

Universal Digital Law Codex (UDLC): Building the Legal Infrastructure for the Digital Era

Andreas Furrer¹ & Wulf Kaal²

Abstract

The emergence of Web3 technologies, including distributed ledger technology (DLT), smart contracts, digital assets, and artificial intelligence (AI), has revolutionized global commerce by enabling decentralized, automated, and borderless transactions. However, their integration into traditional legal systems presents significant challenges, including disruptions to digital assets and contract formation in common and civil law jurisdictions, enforceability issues in civil law systems, jurisdictional conflicts in cross-border transactions, and normative deficiencies in the "code is law" paradigm. These challenges, compounded by a fragmented global regulatory landscape, threaten legal certainty, compliance, and innovation.

This article proposes the Universal Digital Law Codex (UDLC) as a comprehensive legal framework developed as a first draft³ by Andreas Furrer, Wulf Kaal, and Stephan D. Meyer.⁴ UDLC addresses these issues and fosters a robust infrastructure for the digital era. UDLC integrates DLT, AI, and quantum computing into existing legal systems through minimum legal requirements, dynamic compliance mechanisms, and decentralized dispute resolution, ensuring smart contracts align with common and civil law principles. By promoting legal interoperability, respecting jurisdictional diversity, and embedding decentralized governance, UDLC mitigates cross-jurisdictional conflicts and overcomes the limitations of "code is law." Drawing on a critical analysis of global regulatory initiatives, such as UNCITRAL's Model Laws, and exemplified by its application in decentralized dispute resolution mechanisms, this study demonstrates UDLC's transformative potential to ensure legal certainty, trust, and sustainable growth in Web3 markets across diverse legal systems.

Keywords: Smart contract, Web3, Dynamic Regulation, Sunset Provisions, Web3 Governance, Token Models, Cryptocurrencies, Feedback Effects, Emerging Technology, Tokens, Distributed Ledger Technology

JEL Categories: K20, K23, K32, L43, L5, O31, O32

¹ Professor of Law, University of Lucern, Switzerland.

² Professor of Law, University of St. Thomas, Minneapolis, MN, USA. The author is grateful for excellent research assistance from Nicole Katlin, research librarian, and Mickey Bernardi, research assistant.

³ <https://www.udec-association.org/> - UDLC Codex in separate SSRN document.

⁴ Technology Lawyer, Switzerland.

Table of Contents

1. Introduction	1
2. Existing Assessments	2
2.1 Smart Contracts Challenge to Traditional Contract Formation in Common and Civil Law Jurisdictions	2
2.1.1 Disruption of Offer and Acceptance	3
2.1.2 Consideration and Economic Viability	4
2.1.3 Enforceability and External Intervention	4
2.1.4 Legal Adaptation and Regulatory Challenges	5
2.2 Reconciling Harmonization Tendencies	6
2.2.1 Eradicating Outliers and Impeding Innovation	6
2.3 Application of Conflict of Laws Principles to Digital Assets Across Common Law and Civil Law Jurisdictions	6
2.3.1 Jurisdictional Determination in Digital Asset Disputes	7
2.3.2 Choice of Law for Digital Assets	8
2.3.3 Preserving Decentralized Innovation in Digital Asset Governance	9
2.4 Enforcement Challenges Across Jurisdictions	9
2.5 Stifling Jurisdictional Diversity	10
2.5.1 Alternative Approaches to Cross-Jurisdictional Challenges	10
2.6 Dispute Resolution Involving Real World Assets (RWA) Tokenized Through Smart Contracts	10
2.6.1 Online Dispute Resolution (ODR) for Tokenized RWAs	11
2.6.2 Decentralized Dispute Resolution (DDR) Mechanisms	11
2.6.3 Escrow-Based Enforcement Mechanisms	12
2.6.4 Challenges and Future Directions	13
3. Code is Law	13
3.1 Authority: Code vs. Sovereign Law	14
3.2 Flexibility: Determinism vs. Interpretive Discretion	14
3.3 Enforcement: Automation vs. Human Adjudication	15
3.4 Normative Legitimacy: Technological Neutrality vs. Moral Deliberation	15
4. Legal Frameworks and Global Initiatives	16
4.1 General Legal Frameworks in Digital Transactions	16
4.2 Specific Rules in Blockchain Transactions	19
4.2.1 UNCITRAL	19
4.2.2 UNIDROIT	20
4.2.3 UNIDROIT and Hague Conference on Private International Law (HCCH)	21
4.3 Specific Rules for Artificial Intelligence	22
4.3.1 OECD-Principles	22
4.3.2 UNESCO Initiative	23
4.3.3 Council of Europe	24
4.3.4 Self-Regulation	25
4.3.5 Comparative Perspectives	25

4.4 Convergence in Digital Transaction Frameworks	26
4.4.1 Emerging Blockchain Frameworks	26
4.4.2 Search for a Common Framework in AI	27
4.4.3 International Regulatory Instruments	27
5. Normative Analysis	28
5.1 Automation in Code is Law	28
5.2 Authority: Technocratic Protocols vs. Sovereign Legitimacy	29
5.3 Flexibility: Deterministic Execution vs. Legal Adaptability	29
5.4 Enforcement: Automated Rigidity vs. Human Discretion	29
6. UDLC	30
6.1 Positioning UDLC between code and national law	30
6.2 Resolving Challenges in Smart Contract Formation	30
6.3 Ensuring Enforceability of Mandatory Law	32
6.4 Mitigating Conflict of Laws and Jurisdictional Challenges	32
6.5 Overcoming Limitations of the “Code is Law” Paradigm	33
6.6 Practical Implementation: The Arbitration DAO Case Study	34
7. Conclusion	34

1. Introduction

The advent of Web3 technologies, encompassing distributed ledger technology (DLT), smart contracts, digital assets, and artificial intelligence (AI), heralds a paradigm shift in global commerce and governance, promising unprecedented levels of automation, decentralization, and efficiency. These innovations, rooted in blockchain architectures, enable self-executing contracts, tokenized representations of digital and real-world assets (which we address as Digital Objects), and borderless transactions, fundamentally reshaping traditional economic and legal interactions.

However, their integration into existing legal frameworks presents multifaceted challenges that threaten to undermine their transformative potential. In both common and civil law jurisdictions, smart contracts disrupt foundational principles of contract formation, such as offer and acceptance, consideration, and enforceability, due to their automated, immutable execution, which lacks the flexibility of law, which is based on human negotiation and judicial oversight. The self-executing nature of smart contracts conflicts with codified formalities, interpretive discretion, and mandatory judicial remedies, rendering their enforceability uncertain. Cross-jurisdictional transactions involving digital objects further complicate matters, as the decentralized, pseudonymous nature of blockchain obscures territorial connections, creating ambiguity in jurisdictional determination, choice of law, and enforcement. Moreover, the "code is law" paradigm, which posits that software code governs behavior with the same authority as traditional law, introduces normative deficiencies, including technocratic authority, deterministic enforcement, and a lack of moral deliberation, fostering unethical behavior in anonymous transactions and eroding social trust.

These legal and ethical challenges are compounded by the fragmented global regulatory landscape, where national and international frameworks struggle to keep pace with technological advancements. Existing initiatives, such as the UNCITRAL Model Laws and the European Union's Markets in Crypto-Assets Regulation (MiCAR), provide partial solutions but fail to address the full spectrum of issues, particularly the need for interoperable, adaptive governance that preserves blockchain's decentralized ethos. The push for harmonized legal standards, while aimed at enhancing certainty, risks stifling jurisdictional diversity and innovation by imposing centralized frameworks antithetical to Web3's principles. Concurrently, the absence of standardized protocols for dispute resolution and compliance with regulations, such as export controls, hinders the scalability of tokenized real-world assets (RWAs) and other blockchain-based applications. Without a cohesive legal infrastructure, these technologies face barriers to adoption, regulatory arbitrage, and potential systemic risks, necessitating a novel approach to governance in the digital era.

The jurisdiction of a national court and the application of national law to disputes arising from smart contracts cannot be excluded because almost all legal systems provide the parties to contracts with an emergency jurisdiction if they can prove that they would otherwise be unable to bring their action: Such exorbitant or emergency jurisdictions are often linked to the nationality, registered office or place of performance of one of the

parties. The court with jurisdiction will then determine the governing law on the basis of its own conflict of laws rules and decide on the dispute. Thus, national law matters and must be taken into account in all transactions, including those involving smart contracts, blockchains, or AI.

This article proposes the Universal Digital Law Codex (UDLC) as a comprehensive solution to these challenges, offering a hybrid legal framework that integrates DLT, AI, and emerging technologies into existing legal systems while fostering innovation, compliance, and trust. UDLC addresses the disruptions in contract formation by establishing minimum legal requirements and dynamic compliance mechanisms, ensuring smart contracts align with common and civil law principles. It enhances enforceability through decentralized dispute resolution and precedent systems, balancing automation with judicial oversight. For cross-jurisdictional issues, UDLC promotes legal interoperability by aligning with international standards and embedding choice-of-law protocols, while its hybrid governance model respects local diversity. To counter the normative deficiencies of “code is law,” UDLC introduces decentralized governance, reputation systems, and culturally sensitive AI frameworks, aligning technological efficiency with societal values.

Through a detailed analysis of these challenges and the global regulatory landscape, this study elucidates UDLC’s role as a transformative framework, exemplified by its practical application in platforms like the Arbitration DAO, in building the legal infrastructure for the digital age, ensuring the sustainable evolution of Web3 markets across diverse legal systems.

2. Existing Assessments

2.1 Smart Contracts Challenge to Traditional Contract Formation in Common and Civil Law Jurisdictions

The advent of EVM-type smart contracts, enabled by blockchain technology, presents a transformative paradigm for contractual arrangements, challenging foundational principles of contract formation in common law jurisdictions. Such smart contracts challenge traditional concepts of contract formation in common law jurisdictions by automating offer and acceptance, complicating consideration through economic and physical limitations, and straining enforceability due to their reliance on immutable code. Law systems must balance the efficiency of smart contracts with the need for legal certainty, ensuring that technological innovation aligns with statutory principles and public policy.

While law’s flexibility offers potential solutions, as seen in analogies to vending machines, the need for external intervention and regulatory adaptation highlights the limitations of fully autonomous contracts. Legal scholarship underscores that smart contracts cannot wholly supplant traditional contract law, necessitating a hybrid approach that leverages existing frameworks while addressing novel technological realities. As blockchain technology evolves, common and civil law jurisdictions must balance innovation with legal certainty to ensure smart contracts align with established

principles of contractual obligation. This paper examines how smart contracts disrupt traditional concepts of offer, acceptance, consideration, and enforceability, drawing on critical legal scholarship to elucidate the tensions between technological innovation and established legal frameworks.

By analyzing the limitations of smart contracts' autonomy, the necessity of external intervention, and the adaptability of law, this analysis underscores the need for a nuanced legal approach to integrate smart contracts into existing contractual paradigms.

2.1.1 Disruption of Offer and Acceptance

Common law and civil law jurisdictions have one core feature in common: contract formation hinges on a clear offer and acceptance, manifesting mutual assent between parties. Smart contracts, defined as self-executing computer protocols that automate contract terms on a blockchain, challenge this paradigm by replacing human negotiation with predefined code. Goldenfein and Leiter describe the development of “machine-readable transaction modules” that correspond to natural language contracting elements, suggesting that smart contracts standardize and automate the offer-acceptance process.⁵ This automation eliminates traditional bargaining, as parties assent to coded terms without iterative dialogue, raising questions about whether such assent meets the common law requirement of a “meeting of the minds.”

Szczerbowski defines smart contracts as “event-driven programs” that express declarations of will through self-executing code, capable of transferring assets without judicial intervention.⁶ Szczerbowski argues that in civil law the “form and interpretation” of smart contracts pose significant hurdles, as their coded terms may not fully capture the nuanced declarations of will central to civil law contracts.⁷ For example, ambiguities in code or discrepancies between coded terms and parties' subjective intentions cannot be resolved through traditional interpretive methods, potentially leading to disputes that courts are ill-equipped to adjudicate. Zakharkina and Kuznetsova emphasize that the “functional nature” of smart contracts complicates their integration into civil law frameworks, as their self-executing mechanisms may conflict with judicial authority to modify or void contracts based on principles like good faith or unconscionability.⁸ In civil law systems, where courts often prioritize equitable outcomes over strict adherence to terms, the rigidity of smart contracts may result in unenforceable agreements if they fail to align with mandatory legal principles or public policy.

The irrevocability of blockchain transactions complicates the revocation of offers or acceptances. Once a smart contract is deployed, its execution is immutable absent

⁵ Jake Goldenfein & Andrea Leiter, *Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct*, 29 L. & CRITIQUE 141, 144 (2018).

⁶ Jakub J. Szczerbowski, *Place of Smart Contracts in Civil Law: A Few Comments on Form and Interpretation*, in PROC. 12TH ANN. INT'L SCI. CONF. 333 (2018), available at <https://ssrn.com/abstract=3095933>.

⁷ *Id.*

⁸ Anna Zakharkina & Olga Kuznetsova, *Foreign Civil Doctrine of Smart Contracts*, 134 SHS WEB CONF. 00016 (2022), <https://doi.org/10.1051/shsconf/202213400016>.

external intervention, contrasting with common and civil law's allowance for offer withdrawal before acceptance. Schroeder argues that the "logical limitations of all languages, including computer code," prevent smart contracts from fully capturing the dynamic intent required for traditional contract formation.⁹ This rigidity suggests that smart contracts may not align with the flexible, intent-driven nature of offer and acceptance in law.

2.1.2 Consideration and Economic Viability

Consideration, a cornerstone of contracts, requires a bargained-for exchange of value. Smart contracts ostensibly satisfy this requirement through automated exchanges, such as cryptocurrency transfers for goods or services. However, Schroeder highlights the economic impracticality of smart contracts due to the "time value of money," noting that posting cryptocurrency to escrow-like smart contracts is often uneconomic compared to traditional financial instruments.¹⁰ This inefficiency challenges the practical utility of smart contracts as a vehicle for consideration, particularly in high-value or long-term agreements.

Additionally, the physical delivery of goods in sales contracts introduces complexities. Schroeder emphasizes that the necessity of transferring physical possession of conforming goods means breach remains possible, undermining the autonomy of smart contracts.¹¹ Unlike digital assets, physical goods cannot be fully governed by code, requiring external mechanisms to verify compliance with contractual terms. This limitation suggests that smart contracts may struggle to fulfill the consideration requirement in contexts requiring tangible performance, deviating from the parties' justified expectation of enforceable mutual obligations.

2.1.3 Enforceability and External Intervention

Enforceability in law relies on judicial remedies to address breaches or disputes, yet smart contracts' self-executing nature seeks to minimize such interventions. Rühl argues that smart contracts "need contract law just as other, traditional contracts," as their coded parameters cannot fully supplant legal oversight.¹² The immutability of blockchain-based contracts means they cannot be altered by judicial order, creating enforceability challenges when disputes arise outside the code's scope, such as defective performance or unforeseen circumstances.

Szczerbowski notes that the ability of smart contracts to "take custody over and transfer assets" raises questions about their "legality" within civil law frameworks, as such autonomy may bypass mandatory remedies like rescission or damages.¹³ For instance, a smart contract that automatically transfers funds upon a coded condition may execute

⁹ Jeanne L. Schroeder, *Sense, Sensibility and Smart Contracts: A View from a Contract Lawyer*, 49 No. 2 UCC L.J. ART. 2, 2 (2020).

¹⁰ *Id.* at 7-9.

¹¹ *Id.* at 11-17.

¹² Giesela Rühl, *Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts?*, in BLOCKCHAIN, LAW & GOVERNANCE 159, 160 (2021).

¹³ Szczerbowski, *supra* note 6, at 333.

despite a party's claim of mistake or duress, leaving courts unable to intervene post-execution due to blockchain's immutability.

Goldenfein and Leiter note the development of “technological and institutional” tools to “soften the effects of self-executing” transactions, indicating a reliance on external dispute resolution mechanisms.¹⁴ For instance, smart contracts cannot enforce remedies like specific performance for non-coded actions, necessitating traditional legal frameworks. Rohr draws an analogy to vending machines, suggesting that common law's flexibility can adapt to smart contracts by treating them as automated, yet legally binding, transactions.¹⁵ However, this adaptability is strained when smart contracts, such as those enabling automatic collateral repossession, violate legal norms like the UCC's restrictions on strict foreclosure.¹⁶

2.1.4 Legal Adaptation and Regulatory Challenges

The integration of smart contracts into national law frameworks raises questions about whether existing contract law suffices or if new legislative schemes are needed. Rohr advocates for the sufficiency of common law, citing its historical adaptability to technological innovations¹⁷ which is also true for civil law jurisdictions. Conversely, Giancaspro warns that smart contracts face “considerable difficulty adapting to current legal frameworks” due to issues of legal and practical enforceability across jurisdictions.¹⁸ This tension is particularly evident in cross-jurisdictional transactions, where private international law must determine applicable contract law.¹⁹

Grinhaus underscores the regulatory complexities, noting that smart contracts implicate multiple legal disciplines, including securities law and anti-money laundering regulations, which common law alone may not adequately address.²⁰ The absence of standardized rules for smart contract disputes, as Rohr observes, further complicates their integration into national law jurisdictions.²¹

Szczerbowski advocates for setting “boundaries to their legality” by defining the scope of smart contracts within civil law, particularly regarding permissible transactions and mandatory formalities.²² Without such boundaries, smart contracts risk being deemed unenforceable in jurisdictions that prioritize statutory compliance over technological innovation. The development of international standards, as suggested by Zakharkina

¹⁴ Goldenfein & Leiter, *supra* note 5, at 141-142.

¹⁵ Jonathan G. Rohr, *Smart Contracts and Traditional Contract Law, or: The Law of the Vending Machine*, 67 CLEV. ST. L. REV. 67, 85 (2019).

¹⁶ Schroeder, *supra* note 9, at 30-32.

¹⁷ Rohr, *supra* note 15, at 73.

¹⁸ Mark Giancaspro, *Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective*, 33 COMPUT. L. & SEC. REV. 825 (2017).

¹⁹ Rühl, *supra* note 12, at 163.

²⁰ Aaron Grinhaus, *Part 4, Smart Contracts*, in WEB3, BLOCKCHAIN, AND SMART CONTRACT LAW: U.S. AND INTERNATIONAL PERSPECTIVES (Matthew Bender & Co. 2023).

²¹ Rohr, *supra* note 15, at 73.

²² Szczerbowski, *supra* note 6, at 333.

and Kuznetsova, could further enhance enforceability by harmonizing approaches to smart contract regulation across civil law systems.²³

2.2 Reconciling Harmonization Tendencies

The divergent approaches of common and civil law jurisdictions have led some to conclude that the need for harmonized conflict of laws principles to govern digital assets is key. Aleinieh and Zoboli emphasize that standardization could mitigate cross-jurisdictional conflicts by establishing common rules for smart contract interpretation and enforcement.²⁴ Atiyah et al. highlight the UAE's innovative regulatory framework as a model, suggesting that blockchain-based dispute resolution platforms could streamline enforcement across jurisdictions.²⁵ Kasatkina proposes the development of “crypto-legal structures” to address the peculiarities of smart contracts, advocating for international cooperation to align common and civil law approaches.²⁶

2.2.1 Eradicating Outliers and Impeding Innovation

Harmonization's most pernicious effect lies in its eradication of outliers—those unconventional approaches that drive technological and legal innovation. Kasatkina's proposal for “crypto-legal structures” through international cooperation assumes that uniformity is a prerequisite for legal certainty.²⁷ However, blockchain's history demonstrates that breakthroughs, such as decentralized finance (DeFi) protocols and non-fungible tokens (NFTs), often emerge from fringe experiments that challenge established norms. By standardizing conflict of laws principles, harmonization risks eliminating these outliers, constraining the iterative process through which jurisdictions refine solutions to novel challenges like smart contract disputes or digital asset ownership.

2.3 Application of Conflict of Laws Principles to Digital Assets Across Common Law and Civil Law Jurisdictions

The proliferation of digital assets has precipitated complex legal challenges in cross-jurisdictional transactions, particularly in the application of conflict of laws principles. These principles, which determine the applicable law and jurisdiction for disputes, are strained by the decentralized, borderless nature of digital assets.

Conflict of laws principles face significant challenges in governing digital assets across common law and civil law jurisdictions, driven by the decentralized, immutable nature of

²³ Zakharkina & Kuznetsova, *supra* note 8, at 4-5.

²⁴ Tarek Kadour Aleinieh & Laura Zobolit, *Increasing standardization for smart(er) contracts*, 26 UNIF. L. REV. 583, 596 (2021), <https://dx.doi.org/10.1093/ulr/unab022>.

²⁵ Ghassan Adhab Atiyah et al., *Enforcement of Smart Contracts in Cross-Jurisdictional Transactions*, INT'L J.L. & MGMT 12 (2024), <http://dx.doi.org/10.1108/IJLMA-06-2024-0220>.

²⁶ Marina Kasatkina, *The Interpretation of Smart Contracts in the EU and the USA*, 7 INT'L COMPAR. JURIS. 202, 213-214 (2021), <https://doi.org/10.13165/j.icj.2021.12.007>.

²⁷ *Id.*

blockchain technology. Jurisdictional determination is complicated by the lack of territorial connections, choice of law varies due to interpretive differences, and enforcement is hindered by smart contracts' autonomy. While common law systems leverage flexible precedents and civil law systems rely on statutory frameworks, both struggle to adapt to digital assets' unique characteristics.²⁸ Harmonized standards and innovative dispute resolution mechanisms offer potential solutions, but run short of fulfilling the ever evolving technical requirements in the rapid evolution of digital assets and smart contracts.

This paper examines how conflict of laws principles apply to digital assets across common law and civil law jurisdictions, focusing on jurisdictional determination, choice of law, and enforcement challenges. Drawing on scholarly analyses, we examine the tensions between technological innovation and traditional private international law frameworks.

2.3.1 Jurisdictional Determination in Digital Asset Disputes

Conflict of laws principles prioritize identifying the appropriate jurisdiction for disputes, a task complicated by the decentralized nature of digital assets. In common law jurisdictions, such as the United States and the United Kingdom,²⁹ courts often rely on territorial connections, such as the location of parties or assets, to assert jurisdiction. Wyczik notes that common law systems, particularly in the U.K. and U.S., adapt property law to digital assets by recognizing them as intangible property, enabling jurisdictional claims based on the domicile of the owner or the platform hosting the asset.³⁰ However, the pseudonymous and distributed nature of blockchain transactions often obscures these connections, challenging traditional jurisdictional tests.

Most civil law jurisdictions such as Poland, Germany, Switzerland or China have enacted statutory Codes for conflicts of law for determining jurisdiction and governing law. Wyczik highlights that civil law systems struggle to classify digital assets within rigid property law categories, often requiring legislative updates to establish jurisdiction.³¹ Atiyah et al. underscore the variability in jurisdictional approaches, noting that the U.S. benefits from robust electronic transaction laws, while jurisdictions like Iraq lag in recognizing digital assets, complicating cross-border disputes.³² The Sydney Node symposium emphasizes that blockchain's immutability exacerbates jurisdictional issues, as courts may lack authority over decentralized ledgers.³³

²⁸ For the UK see Law Comm'n, *Digital Assets: Final Report* (Law Com No 412, 2023); Law Comm'n, *Digital Assets as Personal Property: Supplemental Report and Draft Bill* (Law Com No 416, 2024), <https://lawcom.gov.uk/project/digital-assets/>.

²⁹ See the Consultation process of The Law Commission, open until 8 September 2025, <https://lawcom.gov.uk/project/digital-assets-and-electronic-trade-documents-in-private-international-law/>.

³⁰ Jakub Wyczik, *Ownership in the 21st Century: Property Law of Digital Assets*, 32 INFO. & COMM'NS TECH. L. 187, 198 (2024), <https://doi.org/10.1080/13600834.2024.2408917>

³¹ *Id.* at 200.

³² Atiyah et al., *supra* note 25 at 4-6.

³³ Philippa Ryan et al., *Sydney Node, 2018 Computational Law & Blockchain Festival, Discuss Track Symposium Report (Part 2 of 2)*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 113, 125 (2019), <https://stanford-jblp.pubpub.org/pub/sydney-2/release/1>.

2.3.2 Choice of Law for Digital Assets

Determining the applicable law for digital asset transactions is a critical aspect of conflict of laws, with significant divergences between common law and civil law approaches.³⁴ Common and civil law jurisdictions often apply the law of the forum or the law chosen by the parties, provided it has a reasonable connection to the transaction. Kasatkina argues that common law systems, particularly in the U.S., adapt existing contract law to smart contracts, treating them as legally binding agreements subject to traditional choice-of-law rules.³⁵ However, the absence of explicit choice-of-law clauses in smart contracts, which are often coded without reference to jurisdiction, complicates this process.

In civil law jurisdictions, choice of law is governed by statutory rules, such as the EU's Rome I Regulation,³⁶ which prioritizes the choice of jurisdiction and law by the parties, subsequently the law of the parties' the place of performance or habitual residence. Kasatkina notes that civil law systems apply traditional contract law principles to smart contracts, but their coded nature may conflict with mandatory statutory requirements.³⁷ Aleinieh and Zoboli highlight the interpretive differences between civil and common law systems, with civil law's reliance on codified interpretation clashing with common law's flexible, precedent-based approach, affecting the choice of law for digital assets.³⁸ Atiyah et al. suggest that blockchain's role in standardizing transactions could facilitate choice-of-law determinations by embedding jurisdictional markers in smart contracts.³⁹

The claim that harmonized conflict-of-law rules for digital assets are needed to increase legal certainty is at odds with the decentralized principles of blockchain technology. As shown above, all claims are anchored in national jurisdiction and therefore have a systemic element of centralization. However, such centralized legal frameworks undermine the diversity of legal systems, and harmonization of conflict of laws could eliminate the outliers in national legal systems that are crucial for innovation. Therefore, conflict-of-laws rules should be used to implement innovative national legal systems that utilize decentralized governance models and respect the autonomy of blockchain. This promotes adaptive, jurisdiction-specific solutions. Therefore, the option to use the conflict-of-laws rules to implement innovative national legal systems that utilize decentralized governance models and respect the autonomy of blockchain should be preserved. These approaches promotes adaptive, jurisdiction-specific solutions.

³⁴ See the comparative overview of Matthias Lehmann, *Kollisionsregeln für die Blockchain im Rechtsvergleich*, 122 ZEITSCHRIFT FÜR VERGLEICHENDE RECHTSWISSENSCHAFT 269-288 (2023).

³⁵ Kasatkina, *supra* note 26 at 209-210.

³⁶ Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), 2008 O.J. (L 177) 6, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0593>.

³⁷ Kasatkina, *supra* note 26, at 209-210.

³⁸ Aleinieh & Zoboli, *supra* note 24 at 593.

³⁹ Atiyah et al., *supra* note 25, at 16.

2.3.3 Preserving Decentralized Innovation in Digital Asset Governance

Blockchain technology, underpinning digital assets and smart contracts, is inherently designed to operate without centralized authority, fostering trust through distributed consensus mechanisms. The push for harmonized conflict of laws principles, as advocated by Aleinieh and Zoboli, seeks to impose standardized rules that centralize interpretive and enforcement frameworks.⁴⁰ The proposition that harmonized conflict of laws principles are necessary to govern digital assets across common law and civil law jurisdictions, as advocated by scholars like Aleinieh, Zoboli, Atiyah, and Kasatkina, misconstrues the foundational ethos of blockchain technology and undermines the innovative potential inherent in decentralized systems. We argue that a constructive balance to the inherent and unavoidable centralized characteristics of national law cannot be found in imposing uniform legal standards on digital assets as this favors the centralist features of law to the decentralized, permissionless nature of blockchain.

What is needed is an option that leverages the diversity of legal systems to promote continuous innovation. It is essential to strike a balance between the need for legal certainty and justified experimentation so that the rapidly changing technological landscape does not become entrenched and hinder the development of adaptable, context-specific smart contract and digital asset solutions.

2.4 Enforcement Challenges Across Jurisdictions

Enforcement of digital asset transactions, particularly those governed by smart contracts, poses significant challenges due to blockchain's immutability and cross-jurisdictional nature. In common law jurisdictions, courts can issue injunctions or damages to enforce contracts, but smart contracts' self-executing mechanisms limit judicial intervention post-execution. Ryan et al. note that immutability issues prevent courts from modifying or reversing blockchain transactions, necessitating alternative dispute resolution mechanisms like arbitration.⁴¹ The U.S.'s robust electronic transaction laws facilitate enforcement by recognizing digital signatures and contracts, but gaps remain for decentralized assets.⁴²

Civil law jurisdictions face greater enforcement hurdles because of the legal uncertainties on the legal qualification of digital assets. Wyczik observes that countries like Germany and Poland struggle to enforce digital asset rights because of unclear property law classifications, requiring courts to interpret the terms of ownership and possession expansively.⁴³ Kasatkina argues that the EU's harmonized frameworks, such as the eIDAS Regulation,⁴⁴ support enforcement by recognizing electronic transactions,

⁴⁰ Aleinieh & Zoboli, *supra* note 24 at 596.

⁴¹ Ryan et al., *supra* note 33, at 126.

⁴² Atiyah et al., *supra* note 25, at 9.

⁴³ Wyczik, *supra* note 30, at 199-202.

⁴⁴ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999-93-EC (eIDAS), 2014 O.J. (L 257) 73, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910>.

but smart contracts' decentralized execution often falls outside these frameworks.⁴⁵ Aleinieh and Zoboli advocate for legal standardization to enhance enforcement, suggesting that uniform rules could bridge interpretive gaps between civil and common law systems.⁴⁶

2.5 Stifling Jurisdictional Diversity

Jurisdictional diversity in common law and civil law systems, while complex, fosters a competitive legal environment that drives innovation in digital asset governance. Common law jurisdictions, with their flexible, precedent-based systems, and civil law jurisdictions, with their codified frameworks, offer distinct laboratories for testing legal adaptations to blockchain technology. Harmonization of the substantive law would suppress this diversity, imposing a one-size-fits-all model that fails to account for cultural, economic, and technological differences, thereby reducing the resilience of global digital asset ecosystems.

2.5.1 Alternative Approaches to Cross-Jurisdictional Challenges

Rather than pursuing harmonization, conflict of laws principles should embrace decentralized governance models that mirror blockchain's architecture. Jurisdictions could adopt flexible frameworks that recognize party autonomy in choosing applicable laws, as seen in some common law systems, while allowing civil law jurisdictions to adapt statutory interpretations contextually. Blockchain-based dispute resolution mechanisms, such as decentralized arbitration protocols (as proposed in UDLC), offer a viable alternative to centralized enforcement, preserving the technology's ethos without sacrificing legal recourse. These approaches maintain the diversity of legal experimentation, ensuring that solutions evolve organically in response to technological advancements.

2.6 Dispute Resolution Involving Real World Assets (RWA) Tokenized Through Smart Contracts

The tokenization of Real World Assets (RWAs) through smart contracts has helped evolve property transactions by facilitating virtual disintermediation and automation. However, disputes arising from these transactions necessitate smart contract based innovative dispute resolution mechanisms that align with the decentralized and self-executing nature of smart contracts.

Dispute resolution for RWAs tokenized through smart contracts encompasses Online Dispute Resolution (ODR), Decentralized Dispute Resolution (DDR), and escrow-based mechanisms, each offering distinct advantages in addressing the complexities of decentralized asset transactions. ODR provides accessible and flexible resolutions, DDR aligns with blockchain's decentralized ethos, and escrow mechanisms ensure automated enforcement.

⁴⁵ Kasatkina, *supra* note 26, at 210.

⁴⁶ Aleinieh & Zoboli, *supra* note 24 at 595.

However, challenges such as technical barriers, jurisdictional ambiguities, and governance risks necessitate ongoing refinement. By integrating hybrid approaches and leveraging emerging technologies like AI and oracles, these methods can enhance the fairness and efficiency of dispute resolution, supporting the global adoption of tokenized RWAs while preserving the integrity of blockchain-based systems. It is important to note that neither ODR nor DDR comply with the minimal requirements of due process as defined and acknowledged in the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards,⁴⁷ which is ratified and enforced in 172 States.

2.6.1 Online Dispute Resolution (ODR) for Tokenized RWAs

ODR has emerged as a primary method for addressing disputes involving tokenized RWAs, leveraging digital platforms to streamline adjudication. Schmitz and Rule advocate for ODR's integration into smart contract ecosystems, noting its capacity to provide efficient and fair resolutions without undermining the automation benefits of blockchain.⁴⁸ ODR platforms, such as those developed for blockchain settings, facilitate mediation or arbitration through virtual interfaces, accommodating disputes over tokenized assets like real estate or chattels. For instance, Garcia-Teruel and Simon-Moreno highlight that tokenized usufruct rights over RWAs require dispute resolution mechanisms to address ownership or transfer issues, which ODR can efficiently handle.⁴⁹

Despite its promise, ODR faces barriers, including limited adoption and concerns over transparency. Rabinovich-Einy and Katsh note that while ODR schemes for blockchain exist, their uptake remains low due to technical complexity and lack of user trust.⁵⁰ Kalantarova proposes mandatory ODR with oracles acting as arbitrators, suggesting a structured process to enhance legal enforceability in smart contract disputes.⁵¹ This approach could apply to tokenized RWAs, ensuring disputes over asset-backed tokens are resolved equitably.

2.6.2 Decentralized Dispute Resolution (DDR) Mechanisms

DDR represents a blockchain-native approach to resolving disputes involving tokenized RWAs, utilizing distributed networks and smart contracts to replace traditional intermediaries. Salger identifies two DDR models: Expert-Pooling and Crowdarbitration. Expert-Pooling involves jurors forming anonymous “expert pools” to adjudicate disputes,

⁴⁷ Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 3, <https://www.newyorkconvention.org/english>.

⁴⁸ Amy J. Schmitz & Colin Rule, *Online Dispute Resolution for Smart Contracts*, 2019 J. DISP. RESOL. 103, 122-124, <https://scholarship.law.missouri.edu/facpubs/726>.

⁴⁹ Rosa M. Garcia-Teruel & Hector Simon-Moreno, *The Digital Tokenization of Property Rights: A Comparative Perspective*, 41 COMPUT. L. & SEC. REV. 8, 11-12 (2021), <https://doi.org/10.1016/j.clsr.2021.105543>.

⁵⁰ Orna Rabinovich-Einy & Ethan Katsh, *Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution*, 2019 J. DISP. RESOL. 47, 74, <https://scholarship.law.missouri.edu/jdr/vol2019/iss2/6>.

⁵¹ Rakhil Kalantarova, *The Ongoing Speculation About Smart Contracts: Smart Enough to Replace Third Party Arbitrators, or Is “Smart” Just A Misnomer?*, 21 CARDOZO J. CONFLICT RESOL. 551, 576-577 (2020), <https://larc.cardozo.yu.edu/cjcr/vol21/iss2/12>.

while Crowdarbitration employs game-theoretic principles, such as the Schelling Point, to incentivize collective decision-making.⁵² These methods are particularly suited for tokenized RWAs, as they align with the decentralized governance of blockchain platforms described by Garcia-Teruel and Simon-Moreno.⁵³

Ast and Deffains describe DDR as “decentralized justice,” emphasizing its potential to radically enhance dispute resolution efficiency through juror networks and smart contract automation.⁵⁴ For tokenized RWAs, DDR can address disputes over ownership or transfer rights by leveraging community-driven consensus, reducing reliance on centralized courts. However, Salger cautions that DDR’s reliance on participant incentives and technical expertise may limit its scalability and fairness, particularly in complex RWA disputes.⁵⁵

2.6.3 Escrow-Based Enforcement Mechanisms

Escrow-based mechanisms, integrated into smart contracts, provide an automated method for dispute resolution and enforcement in tokenized RWA transactions. Salger explains that smart contracts can execute arbitral awards through escrow arrangements, holding tokenized assets until dispute resolution conditions are met.⁵⁶ This approach is particularly relevant for RWAs, as it ensures that ownership transfers, such as those described by Garcia-Teruel and Simon-Moreno, occur only upon verification of contractual compliance.⁵⁷

Zhao and Chen highlight the “preauthorization” model, exemplified by platforms like Taobao, where funds or assets are held in escrow until disputes are resolved, enhancing trust in tokenized transactions.⁵⁸ For tokenized RWAs, escrow mechanisms can mitigate risks of non-delivery or misrepresentation, but their effectiveness depends on robust smart contract design and oracle integration to verify real-world conditions. Schmitz and Rule note that poorly designed escrow systems may exacerbate disputes if transparency or fairness is compromised.⁵⁹

⁵² Christoph Salger, *Decentralized Dispute Resolution: Using Blockchain Technology and Smart Contracts in Arbitration*, 24 PEPP. DISP. RESOL. L.J. 65, 73–78 (2024), <https://digitalcommons.pepperdine.edu/drlj/vol24/iss1/2>.

⁵³ Garcia-Teruel & Simon-Moreno, *supra* note 49, at 9-10.

⁵⁴ Federico Ast & Bruno Deffains, *When Online Dispute Resolution Meets Blockchain: The Birth of Decentralized Justice*, 4 STAN. J. BLOCKCHAIN L. & POL’Y 241, 247 (2021), <https://stanford-jblp.pubpub.org/pub/birth-of-decentralized-justice>.

⁵⁵ Salger, *supra* note 52, at 86-89.

⁵⁶ Salger, *supra* note 52, at 72-73.

⁵⁷ Garcia-Teruel & Simon-Moreno, *supra* note 49, at 6.

⁵⁸ Yun Zhao & Hui Chen, *Enhancing Access to Digital Justice: Digital Governance of Dispute Resolution and Dispute Prevention in Online Commercial Activities*, 15 J. INT’L DISP. SETTLEMENT 273, 290-302 (2024), <https://doi.org/10.1093/jnlids/idae001>.

⁵⁹ Schmitz & Rule, *supra* note 48, at 123.

2.6.4 Challenges and Future Directions

The current methods for dispute resolution involving tokenized RWAs—ODR, DDR, and escrow-based mechanisms—offer innovative solutions but face significant challenges. Rabinovich-Einy and Katsh underscore barriers to ODR adoption, including technical complexity and jurisdictional uncertainties.⁶⁰ DDR's reliance on decentralized networks raises concerns about juror competence and bias, as noted by Salger.⁶¹ Escrow mechanisms, while effective for automation, require reliable oracles and robust governance to prevent manipulation, as emphasized by Zhao and Chen.⁶²

Future developments should focus on hybrid models that combine ODR's accessibility, DDR's decentralization, and escrow's automation. The integration of AI-driven analytics into DDR could enhance decision-making accuracy for RWA disputes. Additionally, Kalantarova's proposal for oracle-based arbitration could standardize dispute resolution processes, ensuring compatibility with tokenized RWA platforms.⁶³

3. Code is Law

The notion of "code is law," pioneered by Lawrence Lessig,⁶⁴ posits that software code, particularly in digital architectures like blockchain and smart contracts, exerts a regulatory force akin to traditional legal systems, shaping behavior through technical constraints. This concept challenges the foundational principles of existing legal systems, which rely on human-crafted statutes, judicial discretion, and societal norms to govern conduct.

The concept of "code is law," as extended by scholars like De Filippi, Wright, and Werbach,⁶⁵ fundamentally contrasts with existing legal systems by shifting authority from sovereign institutions to technical protocols, replacing interpretive flexibility with deterministic enforcement, and substituting normative deliberation with technological neutrality. These contrasts challenge the accountability, adaptability, and moral legitimacy of traditional law, raising critical questions about the governance of digital environments. While code offers efficiency and autonomy, its divergence from legal systems' human-centric principles necessitates a hybrid approach that integrates technological innovation with the equitable, deliberative frameworks of law.

We examine how "code is law" contrasts with traditional legal systems in terms of authority, flexibility, enforcement, and normative legitimacy, highlighting the tensions between deterministic technological governance and the adaptive, interpretive nature of law. Drawing on seminal works, including Lessig's foundational scholarship, this analysis elucidates the implications of code-driven regulation for legal theory and

⁶⁰ Rabinovich-Einy & Katsh, *supra* note 50, at 72-75.

⁶¹ Salger, *supra* note 52, at 83-86.

⁶² Zhao & Chen, *supra* note 58, at 287.

⁶³ Kalantarova, *supra* note 51, at 578.

⁶⁴ LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

⁶⁵ PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 51 (2018).

practice. We critique the traditional scholarship on code is law through the work of Wulf Kaal.

3.1 Authority: Code vs. Sovereign Law

Traditional legal systems derive authority from sovereign institutions—legislatures, courts, and administrative bodies—grounded in democratic or constitutional legitimacy. In contrast, "code is law" vests authority in decentralized technological architectures, where programmers and network protocols dictate rules. Lessig argues that code, as embedded in digital systems, regulates behavior with immediacy and inescapability, bypassing traditional political processes.⁶⁶ This shift from sovereign to technical authority undermines the participatory mechanisms that legitimize legal systems, as code lacks the deliberative input of affected communities.

As already discussed above, national courts and laws remain relevant to smart-contract disputes because most legal systems grant 'exorbitant' or 'emergency' jurisdiction when a party would otherwise lack a forum, usually tied to nationality, registered office, or performance place. Once seized, the court applies its conflict-of-laws rules to select the governing law, so national law still underpins all blockchain and AI transactions.

Primavera De Filippi and Aaron Wright extend this critique, noting that blockchain-based systems, such as smart contracts, encode rules that operate autonomously, independent of state oversight.⁶⁷ Unlike traditional law, which is subject to amendment through legislative or judicial processes, code's authority stems from its immutability and consensus-driven protocols, raising questions about accountability.⁶⁸

3.2 Flexibility: Determinism vs. Interpretive Discretion

Legal systems in both common and civil law traditions are characterized by flexibility, allowing courts to interpret statutes, balance equities, and adapt to societal changes. In contrast, "code is law" enforces rules with deterministic precision, leaving little room for contextual interpretation. Lessig emphasizes that code's rigidity—its ability to perfectly constrain behavior—differs starkly from law's ambiguity, which permits judicial discretion to address unforeseen circumstances.⁶⁹ For instance, a smart contract executing a flawed transaction cannot be altered post-deployment, unlike a contract subject to equitable remedies.

Kevin Werbach critiques this inflexibility, arguing that code's inability to incorporate moral or situational nuance contrasts with legal systems' capacity to evolve through precedent or statutory reform.⁷⁰ In civil law jurisdictions, where codified rules are

⁶⁶ LESSIG, *supra* note 64.

⁶⁷ DE FILIPPI & WRIGHT, *supra* note 67 at 34.

⁶⁸ LAWRENCE LESSIG, CODE: VERSION 2.0 5, 124, 323-24 (2006).

⁶⁹ *Id.* at 124-32.

⁷⁰ KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 150-153 (2018); *cf.* Wulf A. Kaal, *AI Governance Via Web3 Reputation System*, 8 STAN. J. BLOCKCHAIN L. & POL'Y 1 (2025), (arguing that coded automation leads inevitably to corruption of the system and needs to be supplemented with decentralized governance of code, thus leading to preferable outcomes and improved ethics).

interpreted with reference to legislative intent, code's literalism disrupts the hermeneutic process.⁷¹

3.3 Enforcement: Automation vs. Human Adjudication

Enforcement in traditional legal systems relies on human institutions—courts, regulators, and law enforcement—to interpret and apply sanctions, often with discretion to ensure proportionality. The "code is law" paradigm automates enforcement through self-executing protocols, such as smart contracts, which execute outcomes without human intervention. Lessig warns that this automation creates a "perfectly regulable space," where violations are impossible because code preemptively constrains actions.⁷² For example, a blockchain-based escrow releases funds upon coded conditions, regardless of external disputes.

De Filippi and Wright highlight that this automated enforcement bypasses traditional remedies, such as injunctions or damages, limiting recourse for aggrieved parties.⁷³ Unlike legal systems, which balance enforcement with fairness, code's binary execution lacks mechanisms for appeal or mitigation, challenging notions of justice.⁷⁴

3.4 Normative Legitimacy: Technological Neutrality vs. Moral Deliberation

Traditional legal systems derive normative legitimacy from moral deliberation, reflecting societal values through democratic processes or judicial reasoning. In contrast, "code is law" operates on a premise of technological neutrality, where rules are dictated by functionality rather than ethical considerations. Lessig critiques this absence of normative grounding, arguing that code embeds the values of its creators—often unelected technologists—without public scrutiny.⁷⁵ For instance, a smart contract prioritizing efficiency may ignore distributive justice, a core concern of legal systems.

Werbach further contends that blockchain's reliance on code as law risks creating "trustless" systems that erode the social trust underpinning legal.⁷⁶ In common law systems, where precedent reflects evolving societal norms, and civil law systems, where codes embody collective values, code's agnosticism to moral deliberation starkly contrasts with law's normative framework.⁷⁷

⁷¹ Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 555-56, 582-83 (1998).

⁷² LESSIG, *supra* note 68 at 38, 62.

⁷³ DE FILIPPI & WRIGHT, *supra* note 67, at 74-76.

⁷⁴ JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 256-257 (2012).

⁷⁵ LESSIG, *supra* note 64, at 59.

⁷⁶ WERBACH, *supra* note 70, at 95-111.

⁷⁷ Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

4. Legal Frameworks and Global Initiatives

4.1 General Legal Frameworks in Digital Transactions

Efforts to harmonize digital transaction law began in the 1990s when electronic communications and the nascent Internet started to revolutionize commerce. UNCITRAL took the lead in creating general legal rules that allow contracts and documents to be formed and executed electronically with the same legal certainty as paper documents.

The UNCITRAL Model Law on Electronic Commerce (1996)⁷⁸ is a cornerstone instrument that established fundamental principles for e-commerce. The Model Law requires electronic messages and records to receive legal recognition equivalent to traditional writings. This embodies the ideas of functional equivalence and technology neutrality. The Model Law also prohibits discrimination against electronic forms, meaning that laws should not deny the validity of a contract or record solely because it is in electronic format. The 1996 Model Law removed impediments to digital contracting across jurisdictions by providing uniform rules on matters such as electronic signatures, the time and place of dispatch/receipt of electronic communications, and the use of electronic documents in areas such as the carriage of goods. The impact of this model law has been global. Legislation based on or influenced by the Model Law has been adopted in 87 states across 170 jurisdictions.⁷⁹ This remarkable uptake underscores how a non-binding model law can achieve broad international consensus and significantly harmonize national laws.

UNCITRAL then adopted the Model Law on Electronic Signatures (2001)⁸⁰ to bolster trust in electronic transactions. The Model-Law set out criteria for the legal validity of electronic signatures and encouraged a risk-based approach to signature technologies. It required that these technologies be as reliable and appropriate as necessary for the purpose at hand. The Model-Law established the principle that electronically signed records are equivalent to hand-signed paper documents if certain reliability standards are met. Forty states⁸¹ have implemented laws influenced by the Model Law, reflecting a widespread consensus that electronic authentication methods can securely replace ink signatures in commerce. Notably, countries with different legal traditions (e.g., common law and civil law) have adopted these core principles of electronic contracting and signatures, often using UNCITRAL texts as templates for domestic legislation.

⁷⁸ U.N. Comm'n on Int'l Trade L., *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* 1996, U.N. Sales No. E.99.V.4 (1999), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

⁷⁹ U.N. Comm'n on Int'l Trade L., Status: UNCITRAL Model Law on Electronic Commerce (1996), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce/status (last visited July 20, 2025).

⁸⁰ U.N. Comm'n on Int'l Trade L., *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment* 2001, U.N. Sales No. E.02.V.8 (2002), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.

⁸¹ U.N. Comm'n on Int'l Trade L., Status: UNCITRAL Model Law on Electronic Signatures (2001), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status (last visited July 20, 2025).

In addition to model laws, UNCITRAL introduced a significant binding instrument: the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).⁸² Often called the "Electronic Communications Convention," this treaty builds upon earlier UNCITRAL principles and extends them to the international level. It ensures that emails and other electronic communications are recognized for the formation and performance of cross-border contracts. The Convention affirms that a contract should not be denied validity solely because it was formed through electronic communication. It also harmonizes rules regarding the time and place of dispatch and receipt of electronic messages. These are critical issues in determining contract formation and jurisdiction in international transactions. While the Convention's content aligns with the model laws, its legal form differs: as an international convention, it becomes binding law for states that ratify it. As of mid-2025, the Electronic Communications Convention had 20 Contracting States (it entered into force in 2013 after the requisite ratifications).⁸³ These Contracting States include countries from various regions, such as Singapore, Russia, Honduras, and Cameroon. However, several major trading states have not ratified the treaty. Many countries, including the United States, Japan, and European Union members, have achieved the Convention's objectives by implementing equivalent rules in their contract and commerce laws without formally acceding to the treaty.

This pattern illustrates a common dynamic in digital law: binding conventions often see only moderate adoption. Nevertheless, their principles may permeate national legislation inspired by the convention, yielding de facto harmonization.

Overall, the UNCITRAL texts on electronic commerce have established a globally accepted baseline for digital transactions. Key solutions, such as the legal equivalence of electronic and paper documents and the validity of electronic signatures, have achieved near-universal recognition. These solutions are based on the idea of eliminating legal distinctions based on the medium used. What matters is the information and intent conveyed, not whether a document is on paper or digital.

This approach, sometimes called "media neutrality", has been adopted in UNCITRAL's instruments and influential regional frameworks. For instance, the principles of the 1996 Model Law are reflected in the European Union's E-Commerce Directive⁸⁴ and eIDAS Regulation⁸⁵, as well as in the United States' E-SIGN Act⁸⁶ and Uniform Electronic

⁸² U.N. Comm'n on Int'l Trade L., *United Nations Convention on the Use of Electronic Communications in International Contracts*, opened for signature Nov. 23, 2005, 2898 U.N.T.S. 3, https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications.

⁸³ U.N. Comm'n on Int'l Trade L., Status: United Nations Convention on the Use of Electronic Communications in International Contracts, https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications/status (last visited July 27, 2025).

⁸⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1, <http://data.europa.eu/eli/dir/2000/31/oj>.

⁸⁵ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, 2014 O.J. (L 257) 73, <http://data.europa.eu/eli/reg/2014/910/oj>.

⁸⁶ Fed. Deposit Ins. Corp., *Electronic Signatures in Global and National Commerce Act*, in CONSUMER COMPLIANCE EXAMINATION MANUAL (Jan. 2014),

Transactions Act,⁸⁷ demonstrating the Model Law's influence on civil and common law jurisdictions alike. Additionally, while not specific to electronic commerce, the 2015 Principles on Choice of Law in International Commercial Contracts of the Hague Conference on Private International Law (HCCH)⁸⁸ complement these frameworks by confirming party autonomy in choosing the governing law for international contracts (including those formed electronically) and by providing default conflict-of-law rules. Though non-binding, the 2015 HCCH Principles have been widely referenced and adopted in national conflict-of-law rules, furthering the legal environment for cross-border digital agreements.

UNCITRAL has continued to update the general law of digital transactions to address new developments. In 2017, UNCITRAL approved the Model Law on Electronic Transferable Records (MLETR),⁸⁹ which extends the functional equivalence principle to negotiable instruments and documents of title, such as promissory notes, bills of lading, and warehouse receipts, in electronic form. The MLETR establishes legal standards for the use of transferable records on distributed ledgers or other electronic systems. It enables entirely paperless trade transactions while ensuring that an electronic record can fulfill the same functions of uniqueness, control, and negotiability as a paper document. Although the MLETR is nonbinding, it is gaining traction. As of 2024, it has been adopted (in full or with modifications) by ten jurisdictions, including Bahrain (2018), Singapore (2021), the Abu Dhabi Global Market (a jurisdiction within the UAE, 2021), Paraguay, and, most recently, France and the United Kingdom.⁹⁰ Notably, the U.K.'s adoption in 2023 via the Electronic Trade Documents Act brought a G7 economy into alignment with the UNCITRAL approach. This trend suggests a growing international consensus on the legal treatment of electronic transferable documents, which were historically one of the last bastions of paper in commerce.

Another recent instrument that straddles general e-commerce and emerging technology is the 2024 UNCITRAL Model Law on Automated Contracting.⁹¹ In recognition of the increasing prevalence of contracts formed by algorithms or AI agents without direct human involvement, this model law establishes rules to ensure the validity and attribution of such contracts to the parties that deploy the automated systems. The law addresses issues of liability and error in automated transactions, aiming to establish international consistency as businesses increasingly rely on smart contracts and AI-driven negotiations. Adopted by UNCITRAL in 2024, the law is currently under

<https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf>.

⁸⁷ Uniform Electronic Transactions Act (Unif. L. Comm'n 1999), <https://www.uniformlaws.org/viewdocument/final-act-21?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments>.

⁸⁸ Hague Conf. on Priv. Int'l L., Principles on Choice of Law in International Commercial Contracts (approved Mar. 19, 2015), <https://www.hcch.net/en/instruments/conventions/full-text/?cid=135>.

⁸⁹ U.N. Comm'n on Int'l Trade L., UNCITRAL Model Law on Electronic Transferable Records (adopted July 13, 2017), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records.

⁹⁰ U.N. Comm'n on Int'l Trade L., Status: UNCITRAL Model Law on Electronic Transferable Records, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status (last visited July 27, 2025).

⁹¹ U.N. Comm'n on Int'l Trade L., *UNCITRAL Model Law on Automated Contracting*, in REPORT OF THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW, 94-96, <https://doi.org/10.18356/9789211070392>.

consideration for adoption in several jurisdictions, including Singapore, the European Union, and Australia. Early interest in adoption indicates that states recognize the need to update domestic contract law in light of AI and are looking to the UNCITRAL draft as a guiding framework.

In summary, the general rules for digital transactions established through UNCITRAL and related initiatives have laid the groundwork for internationally recognized legal principles, including electronic equivalence, technology neutrality, party autonomy, and the adaptability of traditional legal concepts, such as "writing" and "signature," to new digital forms. Many of these principles are embodied in non-binding models or soft law, but they have been broadly incorporated into binding national laws worldwide.

Meanwhile, targeted binding conventions, such as the Electronic Communications Convention, provide uniform rules for states willing to commit internationally. The interplay of soft and hard law has largely been successful in doctrinal terms. Today, there is a high degree of global consensus on how a contract can be formed electronically and how an e-signature can satisfy legal signature requirements. These general rules have set the stage for addressing more specific issues raised by blockchain technologies and AI. New legal frameworks WILL build upon and depart from established digital transaction principles.

4.2 Specific Rules in Blockchain Transactions

Blockchain and distributed ledger technologies (DLT) introduce decentralization into digital transactions, raising distinct legal issues that general e-commerce laws do not adequately address. Traditional electronic commerce often relies on identified parties, central intermediaries, and easily determined jurisdictions. In contrast, blockchain transactions involve decentralized networks, pseudonymous participants, and assets that exist purely as digital tokens.

This challenges traditional legal concepts of ownership, transfer, and trust. In response, various global frameworks have emerged, primarily in the form of model laws, principles, and regulatory guidelines, to provide legal certainty for blockchain-based transactions and digital assets.

In addition to the international model laws and principles that will be discussed next, national and regional regulators have established specific rules for blockchain-based activities, particularly those related to crypto-assets and financial stability.

4.2.1 UNCITRAL

One significant effort at the international level is the aforementioned UNCITRAL Model Law on Electronic Transferable Records (2017), which is highly relevant to blockchain technology. Although it is a general e-commerce text, it has had the greatest practical impact on trade finance and supply chain use cases of distributed ledger technology (DLT). The MLETR establishes that a singular, exclusive digital record can embody the same rights as a paper document, thereby enabling electronic negotiable instruments (like bills of lading or bills of exchange). The MLETR sets out criteria for an electronic

record to be deemed a "transferable record," focusing on functional equivalence. For example, it ensures that the electronic record can perform the function of providing control to one person at a time, much as possession of a paper document would.

The adoption of this model law in multiple jurisdictions, including Bahrain, Singapore, the UAE (ADGM), the UK, and France, demonstrates a growing consensus that blockchain and other electronic platforms can lawfully replace paper documents, provided that certain safeguards are met. Bahrain's 2018 law and Singapore's Electronic Transactions Act of 2021, for example, both explicitly implement UNCITRAL's rules to recognize blockchain-based trade documents. This facilitates paperless trade transactions across borders. Similarly, the U.K.'s 2023 Act allows digital trade documents influenced by the MLETR's principles.

Although the MLETR is not a binding treaty, its widespread adoption indicates an emerging international legal standard. Countries are aligning on how to give legal status to tokens or electronic records representing goods or financial instruments. This is a foundational step for broader blockchain commerce.

4.2.2 UNIDROIT

The International Institute for the Unification of Private Law (UNIDROIT) led a project addressing digital assets more generally, resulting in the UNIDROIT Principles on Digital Assets and Private Law (2023).⁹² This comprehensive set of non-binding principles and legislative guidance addresses the private law aspects of digital assets. Essentially, it treats certain digital records, such as cryptocurrencies, non-fungible tokens, and other tokenized assets, as objects of property and contractual transactions.

The UNIDROIT Principles explain how the concept of control can serve as a substitute for the possession of intangible digital assets, how transfers of digital assets can be completed definitively, what rights third-party acquirers have, and what responsibilities intermediaries (such as custodial wallet providers or exchanges) have to their clients. The Principles also address conflict of laws, offering approaches to determine which jurisdiction's law applies to a cross-border digital asset transaction.

These principles are not subject to ratification and have no legal force unless enacted domestically; however, they carry significant persuasive weight. Adopted by UNIDROIT's Governing Council in 2023 following input from experts worldwide, these principles are already being studied by governments and law reform bodies in Switzerland, the European Union, and Singapore for potential integration into their national legal frameworks. For example, the European Union has signaled interest in ensuring consistency with UNIDROIT's guidance as it develops its own digital asset market regulations.

⁹² Int'l Inst. for the Unif. of Priv. L., *UNIDROIT Principles on Digital Assets and Private Law* (2023), <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>.

Adopting the UNIDROIT Principles would promote substantive harmonization in how countries treat digital tokens. For example, it would define when a buyer of Bitcoin obtains good title and how security interests in tokens can be created and enforced. Even without a binding effect, these principles serve as an authoritative reference that courts and legislators worldwide can use to answer new legal questions about blockchain assets.

4.2.3 UNIDROIT and Hague Conference on Private International Law (HCCH)

Another key international project is being pursued jointly by UNIDROIT and the Hague Conference on Private International Law (HCCH):⁹³ a framework for determining the applicable law to cross-border holdings and transfers of digital assets and tokens. As of 2025, this initiative is still in progress and seeks to fill a critical gap. In the borderless realm of blockchain, parties and courts struggle to decide which country's law governs disputes. For example, if a hacker overseas steals a crypto asset or if a DeFi contract spans users globally, the applicable law for such a dispute should be clear.

The joint HCCH-UNIDROIT project aims to develop principles or a model law to guide the analysis of conflicts of laws for digital assets. Issues under consideration include connecting factors for digital assets, since traditional location-based tests are ill-suited when an asset may be recorded on nodes worldwide and ensuring that a single governing law can be identified to avoid inconsistent outcomes regarding proprietary issues. Though still in the drafting stage, the project has already garnered interest from major financial centers, including the EU, the U.S., and Hong Kong. Their involvement indicates a broad recognition that legal uncertainty about applicable law is a barrier to the broader adoption of distributed ledger technology (DLT) in finance and commerce. Once finalized and embraced, even as soft guidance, these rules could greatly enhance the predictability of cross-border blockchain transactions.

In addition to these international model laws and principles, national and regional regulators have established specific rules for blockchain-based activities, with a particular focus on crypto-assets and financial stability.

Summary

In short, the legal regulation of blockchain and digital assets is emerging as a combination of international models and national laws that are converging on some key solutions.

There is a clear international trend toward legally recognizing digital tokens as property or negotiable instruments, as evidenced by UNCITRAL's Model Law on Electronic Transactions (MLETR), the UNIDROIT Principles, and laws in the UK and Singapore. We do not explicitly address the well-known regulatory regimes for crypto-asset markets, as seen in the EU's Markets in Crypto-Assets (MiCA) Regulation and analogous efforts elsewhere. Finally, there is a trend toward clarifying the legal status of novel blockchain constructs, such as decentralized autonomous organizations (DAOs)

⁹³ Hague Conf. on Priv. Int'l L., <https://www.hcch.net/en/home> (last visited July 20, 2025).

and smart contracts, as seen in the Abu Dhabi Global Market (ADGM)'s framework and Wyoming's DAO law.

Unlike the treaties that harmonized international sales or negotiable instruments in the past, no single binding global convention exists for blockchain. However, the model laws and principles act as vehicles of consensus. Their nonbinding nature has not prevented them from having widespread influence. Rather, it has allowed states to implement common principles in ways that are compatible with their legal systems.

At the same time, differences remain, particularly between jurisdictions that favor a more permissive or innovation-driven approach and those that prioritize strict control and consumer protection. These differences can lead to regulatory arbitrage or uncertainty in cross-border situations, highlighting the need for continuous international coordination, such as the HCCH-UNIDROIT conflicts project or G20 dialogues.

As blockchain technology continues to evolve in areas such as decentralized finance, non-fungible tokens in art and intellectual property (IP), and supply-chain provenance systems, legal frameworks will likely undergo further iterations. Thus far, however, the trajectory shows a shift from early chaos toward convergence on key legal principles. These principles include the idea that digital ledger entries can represent and transfer real-world rights; that such activities should occur under rule-of-law safeguards, such as property rights, contract enforceability, and regulatory oversight; and that international cooperation is necessary to address the borderless nature of blockchain networks.

4.3 Specific Rules for Artificial Intelligence

The rise of artificial intelligence (AI) and automated decision-making systems has prompted the development of legal and ethical guidelines worldwide. Unlike electronic commerce or blockchain, which focus on transactions and assets, AI regulation engages fundamental values such as privacy, non-discrimination, transparency, and human safety. Therefore, AI systems can profoundly impact societal and individual interests.

Legal frameworks for AI are still in their infancy and evolving. However, a few influential global approaches can be identified. These approaches range from high-level soft law principles endorsed by dozens of countries to the first attempts at binding legislation specifically tailored to AI.

A key challenge in governing AI is achieving international consensus on baseline norms while allowing for flexibility in innovation and differing cultural values.

4.3.1 OECD-Principles

A landmark initiative on the global stage was the OECD Principles on Artificial Intelligence, adopted in May 2019⁹⁴. The first set of intergovernmental policy guidelines

⁹⁴ Org. for Econ. Co-operation & Dev., *Recommendation of the Council on Artificial Intelligence*, OECD (2019), <https://oecd.ai/en/ai-principles> (last visited July 20, 2025).

on AI was agreed to by 42 countries (the 36 OECD member states at the time, plus six others). Shortly thereafter, the G20 endorsed the principles at its 2019 summit, thereby extending their influence on many more countries.

Although the OECD AI Principles are non-binding, they carry significant weight as a consensus among leading economies on what constitutes “trustworthy AI.” Substantively, the principles state that AI should benefit people and the planet by promoting inclusive growth and sustainable development. They also state that AI systems should be designed to respect the rule of law, human rights, democratic values, and diversity. Additionally, they state that AI systems should include appropriate safeguards, such as human oversight. The principles also call for transparency and explainability in AI operations, as well as robustness and security throughout the AI life cycle. Finally, the principles emphasize accountability for those deploying AI.

These values-based principles are complemented by policy recommendations urging governments to invest in AI research, develop an enabling digital infrastructure, provide workers with AI-related skills, and cooperate internationally to promote the responsible stewardship of AI. Although the OECD principles are aspirational, they have proven highly influential. Many national AI strategies have adopted their vocabulary and ethical baseline. Furthermore, the OECD’s follow-up work, including the AI Policy Observatory, has helped countries share best practices for implementing these principles.

For example, the European Commission’s work on AI ethics, as outlined in the guidelines of its High-Level Expert Group, closely aligns with the OECD framework. The United States, Canada, Japan, and other countries have referenced the OECD principles when creating their domestic AI policy documents, which indicates a broad endorsement of these concepts. Although these principles are “soft”, they can guide the development of binding laws and shape industry self-regulation in the interim.

The OECD principles themselves acknowledge their non-binding nature, drawing a parallel to prior OECD guidelines, such as the 1980 Privacy Guidelines, which, despite being voluntary, became the basis for many privacy laws in Europe, Asia, and America. Similarly, the OECD AI principles serve as a global reference point for trustworthy AI, demonstrating how non-binding norms can precede formal regulation.

4.3.2 UNESCO Initiative

Another global initiative emerged from UNESCO. In November 2021, the UNESCO General Conference adopted the Recommendation on the Ethics of AI, which was agreed upon by all 193 member states.⁹⁵ This non-binding instrument delves into ethical principles such as proportionality, safety, fairness, and privacy in AI. It also provides policy guidance on AI governance, data management, and environmental impact.

Although not mentioned in the provided document, the unanimous adoption of the UNESCO Recommendation signaled a global commitment (at least on paper) to shared

⁹⁵ UNESCO, RECOMMENDATION ON THE ETHICS OF ARTIFICIAL INTELLIGENCE (2021), <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

values in AI deployment, including concerns particular to the Global South, such as cultural diversity and inclusive growth. The Recommendation complements the OECD principles and extends them in areas such as the ethical impact assessment of AI and international cooperation for capacity building.

Together, the OECD and UNESCO texts reflect a global consensus on high-level principles: AI should be human-centric and respect human rights, and governments should play an active role in ensuring this outcome.

4.3.3 Council of Europe

In terms of binding instruments, the most significant development is the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law, which was adopted in May 2024⁹⁶. Notably, this treaty is the first international legally binding instrument on AI, covering the entire lifecycle of AI systems.

The aim of the Convention is to reconcile technological innovation with fundamental rights. It requires parties to ensure that the design, development, and deployment of AI systems within their jurisdiction uphold human dignity, freedom, equality, and all other rights guaranteed by the European Convention on Human Rights and related texts. The Convention adopts a risk-based regulatory approach, obligating parties to identify and assess the risks posed by AI systems and take proportionate measures to address them. For instance, if an AI application poses a high risk to democratic processes or personal security, states may need to impose stricter oversight or consider moratoria or bans on certain uses.

The Convention codifies and reinforces the principles established in the soft-law sphere, making requirements of transparency, accountability, non-discrimination, privacy, and safety in AI systems legal obligations. The Convention also mandates that individuals have access to effective legal recourse when their rights are violated by AI systems (e.g., the right to challenge an algorithmic decision). Another innovative feature is the requirement that each party establish independent oversight bodies to monitor AI impacts and compliance, as well as a Conference of the Parties at the international level to review implementation.

Although the Convention is a Council of Europe instrument rooted in the European human rights system, it was opened globally. In fact, several non-European states participated in drafting it and signed it. Notably, Canada, Japan, the United Kingdom, the European Union, the United States, Israel, and others participated as observers or negotiators. As of its opening for signature in September 2024, countries including the UK, the EU, and some non-CoE members such as Uruguay and Mexico have expressed support. The United States signed the convention in 2024 as well, reflecting a shared interest in establishing a common framework, although U.S. ratification may be uncertain.

⁹⁶ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, opened for signature Sept. 5, 2024, C.E.T.S. No. 225, <https://rm.coe.int/1680afae3c>.

The treaty will enter into force once it is ratified by five states. If it receives enough ratifications, the convention could establish a foundation of binding legal obligations for AI governance across multiple continents, similar to how data protection conventions did in earlier decades. It is a prime example of a binding international solution that establishes substantive consensus on principles such as transparency and fairness in AI. It could also pressure non-parties to adhere to similar standards if they wish to maintain interoperability or adequacy. For instance, companies operating in convention-states may effectively adhere to their requirements globally.

4.3.4 Self-Regulation

In addition to these government efforts, there is a layer of industry self-regulation and multi-stakeholder initiatives regarding AI. Aware of regulatory momentum, tech companies have published AI ethical codes and formed collaborations (e.g., Partnership on AI) to establish best practices. Standardization organizations, such as ISO/IEC, are developing technical standards for AI (e.g., bias metrics or transparency documentation) that could be referenced by legislation like the EU AI Act.

There is also an emerging practice of AI auditing and certification that may become more formalized as regulations like the EU AI Act require conformity assessments by notified bodies for high-risk AI. These developments suggest that AI governance is moving toward a more structured, albeit not unified, international regime.

4.3.5 Comparative Perspectives

From a comparative perspective, one can observe a convergence on fundamental, substantive rules for AI. There is broad agreement that AI should be safe, non-discriminatory, and transparent (at least to regulators, if not always to users). Additionally, there is agreement that humans should retain a meaningful degree of control and accountability. These points of consensus are reflected in the OECD/G20 principles, the UNESCO Recommendation, the EU's binding rules, and even China's regulatory documents (though the latter lack human rights language).

However, there is divergence in implementation. The EU, the Council of Europe and International Organizations have chosen binding legal mandates, while the US, UK, and others rely on guidelines and existing laws, creating a split between binding and non-binding. This raises legal theory questions about the efficacy of hard versus soft law in a rapidly advancing technological field. Some argue that flexible, adaptive governance is preferable for AI, while others contend that clear legal prohibitions and rights, like those created by the Council of Europe Convention, are necessary to truly safeguard values.

Additionally, the enforcement mechanisms differ. Europe relies on administrative enforcement with fines, which are similar to those under the GDPR. The Council of Europe Convention relies on state compliance and an oversight body. The US uses litigation and agency oversight on specific harms. China employs government supervision and surveillance of providers. These differences reflect not only deeper

legal and cultural differences, but also experimentation with the most effective ways to govern algorithms.

Looking ahead, the push for international coordination in AI is intensifying. In 2023, the G7 launched the “Hiroshima AI Process” to align AI governance approaches among the world’s most advanced economies. The initiative specifically focuses on generative AI challenges. There are some calls for a new global body for AI, analogous to the International Atomic Energy Agency, though this remains a proposal. As AI-technology rapidly advances, with models like GPT-4 demonstrating increasingly general capabilities, it’s clear that unilateral regulation by one jurisdiction can have global ripple effects. However, this approach faces limitations when AI systems are accessible globally via the internet.

This situation is leading to a pragmatic consensus that some baseline international norms or agreements will be necessary. Much like the aviation, maritime, and trade sectors, the AI sector may eventually be subject to a framework that ensures compatibility and minimum safeguards across borders.

4.4 Convergence in Digital Transaction Frameworks

Legal frameworks for digital transactions have evolved from basic rules enabling electronic commerce to complex regimes addressing blockchain and artificial intelligence technologies. International consensus building has played a pivotal role in this evolution.

Though non-binding, UNCITRAL’s Model Laws on Electronic Commerce and Electronic Signatures achieved near-universal adoption and established the foundational principles that underpin today’s digital economy: the functional equivalence of electronic communications and the non-discrimination against digital forms. These principles have effectively removed legal impediments to online contracting and have provided businesses worldwide with the predictability of knowing that an e-contract or e-signature will be honored across jurisdictions.

In parallel, instruments such as the 2005 Electronic Communications Convention offered binding harmonization to states willing to ratify, ensuring uniform cross-border rules and signaling formal acceptance of electronic transactions in international law.

The interplay of model laws and conventions reveals a broader pattern: Model laws and soft-law principles act as incubators of legal norms, enabling states to experiment with and align their laws voluntarily. Conventions and regulations, on the other hand, formalize commitments once political conditions permit or when uniformity becomes critical.

4.4.1 Emerging Blockchain Frameworks

In the realm of blockchain, where technology outpaced regulation initially, we now see a coalescence around key legal solutions. There is growing international agreement that digital tokens can represent legal rights (whether documents of title via MLETR or

crypto-assets via property law reforms) and that possessing control of a token is analogous to possessing a tangible good for legal purposes. The work of UNIDROIT and UNCITRAL has provided reference frameworks so that countries as diverse as Singapore, France, and Paraguay can adopt laws that are different in detail but harmonious in principle – for example, each recognizing the concept of a singular authoritative electronic record that can be transferred with finality.

The fact that even historically "light-touch" jurisdictions are introducing licenses for crypto businesses indicates a shared recognition of risk and a move toward international regulatory interoperability for digital asset markets.

4.4.2 Search for a Common Framework in AI

The international legal consensus on artificial intelligence is in the early stages, focusing on ethics and principles. However, Europe's rapid development of binding rules has shifted the conversation from principles to practices.

The EU AI Act's risk-based framework is already influencing discussions in countries such as Canada and Australia. This suggests that a *de facto* standard for AI governance may emerge, similar to how EU data protection law influenced global privacy standards.

If widely ratified, the Council of Europe's AI Convention could globalize a human-rights-centric approach to AI, creating an interoperable legal space with common definitions and remedies for AI-related harms. Importantly, the Convention also exemplifies the integration of international and national law. It allows parties flexibility in implementing AI obligations domestically, either by directly applying treaty rules to the private sector or via national measures. This approach acknowledges different legal systems while upholding shared principles. This flexible compliance mechanism could serve as a model for future international AI agreements, balancing sovereignty and uniformity.

4.4.3 International Regulatory Instruments

A recurring theme is the distinction between binding and non-binding frameworks, and how they can each be effective in different ways.

Non-binding instruments, such as model laws, principles, and guidelines, have proven crucial in areas where technology is advancing rapidly and where states have not yet reached a consensus on specific details, but have agreed on general principles. These instruments allow for experimentation and the progressive development of the law. UNCITRAL's model laws on e-transactions and the OECD's AI principles are prime examples. Neither had the force of law on its own, yet both have reshaped numerous national laws and policies through persuasion and expert endorsement. These instruments also often serve as drafts for later binding instruments. Indeed, elements of the UNCITRAL model laws were reflected in the Electronic Communications Convention and numerous free trade agreements. Additionally, the OECD AI principles are echoed in the recitals of the EU AI Act.

Binding instruments provide certainty and enforcement. Once adopted, they commit states to a course of action and enable private parties to invoke clear rules. The Electronic Communications Convention unified cross-border e-contracting rules among its signatories, and the forthcoming AI Convention will create rights and duties that individuals and organizations can rely on for those who join (e.g., the right to a remedy for AI-related harm). Similarly, binding regional laws, like EU regulations, ensure uniform application and avoid the fragmentation that can result from purely voluntary adoption.

Another critical aspect is the adoption by states. A legal framework's influence is ultimately measured by how many jurisdictions implement it and how. We observed that UNCITRAL's e-commerce law achieved an impressive adoption rate (87 states) by aligning with what stakeholders needed – it addressed commercial certainty without forcing any particular regulatory ideology. In newer areas, adoption is still ongoing: MLETR's roster of adopters is steadily growing, and the UNIDROIT Digital Assets Principles are under active review by leading financial centers. The EU's AI Act will automatically cover 27 countries, and already the transnational nature of AI means that companies worldwide are preparing to meet its standards (just as non-European companies adjusted to the GDPR).

Thus, one can anticipate a ripple effect. Other countries may choose to "transpose" the EU AI Act into their own laws, or they may accept it as the de facto compliance standard for AI systems entering their markets, even if they do not have their own AI laws. In the blockchain sphere, smaller jurisdictions looking to attract fintech businesses have been early adopters of model laws. For example, Mauritius and Kazakhstan are considering the Multilateral Convention on Mutual Legal Assistance in Civil Matters (MLETR), and Liechtenstein and Bermuda have enacted laws aligned with global principles. Larger economies often take longer to harmonize, but when they do, as France and the UK did with the Model Law on Electronic Transmission of Records (MLETR) and as Japan did with some UNCITRAL principles in its Civil Code amendments, it significantly propels international uniformity.

5. Normative Analysis

5.1 Automation in Code is Law

The automation of smart contracts under "code is law" incentivizes unethical behavior by enabling anonymous, opportunistic actions, reducing repeat business and undermining transaction cost minimization. The absence of accountability, coupled with the perception that no external law applies, exacerbates this issue.

We argue that the absence of accountability mechanisms in anonymous, automated smart contracts encourages a "take the money and run" mentality, necessitating a historical record of conduct and incentives for ethical behavior. Evolving decentralized governance, incorporating reputation credits for good conduct, extends the benefits of

"code is law" while aligning it with societal values, contrasting sharply with the authority, flexibility, enforcement, and normative legitimacy of traditional legal systems.

Decentralized governance, incorporating historical conduct records and reputation credits, mitigates these flaws by fostering accountability and incentivizing ethical behavior. By aligning code's efficiency with law's equitable principles, this approach extends the benefits of "code is law" for societal betterment, ensuring trust and sustainability in decentralized systems.

5.2 Authority: Technocratic Protocols vs. Sovereign Legitimacy

Traditional legal systems derive authority from sovereign institutions, grounded in democratic processes, ensuring legitimacy through public participation. In contrast, "code is law" vests authority in technocratic protocols, where programmers dictate rules without democratic input. This fosters unethical behavior, as anonymous smart contract participants face no reputational consequences, encouraging exploitative actions that deter repeat business.⁹⁷ Decentralized governance, such as through decentralized autonomous organizations (DAOs), democratizes rule-making by enabling stakeholder consensus, incorporating reputation systems to incentivize ethical conduct and restore accountability absent in code-driven systems.⁹⁸

5.3 Flexibility: Deterministic Execution vs. Legal Adaptability

Legal systems exhibit flexibility, allowing judicial interpretation to address societal changes and ethical considerations. Conversely, smart contracts' deterministic execution rigidly enforces coded terms, incentivizing participants to exploit loopholes for immediate gain, as there is no mechanism to adapt rules contextually.⁹⁹ Decentralized governance, through on-chain voting, enables dynamic rule amendments and introduces reputation credits, discouraging unethical behavior by rewarding long-term cooperation, thus aligning code's functionality with law's adaptability.

5.4 Enforcement: Automated Rigidity vs. Human Discretion

Traditional legal systems enforce rules through human institutions, incorporating discretion to ensure equitable outcomes. Smart contracts automate enforcement, executing terms without appeal, which encourages participants to prioritize short-term profits over ethical conduct, knowing no external law applies.¹⁰⁰ Decentralized dispute resolution, integrated with historical conduct records, complements automation by enabling fair adjudication and penalizing unethical actions, contrasting with law's balanced enforcement approach.

⁹⁷ CRAIG CALCETTERA & WULF A. KAAL, DECENTRALIZATION 114 (2021).

⁹⁸ Wulf A. Kaal, *Blockchain-Based Corporate Governance*, 3 STAN. J. BLOCKCHAIN L. & POL'Y 1 (2020), <https://stanford-jblp.pubpub.org/pub/blockchain-corporate-governance/release/1>.

⁹⁹ Wulf A. Kaal, *Decentralized Autonomous Organizations: Internal Governance and External Legal Design*, 5 ANNALS CORP. GOV. 237, 272-73 (2021), <http://dx.doi.org/10.1561/109.00000028>.

¹⁰⁰ Wulf A. Kaal & Craig Calcaterra, *Crypto Transaction Dispute Resolution*, 73 BUS. LAW. 109, 111 (2018).

6. UDLC

The UDLC emerges as a pioneering legal framework designed to govern the integration of Web3 technologies—specifically distributed ledger technology (DLT), AI, and quantum computing—into global legal systems. This framework addresses the multifaceted legal challenges associated with smart contracts and digital assets, as identified in prior scholarship, which include disruptions in contract formation under common law, enforceability issues in civil law jurisdictions, jurisdictional conflicts in cross-border transactions, and the normative deficiencies of the “code is law” paradigm. These challenges threaten the seamless adoption of blockchain-based innovations by creating legal uncertainty, regulatory fragmentation, and ethical concerns.

By establishing a hybrid legal framework that reconciles technological autonomy with established legal principles, UDLC provides a robust solution that fosters legal certainty, compliance, and innovation while preserving the decentralized ethos of Web3 systems. This analysis comprehensively elucidates how UDLC systematically resolves these issues, ensuring that smart contracts and digital assets align with traditional legal frameworks across diverse jurisdictions while enabling the evolution of digital markets.

6.1 Positioning UDLC between code and national law

As shown above, there has been an ongoing academic discussion on the pros and cons of national law, conflicts of law, and the idea that 'code is law'. We have also demonstrated that neither conflict of laws nor legal harmonization can provide a sustainable, systemic solution. Ultimately, these approaches result in the fossilization of legal relationships, meaning they can only adapt to innovative, decentralized and constantly changing technical conditions with a delay, if at all. Suppliers and users of digital systems can mitigate this issue by drafting sophisticated agreements and terms and conditions that legally address some of the aforementioned challenges.

The UDLC provides an optimized solution: users of digital systems can use this codex as the basis for their contractual obligations and benefit from the evolving experience of the community. The codex combines national law, code and business requirements, takes into account different legal systems, and offers an inherent dispute resolution mechanism. In short, UDLC covers the entire legal process, from concluding agreements to performing contractual obligations, dealing with contractual disruptions, and resolving disputes.

6.2 Resolving Challenges in Smart Contract Formation

Smart contracts, defined as self-executing computer protocols on blockchain platforms, fundamentally disrupt traditional contract formation in common and civil law jurisdictions by automating offer and acceptance, complicating the doctrine of consideration, and necessitating external intervention due to their immutable execution. The automation of offer and acceptance eliminates iterative human negotiation, raising questions about whether coded assent satisfies the common law requirement of a “meeting of the minds.” Economic inefficiencies, such as the time value of money in escrow-like

arrangements, challenge the practicality of consideration, particularly in high-value or long-term agreements. Moreover, the immutability of blockchain transactions precludes judicial remedies or modifications, straining enforceability when disputes arise outside the code's scope.

UDLC addresses these disruptions through a structured legal private framework that ensures smart contracts comply with established common law principles of national law while leveraging technological efficiency. First, UDLC establishes minimum legal requirements for smart contracts, ensuring that coded agreements reflect mutual assent and bargained-for exchange. By adopting the principle of functional equivalence, UDLC translates machine-readable transaction modules into legally recognizable expressions of intent, akin to traditional contracts. For example, UDLC mandates that smart contracts incorporate clear, human-readable terms alongside coded protocols, ensuring that parties' assent to automated terms meets the common law standard of mutual understanding. This approach mitigates the risk of misalignment between coded execution and contractual intent, addressing concerns about the absence of dynamic bargaining.

Second, UDLC tackles economic inefficiencies in consideration by embedding dynamic compliance mechanisms within smart contracts. These mechanisms allow contracts to adapt to market conditions, such as fluctuations in cryptocurrency value or delays in physical delivery, thereby enhancing the economic viability of digital transactions. For instance, UDLC enables smart contracts to adjust escrow terms based on real-time economic data, reducing the opportunity cost of locked funds and aligning with the practical utility required for consideration. Additionally, UDLC integrates DLT-based verification systems to confirm the transfer of physical goods, ensuring that contractual obligations involving tangible assets are fulfilled, thus bridging the gap between digital and physical performance.

Third, UDLC covers concepts such as good faith and fair dealing, equity, fiduciary duties, estoppel, misrepresentation, and duress. Even though these concepts take different forms in each applicable jurisdiction, UDLC provides a consistent approach.

Fourth, UDLC facilitates external intervention through decentralized dispute resolution mechanisms, preserving common law's flexibility in addressing disputes. By integrating arbitration platforms, such as the Decentralized Autonomous Organizations for Arbitration of digital disputes, UDLC provides a forum for human oversight when immutable code fails to resolve conflicts, such as defective performance or unforeseen circumstances. These platforms allow parties to submit disputes to expert arbitrators, whose decisions are recorded on a transparent blockchain ledger, ensuring enforceability while maintaining the efficiency of automation. This hybrid approach aligns with common law's adaptability, as seen in historical analogies to vending machines, and ensures that smart contracts remain legally binding while accommodating judicial remedies when necessary.

6.3 Ensuring Enforceability of Mandatory Law

Smart contracts pose significant challenges to enforceability due to mandatory provisions, e.g. requiring contracts to meet specific formalities, such as written or notarized documents, which smart contracts often lack. The immutable nature of coded terms limits interpretive flexibility, preventing courts from resolving ambiguities or aligning agreements with principles of good faith. Moreover, the self-executing nature of smart contracts bypasses judicial authority, undermining mandatory remedies like rescission or damages in cases of breach or fraud.

UDLC deals these challenges by providing a legal framework that integrates smart contracts into law systems while respecting their codified principles. To address formalities, UDLC establishes guidelines for smart contracts to comply with statutory requirements through electronic equivalents. For example, UDLC mandates the use of DLT-based records as substitutes for written documents, ensuring that smart contracts meet the formal attestation standards required for transactions like real estate transfers. By aligning with international frameworks, such as UNCITRAL's Model Law on Electronic Transferable Records (MLETR), UDLC ensures that these electronic records are legally recognized across civil law jurisdictions, enhancing enforceability.

6.4 Mitigating Conflict of Laws and Jurisdictional Challenges

The borderless nature of digital assets, underpinned by decentralized blockchain networks, complicates the application of conflict of laws principles, including jurisdictional determination, choice of law, and enforcement. Traditional legal systems rely on territorial connections, such as the location of parties or assets, to assert jurisdiction, but blockchain's pseudonymous and distributed architecture obscures these connections. Determining the applicable law is equally challenging, as smart contracts often lack explicit choice-of-law clauses, leading to interpretive divergences between common and civil law jurisdictions. Enforcement is hindered by the immutability of blockchain transactions, which limits judicial intervention, and the absence of centralized intermediaries in decentralized systems.

UDLC mitigates these challenges by promoting legal interoperability and leveraging technological solutions to enhance cross-border governance. To address jurisdictional ambiguity, UDLC aligns smart contracts with international standards, such as those developed by UNIDROIT and UNCITRAL, ensuring that digital transactions operate seamlessly across jurisdictions. By embedding choice-of-law protocols within smart contracts, UDLC provides clarity on the governing law, reducing the risk of conflicting interpretations. For example, UDLC enables parties to specify applicable law through coded parameters, which are verified by DLT-based records, ensuring predictable outcomes in cross-border disputes. This approach mirrors the objectives of the HCCH-UNIDROIT project, which seeks to harmonize conflict of laws principles for digital assets.

UDLC's hybrid governance model further resolves jurisdictional challenges by balancing universal ethical standards with localized adaptations. This model ensures that digital

assets respect jurisdictional diversity, such as cultural or economic differences, while maintaining global consistency to prevent regulatory fragmentation. For instance, UDLC allows jurisdictions to tailor smart contract requirements to local statutory frameworks while adhering to a baseline of ethical principles, such as transparency and non-discrimination. This flexibility preserves the innovative potential of blockchain by avoiding the homogenizing effects of harmonized legal standards, which could stifle jurisdictional experimentation.

Enforcement challenges are addressed through UDLC's integration of DLT and AI-based tools, which provide transparent and verifiable evidence for cross-border transactions. DLT ensures tamper-proof records of contractual negotiations, execution, and performance, enabling courts and regulators to enforce agreements with confidence. AI-driven compliance mechanisms monitor transactions in real-time, ensuring adherence to export controls, financial regulations, and anti-money laundering requirements. For example, UDLC enables smart contracts to automatically flag transactions involving controlled assets, such as tokenized real-world assets (RWAs), ensuring compliance with regulations like the U.S. Export Administration Regulations (EAR) or the EU Dual-Use Regulation. By combining technological efficiency with legal interoperability, UDLC streamlines enforcement across common and civil law jurisdictions, fostering trust in decentralized systems.

6.5 Overcoming Limitations of the “Code is Law” Paradigm

The “code is law” paradigm, which posits that software code regulates behavior with the same authority as traditional law, introduces significant normative deficiencies, including technocratic authority, deterministic enforcement, and a lack of moral deliberation. By vesting authority in unelected programmers and immutable protocols, this paradigm undermines democratic legitimacy, encouraging unethical behavior in anonymous transactions. The deterministic execution of smart contracts precludes contextual adaptation, incentivizing participants to exploit loopholes for short-term gain. Moreover, the absence of normative grounding erodes social trust, as code prioritizes functionality over ethical considerations, creating systems that lack accountability and fairness.

UDLC addresses these limitations by integrating decentralized governance mechanisms that align technological efficiency with societal values. To counter technocratic authority, UDLC democratizes rule-making through stakeholder consensus, such as within decentralized autonomous organizations (DAOs). By enabling participants to vote on protocol updates, UDLC ensures that rules reflect collective input, restoring legitimacy absent in code-driven systems. Additionally, UDLC incorporates reputation systems and historical conduct records, incentivizing ethical behavior by rewarding long-term cooperation. For example, participants who act in good faith earn reputation credits, while those engaging in opportunistic actions face penalties, mitigating the “take the money and run” mentality fostered by anonymity.

To overcome deterministic enforcement, UDLC introduces an adaptive legal framework that allows smart contracts to evolve with legal and ethical standards. Through on-chain voting and dynamic compliance mechanisms, UDLC enables contractual terms to be

amended in response to societal changes or unforeseen circumstances, aligning code with the flexibility of traditional law. For instance, smart contracts can incorporate clauses that trigger human review in cases of ambiguity, ensuring equitable outcomes akin to judicial discretion. This adaptability contrasts with the rigidity of “code is law,” which executes terms without appeal, and ensures that smart contracts remain responsive to contextual nuances.

UDLC further embeds normative legitimacy by mandating transparency, accountability, and cultural sensitivity in Web3 systems. By requiring clear and auditable terms within smart contracts, UDLC enables regulatory oversight and fosters trust among participants. The inclusion of multi-stakeholder engagement, involving governments, industry, and civil society, ensures that technological governance reflects moral deliberation and societal values. Moreover, UDLC’s emphasis on cultural sensitivity allows AI and DLT systems to respect diverse ethical standards, preventing the homogenization of technology and promoting inclusive innovation. For example, UDLC enables AI governance to be tailored to local norms, ensuring that digital transactions align with cultural expectations while adhering to universal principles like fairness and non-discrimination.

6.6 Practical Implementation: The Arbitration DAO Case Study

The practical application of UDLC is exemplified through its integration into the Arbitration DAO, a decentralized platform for resolving smart contract disputes. The Arbitration DAO operates through a network of expert arbitrators who adjudicate disputes based on transparent, DLT-based evidence, ensuring efficiency and fairness. UDLC enhances this platform by providing a legal foundation that ensures compliance with national and international laws. By defining legal standards for smart contracts, UDLC ensures that disputes are resolved within a legally sound framework, enabling arbitration awards to be enforced by courts. The precedent system records outcomes in a transparent ledger, promoting consistency and predictability in future resolutions. Additionally, UDLC’s dynamic regulatory mechanisms allow the Arbitration DAO to adapt to evolving legal requirements, while AI-driven tools monitor compliance with financial and export regulations. This integration demonstrates UDLC’s capacity to bridge the physical and digital worlds, fostering trust and scalability in Web3 ecosystems.

7. Conclusion

UDLC represents a transformative approach to resolving the legal challenges of smart contracts and digital assets, offering a hybrid framework that integrates DLT, AI, and quantum computing into existing legal systems. By ensuring compliance with common and civil law principles, promoting interoperability across jurisdictions, and aligning technological governance with societal values, UDLC fosters legal certainty, trust, and innovation. Its emphasis on dynamic compliance, decentralized dispute resolution, and culturally sensitive governance positions UDLC as a pivotal tool for enabling the sustainable growth of digital transactions and markets. Through practical implementations like the Arbitration DAO, UDLC demonstrates its potential to bridge the

physical and digital realms, ensuring that Web3 technologies evolve within a framework of legal certainty and ethical accountability.

UDLC is a project that is constantly evolving. The first draft will be published in the autumn 2025, after which the corresponding institutional structures will be set up based on a DAO. This will ensure that UDLC can adapt to future technical, legal and economic challenges, and that practical experience can be integrated into UDLC processes.