Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 2, October 2026, pp. 228∼241
E-ISSN: 3164-6794 | P-ISSN: 3164-6697, DOI: 10.68012

Smart Contract Regulation for Decentralized Justice and Cross-Border Digital Transactions

Shofiyul Millah[1], Steven Harazaki Lase[2], Natalie Septiani[3*], Suca Rusdian[4]
[1,2]Faculty of Economics and Business, Universitas Raharja, Indonesia
[3]Department of Digital Law and Technology Governance, Ijiis Incorporation, Singapore
[4]Faculty of Management, Yasa Anggana College of Economics, Indonesia
[1]shofiyul@raharja.info, [2]steven.harazaki@raharja.info, [3]nataliseptiani@ijiis.asia, [4]sucarusdian@stieyasaanggana.ac.id
***Corresponding Author**

Article Info

Article history:

Submission April 22, 2026
Revised September 21, 2026
Accepted September 25, 2026
Published September 30, 2026

Keywords:

Smart Contracts
Digital Rights
Decentralized Justice
Regulatory Interoperability
Cross-Border Digital Transactions

ABSTRACT

Blockchain-based smart contracts have introduced new mechanisms for executing cross-border digital transactions through automated and decentralized contractual arrangements. However, their code-based execution creates legal challenges concerning jurisdiction, enforceability, accountability, dispute resolution, and the protection of fundamental legal rights. **This study aims** to develop a human-centric regulatory framework for smart contracts that strengthens legal certainty, accountability, and access to justice in decentralized and cross-border digital transactions. **This study employs normative** legal research with a comparative regulatory approach. Primary legal materials, including national legislation and international regulatory instruments governing electronic transactions, blockchain, digital contracts, and dispute resolution, are analyzed through statutory, conceptual, and comparative approaches. The analysis identifies regulatory gaps and formulates principles for interoperable smart contract governance. **The study demonstrates** that existing legal frameworks insufficiently address automated contractual execution, cross-border jurisdiction, liability for code-based outcomes, and human intervention in decentralized dispute resolution. The proposed framework integrates seven regulatory principles: legal validity and enforceability, transparency and explainability, accountability and liability, human oversight, cross-border jurisdiction, data protection and digital rights, and regulatory interoperability. **The framework provides** a human-centric regulatory architecture for aligning smart contract automation with fundamental legal principles and cross-border regulatory requirements. It contributes to decentralized justice by preserving technological efficiency while ensuring procedural fairness, legal accountability, and protection of digital rights.

This is an open access article under the CC BY 4.0 license.

DOI: https://doi.org/10.68012/law.v1i2.170
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

1. INTRODUCTION

Blockchain technology has transformed the architecture of digital transactions by enabling parties to exchange value and establish contractual arrangements without relying exclusively on centralized intermediaries [1]. One of its most significant applications is the smart contract, which allows predefined contractual

conditions to be executed automatically through blockchain-based code. This mechanism can improve transactional efficiency, reduce intermediary dependence, and increase the traceability of digital agreements. Smart contracts have consequently become increasingly relevant to cross-border digital commerce, decentralized finance, digital assets, and other web-based economic activities [2]. Nevertheless, technological automation does not automatically resolve the legal questions surrounding contractual validity, liability, jurisdiction, and enforcement.

Smart contracts present a distinctive regulatory challenge because their operational logic is embedded in executable code rather than expressed solely through conventional legal language. Once deployed on a blockchain network, contractual provisions may be executed automatically even when their consequences conflict with the parties' expectations or subsequently applicable legal requirements [3]. This creates tension between the principle of automated execution and the legal principles of fairness, proportionality, accountability, and judicial intervention. A malfunctioning code, inaccurate external data, unauthorized transaction, or unforeseen contractual circumstance may generate consequences that cannot easily be reversed through conventional legal mechanisms [4]. The resulting problem is therefore not merely whether smart contracts should be recognized as legally valid agreements, but how legal systems should govern their execution while preserving fundamental principles of justice and legal protection [5]. The challenge becomes more complex when smart contracts are used for cross-border transactions. Participants may be located in different jurisdictions, while the blockchain infrastructure supporting the transaction can operate across multiple territorial boundaries. Consequently, determining the applicable law, competent jurisdiction, and appropriate enforcement mechanism becomes increasingly difficult. Differences among national approaches to electronic contracts, digital signatures, blockchain transactions, consumer protection, data governance, and dispute resolution further contribute to regulatory fragmentation [6]. Conventional conflict-of-laws principles are primarily designed around identifiable parties, territorial connections, and centralized institutions, whereas decentralized blockchain transactions can involve pseudonymous participants, distributed infrastructure, and automated execution. Without an interoperable regulatory approach, legal uncertainty may undermine the reliability and legitimacy of cross-border smart contract transactions [7].

Smart contracts also have significant implications for decentralized justice and web-based dispute resolution. Automated contractual execution can facilitate decentralized mechanisms for resolving disputes by incorporating predetermined procedures, arbitration clauses, escrow mechanisms, or decentralized governance arrangements into blockchain infrastructure [8]. Such mechanisms may provide faster and more accessible alternatives to traditional dispute resolution. However, decentralization may also weaken conventional safeguards associated with due process, impartiality, human review, and access to effective remedies [9]. An entirely code-driven dispute mechanism may reproduce the assumption that algorithmic execution is inherently neutral, despite the fact that contractual code is designed by human actors and may contain errors, biases, or ambiguous assumptions. Accordingly, decentralized justice requires a regulatory architecture that preserves technological efficiency without allowing automation to displace human-centered principles of justice [10].

Existing scholarship has examined smart contracts from several perspectives, including their legal classification, contractual validity, enforceability, technological architecture, and application in decentralized finance [11]. Other studies have addressed blockchain-based dispute resolution and the broader regulatory challenges associated with digital transactions. However, these approaches frequently examine contractual regulation, dispute resolution, and cross-border governance as separate regulatory questions [12]. Limited attention has been given to an integrated framework that connects smart contract regulation, decentralized justice, and cross-border digital transactions within a unified legal architecture. Existing approaches commonly examine contractual validity and enforceability, blockchain-based dispute resolution, or cross-border jurisdiction as distinct regulatory concerns [13]. In contrast, this study contributes a seven-principle framework that integrates legal validity and enforceability, transparency and explainability, accountability and liability, human oversight and intervention, jurisdiction and applicable law, data protection and digital rights, and regulatory interoperability across the smart contract lifecycle [14]. The novelty of the framework therefore lies not only in identifying these principles individually, but in positioning them as interconnected legal safeguards that operate from contractual formation and deployment through execution, dispute resolution, and enforcement [15]. This integrated structure provides a human-centric legal architecture for connecting technological automation with legal authority, procedural fairness, and cross-border regulatory coordination.

Addressing this gap requires a shift from a technology-centered approach toward a human-centric model of smart contract governance [16]. Regulation should not seek to eliminate the autonomous charac-

teristics that make smart contracts valuable; rather, it should establish legal safeguards around their lifecycle, from contractual formation and code deployment to automated execution, dispute resolution, and enforcement [17]. Such an approach requires attention to legal validity and enforceability, transparency and explainability, accountability and liability, human oversight and intervention, jurisdiction and applicable law, data protection and digital rights, and regulatory interoperability [18]. These dimensions directly connect smart contract regulation with the interdisciplinary scope of Legal Autonomous Web-based Governance (LAW), particularly blockchain and smart contract governance, technology law and digital policy, online dispute resolution, digital justice, and decentralized governance systems. Decentralized justice contributes to web-based governance by embedding dispute-resolution procedures within digitally mediated environments, while regulatory interoperability provides mechanisms for connecting autonomous technological systems with legal institutions across jurisdictions [19]. The human-centric orientation further ensures that autonomous digital systems remain subject to legal accountability, procedural fairness, and meaningful human intervention.

Against this background, this study aims to develop a human-centric regulatory framework for smart contracts used in decentralized justice and cross-border digital transactions. The study addresses two central questions:

- What legal and regulatory challenges arise from the use of smart contracts in decentralized justice and cross-border digital transactions?
- What regulatory framework can reconcile automated blockchain-based execution with legal certainty, accountability, procedural fairness, and cross-border regulatory interoperability?

Through normative legal and comparative analysis, this study positions smart contract governance as an essential component of contemporary web-based justice and digital legal governance rather than merely a matter of technological regulation [20]. The study contributes an integrated seven-principle framework that connects contractual regulation, decentralized justice, and cross-border governance throughout the smart contract lifecycle.

2. LITERATURE REVIEW

2.1. Smart Contracts and Legal Regulation

Smart contracts represent a form of programmable contractual arrangement in which predetermined conditions are translated into computer-executable instructions and automatically performed through blockchain infrastructure [21]. Their distinctive characteristic lies in the combination of contractual logic and technological execution. Unlike conventional contracts, in which performance generally depends on the parties or authorized intermediaries, smart contracts can automatically transfer digital assets, trigger payments, or enforce predetermined obligations once specified conditions are satisfied. However, automatic execution does not by itself determine whether the underlying arrangement constitutes a legally enforceable contract [22]. Legal qualification continues to depend on established contractual doctrines concerning agreement, consent, contractual terms, validity, and applicable law. Accordingly, the first principle of legal validity and enforceability requires smart contract systems to preserve evidence of consent and contractual obligations and to maintain access to legally recognized remedies when automated performance fails or produces disputed outcomes. Similarly, jurisdiction and applicable law should remain connected to established private international law doctrines, including party choice, territorial or personal connecting factors, and the determination of a competent forum. Remedies and enforcement should likewise remain institutionally recognizable rather than being treated as purely technical consequences of blockchain execution [23]. Recent scholarship therefore distinguishes between conventional legal contracts implemented through blockchain, code-based arrangements, and hybrid structures that combine natural-language contractual terms with executable code.

From a regulatory perspective, the central issue is the relationship between executable code and natural-language contractual terms. Code determines how a transaction is technically executed, but it should not independently determine the legal consequences of every circumstance arising from the transaction [24]. Where executable code conflicts with the underlying natural-language agreement, the legally authoritative terms should be determined through applicable contractual interpretation and mandatory legal rules, rather than solely through the technical outcome produced by the code. This issue becomes particularly significant where

coding errors, ambiguous contractual provisions, invalid or uninformed consent, mandatory statutory provisions, fraud, or unforeseen circumstances affect the transaction. A technically successful execution therefore does not necessarily establish a legally valid or enforceable outcome [25]. Errors in programming, inaccurate external information, fraudulent conduct, or circumstances that were not anticipated when the code was written may produce outcomes that technically comply with the programmed conditions but conflict with the parties' legitimate expectations or applicable legal norms. Consequently, legal regulation should not treat technological execution as equivalent to legal validity. Instead, smart contract governance requires mechanisms that connect automated execution with conventional principles of contractual interpretation, liability, remedies, and judicial oversight [26]. This distinction provides an important theoretical foundation for the present study. Smart contracts should be understood not merely as technological substitutes for conventional contracts but as hybrid legal-technological instruments whose validity and enforceability remain embedded within legal institutions. Such an approach supports the development of regulatory safeguards concerning transparency, accountability, human intervention, and remedies without eliminating the efficiency associated with automated execution [27].

2.2. Decentralized Justice and Web-Based Dispute Resolution

Decentralized justice should be distinguished from related forms of digital dispute resolution. Online Dispute Resolution (ODR) generally refers to the use of digital platforms to facilitate negotiation, mediation, or adjudicative processes, while blockchain-based arbitration applies distributed ledger technology to support arbitration procedures and enforcement [28]. Automated dispute resolution, by contrast, relies on predefined computational rules to process disputes or trigger predetermined outcomes. Decentralized justice encompasses a broader governance arrangement in which dispute-related procedures, evidence, decision-making support, and enforcement may be distributed across technological and institutional actors [29]. In this framework, smart-contract execution should not be understood as an independent substitute for formal judicial adjudication. Rather, smart contracts primarily facilitate predetermined procedural or enforcement functions, while legally consequential adjudication remains subject to authorized human decision-makers and applicable legal institutions [30]. Earlier scholarship identified the potential of blockchain-based systems to create self-enforcing forms of dispute resolution that could reduce reliance on traditional courts and intermediaries. At the same time, blockchain-based dispute resolution creates tension with the territorial and institutional foundations of conventional adjudication, particularly because decentralized networks do not correspond neatly to the jurisdictional boundaries of states [31].

Web-based dispute resolution can provide important advantages for digital transactions, including procedural efficiency, lower transaction costs, automated enforcement, and accessibility across geographical boundaries. Smart contracts may, for example, incorporate escrow arrangements, predetermined dispute procedures, or automated consequences following a dispute-resolution decision [32]. Accordingly, the use of the term decentralized justice in this study refers to a technology-enabled dispute-resolution and governance mechanism rather than the creation of a parallel judicial system. Its legal legitimacy depends on the availability of human review, procedural safeguards, legally recognized remedies, and institutional authority. Recent research has further explored decentralized dispute resolution in international trade and demonstrated the potential of blockchain-based mechanisms to facilitate transparent and efficient resolution processes. Nevertheless, decentralization cannot be equated with the absence of legal institutions [33]. A technically self-executing dispute-resolution mechanism may still encounter difficulties concerning due process, impartiality, evidence, recognition of decisions, and the availability of judicial remedies. Research on blockchain justice has also emphasized that existing decentralized dispute-resolution models raise questions about the role of trusted third parties, decision-making mechanisms, and the appropriate balance between technological autonomy and legal legitimacy [34].

Accordingly, this study adopts a human-centric conception of decentralized justice. Under this approach, technological decentralization is valuable only when it remains compatible with fundamental legal safeguards [35]. Human oversight is therefore not treated as a rejection of automation but as a corrective mechanism for exceptional situations in which automated execution may produce unlawful, disproportionate, or manifestly unfair outcomes. This perspective is particularly consistent with LAW's interdisciplinary focus on web-based dispute resolution, blockchain and smart contract governance, technology law, digital justice, and decentralized governance systems [36]. In this context, decentralized justice is not understood as a replacement for legal institutions, but as a web-based governance mechanism that must remain connected to human oversight, legal accountability, and effective remedies.

2.3. Cross-Border Digital Transactions and Regulatory Interoperability

Cross-border smart contract transactions create a distinct problem because the technological infrastructure of a blockchain network is distributed across multiple jurisdictions, while legal authority remains primarily territorial. Conventional private international law generally relies on connecting factors such as the location or domicile of the parties, the place of contracting, the place of performance, and the parties' choice of law [37]. These connecting factors become more difficult to apply when a transaction is executed through decentralized infrastructure involving pseudonymous participants and geographically distributed network nodes [38]. Recent research confirms that jurisdiction, applicable law, and enforcement remain fundamental unresolved issues in cross-jurisdictional smart contract transactions. Differences among domestic legal systems concerning contractual validity and the legal recognition of digital arrangements may generate uncertainty when disputes arise. The absence of uniform legislation can therefore affect both the enforceability of smart contracts and the ability of parties to obtain effective remedies [39].

Regulatory interoperability consequently becomes an essential component of cross-border smart contract governance. Interoperability does not necessarily require complete harmonization of national laws. Rather, it requires compatible legal principles and procedural mechanisms that enable different jurisdictions to recognize contractual arrangements, determine applicable law, allocate jurisdiction, and enforce dispute-resolution outcomes. In this context, cross-border regulation should establish predictable connecting factors while preserving the legitimate regulatory authority of individual states [40].

The literature also demonstrates that smart contract regulation increasingly requires coordination between technological design and legal safeguards. Recent comparative discussions identify the continuing importance of traditional private-international-law mechanisms while recognizing the need for technological controls, contractual drafting mechanisms, and dispute-resolution arrangements capable of responding to blockchain-specific risks. Thus, regulatory interoperability should encompass both legal interoperability, concerning recognition and enforcement across jurisdictions, and technical interoperability, concerning the ability of smart contract systems to incorporate legally valid intervention, evidence, and remedial mechanisms.

2.4. Integrated Theoretical Framework

The literature reviewed above demonstrates that smart contract regulation cannot be examined through contractual law alone. Three interconnected dimensions must be considered. First, legal enforceability determines whether automated contractual arrangements can receive legal recognition and effective remedies. Second, decentralized justice determines how disputes arising from automated transactions can be resolved while maintaining procedural fairness and human oversight. Third, cross-border regulatory interoperability determines how these arrangements operate when parties, assets, infrastructure, and enforcement mechanisms extend across different jurisdictions.

Based on these three dimensions, this study develops a regulatory framework consisting of seven interconnected principles:

- Legal validity and enforceability.
- Transparency and explainability.
- Accountability and liability.
- Human oversight and intervention.
- Jurisdiction and applicable law.
- Data protection and digital rights.
- Regulatory interoperability.

These principles are not treated as independent regulatory requirements but as complementary safeguards throughout the smart contract lifecycle. The framework positions technological automation as an instrument rather than a substitute for legal authority. Smart contracts may facilitate efficient transactions and decentralized dispute resolution, but their operation must remain connected to identifiable legal responsibilities, accessible remedies, and mechanisms for human intervention. This theoretical position provides the basis for examining how decentralized justice can be integrated into cross-border digital transactions without sacrificing legal certainty, procedural fairness, accountability, and fundamental digital rights.

3. RESEARCH METHOD

3.1. Research Design and Legal Approach

This study employs a normative legal research method to examine the regulatory challenges associated with smart contracts in decentralized justice and cross-border digital transactions. A normative approach is appropriate because the study focuses on legal norms, principles, regulatory structures, and institutional mechanisms rather than empirical measurement of user behavior or transactional performance. The research is designed to assess whether existing legal frameworks are sufficiently capable of governing automated contractual execution while maintaining legal certainty, accountability, procedural fairness, and effective remedies.

The study applies three complementary legal approaches: statutory, conceptual, and comparative approaches. The statutory approach examines relevant laws and regulatory instruments governing electronic contracts, digital transactions, blockchain-based activities, dispute resolution, data protection, and cross-border transactions. The conceptual approach is used to clarify the legal meaning and relationship between smart contracts, automated contractual execution, decentralized justice, human oversight, and regulatory interoperability. The comparative approach examines how different jurisdictions address smart contract validity, enforceability, jurisdiction, dispute resolution, and digital regulatory governance. The comparison is used not to identify a single superior legal system, but to formulate regulatory principles that can operate across jurisdictions.

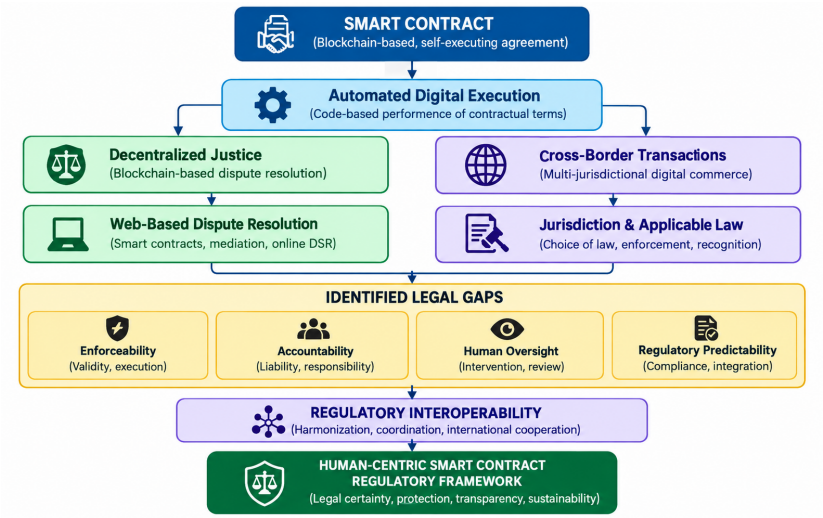


Figure 1. Research Framework for Smart Contract Regulatory Analysis

Figure 1 explains the analytical sequence used in this study. The analysis begins with the technological characteristics of smart contracts and examines their implications for decentralized justice and cross-border transactions. The identified legal gaps are subsequently evaluated through the principles of enforceability, accountability, human oversight, and regulatory interoperability to formulate a human-centric regulatory framework.

3.2. Legal Materials, Collection, and Analytical Procedure

The legal materials consist of primary and secondary legal materials. Primary materials include legislation, regulations, international legal instruments, and other authoritative regulatory documents concerning electronic transactions, digital contracts, blockchain, dispute resolution, data protection, and cross-border digital activities. Secondary materials comprise peer-reviewed journal articles, academic books, legal commentaries, and scholarly studies addressing smart contract regulation, blockchain governance, decentralized justice, and private international law. Legal materials are selected based on their relevance to the research questions, regulatory authority, analytical significance, and capacity to explain the relationship between technological automation and legal governance.

Table 1. Categories of Legal Materials

Category	Materials Examined	Analytical Purpose
Primary legal materials	National legislation and regulations	Identify applicable legal norms and regulatory obligations
International instruments	International conventions, principles, and regulatory frameworks	Examine cross-border legal standards and regulatory coordination
Judicial and institutional materials	Relevant decisions, official guidelines, and institutional documents	Identify practical interpretations and governance mechanisms
Secondary legal materials	Peer-reviewed articles and academic books	Develop theoretical and conceptual foundations
Comparative materials	Selected foreign regulatory frameworks	Identify approaches to smart contract validity, jurisdiction, and enforcement

Table 1 presents the classification of materials used to establish the normative and comparative foundation of the research. Primary legal materials provide the principal source for determining applicable legal norms, while secondary and comparative materials support interpretation, contextualization, and identification of regulatory gaps. The collection and analysis of legal materials are conducted through systematic legal document analysis. Relevant materials are identified according to keywords and concepts directly connected with the research questions, including smart contract, blockchain-based contract, decentralized justice, online dispute resolution, cross-border digital transaction, jurisdiction, applicable law, enforceability, human oversight, and regulatory interoperability. Each material is then examined to determine its regulatory scope, governing principles, legal obligations, enforcement mechanisms, and relevance to automated contractual systems.

Table 2. Analytical Dimensions and Indicators

Analytical Dimension	Key Issues Examined	Expected Regulatory Function
Legal validity and enforceability	Contract formation, consent, validity, remedies	Establish legal recognition and enforceability
Transparency and explainability	Code accessibility, contractual terms, automated outcomes	Enable understanding and legal review
Accountability and liability	Developer, provider, deployer, and user responsibility	Allocate responsibility for unlawful outcomes
Human oversight	Intervention, reversal, review, exceptional circumstances	Preserve procedural fairness and effective remedies
Jurisdiction and applicable law	Choice of law, competent forum, territorial connection	Reduce cross-border legal uncertainty
Data protection and digital rights	Privacy, data processing, digital autonomy	Protect fundamental rights in automated systems
Regulatory interoperability	Recognition, coordination, and enforcement across jurisdictions	Facilitate coherent cross-border governance

Table 2 operationalizes the analytical framework used to evaluate existing legal regimes. Each dimension represents a regulatory problem identified from the literature and legal materials, while its corresponding function specifies the regulatory outcome required to establish a legally accountable smart contract ecosystem. The analysis proceeds through four stages: identifying and classifying relevant legal materials according to their regulatory authority and substantive relevance; interpreting statutory provisions and legal concepts governing smart contracts, digital transactions, and dispute resolution; conducting comparative analysis to identify similarities, differences, and regulatory gaps; and synthesizing the findings into an integrated regulatory model based on the seven dimensions in Table 2.

The resulting framework evaluates whether automated smart contract execution can be reconciled with legal certainty, accountability, procedural fairness, human oversight, digital rights, and cross-border regulatory interoperability. By deriving the framework from identified legal problems and regulatory gaps, the analysis seeks to preserve the functional advantages of decentralized technology while maintaining the legal safeguards required for legitimate and sustainable web-based governance.

4. RESULTS AND DISCUSSION

4.1. Regulatory Gaps in Smart Contract Governance

The normative and comparative analysis indicates that the primary regulatory challenge of smart contracts lies in the gap between automated code-based execution and established legal principles. Although smart contracts can automatically execute predetermined obligations, technological execution does not independently establish contractual validity, enforceability, legal responsibility, applicable law, or available remedies. Therefore, smart-contract design should establish a legally documented relationship between natural-language contractual terms and executable code, with mechanisms for suspension, legal review, correction, reversal, or other remedies where inconsistencies, programming errors, inaccurate information, unauthorized transactions, or unforeseen circumstances occur. Accountability should be allocated according to the roles, control, contribution to harm, foreseeability, knowledge of risks, and contractual or statutory duties of developers, deployers, service providers, platform operators, and users, rather than imposing automatic liability on all participants. At the same time, human oversight should remain available for unlawful, unauthorized, disproportionate, or manifestly erroneous outcomes, including disputed consent, suspected fraud, coding errors, conflicts between code and contractual terms, breaches of mandatory law, and materially unforeseen circumstances. Accordingly, smart-contract regulation should adopt a lifecycle-based approach that preserves the efficiency of automation while ensuring legal certainty, identifiable responsibility, human oversight, procedural fairness, and access to appropriate remedies.

4.2. Smart Contracts and Decentralized Justice

The analysis demonstrates that smart contracts can support decentralized justice by facilitating predetermined dispute procedures, escrow mechanisms, automated consequences, and web-based dispute resolution. These mechanisms may improve procedural efficiency, reduce transaction costs, and provide dispute-resolution options across geographical boundaries. However, decentralization does not automatically guarantee justice. Code-based dispute mechanisms may encounter difficulties concerning due process, impartiality, evidence, human review, and access to remedies. Automated decisions may also fail to account for circumstances that were not anticipated during the development of the code. Since contractual code is designed by human actors, it may contain errors, biases, or assumptions that affect the resulting outcome. Accordingly, the findings support a human-centric conception of decentralized justice. Human oversight should not be viewed as a rejection of automation but as a safeguard for exceptional situations in which automated execution may conflict with legal requirements or fundamental principles of fairness. Decentralized mechanisms can therefore perform routine and predetermined functions while human review remains available for complex disputes and potentially unjust outcomes.

4.3. Cross-Border Jurisdiction and Regulatory Interoperability

Cross-border smart contract transactions create legal uncertainty because parties, digital assets, service providers, and blockchain infrastructure may span multiple jurisdictions. Traditional private international law relies on connecting factors such as the parties' location or domicile, place of contracting, place of performance, and choice of law, but their application becomes more complex with pseudonymous participants and decentralized blockchain infrastructure. The analysis therefore identifies jurisdiction, applicable law, and enforcement as central regulatory concerns. Blockchain infrastructure cannot determine the governing legal system by itself; instead, applicable law and competent jurisdiction should be determined through established connecting factors, including the parties' location or domicile, place of contracting and performance, valid governing-law or jurisdiction clauses, and, where relevant, the location of assets connected to the dispute. These factors should be assessed collectively rather than relying solely on blockchain nodes or the technical location of transaction execution. Where parties have made a valid choice of law or jurisdiction, such agreement should remain subject to mandatory rules and jurisdictional limitations of the applicable legal system.

In the absence of an effective choice-of-law or jurisdiction clause, courts or competent authorities may rely on the most relevant connecting factors under applicable private international law. Cross-border conflicts may be addressed through recognition and enforcement rules, contractual dispute-resolution mechanisms, applicable international instruments, and regulatory interoperability. Smart contract governance should therefore establish predictable connecting factors and appropriate mechanisms for determining applicable law and competent forums. Regulatory interoperability does not require complete harmonization of national laws, but sufficient compatibility among legal and procedural mechanisms to facilitate recognition of contractual

arrangements, determination of jurisdiction, and enforcement of dispute-resolution outcomes across borders. This approach can reduce regulatory fragmentation, improve predictability for cross-border smart contract transactions, and preserve the legitimate legal authority of individual states.

4.4. Integrated Seven-Principle Regulatory Framework

Based on the identified regulatory gaps, this study proposes an integrated framework consisting of seven interconnected principles. These principles are designed to operate as complementary safeguards throughout the smart contract lifecycle, from contractual formation and deployment to execution, dispute resolution, and enforcement. Operationally, the seven principles can be translated into governance mechanisms, responsible actors, and legal checkpoints at each stage of the smart-contract lifecycle. During contractual formation, legal validity and enforceability require verification of party identity where legally necessary, evidence of informed consent, clear contractual obligations, identification of mandatory legal requirements, and determination of applicable law and remedies. At this stage, the principal legal checkpoint is confirmation that the proposed arrangement is valid, sufficiently clear, and entered into through legally recognizable consent.

During deployment, transparency and explainability require documentation of the relationship between natural-language contractual terms and executable code, independent or qualified code review where appropriate, and identification of responsible developers, deployers, and service providers. The legal checkpoint at this stage is confirmation that the deployed code corresponds materially to the agreed contractual terms and that relevant responsibilities are documented before execution begins. During execution, platform operators and other designated actors should monitor transactions and maintain alerts or intervention mechanisms for exceptional conditions, including suspected fraud, unauthorized transactions, coding errors, or potentially unlawful outcomes. The relevant legal checkpoint is the activation of human review or temporary suspension where predefined intervention criteria are satisfied.

During dispute resolution, authorized reviewers, arbitrators, or other legally competent actors should ensure evidence submission, procedural fairness, human assessment, and access to legally recognized remedies. The legal checkpoint at this stage is confirmation that automated procedures do not prevent meaningful human review or access to an appropriate dispute-resolution mechanism. Finally, during enforcement, competent authorities, courts, arbitral institutions, or designated enforcement actors should determine applicable law, jurisdiction, recognition, and cross-border enforcement procedures. The legal checkpoint is confirmation that an automated or dispute-resolution outcome satisfies the requirements for legal recognition and enforcement in the relevant jurisdiction. Through these mechanisms, the seven principles operate as lifecycle-based safeguards rather than abstract regulatory objectives.

Table 3. Integrated Regulatory Framework for Smart Contract Governance

Regulatory Principle	**Key Regulatory Focus**	**Expected Outcome**
Legal validity and enforceability	Contract formation, consent, validity, and remedies	Legal recognition and enforceability
Transparency and explainability	Contractual terms, code accessibility, and automated outcomes	Understandable and reviewable execution
Accountability and liability	Responsibility of developers, providers, deployers, and users	Clear allocation of legal responsibility
Human oversight and intervention	Review, intervention, reversal, and exceptional circumstances	Procedural fairness and effective remedies
Jurisdiction and applicable law	Choice of law, competent forum, and territorial connections	Reduced cross-border uncertainty
Data protection and digital rights	Privacy, data minimization, pseudonymity, lawful data processing, individual data rights, and digital autonomy	Protection of fundamental rights
Regulatory interoperability	Recognition, coordination, and enforcement across jurisdictions	Coherent cross-border governance

Table 3 presents the seven principles of the integrated regulatory framework for smart contract governance and their corresponding regulatory focuses and expected outcomes. The first principle establishes that automated execution should remain connected to legally recognized requirements concerning contractual

validity and enforceability. The second ensures that parties and relevant legal institutions can understand the contractual terms and consequences of automated execution. The third allocates responsibility among actors involved in developing, deploying, operating, and using smart contract systems.

The fourth principle establishes human review for exceptional or potentially unlawful automated outcomes, while the fifth provides predictable mechanisms for determining applicable law and competent forums in cross-border transactions. The sixth addresses the tension between blockchain immutability and data-protection rights by requiring data minimization and avoiding unnecessary storage of identifiable personal information on-chain. Where data processing is necessary, pseudonymization, off-chain storage, access controls, and separation of transaction records from identifiable data should be considered, while mechanisms for information, access, correction, objection, restriction, and other applicable rights should be maintained. Pseudonymity should not be treated as complete anonymity where transaction data can be linked to external information. These safeguards should minimize unnecessary personal-data exposure while preserving sufficient evidence for accountability, dispute resolution, and enforcement. Finally, regulatory interoperability supports legal recognition, coordination, and cross-border enforcement, enabling smart-contract efficiency while maintaining legal certainty, accountability, procedural fairness, human oversight, and digital rights.

Table 4. Operationalization of the Seven-Principle Framework Across the Smart Contract Lifecycle

Smart Contract Lifecycle Stage	**Governance Mechanism**	**Relevant Regulatory Principles**	**Expected Legal Safeguard**
Formation	Verification of parties, evidence of consent, clear contractual terms, and determination of applicable law	Legal validity and enforceability, Jurisdiction and applicable law	Valid and legally recognizable contractual arrangement
Deployment	Documentation of code-contract relationships, code review, and identification of responsible actors	Transparency and explainability, Accountability and liability	Explainable code and identifiable legal responsibility
Execution	System monitoring, transaction verification, risk alerts, temporary suspension, human review, and intervention mechanisms for exceptional or legally problematic conditions	Accountability and liability, Human oversight and intervention	Controlled and legally accountable automated execution
Dispute Resolution	Evidence submission, human review, impartial assessment, and access to remedies	Human oversight and intervention, Data protection and digital rights	Procedural fairness and effective remedies
Enforcement	Determination of competent forum, applicable law, recognition, and cross-border enforcement procedures	Jurisdiction and applicable law, Regulatory interoperability	Effective and predictable cross-border enforcement

Table 4 demonstrates how the seven regulatory principles can be operationalized across the smart contract lifecycle. Rather than functioning as separate legal requirements, the principles provide interconnected safeguards from contractual formation through deployment, execution, dispute resolution, and enforcement. This lifecycle-based approach connects the conceptual framework with practical governance mechanisms, including consent verification, code documentation, responsibility allocation, transaction monitoring, human intervention, evidence review, and cross-border enforcement. It therefore provides a practical legal structure for maintaining technological efficiency while strengthening accountability, procedural fairness, and access to

effective remedies. The proposed human-centric smart contract governance framework also supports SDG 16 by strengthening legal certainty, accountability, procedural fairness, and access to justice through legal safeguards and accessible dispute resolution. It contributes to SDG 9 by supporting blockchain innovation and digital infrastructure within predictable and interoperable regulatory environments. By integrating automation with legal safeguards throughout the smart contract lifecycle, the framework promotes digital innovation while preserving institutional accountability and fundamental rights.

5. MANAGERIAL IMPLICATIONS

The findings provide practical implications for managers, digital businesses, blockchain developers, and platform operators that utilize smart contracts in cross-border digital transactions. Organizations should not treat smart contract deployment as a purely technical decision, but should integrate legal review and governance mechanisms throughout the contract lifecycle. In particular, managers should ensure that contractual terms and code are sufficiently transparent, responsibilities among developers, providers, deployers, and users are clearly defined, and appropriate human intervention mechanisms are available for exceptional or potentially unlawful outcomes. For cross-border operations, managers should also establish clear provisions concerning applicable law, jurisdiction, dispute resolution, data protection, and regulatory compliance. Implementing these principles can help organizations maintain the efficiency and automation of smart contracts while reducing legal uncertainty.

6. CONCLUSION

This study examined the regulatory challenges of smart contracts in decentralized justice and cross-border digital transactions through a normative legal and comparative approach. The findings demonstrate that automated code-based execution cannot independently determine contractual validity, enforceability, legal responsibility, jurisdiction, applicable law, remedies, or procedural fairness. The analysis identifies regulatory gaps concerning the relationship between natural-language contractual terms and executable code, particularly where programming errors, inaccurate information, unauthorized transactions, fraud, or unforeseen circumstances may produce outcomes that conflict with legal requirements or the parties' legitimate expectations. These findings demonstrate that technological execution should remain connected to established principles of contractual law, legal validity, enforceability, and access to legally recognized remedies.

The study also identifies significant challenges concerning accountability, liability, human intervention, and cross-border jurisdiction. Responsibility should remain identifiable according to the role and contribution of developers, deployers, service providers, platform operators, and users, taking into account control, foreseeability, knowledge of risks, contractual and statutory duties, causation, and contribution to harm. Decentralization should therefore not be interpreted as the absence of legal responsibility. In cross-border transactions, applicable law and competent jurisdiction should be determined through relevant connecting factors, including the parties' location or domicile, place of contracting and performance, valid governing-law or jurisdiction clauses, and other legally relevant connections. Regulatory interoperability should support recognition, coordination, and enforcement across jurisdictions without requiring complete harmonization of national laws.

To address these challenges, the study proposes an integrated seven-principle regulatory framework comprising legal validity and enforceability, transparency and explainability, accountability and liability, human oversight and intervention, jurisdiction and applicable law, data protection and digital rights, and regulatory interoperability. The principles operate as interconnected safeguards throughout the smart contract lifecycle, from formation and deployment to execution, dispute resolution, and enforcement. Their operationalization includes consent verification, documentation of the relationship between contractual terms and code, identification of responsible actors, transaction monitoring, human intervention, evidence assessment, access to remedies, and cross-border enforcement mechanisms. Human oversight remains available for exceptional circumstances such as disputed consent, suspected fraud, coding errors, unauthorized transactions, conflicts between code and contractual terms, breaches of mandatory law, or materially unforeseen circumstances, while data protection is supported through data minimization, pseudonymization, off-chain storage, and applicable individual rights. The framework provides a human-centric foundation that preserves technological efficiency while strengthening legal certainty, accountability, procedural fairness, digital rights, and effective cross-border enforcement,

while supporting SDG 16 and SDG 9 through accountable digital governance, access to justice, and predictable blockchain infrastructure.

7. DECLARATIONS

7.1. About Authors

Shofiyul Millah (SM) https://orcid.org/0000-0002-6696-9450
Steven Harazaki Lase (SL) https://orcid.org/0009-0002-6647-7541
Natalie Septiani (NS) https://orcid.org/0009-0008-9303-5478
Suca Rusdian (SR) https://orcid.org/0009-0008-4805-1524

7.2. Author Contributions

Conceptualization: SM; Methodology: SR; Software: NS; Validation: SL, SM and NS; Formal Analysis: SR and NS; Investigation: SM; Resources: SL; Data Curation: SL and SR; Writing Original Draft Preparation: SL and SM; Writing Review and Editing: SL and NS; Visualization: SL; All authors, SM, SL, NS, and SR, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] C. Poncibò, A. Gangemi, and G. S. Ravot, "Blockchain justice: Exploring decentralising dispute resolution across borders," *JL, Mkt. & Innovation*, p. 14, 2024.
[2] S. Yadav and R. R. Singh, "Decentralized dispute resolution in international trade with blockchain and smart contracts," *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, vol. 18, no. 2, p. 04526006, 2026.
[3] R. Widayanti, M. H. R. Chakim, C. Lukita, U. Rahardja, and N. Lutfiani, "Improving recommender systems using hybrid techniques of collaborative filtering and content-based filtering," *Journal of Applied Data Sciences*, vol. 4, no. 3, pp. 289–302, 2023.
[4] G. A. Atiyah, N. A. Manap, and S. N. Abd Aziz, "Legitimacy of smart contracts written in encrypted code on blockchain technology under current contract law: a comparative study," *Intellectual Discourse*, vol. 31, no. 2, 2023.
[5] D. Chaudhary, "Smart contracts and legal enforcement across jurisdictions," *Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT)*, vol. 3, no. 1, pp. 1–10, 2026.
[6] H. Purnomo, K. D. Hartomo, U. Rahardja, A. Ramadan *et al.*, "The impact of smart contracts on cyberpreneurship in contemporary business marketing," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–6.
[7] A. S. Khalifa and N. S. Samad, "Smart contracts and the challenges of conflict of laws in digital space," *Indonesian Journal of Law and Economics Review*, vol. 20, no. 4, pp. 10–21 070, 2025.

[8] A. Desai, "Integrating smart contracts with hybrid online dispute resolution mechanisms in cross-border commercial transactions," *Jus Corpus LJ*, vol. 5, p. 194, 2024.
[9] N. Lutfiani, U. Rahardja, S. Wijono, K. D. Hartomo, and H. Purnomo, "Unlocking the potential of ai-enabled startup through digital talent in higher education," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–6.
[10] R. Qodar, M. Aprilia, and M. A. Zulkifli, "Standardizing asean smart contract law: Protecting msmes and advancing transactional justice in the digital era," in *Proceedings of Annual Conference on Scientific Writing*, vol. 3, 2026, pp. 221–233.
[11] S. Sadulla, "Smart contract enforcement and legal liability in decentralized cross-national digital transactions," *Sirashmi Perspectives in Cyber Law, Intellectual Property, and Legal Studies*, pp. 20–37, 2026.
[12] T. Sendjaja, D. J. Rachbini, R. Astini, and D. Asih, "Driving socialpreneurship and diving into digital transformation to enhance donation intentions in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 687–700, 2025.
[13] M. Vatiero, "Smart contracts vs incomplete contracts: A transaction cost economics viewpoint," *Computer Law & Security Review*, vol. 46, p. 105710, 2022.
[14] M. J. Schmidt-Kessen, H. Eenmaa, and M. Mitre, "Machines that make and keep promises-lessons for contract automation from algorithmic trading on financial markets," *Computer Law & Security Review*, vol. 46, p. 105717, 2022.
[15] U. Rusilowati, F. P. Oganda, R. Rahardja, T. Nurtino, and E. Aimee, "Innovation in smart marketing: The role of technopreneurs in driving educational improvement," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 305–318, 2023.
[16] F. Gamper, "A non-contractual approach to smart contracts," *International Journal of Law and Information Technology*, vol. 31, no. 3, pp. 231–252, 2023.
[17] V. Papadouli and V. Papakonstantinou, "A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs," *Computer Law & Security Review*, vol. 51, p. 105869, 2023.
[18] H. Herman, N. P. L. Santoso, A. Avandi, N. Septiani, and O. Sy, "Legal governance of artificial intelligence in sustainable digital business ecosystems," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 209–221, 2026.
[19] G. A. Atiyah, A. I. Ibrahim, and A. A. Jasim, "Enforcement of smart contracts in cross-jurisdictional transactions," *International Journal of Law and Management*, vol. 68, no. 2, pp. 319–344, 2026.
[20] J. Y. L. Song and E. Tan, "Beyond traditional contracts: the legal recognition and challenges of smart contracts in malaysia and singapore," *JL, Mkt. & Innovation*, p. 323, 2024.
[21] Q. Aini, S. H. Lase, A. Adiwijaya, F. I. Ningrum, D. A. Prabowo, and T. Green, "Adaptive legal architectures for governing autonomoustechnologies in sustainable digital societies," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 56–67, 2026.
[22] C. Chambefort and M. Chaudey, "Blockchain, tokens, smart contracts, and "decentralized autonomous organization": Expanding and renewing the mechanisms of governance?" *European Management Review*, vol. 21, no. 3, pp. 511–515, 2024.
[23] T. T. M. Jiang, "Smart contracts and legal enforceability: Bridging the," in *Proceedings of the 5th International Conference on Economic Development and Business Culture (ICEDBC 2025)*. Springer Nature, 2026, p. 24.
[24] I. Sembiring, B. K. Aji, and T. I. Bayu, "Consortium blockchain framework for secure digital medical record innovation," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 138–151, 2026.
[25] Y. Gabuthy, "Blockchain-based dispute resolution: insights and challenges," *Games*, vol. 14, no. 3, p. 34, 2023.
[26] F. Ast, W. George, J. Kamalova, A. Sharma, and Y. Aouidef, "Decentralized justice: state of the art, recurring criticisms and next-generation research topics," *Frontiers in Blockchain*, vol. 6, p. 1204090, 2023.
[27] Q. Aini, E. P. Harahap, N. P. L. Santoso, S. N. Sari, and P. A. Sunarya, "Blockchain based certificate verification system management," *Aptisi Transactions on Management (ATM)*, vol. 7, no. 3, pp. 1–10, 2023.
[28] A. Zhuk, "Applying blockchain to the modern legal system: Kleros as a decentralised dispute resolution system," *International Cybersecurity Law Review*, vol. 4, no. 3, pp. 351–364, 2023.

[29] D. Sulistianingsih, A. A. Rante Lembang, Y. P. Adhi, and M. S. Prabowo, "Online dispute resolution: Does the system actually enhance the mediation framework?" *Cogent Social Sciences*, vol. 9, no. 1, p. 2206348, 2023.

[30] U. Rahardja, Q. Aini, A. Khairunisa, and S. Millah, "Implementation of blockchain technology in learning management system (lms)," *APTISI Transactions on Management (ATM)*, vol. 6, no. 2, pp. 112–120, 2022.

[31] L. T. Handoyo, A. W. Prawira, and A. Aswanto, "The future of smart contracts in indonesia's commercial and business law system," *Iustitia: Journal of Legal Theory, Politics, and International Relations*, vol. 1, no. 2, pp. 64–80, 2026.

[32] C. Salger, "Decentralized dispute resolution: using blockchain technology and smart contracts in arbitration," *Pepp. Disp. Resol. LJ*, vol. 24, p. 65, 2024.

[33] K. M. Wongkar, T. F. Satriawan, N. P. L. Santoso, and N. Rangi, "Leveraging blockchain governance and smart contracts for entrepreneurs in social media," *Blockchain Frontier Technology*, vol. 6, no. 1, pp. 86–96, 2026.

[34] M. T. Ngcobo, "Artificial intelligence and blockchain technologies in online dispute resolution: A solution to consumer disputes in south africa?" *Potchefstroom Electronic Law Journal (PELJ)*, vol. 27, no. 1, pp. 1–25, 2024.

[35] C. C. Kadioglu Kumtepe, "Unpacking the technology of trust: establishing trust and fairness in online dispute resolution through blockchain and smart contracts," *International Journal of Law and Information Technology*, vol. 33, p. eaaf017, 2025.

[36] A. Theriana, S. W. Fitriati, R. P. Haryani, K. Rustipa, and J. Edwards, "Blockchain governance and teacher empowerment to enhance digital edupreneurship in the merdeka curriculum," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 60–70, 2025.

[37] C. C. Kadioglu Kumtepe, "Blockchain and smart contracts for avoiding and resolving construction disputes and enforcing dispute adjudication board decisions," *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, vol. 17, no. 3, p. 04525023, 2025.

[38] D. Budhijanto, P. Amalia, and N. A. Shiddiq, "Blockchain arbitration: roadmap to recognition and enforcement of arbitral award," *Cogent Social Sciences*, vol. 11, no. 1, p. 2536726, 2025.

[39] Singapore Courts, "Registrar's circular no. 2 of 2026: Establishment of digital economy specialised list," Mar. 2026, registrar's Circular No. 2 of 2026. [Online]. Available: https://www.judiciary.gov.sg/news-and-resources/registrar%27s-circulars/circular-details/registrar%27s-circular-no.-2-of-2026-supreme-court

[40] D. A. Zetzsche, L. Anker-Sørensen, M. L. Passador, and A. Wehrli, "Dlt-based enhancement of cross-border payment efficiency–a legal and regulatory perspective," *Law and Financial Markets Review*, vol. 15, no. 1-2, pp. 70–115, 2021.