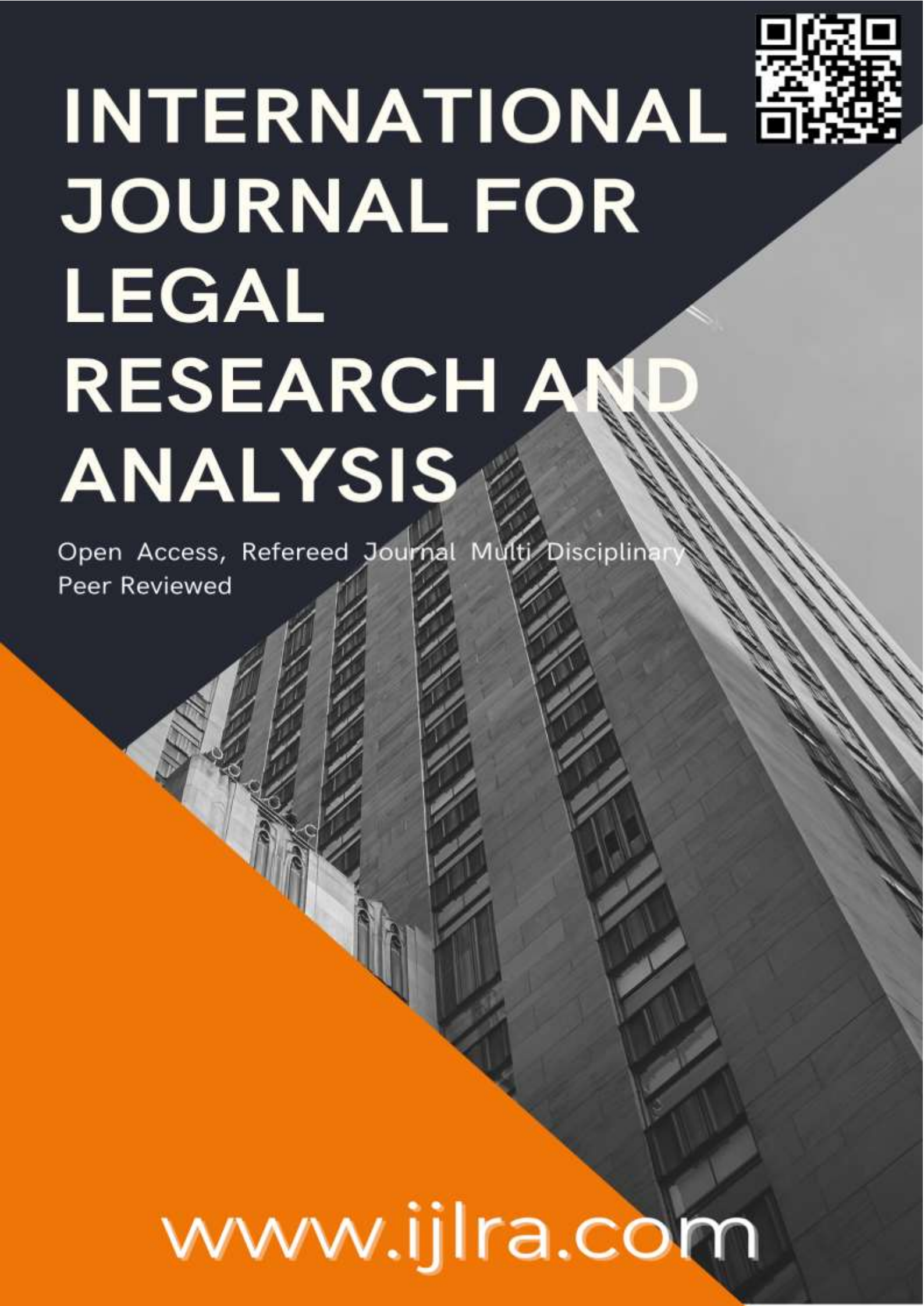
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

LIABILITY IN SMART CONTRACTS:A CRITICAL ANALYIS UNDER INDIAN CONTRACT LAW

AUTHORED BY - VANSH CHAUHAN
Amity University

ABSTRACT:

The increasing integration of blockchain technology into commercial transactions has led to the emergence of smart contracts—self-executing agreements governed by code rather than traditional legal language. While these contracts promise efficiency, transparency, and reduced transactional costs, they simultaneously introduce significant legal uncertainties, particularly concerning liability. This paper critically examines the concept of liability in smart contracts within the framework of Indian Contract Law. It explores whether traditional legal doctrines such as consent, breach, and negligence can effectively address disputes arising from automated contractual systems. The study further evaluates challenges such as coding errors, decentralization, anonymity, and jurisdictional ambiguity. It argues that while existing legal provisions offer partial solutions, they are inadequate to fully regulate smart contracts. The paper concludes by advocating for a hybrid regulatory model that combines technological innovation with legal accountability.

INTRODUCTION:

The evolution of contract law has consistently been influenced by technological advancements. From oral agreements to written contracts and now to digital transactions, the law has adapted to accommodate changing commercial realities. The introduction of smart contracts marks a significant shift in this trajectory. Unlike traditional contracts that rely on textual interpretation and judicial enforcement, smart contracts operate through automated code deployed on blockchain networks.

Smart contracts are designed to execute predefined actions once certain conditions are met, thereby minimizing the need for intermediaries. While this feature enhances efficiency and reduces costs, it also raises fundamental legal concerns. One of the most pressing issues is the allocation of liability when things go wrong. In conventional contracts, liability is determined based on breach, intention, and fault. However, in smart contracts, where execution is automatic and often irreversible, identifying the responsible party becomes complex.

In India, the absence of specific legislation governing smart contracts further complicates the issue. Existing statutes such as the Indian Contract Act, 1872, and the Information Technology

ISSN: 2582-6433

ISSN: 2582-6433

Act, 2000, provide a general framework for electronic agreements, but they do not adequately address the unique challenges posed by blockchain-based transactions.

Conceptual Framework of Smart Contracts :

Smart contracts can be understood as computer programs that facilitate, verify, and enforce the performance of contractual obligations. They are typically deployed on blockchain platforms, where they operate in a decentralized and tamper-resistant environment. The defining characteristic of smart contracts is their ability to execute automatically without requiring human intervention.

However, it is important to distinguish between "smart contract code" and "legal contracts." Not all smart contracts constitute legally binding agreements. For a smart contract to be recognized as a valid contract under Indian law, it must satisfy essential elements such as offer, acceptance, lawful consideration, and free consent.

A critical issue arises from the fact that smart contracts are expressed in programming languages rather than natural language. This creates a disconnect between legal intent and technical execution. While traditional contracts allow for interpretation and flexibility, smart contracts operate strictly according to their coded instructions. This rigidity can lead to unintended consequences, particularly when the code does not accurately reflect the parties' intentions.

ISSN: 2582-6433

Legal Framework Governing Smart Contracts in India:

1- Indian Contract Act, 1872

The Indian Contract Act lays down the fundamental principles governing contractual relationships. For a contract to be valid, it must involve:

A lawful offer and acceptance

* Consideration

* Free consent

* Competency of parties

Smart contracts can satisfy these requirements. For instance, offer and acceptance can be represented through digital interfaces, and consideration can be executed through cryptocurrency or digital payments. However, the requirement of free consent raises concerns in automated systems where execution occurs without active human participation at the time of performance.

2- Information Technology Act, 2000:

The Information Technology Act recognizes electronic records and digital signatures, thereby providing legal validity to electronic contracts. This Act supports the enforceability of smart contracts to some extent. However, it does not address issues such as automated execution, coding errors, or decentralized systems.

3- Indian Evidence Act, 1872:

The admissibility of electronic records is governed by Sections 65-A and 65-B of the Evidence Act. Blockchain records may be admissible as evidence, but their technical nature poses challenges in interpretation. Courts may require expert testimony to understand the functioning of smart contracts, which adds complexity to dispute resolution.

ISSN: 2582-6433

Nature of Liability in Contract Law:

Liability in contract law typically arises when a party fails to perform its obligations. The legal system identifies liability based on principles such as breach, negligence, and intention.
Remedies may include damages, specific performance, or injunctions.

In the context of smart contracts, these traditional principles are difficult to apply due to: The absence of human intervention

* The automated execution of obligations

* The irreversible nature of blockchain transactions

This creates a situation where liability cannot be easily attributed to using conventional legal doctrines.

ISSN: 2582-6433

Key Issues in Determining Liability:

1 Coding Errors and Software Vulnerabilities

One of the most critical challenges in smart contracts is the risk of coding errors. Since these contracts rely entirely on software, even minor bugs can lead to significant financial losses. Unlike traditional contracts, where errors can be rectified through negotiation or judicial intervention, smart contracts execute automatically without scope for correction.From a legal perspective, the question arises whether developers should be held liable for such errors. While negligence principles may apply, proving fault is difficult in decentralized and open-source environments.

2- Absence of Human Control

Smart contracts operate independently once deployed. This lack of human oversight creates uncertainty regarding responsibility. If a contract executes in a manner that causes harm, it is unclear whether liability should be assigned to the parties, the developer, or the platform.

3- Immutability and Irreversibility

ISSN: 2582-6433

Blockchain technology is designed to be immutable, meaning that once a transaction is recorded, it cannot be altered. While this ensures transparency and security, it also limits the ability to correct mistakes. Courts may find it difficult to provide effective remedies in such situations.

4- Consent and Intention

Traditional contract law emphasizes the importance of mutual consent. In smart contracts, however, consent is often embedded in code, raising questions about whether parties fully understand the terms of the agreement. This issue becomes particularly relevant when complex coding structures are involved.

5- Anonymity and Identification of Parties

Blockchain transactions often involve pseudonymous participants, making it difficult to identify the parties involved. This poses a significant challenge in enforcing liability, as legal action requires identifiable defendants.

6- Jurisdictional Complexity

Smart contracts operate across borders, making it difficult to determine the applicable law and jurisdiction. This creates uncertainty in dispute resolution and enforcement of judgments.

7 -Role of Third Parties (Oracles and Platforms)

Smart contracts frequently rely on external data sources known as oracles. If incorrect data is provided, the contract may execute improperly. In such cases, the liability of oracle providers becomes a critical issue.

The "Code vs Contract" Debate

A central question in smart contract law is whether the code itself constitutes the contract or merely represents a mechanism for execution. The "code is law" theory suggests that the code defines the rights and obligations of the parties. However, this approach is problematic because it ignores the importance of legal interpretation and fairness. Courts are more likely to treat smart contracts as tools for implementing legal agreements rather than substitutes for them. This perspective allows for the application of traditional legal principles in resolving disputes.

ISSN: 2582-6433

Application of Traditional Legal Doctrines

1- Mistake

Errors in coding may be treated as mistakes under contract law. Depending on the circumstances, these may be classified as unilateral or mutual mistakes.

2 -Frustration

If unforeseen events prevent the execution of a smart contract, the doctrine of frustration may apply. However, the automated nature of these contracts limits the flexibility required for this doctrine.

3 -Unjust Enrichment

If one party benefits unfairly due to a flaw in the contract, the principle of unjust enrichment may provide a basis for restitution.

Comparative Analysis:

International jurisdictions have begun to address the legal challenges posed by smart contracts. In countries like the United States and the United Kingdom, courts have shown a willingness to recognize smart contracts while applying traditional legal principles. However, even in these jurisdictions, there is no consensus on how to assign liability. This highlights the need for a comprehensive legal framework.

ISSN: 2582-6433

Case Study: The DAO Incident

The DAO hack of 2016 serves as a significant example of the risks associated with smart contracts. A vulnerability in the code was exploited, resulting in substantial financial losses.

ISSN: 2582-6433

Despite the technical legality of the transaction, it raised serious ethical and legal concerns.This case demonstrates the limitations of relying solely on code and underscores the need for legal oversight.

Challenges in the Indian Context:

India faces several challenges in regulating smart contracts:

* Lack of specific legislation

* Limited judicial experience with blockchain technology

* Technical complexity of disputes

* Absence of regulatory guidelines

Recommendations:

1- Development of a Regulatory Framework

India should introduce specific regulations addressing smart contracts, including provisions on liability and dispute resolution.

2- Adoption of Hybrid Contracts

Combining traditional legal agreements with smart contract execution can provide clarity and flexibility.

3- Clear Allocation of Risk

Contracts should explicitly define liability for coding errors and technical failures.

4 -Judicial and Technical Training

Judges and legal professionals must be trained to understand blockchain technology.

ISSN: 2582-6433

CONCLUSION:

Smart contracts represent a transformative development in the field of contract law. While they offer significant advantages in terms of efficiency and automation, they also introduce complex legal challenges, particularly in relation to liability.

The existing legal framework in India is not fully equipped to address these challenges. A proactive approach involving legislative reform, judicial adaptation, and technological integration is essential to ensure that smart contracts can function effectively within the legal system.