilitate the use of automation in contracts, including smart contracts and machine-to-machine transactions (UNCITRAL, 2024). Accordingly, the proposed regulation should build upon the existing UNCITRAL framework while providing more specific rules for blockchain-based smart contracts.

2. Standardization of Blockchain-Based Evidence

A harmonized regulatory framework should establish common standards concerning the admissibility, authenticity, integrity, reliability, and evidentiary value of blockchain records. Blockchain technology can provide a traceable and tamper-resistant record of transactions; however, different jurisdictions may apply different standards when assessing digital evidence (UNCITRAL, 2001).

International standards should clarify how blockchain records, transaction hashes, timestamps, wallet addresses, distributed ledger records, and other forms of digital evidence may be authenticated and presented before courts or arbitral tribunals. Such standardization would strengthen legal certainty and facilitate the cross-border recognition of blockchain-based evidence. The development of such standards should also be consistent with the broader UNCITRAL approach to electronic records, including the principle that electronic information should not be denied legal effect merely because it exists in electronic form (UNCITRAL, 1996).

3. Regulation of Digital Signatures

The regulatory framework should provide clear rules concerning the legal validity and recognition of digital signatures used in smart-contract transactions. Digital signatures are important for establishing the identity of contracting parties, demonstrating consent, attributing an electronic communication to its originator, and ensuring the integrity of electronically executed agreements.

International harmonization should establish minimum standards concerning authentication, reliability, attribution, and recognition of electronic signatures across jurisdictions. The UNCITRAL Model Law on Electronic Signatures 2001 establishes criteria of technical reliability for the legal equivalence between electronic and handwritten signatures and adopts a technology-neutral approach (UNCITRAL, 2001). Therefore, the proposed framework for smart contracts should complement existing international standards rather than create a separate and conflicting system of digital-signature regulation.

4. Blockchain-Based Arbitration and Online Dispute Resolution

Smart-contract disputes require efficient dispute-resolution mechanisms capable of addressing the technological and cross-border characteristics of blockchain transactions. An international regulatory framework should therefore recognize blockchain-supported arbitration and online dispute resolution (ODR) as appropriate mechanisms for resolving disputes arising from smart contracts.

Such mechanisms may facilitate dispute resolution through electronic submissions, digital evidence, remote hearings, and technologically supported procedural processes. However, technological efficiency should not undermine fundamental procedural safeguards, including independence and impartiality of arbitrators, equality of the parties, due process, transparency, and the enforceability of arbitral awards. UNCITRAL's Technical Notes on Online Dispute Resolution emphasize principles including fairness, transparency, due process, and accountability in the development of ODR systems (UNCITRAL, 2017a).

The recognition of blockchain-based arbitration should also remain compatible with the Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958 (New York Convention), which provides the principal international framework for recognition and enforcement of foreign and non-domestic arbitral awards.

5. Choice of Law

Choice-of-law provisions are particularly important because smart contracts may involve parties, assets, blockchain nodes, service providers, and other technological infrastructure located in different jurisdictions. The decentralized nature of blockchain transactions may therefore make it difficult to determine automatically which national law should govern the contractual relationship.

The parties should consequently be permitted to determine the substantive law applicable to their smart-contract relationship, subject to mandatory provisions and fundamental principles of the relevant legal system. A harmonized international framework should provide clear rules concerning the validity and interpretation of choice-of-law clauses incorporated into smart contracts.

Where the parties have not expressly selected the applicable law, the proposed framework should provide objective connecting factors for determining the applicable law. This would enhance predictability and reduce uncertainty concerning the substantive law governing cross-border blockchain transactions. Such an approach would also be consistent with the broader principle of party autonomy recognized in contemporary international commercial law (UNCITRAL, 2024).

6. Choice of Forum

The international regulation of smart contracts should also establish clear rules concerning choice of forum and jurisdiction. Because blockchain transactions may involve parties located in multiple jurisdictions, disputes may create uncertainty regarding which national court or arbitral tribunal has jurisdiction.

Smart contracts should therefore be permitted to contain an express choice-of-forum clause identifying the competent court or arbitral institution, subject to applicable mandatory rules. Clear international rules concerning jurisdiction would improve predictability, prevent competing jurisdictional claims, and reduce unnecessary procedural disputes.

The proposed framework should also distinguish between choice of court and choice of arbitration, because these mechanisms are subject to different international legal regimes. In the case of arbitration, the parties' agreement should be interpreted consistently with international standards governing the recognition and enforcement of arbitration agreements and arbitral awards (United Nations, 1958).

7. Mandatory Code-Auditing Standards

Because smart contracts operate through computer code, legal regulation should address the possibility of programming errors, security vulnerabilities, malicious exploitation, and unintended execution. A regulatory framework should therefore establish mandatory or risk-based code-auditing standards for smart contracts used in significant commercial transactions.

Independent technical audits could assess the functionality, security, accuracy, and reliability of the underlying code and determine whether the technical implementation corresponds to the parties' contractual intentions. Code auditing should also identify vulnerabilities that could result in unauthorized transfers, manipulation, exploitation, or unintended contractual performance.

This requirement is particularly important because the automated execution of a smart contract may produce legal and economic consequences even when the underlying code contains an error. Accordingly, the proposed regulatory model should establish rules concerning responsibility for coding errors, audit failures, inadequate disclosure of

vulnerabilities, and discrepancies between the legal agreement and its technical implementation.

8. Digital Consumer Protection

The use of smart contracts in digital markets creates particular risks for consumers because contractual obligations may be automatically executed without meaningful opportunities for intervention, modification, or correction. Consumers may also face difficulties understanding technical code or determining the legal consequences of automated contractual execution.

An international regulatory framework should therefore establish minimum consumer-protection standards, including transparency, informed consent, disclosure of contractual terms, protection against unfair contractual provisions, and mechanisms for addressing erroneous or unauthorized transactions.

Consumer protection is particularly important where smart contracts are used in decentralized platforms, digital marketplaces, financial services, digital assets, and other cross-border digital transactions. The regulatory framework should ensure that technological automation does not undermine fundamental principles of consumer protection or create an imbalance of contractual power between businesses and consumers.

9. Cybersecurity Standards

Cybersecurity should constitute an essential component of any international regulatory framework for smart contracts. Vulnerabilities in smart-contract code, blockchain infrastructure, digital wallets, external data sources, or oracle mechanisms may result in significant financial and legal consequences.

International standards should therefore establish minimum cybersecurity requirements, including risk assessment, vulnerability testing, security auditing, incident-response mechanisms, access controls, and appropriate safeguards against unauthorized access, manipulation, and exploitation.

Cybersecurity regulation should also recognize that blockchain security is not limited to the blockchain protocol itself. Risks may arise from smart-contract code, private-key management, external applications, bridges, oracles, and other technological components connected to the blockchain ecosystem. Consequently, the proposed regulatory framework should adopt a comprehensive and risk-based approach to cybersecurity.

10. Cross-Border Enforcement Mechanisms

The effectiveness of smart-contract regulation ultimately depends upon the ability to enforce contractual rights and dispute-resolution outcomes across jurisdictions. An international framework should therefore establish mechanisms for the recognition and enforcement of judgments, arbitral awards, and other legally binding decisions relating to smart-contract transactions.

Cross-border enforcement rules should be compatible with existing international instruments, particularly the New York Convention concerning foreign arbitral awards (United Nations, 1958). At the same time, the framework should address the specific characteristics of blockchain-based transactions, including the identification of parties, the location of digital assets, the evidentiary status of blockchain records, and the relationship between automated execution and judicial or arbitral remedies.

Effective cross-border enforcement would ensure that legal rights recognized in one jurisdiction can be meaningfully protected and enforced in another. Without effective enforcement mechanisms, formal recognition of smart contracts would provide limited practical value.

Integrated Regulatory Model

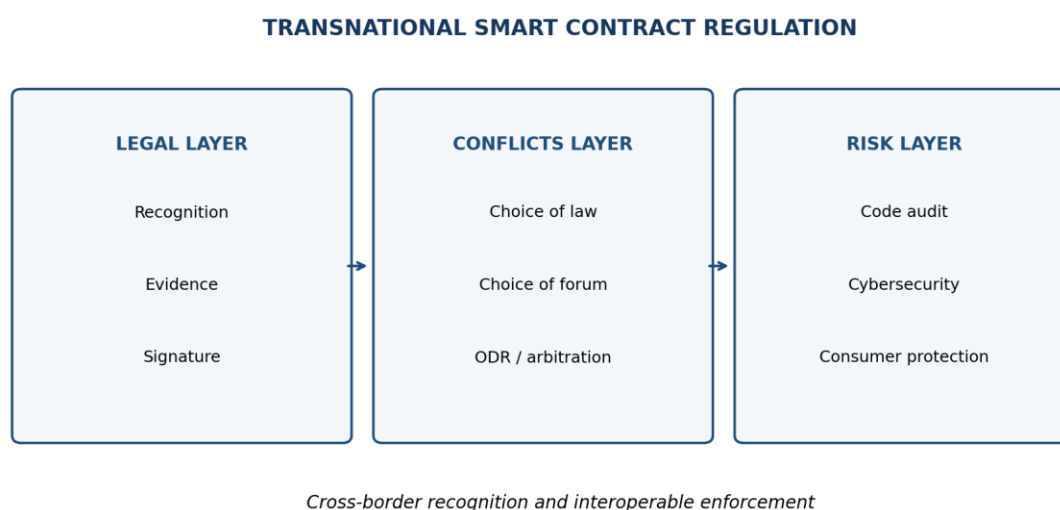
Taken together, these ten elements constitute an integrated regulatory framework for smart contracts. The proposed model does not seek to replace existing national contract laws. Rather,

it seeks to establish common international principles and minimum standards capable of reducing regulatory fragmentation and increasing legal certainty in cross-border blockchain transactions.

The proposed regulatory structure may therefore be conceptualized as follows:

International Legal Recognition ↓ Blockchain-Based Evidence ↓ Digital Signatures ↓ Dispute Resolution ↓ Choice of Law ↓ Choice of Forum ↓ Code Auditing ↓ Consumer Protection ↓ Cybersecurity ↓ Cross-Border Enforcement

These ten elements support the broader concept of Transnational Smart Contract Regulation, which integrates the principles of legal certainty, international legal harmonization, and law and technology into a coherent regulatory framework for cross-border blockchain transactions.



Source: Authors' formulation, 2026.

Figure 1. Transnational Smart Contract Regulation architecture

The central argument of this research is that smart contracts require a regulatory approach that goes beyond traditional territorial contract law. Because blockchain transactions may involve parties from different jurisdictions and automated execution through decentralized technological infrastructure, their regulation requires greater international coordination and harmonization.

Accordingly, this research proposes the development of a more specific UNCITRAL-oriented framework for smart contracts, building upon the existing UNCITRAL Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signatures, the UNCITRAL Model Law on Electronic Transferable Records, and, most importantly, the UNCITRAL Model Law on Automated Contracting 2024 (UNCITRAL, 2024).

The proposed Transnational Smart Contract Regulation may therefore serve as a conceptual foundation for further development of international legislative standards addressing jurisdiction, applicable law, digital evidence, automated contractual performance, dispute resolution, cybersecurity, consumer protection, and cross-border enforcement.

Model Law on Electronic Transferable Records (2017), and the Model Law on Automated Contracting (2024). The latter expressly covers smart contracts and provides an important contemporary foundation for further development of transnational smart-contract regulation.

Such a model could serve as the foundation for the harmonization of international business law in the digital economy era (Dalhuisen, 2022).

This research contributes to the development of international business law through the formulation of the concept of Transnational Smart Contract Regulation, which integrates the theories of legal certainty, legal harmonization, and law and technology within a unified cross-border regulatory framework. This concept may serve as a basis for the development of a new international instrument under the auspices of the United Nations Commission on International Trade Law (UNCITRAL) to address jurisdictional issues, choice of law, and legal enforcement challenges arising from global blockchain transactions.

Case Chronology

Company A, a corporation domiciled and incorporated in Indonesia, entered into an investment transaction through a Decentralized Finance (DeFi) platform developed and operated by Company B, a corporation established and domiciled in Singapore. The transaction was conducted entirely through a blockchain-based smart contract, without the involvement of conventional intermediary institutions, such as banks, securities firms, or other financial service providers (Szabo, 1996; De Filippi & Wright, 2018).

The smart contract incorporated an automated liquidation clause designed to manage the risk associated with fluctuations in the value of the crypto-assets deposited by Company A. Under the relevant provision, if the market value of the crypto-assets fell below a predetermined threshold, the smart contract would automatically activate the liquidation mechanism and dispose of the relevant assets without requiring further consent, instruction, or intervention from either party. Such automated execution represents one of the principal characteristics of smart contracts, namely the ability of contractual terms to be translated into computer code and automatically executed when predefined conditions are satisfied (Raskin, 2017; Szabo, 1997).

During a period of extreme volatility in the crypto-asset market, the value of the assets held by Company A declined rapidly. The smart contract consequently detected that the predetermined liquidation threshold had been reached and automatically initiated the liquidation process. As a result, Company A's crypto-assets were liquidated, causing substantial financial losses to Company A.

Following the liquidation, Company A disputed the validity and correctness of the automated execution. Company A alleged that an algorithmic error or programming defect had caused the liquidation mechanism to be activated prematurely, before the contractual threshold had actually been reached. According to Company A, the execution of the code should not automatically be regarded as conclusive evidence of contractual compliance where the underlying code contains an error, malfunction, or inconsistency with the parties' legally agreed terms (Raskin, 2017).

In contrast, Company B rejected Company A's allegation and maintained that the smart contract had operated in accordance with its programmed parameters. Company B relied, among other things, on the technological principle commonly associated with blockchain transactions, namely "code is law." From this perspective, once the conditions encoded in the smart contract have been satisfied, the resulting transaction is automatically executed and recorded on the blockchain. The execution is therefore regarded by Company B as final and resistant to unilateral alteration (Wright & De Filippi, 2015).

The dispute consequently raises a fundamental legal question concerning the relationship between contractual intent, computer code, and legal enforceability. The central issue is whether the automatic execution of a smart contract should prevail where there is an alleged discrepancy between the programmed code and the parties' underlying contractual agreement (Raskin, 2017).

In particular, the dispute raises questions concerning whether an algorithmic error may constitute a breach of contract, a programming-related fault, or another legally recognized

ground for challenging the consequences of an automatically executed transaction. This issue demonstrates that the technological automation of contractual performance does not necessarily eliminate the application of conventional principles of contract law (Raskin, 2017; UNIDROIT, 2023).

The cross-border character of the transaction further complicates the legal analysis. Company A is established in Indonesia, whereas Company B is incorporated in Singapore, while the transaction itself was executed through a decentralized blockchain infrastructure that may involve nodes, validators, wallets, and digital assets operating across multiple jurisdictions. Consequently, determining the applicable law, jurisdiction, contractual liability, dispute-resolution mechanism, and enforcement of remedies may become substantially more complex than in conventional commercial transactions (UNIDROIT, 2023).

The absence of a conventional intermediary creates an additional regulatory challenge. In traditional financial transactions, intermediary institutions may perform functions relating to verification, supervision, transaction processing, dispute resolution, and investor protection. In a DeFi environment, these functions may be substantially reduced, decentralized, or replaced by automated technological mechanisms. This creates potential legal and regulatory uncertainty when an automated transaction produces an outcome that one party alleges to be inconsistent with the parties' contractual intention (UNIDROIT, 2023).

From the perspective of international business law, this dispute demonstrates that technological execution does not necessarily eliminate traditional legal questions concerning contract formation, contractual interpretation, liability, applicable law, jurisdiction, and remedies. The fact that a transaction is automatically executed through blockchain technology does not, by itself, resolve whether the underlying transaction satisfies the legal requirements applicable to cross-border commercial contracts (Raskin, 2017).

Accordingly, the case illustrates a broader tension between technological finality and legal certainty. The principle of “code is law” emphasizes predictability and technical finality, whereas conventional contract law emphasizes party autonomy, contractual intention, good faith, fairness, and the availability of legal remedies when contractual performance is defective (Wright & De Filippi, 2015; Raskin, 2017).

Where these two dimensions conflict, the absence of harmonized international rules may create uncertainty regarding the legal status and enforceability of smart contracts. This is particularly significant in cross-border transactions, where different jurisdictions may adopt different approaches to the legal recognition of digital assets, smart contracts, contractual liability, and dispute resolution.

The dispute between Company A and Company B therefore illustrates how the rapid development of blockchain-based DeFi transactions has outpaced the development and harmonization of international business law. The absence of uniform international rules governing smart-contract validity, algorithmic errors, liability, choice of law, jurisdiction, dispute resolution, and cross-border enforcement may create significant uncertainty for businesses engaging in blockchain-based transactions (UNCITRAL, 2022).

Consequently, the establishment of a harmonized international regulatory framework for blockchain-based smart contracts has become increasingly important. Such a framework should not merely regulate the technological operation of smart contracts, but should also establish legally predictable mechanisms for addressing discrepancies between code and contractual intent, allocating liability for algorithmic or oracle failures, determining applicable law and jurisdiction, providing effective dispute-resolution mechanisms, and ensuring the enforceability of remedies in cross-border transactions (UNCITRAL, 2022; UNIDROIT, 2023).

In this context, the Company A–Company B dispute can be understood as a representative case illustrating the regulatory and legal challenges of cross-border smart contracts in the DeFi

ecosystem. It demonstrates the necessity of reconciling technological principles such as automation, decentralization, immutability, and “code is law” with fundamental principles of international business law, particularly legal certainty, contractual autonomy, fairness, accountability, and effective legal protection (Raskin, 2017; UNCITRAL, 2022; UNIDROIT, 2023).

Regulatory Implications for Indonesia and International Business Actors

For Indonesia, regulatory reform should begin by clarifying that an electronic contract may be formed or performed through an automated system without losing legal effect solely because no natural person reviews each operational step. Such recognition should be framed through functional equivalence and technological neutrality, not through statutory endorsement of one blockchain architecture. The central legal inquiry remains whether the arrangement can reliably identify the relevant parties or attributed systems, preserve accessible contractual terms, demonstrate consent, and produce evidence whose integrity can be assessed. This approach allows existing principles under the Civil Code and electronic-transactions legislation to remain operative while filling the uncertainty surrounding machine-generated communications and automated performance. It also prevents the mistaken conclusion that every deployed program is necessarily a contract. Some programs merely perform part of an agreement, while others coordinate transactions without containing the full legal relationship. Regulation should therefore distinguish a smart legal contract, whose legally operative terms are partly expressed or performed in code, from software that has no independent contractual status.

A second implication concerns the hierarchy between natural-language terms and executable code. Commercial parties should be permitted to determine that hierarchy expressly, but mandatory law must prevail over both. A dual-layer agreement should identify which provisions are authoritative when the prose and code diverge, explain the events that trigger automated performance, state the source and method of external data, and allocate responsibility for coding and oracle failures. In the absence of an express hierarchy, adjudicators should reconstruct the parties’ objectively manifested intention by considering the negotiated text, technical documentation, interface disclosures, audit records, transaction history, and surrounding commercial purpose. Technical execution is relevant evidence of performance, but it should not create an irrebuttable presumption that the legal obligation was correctly performed. This distinction is essential because immutability describes the persistence of a ledger entry; it does not determine the validity of consent, eliminate mistake or fraud, or prevent a court or tribunal from ordering restitution, damages, or corrective performance through a subsequent transaction.

Third, responsibility should be allocated according to function, control, knowledge, and risk creation. The contracting parties remain responsible for their commercial promises, yet other actors may assume distinct duties when they exercise meaningful control over the technical environment. A developer may be responsible where negligent design or undisclosed vulnerabilities cause foreseeable loss; an auditor may be responsible within the scope of its engagement where it fails to apply an appropriate professional standard; an oracle provider may bear responsibility for unreliable or manipulated data; and a platform operator may incur duties when it controls user access, governance, upgrades, or emergency intervention. Conversely, open-source contributors should not automatically be treated as contractual guarantors merely because their code is reused. A risk-based regime must avoid both extremes: complete immunity based on decentralization and unlimited liability based only on technological involvement. Clear disclosure, causation, reasonable security practices, contractual allocation, and the ability to prevent or mitigate harm should guide responsibility.

Fourth, the proposed framework requires procedural mechanisms capable of translating blockchain facts into legally cognizable evidence. A transaction hash can demonstrate that

particular data existed on a ledger at a given stage, but it does not independently prove the identity, capacity, intention, or authority of the person associated with a wallet. Courts and arbitral tribunals therefore need standards for connecting on-chain records with off-chain evidence, authenticating wallet control, evaluating digital signatures, preserving forensic data, and explaining technical evidence through qualified experts. Parties should be required to retain human-readable copies of relevant terms, version histories, audit reports, oracle inputs, and governance decisions. Evidentiary standards should remain technology-neutral while recognizing the distinctive probative value of distributed records. This enables judges and arbitrators to benefit from blockchain integrity without treating technical opacity as proof of correctness or shifting an impossible burden onto the weaker party.

Fifth, effective dispute design must be embedded before deployment. Cross-border smart contracts should contain an accessible governing-law clause, a valid choice-of-court or arbitration agreement, a service-of-notice mechanism, and procedures for urgent relief. Where immediate and irreversible execution may create disproportionate harm, risk-sensitive pause, escrow, multi-signature, or reversal mechanisms should be considered. Online dispute resolution can reduce cost and delay, particularly for high-volume transactions, but it must preserve notice, impartiality, the opportunity to present evidence, reasoned outcomes where appropriate, and access to judicial review required by mandatory law. Blockchain-based arbitration may record procedural events or facilitate automated compliance, yet arbitral authority and award enforcement still depend on consent and established international instruments. Regulatory design should therefore connect technical remedies with the New York Convention rather than assume that a decentralized protocol can replace public enforcement.

Sixth, implementation should be phased and coordinated. Indonesian policymakers could first issue interpretive guidance and regulatory sandboxes for narrowly defined business uses, followed by amendments that recognize automated contracting and establish minimum safeguards. High-risk applications involving consumers, financial services, essential assets, or large-value transactions should face stronger requirements for independent audits, incident reporting, explainability, and corrective controls than low-risk business-to-business applications. Regulators should coordinate with standards bodies, arbitral institutions, cybersecurity authorities, consumer-protection agencies, and industry associations. At the international level, adoption of common UNCITRAL-oriented principles would permit states to preserve domestic public policy while reducing conflicts in recognition, attribution, evidence, and enforcement. Harmonization need not mean identical legislation; it means ensuring that different legal systems can reach compatible outcomes on the core legal effects of automated contracting.

For international business actors, the practical lesson is that technological certainty and legal certainty must be designed together. Before deployment, parties should conduct legal mapping across relevant jurisdictions, document the relationship between prose and code, audit the program and connected infrastructure, test extreme scenarios, allocate insurance and liability, and select dispute and enforcement mechanisms. They should also assess sanctions, anti-money-laundering rules, data protection, consumer law, taxation, insolvency, and sector-specific licensing because smart-contract recognition does not displace these obligations. Continuous governance is equally important: software upgrades, changes to oracle sources, cybersecurity incidents, and shifts in regulatory classification can alter the risk profile after formation. A legally resilient smart contract is therefore not a self-sufficient piece of code but a governed socio-technical arrangement supported by intelligible terms, accountable actors, reliable evidence, and enforceable remedies.

The research novelty lies in the Transnational Smart Contract Regulation model, which does not equate legal recognition with sufficient regulation. It connects three layers that are usually treated separately: a legal layer for recognition, attribution, signatures, and evidence; a

conflict-of-laws layer for party autonomy, forum selection, dispute resolution, and enforcement; and a risk-governance layer for code auditing, cybersecurity, oracle accountability, and consumer protection. This integrated architecture converts the abstract demand for harmonization into ten minimum regulatory components and a hierarchy of responsibility. Code may automate performance, but it does not displace the legal agreement, mandatory law, or corrective authority. The model therefore offers both a conceptual contribution to international business law and an operational basis for an UNCITRAL-oriented instrument or coordinated national reform.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Blockchain-based smart contracts represent a significant innovation in the evolution of international business law, offering enhanced efficiency, transparency, and security in commercial transactions (Szabo, 1996; De Filippi & Wright, 2018). Nevertheless, the implementation of such technology gives rise to various legal challenges concerning contractual validity, jurisdiction, applicable law, dispute resolution mechanisms, and the cross-border enforcement of legal obligations (Raskin, 2017).

The absence of a harmonized international regulatory framework has resulted in considerable legal uncertainty for participants in global commerce (Wright & De Filippi, 2015). Accordingly, there is a pressing need for the harmonization of international legal norms through the development of a dedicated legal instrument capable of comprehensively regulating smart contracts and their cross-jurisdictional operation (UNCITRAL, 1996, 2017b, 2024).

In this regard, a UNCITRAL Smart Contract Framework may serve as a viable legal model for establishing greater legal certainty while simultaneously fostering the sustainable growth of digital trade and the broader digital economy at the international level (UNCITRAL, 2024).

Accordingly, smart contracts should be recognized as technologically mediated contractual arrangements whose legal effect remains conditioned by consent, legality, capacity, good faith, and mandatory protections. The comparative analysis shows that the United States, European Union, and Singapore offer useful but partial solutions, while Indonesia continues to rely on general contract and electronic-transaction law. Harmonization is necessary because territorial rules cannot alone resolve distributed performance, algorithmic failures, or enforcement across jurisdictions. The proposed model answers this deficit by integrating ten minimum standards under a coherent transnational framework.

Limitations

This study is limited to normative and comparative analysis of selected jurisdictions and international instruments. It does not measure market behavior, judicial outcomes, audit costs, or the technical performance of particular blockchain protocols. The Company A–Company B scenario is illustrative rather than an adjudicated dispute. Regulatory developments in digital assets also evolve rapidly; consequently, the proposed model must be tested against future legislation, sector-specific requirements, and empirical data from businesses, developers, consumers, arbitral institutions, and regulators.

Recommendations

UNCITRAL should consider developing implementation guidance or a supplementary instrument for blockchain-based automated contracts that operationalizes the Model Law on Automated Contracting. Indonesia should expressly recognize automated contracting while regulating the relationship between natural-language terms and executable code, allocation of responsibility for developers and oracle providers, risk-based code audits, electronic evidence,

consumer safeguards, and dispute-resolution clauses. Businesses should employ dual-layer agreements, disclose code risks, select governing law and forum, provide pause or correction functions where proportionate, retain auditable records, and establish cybersecurity and incident-response procedures. Future research should empirically test the model and examine its compatibility with insolvency, taxation, competition, data protection, and sectoral financial regulation.

Author Contributions

All authors contributed significantly to the conceptualization of the study, development of the theoretical framework, collection and analysis of legal materials, comparative assessment, formulation of the regulatory model, preparation of the manuscript, scholarly revision, and approval of the final version.

Acknowledgment

The authors express their appreciation to their respective institutions and academic colleagues whose discussions supported the development and refinement of this research.

REFERENCES

- Allen, J. G. (2018). Wrapped and stacked: Smart contracts and the interaction of natural and formal language. *European Review of Private Law*, 26(4), 307–343.
- Arizona Revised Statutes § 44-7061 (2017).
- Brownsword, R. (2019). *Law, technology and society: Re-imagining the regulatory environment*. Routledge.
- Dalhuisen, J. H. (2022). *Dalhuisen on transnational comparative, commercial, financial and trade law*. Hart Publishing.
- De Cruz, P. (2016). *Comparative law in a changing world* (3rd ed.). Routledge.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Dickinson, A. (2010). *The Rome II Regulation: The law applicable to non-contractual obligations*. Oxford University Press.
- European Commission. (2020). *A European strategy for data*. European Union.
- European Commission. (2023). *A Europe fit for the digital age*. European Union.
- European Union. (2022a). *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)*.
- European Union. (2022b). *Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act)*.
- European Union. (2023a). *Regulation (EU) 2023/1114 on markets in crypto-assets*.
- European Union. (2023b). *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*.
- Glenn, H. P. (2014). *Legal traditions of the world* (5th ed.). Oxford University Press.
- Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Edward Elgar Publishing.
- Indonesia. (2019). *Government Regulation Number 71 of 2019 concerning the implementation of electronic systems and transactions*.
- Indonesia. (2023). *Law Number 4 of 2023 concerning development and strengthening of the financial sector*.
- Indonesia. (2024). *Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 on electronic information and transactions*.
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Levy, K. E. C. (2017). Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, 3, 1–25.

- Marzuki, P. M. (2019). Pengantar ilmu hukum. Kencana.
- Monetary Authority of Singapore. (2020). Project Ubin: Central bank digital money using distributed ledger technology.
- Monetary Authority of Singapore. (2024). Singapore FinTech ecosystem report.
- Nevada Revised Statutes, Chapter 719 (2017).
- Pramono, N. (2021). Hukum kontrak di Indonesia. Kencana.
- Radbruch, G. (1932). Legal philosophy. Harvard University Press.
- Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review*, 1(2), 304–341.
- Reed, C. (2012). Making laws for cyberspace. Oxford University Press.
- Reyes, C. L. (2018). Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation. *Villanova Law Review*, 61, 191–234.
- Singapore. (2010). Electronic Transactions Act 2010 (2021 Revised Edition).
- Singapore. (2019). Payment Services Act 2019.
- Szabo, N. (1996). Smart contracts: Building blocks for digital markets.
- Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9).
- Tennessee Code Annotated § 47-10-201 et seq. (2018).
- UNCITRAL. (1996). Model Law on Electronic Commerce. United Nations.
- UNCITRAL. (2001). Model Law on Electronic Signatures. United Nations.
- UNCITRAL. (2005). United Nations Convention on the Use of Electronic Communications in International Contracts. United Nations.
- UNCITRAL. (2017a). Technical Notes on Online Dispute Resolution. United Nations.
- UNCITRAL. (2017b). Model Law on Electronic Transferable Records. United Nations.
- UNCITRAL. (2022). Taxonomy of legal issues related to the digital economy. United Nations.
- UNCITRAL. (2024). Model Law on Automated Contracting. United Nations.
- UNCTAD. (2024). Digital economy report 2024. United Nations.
- UNIDROIT. (2016). Principles of International Commercial Contracts 2016.
- UNIDROIT. (2023). Principles on Digital Assets and Private Law.
- United Nations. (1958). Convention on the Recognition and Enforcement of Foreign Arbitral Awards.
- Van Hoecke, M. (2002). Law as communication. Hart Publishing.
- Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, 67, 313–382.
- Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*.