



INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

SMART CONTRACTS AND CORPORATE COMPLIANCE IN INDIA: ASSESSING THE LEGAL CHALLENGES OF AUTOMATED

AUTHORED BY - SHANMUGAM PRUDHVI

Abstract

This paper examines the legal challenges posed by smart contracts in the context of corporate compliance in India, with particular attention to the emerging model of automated governance. As blockchain-based systems increasingly enable self-executing contractual arrangements, they offer the potential to improve transparency, auditability, efficiency, and real-time compliance monitoring in corporate operations. However, their adoption within the Indian legal framework raises important questions concerning contractual enforceability, legal recognition, and evidentiary reliability, and jurisdiction, liability for coding errors, privacy, and regulatory oversight. Using a doctrinal and analytical method, the paper evaluates the compatibility of smart contracts with Indian contract law, electronic evidence rules, company law obligations, and the broader regulatory environment. It also considers how automated compliance tools may function within corporate governance while remaining subject to human supervision and legal accountability. The study finds that while Indian law is partially capable of accommodating smart contracts, significant doctrinal and institutional uncertainties remain, especially in relation to consent, dispute resolution, and the limits of code-based execution. The paper concludes that smart contracts can support corporate compliance in India, but their effective use requires clearer statutory recognition, hybrid legal-technical drafting, and stronger regulatory guidance to ensure that automation strengthens rather than undermines governance and accountability.

Keywords:

Smart contracts, corporate compliance, automated governance, blockchain, Indian contract law, Legal enforceability.

1. Introduction

Digital technologies are evolving rapidly and have revolutionized the way businesses operate, communicate and meet legal and regulatory requirements¹. One of the most important technological advancements of the 21st century is the invention of blockchain technology, a disruptive force that may change legal, financial, and corporate governance systems. Although blockchain technology was originally designed to facilitate transactions in cryptocurrencies² like Bitcoin, it has since expanded with the potential of many uses besides cryptocurrencies. Smart contracts are perhaps one of the most significant developments of blockchain technology that allows for the automatic execution of contractual obligations through computer code running on a decentralized network³. Smart contracts are a growing interest as a way to automate corporate compliance and governance processes as efficiency, transparency, and accountability become more important for organizations. Smart contracts were originally introduced by Nick Szabo in the 1990s as computer programs that self-execute the conditions of an agreement⁴. Smart contracts are self-executing contracts, unlike traditional contracts, which are enforced through human interaction, administration, or the judiciary system. They are then deployed based on preprogrammed instructions, and when they are deployed, they can automatically fulfill contractual obligations of releasing payments, granting access rights, making records or verifying compliance conditions. Blockchain technology can also help to prevent fraud, manipulation, and unauthorized record changes, as transactions are recorded in an immutable and transparent way. Smart contracts have therefore been accepted as tools that can help to optimize the operation, lower transaction costs, cut down on delays, and increase trust between those involved.

Smart contracts are gaining traction and having a major impact on corporate governance and compliance management.⁵ Corporate compliance is a mechanism, a policy and a set of procedures that corporations use to make sure they are complying with the law, regulatory standards, internal policies and ethical obligations. The enforcement of corporate compliance is getting complex in India as a result of the growing number of laws and regulations that regulate companies, such as the Companies Act, 2013, the Securities and Exchange Board of India (SEBI) securities regulations, directives issued by the Reserve Bank of India (RBI), anti-money laundering requirements, data protection obligations, and industry-specific compliance frameworks⁶. The process of ensuring compliance with these obligations can be very time-consuming, with ongoing

monitoring, reporting on a periodic basis, and significant record-keeping⁷. Consequently, the corporate sector is increasingly looking to technological solutions that can help to streamline compliance processes, improve accuracy and accountability. Smart contracts present the potential to create a proactive and automated system for corporate compliance, rather than a reactive and manual one. Having compliance requirements embedded in programmable code enables organizations to develop governance systems which automatically checks conditions, alerts, approves, maintains audit trails for compliance and enforces procedure. In the case of smart contracts, for instance, they can be applied to automate the approval process at the board, ensure compliance with deadlines for regulatory filings, track contractual obligations, limit access privileges, and fund transfers only after specific conditions are met.⁸ Such applications make compliance part of the organisation's day-to-day functioning as opposed to an independent supervisory task.

Additionally, the immutability of blockchain records can help improve transparency and make auditing easier by being able to provide verifiable evidence of corporate actions and compliance activities. However, the use of smart contracts in corporate governance brings up many legal and regulatory issues. Often, corporate governance requires judicial decisions, interpretation of law, discretion, contextual judgment and fiduciary duties that cannot be programmed. Corporate directors and officers continue to have the duty of compliance with statutory obligations, the exercise of independent judgment and acting in the best interests of the company. As governments become more and more dependent on automated governance systems, accountability, oversight and responsibility issues need to be addressed when technology fails or has unanticipated effects. The definition of smart contracts' legal status is also a topic of discussion. While the Indian Information Technology Act, 2000, has made electronic contracts and electronic records legally valid, there is no comprehensive legislation that comprehensively addresses blockchain-based smart contracts⁹. The enforceability of smart contracts needs, therefore, to be evaluated under the existing legal principles such as are laid down in the Indian Contract Act, 1872. Is it enough to satisfy the classic elements of offer, acceptance, free consent, lawful consideration and intention to create legal relations¹⁰? Further issues arise when there are differences between what is expected in the contract (as stated in natural language) and how it will be executed in computer code. Under these conditions, courts might need to decide whether the law is to be applied based on the binding

contract or on the implementation of the code.

Moreover, in the corporate compliance environment, issues of liability, cyber security, data protection, jurisdiction, and dispute resolution arise. Unintended execution of contractual obligations or compliance failures may result from coding errors, software vulnerabilities or security breaches. Many smart contracts rely on an external data provider – oracles – to provide data required to execute a smart contract. Where this information is incorrect or altered, the consequences could lead to lawsuits and compliance issues. Likewise, the cross-border and decentralized nature of blockchain networks makes it difficult to decide on governing law, jurisdiction, regulatory oversight and enforcement

The unalterability of blockchain's records can also generate conflicts with privacy and data protection demands, specifically when there are legal obligations for corrections, modifications or deletions of data. Smart Contracts Governance solutions offer opportunities and challenges in the Indian regulatory context. There is a certain level of support in the Information Technology Act, 2000; Bharatiya Sakshya Adhiniyam, 2023; and the Companies Act, 2013 for the digital transactions and electronic records; however, there isn't a specific legal framework for automated governance. No comprehensive policy has been framed by the regulatory authorities like MCA, SEBI, RBI, etc. and the Ministry of Electronics and Information Technology (MeitY) yet, which covers the governance aspects of smart contracts¹¹. As a result, companies wanting to adopt automated compliance solutions have to deal with a complex legal landscape where there is uncertainty over enforcement, accountability, and regulatory acceptance. In the backdrop of this, this study explores the utility of smart contracts in the corporate compliance and governance regime in the Indian legal framework. It explores the possibility of smart contracts to automate compliance tasks, increase transparency, and increase the efficiency of governance while also evaluating legal and regulatory issues surrounding their use. The enforceability, consent, liability, oracle dependence, jurisdiction, privacy, dispute resolution and regulatory oversight issues are given particular attention. The study also examines the scope of existing Indian laws to support smart contract based governance system, and discusses the proposed reforms to make them suitable and enabling for a responsible use. To date, the interaction between new technologies and corporate law has been examined and captured by this paper, which aims to contribute to the

ongoing debate on automated governance and offer a blueprint to balance innovation, transparency, and legal security for corporate India.

2. Literature Review

The growing integration of blockchain technology into commercial and corporate operations has generated significant scholarly interest regarding the legal status and practical implications of smart contracts. In the Indian context, researchers have increasingly examined the potential of smart contracts to automate compliance functions, enhance transparency, and improve governance efficiency.¹² Existing literature generally recognizes smart contracts as self-executing agreements operating through blockchain networks, capable of reducing administrative intervention and creating immutable records of transactions. Scholars have argued that these characteristics may strengthen accountability and facilitate more efficient compliance monitoring within corporate organizations. At the same time, concerns have been raised regarding the compatibility of automated governance systems with traditional legal principles governing contracts, corporate regulation, and regulatory oversight.¹³

Several studies have focused on the enforceability of smart contracts under Indian law. The literature suggests that although the Indian Contract Act, 1872 and the Information Technology Act, 2000 provide a legal foundation for electronic transactions, they do not explicitly recognize blockchain-based smart contracts as a distinct legal instrument.¹⁴ Researchers have emphasized that smart contracts must continue to satisfy traditional contractual requirements such as offer, acceptance, free consent, lawful consideration, and intention to create legal relations.¹⁵ While existing legal doctrines may accommodate certain forms of automated agreements, the absence of specific legislative guidance has created uncertainty regarding interpretation, liability, and dispute resolution in blockchain-based transactions.

A significant body of scholarship also examines the relationship between smart contracts and corporate compliance. Authors have observed that the Companies Act, 2013, SEBI regulations, and various sector-specific compliance obligations impose extensive reporting, disclosure, and governance requirements upon corporate entities¹⁶. Smart contracts have been identified as potential tools for automating compliance monitoring, regulatory reporting, audit trails,

shareholder voting processes, and internal governance mechanisms.¹⁷ Studies indicate that automation may reduce compliance costs, minimize human error, and improve operational efficiency. However, scholars caution that corporate governance frequently requires discretion, fiduciary judgment, and contextual decision-making, functions that cannot always be effectively translated into computer code.¹⁸

The literature further highlights several legal and regulatory challenges associated with automated governance. Particular attention has been given to issues of coding errors, cybersecurity vulnerabilities, oracle dependence, data protection obligations, and accountability for system failures¹⁹. Researchers have noted that blockchain's immutable structure may conflict with privacy and data protection requirements, especially following the enactment of the Digital Personal Data Protection Act, 2023²⁰. Concerns have also been expressed regarding the allocation of liability where automated systems execute unintended actions or where governance failures occur without direct human intervention.

Another recurring theme in the literature is the fragmented nature of India's regulatory approach toward blockchain technology. Various scholars have examined the roles of the Ministry of Corporate Affairs, the Securities and Exchange Board of India, the Reserve Bank of India, and the Ministry of Electronics and Information Technology in regulating digital transactions and compliance technologies.²¹ Although certain initiatives demonstrate increasing regulatory acceptance of blockchain applications²², the absence of a coordinated national framework continues to generate uncertainty for corporations seeking to adopt smart contract-based governance systems. Several authors have therefore recommended the introduction of regulatory sandboxes, technical standards, and statutory reforms to provide greater legal certainty and encourage responsible innovation.

The existing literature provides valuable insights into the legal and technological dimensions of smart contracts. However, most studies focus either on the general enforceability of smart contracts or on blockchain technology as a broader regulatory phenomenon. Relatively limited attention has been devoted to the specific application of smart contracts within India's corporate compliance framework²³ and the challenges associated with integrating automated governance mechanisms

into existing corporate law structures. This research seeks to address that gap by critically examining the legal challenges, regulatory limitations, and governance implications of smart contract-based compliance systems in India.

3. Methodology

This paper adopts a doctrinal legal study with analytical and comparative elements. The doctrinal method is appropriate because the central questions concern legal validity, enforceability, evidentiary treatment, and regulatory compatibility rather than technical programming design. Accordingly, the paper examines how smart contracts and automated governance interact with existing Indian legal doctrine, especially where contract formation, corporate compliance, and electronic evidence are concerned. The analytical element is used to assess the practical implications of automation for corporate governance, while the comparative element helps identify how similar issues have been addressed in other legal systems and what lessons may be relevant for India.

The study is structured around the assumption that smart contracts should be evaluated not merely as software tools but as legally significant arrangements that may alter the way corporate obligations are performed, monitored, and enforced. For that reason, the analysis focuses on the extent to which existing legal norms can accommodate self-executing transactions and whether the current Indian framework requires clarification or reform. This approach is consistent with recent scholarship that evaluates smart contracts against traditional contractual requirements such as offer, acceptance, consent, consideration, and legality, while also comparing India's position with more developed regulatory approaches abroad.

The sources used in this paper are drawn from four main categories. First, it relies on statutes, including the Indian Contract Act, 1872, the Information Technology Act, 2000, the Companies Act, 2013, and the Bharatiya Sakshya Adhiniyam, 2023, because these enactments frame enforceability, digital execution, governance duties, and electronic evidence. Second, it uses case law and judicial principles to evaluate how courts may approach questions of consent, interpretation, and liability in automated transactions. Third, it refers to government and regulatory materials, including policy documents, regulatory guidance, and institutional statements relevant

to blockchain, compliance, and corporate governance. Fourth, it draws on academic articles and policy reports that examine smart contracts, compliance automation, blockchain governance, and reform options in India and abroad.

The analytical framework is legal-interpretive rather than technical, asking how law should respond when code performs obligations that would otherwise be carried out by human actors and where human oversight remains essential. This approach identifies both the opportunities and the limits of smart contracts in Indian corporate compliance, grounded in existing legal sources and reform-oriented analysis.

4. Smart contracts and automated governance

Smart contracts are essentially self-executing contracts where the execution of the code is automatically triggered by a pre-programmed condition. When the condition is met in a blockchain environment, the contract logic is deployed on a distributed ledger, and when the condition is met, the network automatically performs the necessary actions, without the need for another manual action. Their value is that they are rules-based, time-stamped, and hard to change once deployed, therefore suitable for environments in which compliance is an issue, with consistency and traceability being critical factors²⁴. In the corporate governance context, this translates into embedding some of the routine requirements as part of the corporate governance operating system and thus making them part of the compliance process, instead of an event after the fact review system.²⁵ But it's not just the speed of smart contracts that's appealing to companies, it's control. A compliance obligation, once translated into code, can result in approval workflow, prohibit unauthorized activities, or when documentation and verification requirements are met, it can release payment. According to scholars, blockchain helps to minimize the need for intermediaries and discretionary decision making by governance, which decreases the transaction costs and increases the audibility. For corporations, it can prove especially useful when there are recurring events or obligations that are measurable and can be objectively verified, such as filing deadlines, payment releases, permissions to access, internal approvals, etc. Meanwhile, there is a consistent message in the literature that these systems are more effective

4.1 Corporate compliance functions

In corporate compliance, smart contracts can be used to support a wide range of functions. One application is board approvals, where a smart contract can require the digital approval of authorized directors or officers before a transaction is executed, helping ensure procedural compliance and internal accountability. Another use is disclosure management, where time-sensitive filings or disclosures can be tracked and flagged automatically so that corporate teams receive alerts before a deadline is missed. In this sense, automation can turn compliance from a periodic task into a continuous monitoring function.

Smart contracts are also well suited to audit trails because blockchain records are time-stamped and difficult to alter, which makes them useful for later verification by auditors, regulators, or internal compliance teams. Relatedly, internal controls can be embedded directly into the code so that only approved users can authorize sensitive actions, or so that multi-signature approval is required for important corporate decisions. For payment triggers, smart contracts can release funds only after verified conditions are satisfied, such as completion of a milestone, receipt of documentation, or confirmation from a trusted data source. They can also support monitoring obligations by producing continuous logs of compliance activity and by alerting stakeholders when a required step has not been completed. Finally, record verification becomes easier because the ledger can preserve a tamper-resistant history of corporate actions, which strengthens evidentiary reliability and internal transparency²⁶.

4.2 Indian legal framework

The Indian legal framework already provides partial support for digital transactions, but it does not yet offer a dedicated framework for smart contracts as a distinct governance tool. The Information Technology Act, 2000 is important because it gives legal recognition to electronic records and digital signatures and supports electronic contracting through Section 10A. This means that Indian law can recognize contracts formed electronically, but it does not specifically address how to treat self-executing code that performs contractual terms without further human intervention. The Act therefore provides a foundation, but not a complete answer, for automated governance.²⁷

The Indian Contract Act, 1872 remains central because any smart contract must still satisfy the basic requirements of contract formation, including lawful consideration, free consent, lawful

object, and the intention to create legal relations. The literature emphasizes that smart contracts are not outside contract law; rather, they must fit within it, even if execution occurs through code. expects interpretable consent, while code often operates in a binary and rigid manner. For corporate compliance, that means a smart contract may be useful only if its coded performance still reflects This creates a tension between legal doctrine and technological automation, because the law the parties' lawful agreement and the legal consequences remain intelligible in court.

The Companies Act, 2013 is also relevant because corporate governance in India depends on duties relating to disclosure, oversight, record-keeping, internal controls, board processes, and accountability. Smart contracts may help operationalize these duties, but they cannot replace directors' legal responsibilities or the statutory role of corporate organs. Similarly, the Bharatiya Sakshya Adhiniyam, 2023 strengthens the broader evidentiary environment for electronic and digital records,²⁸ which is important because smart contracts will often need to be proven through electronic logs, hashes, or blockchain records in litigation or regulatory review. In addition, SEBI and RBI directions matter because corporate compliance in India often intersects with securities regulation, financial reporting, digital transactions, and regulated payment systems. The result is a fragmented but potentially supportive legal landscape.

4.3 Legal challenges

4.3.1 Enforceability and consent

The first question is whether the code-based performance is a valid legal consent and contractual intention²⁹. Smart contracts might demonstrate that parties agreed to some terms, but there must be a possible agreement that is intelligible and lawful, and can be understood by law. The literature indicates that smart contracts can be considered enforceable as long as there is agreement between the parties about the elements of the contract, but if the code is different from the parties' agreement, there is ambiguity. In corporate compliance settings, this is particularly significant, as governance requirements may be intricate and not necessarily be backed up to binary requirements.

4.3.2 Coding errors and liability

The second problem concerns liability in the event of a mistake in the coding of a smart contract, misfiring, or malfunctioning³⁰. Automated execution of smart contracts can have immediate and expensive repercussions from a tiny programming error. Vulnerabilities, programming errors and security lapses can result in unintended execution or non-performance and thereby make it unclear

who is liable – the programmer, the deployer, the corporate user, or the regulating management body. In a corporate compliance setting, this is a big problem since the errors can lead to disclosures, payments or approvals being made that aren't done by the right person.

4.3.3 Oracle dependence

A third problem is “oracle dependence.” An Oracle can provide many smart contracts with external data necessary to determine if a condition has been met³¹. Even if the smart contract is correct, but the outside input is wrong, incomplete, and/or altered, the contract may perform in an incorrect manner. This results in technical and legal risk with the contract's reliability becoming a dependent of a third-party data chain that might not be fully transparent or reliable. Oracle dependency can be an issue in compliance systems in cases where the input involves facts related to compliance such as price, regulatory status, or delivery information.

4.3.4 Jurisdiction and governing law

The governance of laws and jurisdictions over cross-border smart contracts is difficult. In decentralized systems, the competent forum may not be obvious because there could be a number of users, servers, and transaction points in various jurisdictions. As noted in the literature, blockchain transactions can be located in a variety of jurisdictions and anonymous, making applicable-law analysis, service and enforcement more difficult. Indian corporate compliance thus extends beyond just the code to the contractual documentation and requires companies not to be satisfied with code alone to settle a jurisdictional question, but rather have it accompanied by clauses governing the law under which the contract is to be governed and which will be used to resolve disputes.

4.3.5 Privacy and data protection

There is another significant challenge with privacy, which is that correcting records, deleting blocks, or maintaining confidentiality on the blockchain may be in conflict with the immutability of blockchain technology. Although there are reason to change it or delete it, once data is written into a blockchain, it can be difficult to change or delete. That puts a strain on data protection concepts and on corporate responsibility to protect the business's ³²sensitive data. This becomes a concern in regulated environments, as corporate information can be filled with information regarding personal, financial or commercially sensitive information which may not be permanently published or widely reproduced.

4.3.6 Dispute resolution

Furthermore, smart contracts present difficulties to conventional dispute resolution forums as well³³. Due to the fact that a dispute may become apparent when the contract has already been executed, conventional litigation may not only be too lengthy, but could also fail to deliver a remedy which would be practical enough in this context. The literature suggests that, in such cases, arbitration and online dispute resolution are better suited for resolving smart contract disputes than any other method of dispute resolution.

4.3.7 Regulatory oversight

The final challenge is regulatory oversight. Corporate regulators need visibility into automated governance without stifling innovation, and that requires a careful balance between supervision and flexibility. The literature suggests that auditability, internal controls, and continuous monitoring are essential, but regulators also need standards for accountability, security, and disclosure.³⁴ Without such oversight, smart contracts may increase efficiency in isolated transactions while weakening overall governance control.

4.5 Reform options

From the literature, there are a number of potential reforms available to India. Hybrid contracts are one of the best ways to proceed as they ensure the code does not supersede the legal language. Sandboxing regulations can also be used in a way where testing is done under supervision before large scale implementation. It is important that strong board oversight takes place as the directors should remain responsible for governance regardless of the automation of compliance processes³⁵. One other reform measure is the establishment of clear legal status for smart contracts in Indian laws. Lastly, the strongest recommendation in terms of policy is the coordination of regulations among MCA, SEBI, RBI, and MeitY such that they are not operating independently of each other.

5. Comparative Analysis: International Approaches to Smart Contract Regulation

An examination of international regulatory approaches reveals that a number of jurisdictions have moved decisively to provide legal certainty for smart contracts, and their experiences offer instructive lessons for India. A comparative analysis of the United States, Singapore, the European

Union, and the United Kingdom highlights the range of legislative strategies available and underscores the importance of coordinated, purposive regulation.

5.1 United States

Some U.S. states take charge when it comes to rules about smart contracts. Wyoming stands out, passing laws through its Blockchain Task Force that give real world legal status to groups run by code so called DAOs and accept computer code itself as a proper signed document. Instead of waiting for federal moves, places like Arizona jump in too; their updated Electronic Transactions Act³⁶ says an agreement stays valid even if it runs automatically online. Nevada joins alongside Tennessee, each shaping local policy so digital deals hold weight without question. Because of these efforts, coded contracts meet traditional standards for writing and signatures across several regions no extra steps needed.

Right now, state laws follow updated rules written by the Uniform Law Commission, which include how digital items and online deals should be handled under shared standards. Even though these are not federal mandates, they set common ground where states choose to adopt them. Overseeing finance, the SEC along with the CFTC stepped in separately, explaining how current market regulations still apply even when trades happen through code on blockchains. Their position makes clear: automation cannot override established duties. From all this, one thing stands out U.S. policy leans on local adoption paired with national watchdogs stepping carefully instead of sweeping new acts passed in Congress.

5.2 Singapore

Out there in Asia, few places match Singapore's approach to rules around blockchain and smart contracts. Not focused on tech itself, the country's central bank leans into outcomes - how deals work matters more than what builds them. Laws like the Electronic Transactions Act³⁷ back up online agreements by default. So does the law covering e-commerce. Guidance rolls out clearly when tokens pop up in finance, or firms start moving money using ledgers. Clarity shapes behavior, quietly shaping trust without fanfare.

Notably, Singapore launched Project Ubin along with a FinTech sandbox where blockchain uses like smart contract systems are tested carefully under watchful oversight. Instead of waiting, the country's legal experts through the Academy of Law explored how these digital agreements hold

up in court, using familiar legal rules as reference. One insight stands out: if the original deal is clear enough and the code matches what both sides intended, then it may be legally valid. Rather than relying on theory alone, real progress came by linking hands-on trials, flexible policy spaces, and deep legal review into one steady approach. This mix helped shape something rare a working model for trustable automated contracts grounded in actual practice.

5.3 European Union

Starting off differently, Europe shaped its digital rules around personal rights, affecting how smart contracts operate. Because MiCA became active in 2023, it brought uniform standards for crypto firms in every member country, covering tokens and systems built on blockchains. Instead of treating digital deals as less valid, the eIDAS law³⁸ ensures electronic signatures hold the same weight as paper ones throughout the EU's shared economy. So legality follows technology now, without extra steps needed.

One big challenge comes when GDPR meets smart contracts - blockchains keep data fixed, but people have the right to delete or fix their information. Because of this mismatch, records that cannot change might break privacy rules meant to empower individuals. Guidance from Europe's data watchdog suggests building systems with privacy in mind from day one. Storing private details outside the chain appears safer under current law. Newer legislation called the Data Act adds more clarity by insisting key contract terms stay readable to humans. It also ensures automatic processes do not lock out human decisions completely. Rules like these show how legal systems want fairness built into digital agreements. What happens in Europe may help shape smarter approaches elsewhere too. India could learn from such models while shaping its own path forward.

5.4 United Kingdom

The United Kingdom has pursued an influential common law approach to smart contract recognition. The UK Jurisdiction Taskforce,³⁹ operating under the auspices of the LawTech Delivery Panel, published its landmark Legal Statement on Cryptoassets and Smart Contracts in 2019, concluding that smart contracts are capable of satisfying the requirements of English contract law and that blockchain-recorded transactions can constitute legally valid agreements. This statement, while not legislative in character, has been widely treated as authoritative and has guided both judicial reasoning and commercial practice.

Subsequently, the Law Commission⁴⁰ of England and Wales published a comprehensive report on smart legal contracts in 2021, examining how common law principles apply to coded agreements and recommending that no new primary legislation is required for smart contracts to function within existing English law, though it acknowledged the need for supplementary reform in areas such as electronic trade documents and automated dispute resolution. The Property (Digital Assets etc.) Act 2024 further confirmed the legal status of digital assets under English law. The UK's approach demonstrates that principled common law reasoning, combined with targeted legislative clarification, can provide an effective foundation for smart contract governance without requiring wholesale statutory overhaul. Given India's common law heritage, the UK model is of particular doctrinal relevance.

5.5 Lessons for India

The comparative survey yields several lessons directly applicable to India's regulatory reform agenda. First, statutory recognition need not be comprehensive to be effective; targeted amendments to existing legislation, supported by authoritative institutional statements, can significantly reduce legal uncertainty. Second, regulatory sandboxes have proven valuable across all reviewed jurisdictions as mechanisms for managing innovation risk while generating the empirical evidence necessary for evidence-based regulation. Third, privacy and data protection must be integrated into smart contract frameworks from inception rather than retrofitted after deployment. Fourth, jurisdictions with strong common law traditions have successfully leveraged judicial reasoning and institutional legal analysis to fill legislative gaps, suggesting that India's courts and law reform bodies could play an important transitional role before comprehensive legislation is enacted. Fifth, and most critically, coordinated multi-regulator governance frameworks exemplified by the EU's pan-institutional approach and Singapore's whole-of-government strategy are essential for managing the cross-sectoral implications of smart contracts in corporate compliance.

6. Findings and Recommendations

6.1 Major Findings

The study reveals that blockchain technology possesses significant potential to transform corporate governance by enhancing transparency, accountability, and operational efficiency. The

decentralized and immutable nature of blockchain enables the creation of secure and tamper-resistant corporate records, thereby reducing opportunities for fraud, manipulation, and unauthorized alterations. By maintaining a permanent audit trail of transactions and governance activities, blockchain can strengthen stakeholder confidence and improve the overall integrity of corporate decision-making processes. The research further finds that smart contracts can substantially improve corporate compliance mechanisms through automation. Smart contracts are capable of executing predetermined obligations automatically once specified conditions are fulfilled, thereby reducing reliance on manual intervention and minimizing the risk of human error. Their application in areas such as regulatory reporting, shareholder voting, dividend distribution, and contractual performance can contribute to greater efficiency and cost reduction within corporate entities. The analysis of the Indian legal framework indicates that existing laws provide only partial recognition to blockchain-based transactions and smart contracts. While the Information Technology Act, 2000 recognizes electronic records and electronic transactions, there is no explicit statutory recognition of smart contracts as a distinct legal instrument. Consequently, questions regarding contractual validity, enforceability, interpretation, and dispute resolution continue to create legal uncertainty.

The study also finds that several challenges hinder the widespread adoption of blockchain-enabled corporate governance in India. These include concerns relating to data protection, cybersecurity, jurisdictional conflicts, liability for coding errors, and the absence of a comprehensive regulatory framework. The immutable nature of blockchain may also create tensions with data protection requirements, particularly regarding the modification or deletion of personal information.

Comparative analysis confirms that jurisdictions such as the United States, Singapore, the EU, and the UK have adopted more proactive approaches toward blockchain regulation, offering valuable lessons for India in developing balanced frameworks that encourage innovation while ensuring legal certainty. Finally, the research concludes that blockchain technology and smart contracts should not be viewed as complete replacements for existing corporate governance structures. Rather, they should be regarded as complementary tools capable of enhancing governance efficiency, strengthening compliance mechanisms, and improving transparency when supported by an appropriate legal and regulatory framework.

6.2 Recommendations

In light of the findings, it is recommended that India introduce explicit statutory recognition of smart contracts through amendments to existing legislation or through the enactment of a dedicated legal framework governing blockchain-based transactions. Clear legal recognition would reduce uncertainty regarding the validity and enforceability of smart contracts and encourage greater adoption by corporate entities. The Government of India, in coordination with regulatory authorities such as the Ministry of Corporate Affairs (MCA), the Securities and Exchange Board of India (SEBI), and the Reserve Bank of India (RBI), should formulate comprehensive guidelines governing the use of blockchain technology in corporate governance. Such guidelines should establish minimum standards for implementation, accountability, security, and compliance.

A standardized framework for blockchain-based corporate compliance should be developed to facilitate uniform adoption across industries. This framework may include technical standards for smart contract development, audit procedures, security protocols, and mechanisms for monitoring compliance with statutory obligations. Standardization would enhance interoperability and reduce implementation risks. Special attention should be given to cybersecurity and risk management. Organizations adopting blockchain-based governance systems should be required to conduct regular security audits, vulnerability assessments, and smart contract testing procedures. Regulatory authorities may consider establishing certification mechanisms for blockchain applications used in corporate governance and compliance functions. India should also establish regulatory sandbox mechanisms specifically designed for blockchain and smart contract innovations in the corporate sector. Regulatory sandboxes would allow companies to test new technologies within a controlled environment while enabling regulators to assess potential risks and develop appropriate policy responses.

To address concerns relating to data protection and privacy, blockchain governance frameworks must be aligned with the Digital Personal Data Protection Act, 2023. Policymakers should formulate specific guidelines regarding the storage, processing, and protection of personal data on distributed ledger systems, ensuring that technological innovation remains consistent with privacy rights. Furthermore, capacity-building initiatives should be undertaken to improve awareness and expertise among regulators, corporate managers, legal professionals, auditors, and compliance officers. Training programs and specialized educational initiatives can facilitate a better understanding of blockchain technology and its legal implications, thereby promoting informed

decision-making and effective implementation. Finally, India should engage with international organizations to develop harmonized regulatory standards for blockchain and smart contracts, given the inherently cross-border nature of distributed ledger systems and the need for regulatory consistency across jurisdictions.

7. Conclusion

This research has investigated the emerging trend of smart contracts in corporate compliance in India and found that smart contracts are one of the most promising applications of blockchain technology in the modern governance. Their key benefits are that they can streamline repetitive tasks, make records more accurate, decrease reliance on manual processes, and maintain an audit trail that is transparent and time-stamped. Given the growing complexity of corporate compliance due to multiple legal, regulatory, and reporting regulations, smart contracts can become an effective solution in terms of efficiency and accountability. They can facilitate functions like compliance workflows, compliance alerts, reporting schedules, conditions verification, payment triggers, and records maintenance, making compliance a continuous and embedded governance process, rather than a periodic, reactive one.

This study also reveals that smart contracts are not a panacea for replacing traditional legal frameworks or judgment. Corporate governance is not just about doing things mechanically, it's about making decisions, interpretation, fiduciary responsibility and discretion. Directors and officers are not relieved from statutory duties by delegating them to code, or by stating that only other code should be responsible for them. Despite the extent to which automation is employed, legal responsibility should always be tied to human oversight as there is greater complexity in legal decisions that cannot be fully captured in code. Smart contracts are thus not legal entities that supplant the function of law, management or regulation but rather as governance tools that help with compliance.

Analysis of Indian legal regime reveals that there is partial support for digital transactions and electronic records, but there is no comprehensive and explicit legal regime for blockchain based smart contracts as separate and distinct instruments. The Information Technology Act, 2000 and

other laws relating to electronic contracting offer some useful groundwork for self-executing code, but do not answer questions of enforceability, interpretation, liability or evidentiary value. Likewise, the Indian Contract Act 1872 remains relevant and applicable to the validity of agreements, meaning that smart contracts will still need to meet the requirements of a contract, including free consent, lawful considerations, lawful object, intention to create legal relations, offer and acceptance. This puts at odds the binary, automated logic of code (and the code-as-language-of-the-world theory) with contract law. If there is an agreement in writing and a code, courts may have to decide which of the two governs or whether there is any relationship between the two. One of the biggest challenges to the broader adoption of this has been the uncertainty.

The paper also reveals that there are serious risks associated with the promise of smart contracts which cannot be disregarded. Unintended execution or non-performance due to coding error, software bug, cyber security breach, and/or faulty oracle inputs can lead to legal, financial, and reputational damage. When it comes to compliance, an even minor technical error can have a significant impact such as unauthorized payments, missing submissions, approvals, or transfers. Who is liable then, developer, deployed, corporate body or the person who authorized use of the system? Similarly, the reliance on external data sources introduces another risk factor as the data fed into the smart contracts could be inaccurate or manipulated, causing the automated actions to be incorrect. These concerns reveal the importance of developing automated governance with strong technical protections, careful drafting of contracts and clear risk allocation.

Data protection is also integral to the agenda, as is privacy. The immutability of blockchain is beneficial in relation to auditing but can run into problems with data retention and deletion, as well as confidentiality and other legal obligations. The privacy-design requirements, as well as thoughtful considerations of what data to bring onto-chain and what data to leave off-chain, must be factored into the design of smart contract systems. The very characteristics that blockchain is so desirable could present legal compliance challenges as well if they are not dealt with at the beginning. Accordingly, the paper argues that technological innovations in this field must go hand-in-hand with legal sagacity and regulatory certainty.

Looking closer backs up what we already see. Places like the United States, Singapore, the

European Union, besides the United Kingdom make it clear: when smart contracts get proper acknowledgment, along with specific rules and test runs in safe environments, confusion drops while sensible progress grows. What stands out here is how change doesn't demand rewriting every law from scratch. Often enough, small updates, clarifying notes, agreed upon specs, together with aligned oversight do just fine to bring stability into the picture. Still, India shows how balance works doable, even required. Flexibility stays intact when clarity steps in, not before. Enterprise moves forward where rules make sense, without losing room to adapt. Stakeholders gain ground when uncertainty narrows but does not vanish. The path ahead holds space for both. The main finding of this study is that smart contracts can meaningfully strengthen corporate compliance in India, but only within a framework that preserves legal accountability, regulatory oversight, and human supervision. Their most realistic role is not to replace the existing corporate law regime but to enhance it by making certain obligations more reliable, visible, and efficient. If used carefully, they can improve governance quality, lower compliance costs, and strengthen stakeholder trust. If adopted without adequate safeguards, however, they may create fresh legal uncertainty and shift risk into poorly understood technical systems.

One way forward for smart contracts in India might come through blended oversight. Instead of choosing only law or tech paths, mixing both could help. Legal backing paired with clear technical rules may create better results. Regulatory test zones, security standards, and verification steps can fit into this setup. Key bodies like the Ministry of Corporate Affairs, SEBI, RBI, and MeitY would share responsibility. Close work between lawyers, compliance experts, and developers becomes necessary here. When code matches real legal meaning, trust grows. Systems must stay open to review, understandable, and balanced over time. Progress won't hinge just on how strong blockchains are. How well Indian laws evolve matters just as much.

In the end, the study sees smart contracts less as self-running systems and more like aids in oversight. These digital tools help Indian businesses stick to rules by streamlining tasks, adding clarity, along with consistency - still, laws, ethics, and institutions remain irreplaceable. Without thoughtful regulation, automated steps might undermine control instead of improving it. Should India build strong guidelines, such technology could quietly take root within a sturdier, clearer system for keeping companies responsible.

8. Bibliography

8.1 Primary Sources

8.1.2 Statutes

- The Indian Contract Act, 1872.
- The Information Technology Act, 2000.
- The Companies Act, 2013.
- The Bharatiya Sakshya Adhiniyam, 2023.
- The Digital Personal Data Protection Act, 2023.

8.1.3 Rules, Regulations and Regulatory Instruments

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Information Technology (Certifying Authorities) Rules, 2000.
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.
- SEBI (Prohibition of Insider Trading) Regulations, 2015.
- RBI directions, circulars and master directions relevant to digital transactions and compliance.
- MCA notifications, circulars and compliance-related guidance on electronic filings and corporate governance.
- MeitY policy materials and blockchain-related guidance, where applicable.

8.1.4 Government and Policy Documents

- Government of India, Ministry of Electronics and Information Technology, policy documents on blockchain and emerging technologies.
- Government of India, Ministry of Corporate Affairs, circulars and notifications on corporate compliance and governance.
- Securities and Exchange Board of India, consultation papers and guidance notes on compliance and disclosure.
- Reserve Bank of India, reports and circulars relevant to digital payment systems and technology-enabled governance.

- NITI Aayog, reports on blockchain technology and its potential uses in governance and public administration.
- Law Commission of India, reports relevant to digital evidence, governance, or contract reform, if cited in the paper.

8.1.5 Cases

- *Trimex International FZE Ltd v Vedanta Aluminium Ltd.*
- *State of Maharashtra v Dr Praful B Desai.*
- *Shakti Bhog Foods Ltd v Kola Shipping Ltd.*
- *Kali Ram v State of Himachal Pradesh.*
- *Ambalal Sarabhai Enterprise Ltd v KS Infraspace LLP Ltd.*

8.2 Books

- Nicholas Szabo, writings on smart contracts and digital trust.
- Chris Reed and John Zeleznikow, works on legal informatics and digital dispute resolution.
- Jason Allen, writings on blockchain, smart contracts, and legal automation.
- Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code.*
- Kevin Werbach, works on blockchain governance and regulation.
- HLA Hart, *The Concept of Law.*
- Avtar Singh, *Law of Contract and Specific Relief.*
- Pollock and Mulla, *Indian Contract and Specific Relief Acts.*
- C K Takwani, *Civil Procedure.*
- M P Jain, *Indian Constitutional Law.*
- Taxmann or similar practitioner commentaries on the Companies Act, 2013 and compliance regulation.

8.2.1 Journal Articles

- Articles on the enforceability of smart contracts under Indian law.
- Articles on blockchain-based corporate governance and automated compliance.
- Articles on electronic contracting and digital signatures in India.
- Articles on the legal status of smart contracts under the Indian Contract Act, 1872 and the Information Technology Act, 2000.
- Articles on the evidentiary value of blockchain records and electronic evidence.

- Articles on data protection, cybersecurity, and privacy issues in blockchain governance.
- Articles comparing India's approach with the United States, Singapore, the European Union, and the United Kingdom.
- Articles on oracle dependence, liability for coding errors, and dispute resolution in automated systems.

8.2.2 Reports and Industry Publications

- NITI Aayog reports on blockchain technology and its use in governance.
- Reports by the Ministry of Electronics and Information Technology on emerging technologies and digital governance.
- Reports and consultation papers by the Ministry of Corporate Affairs on corporate compliance and governance.
- SEBI consultation papers, annual reports, and discussion papers on digital compliance and market regulation.
- RBI reports, circulars, and discussion papers on digital payments and technology-enabled finance.
- World Economic Forum reports on blockchain, smart contracts, and governance.
- OECD reports on digital regulation, automation, and corporate governance.
- Industry white papers from legal tech and blockchain research bodies.
- Reports from law firms and policy think tanks on blockchain regulation in India

¹ Klaus Schwab, *The Fourth Industrial Revolution* 7–11 (2016).

² Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 1–8 (2008), <https://bitcoin.org/bitcoin.pdf>

³ Max Raskin, *The Law and Legality of Smart Contracts*, 1 Geo. L. Tech. Rev. 305, 305–09 (2017).

⁴ Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, *Extropy*, no. 16, 1996, at 18.

⁵ Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 Duke L.J. 313, 318–25 (2017).

⁶ Companies Act, 2013, No. 18 of 2013, India Code; Securities and Exchange Board of India Act, 1992, No. 15 of 1992, India Code; Prevention of Money-Laundering Act, 2002, No. 15 of 2003, India Code.

⁷ Organisation for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance* 45–49 (2023).

⁸ Kevin Werbach, *The Blockchain and the New Architecture of Trust* 121–32 (2018).

⁹ Information Technology Act, 2000, No. 21 of 2000, §§ 4, 10A (India); Indian Contract Act, 1872, No. 9 of 1872, § 10 (India).

¹⁰ Indian Contract Act, 1872, No. 9 of 1872, §§ 2, 10 (India).

¹¹ NITI Aayog, *Blockchain: The India Strategy* 22–35 (2020).

¹² NITI Aayog, *Blockchain: The India Strategy* (Government of India 2020).

- ¹³ Nidhi Singh Iyer and Madhavi Simhadri, 'Smart Contracts in India: A Legal Analysis' (2020) 5 Indian Journal of Law and Technology 45.
- ¹⁴ S Rajagopalan and V Sundarajan, 'Smart Contracts and the Information Technology Act, 2000: Assessing the Legislative Framework for Electronic Contract Enforceability in India' (2023) Indian Journal of Law and Technology.
- ¹⁵ Indian Contract Act 1872; Information Technology Act 2000, s 10A.
- ¹⁶ R Sharma and P Mehta, 'Corporate Compliance Automation in India: The Companies Act, 2013, SEBI Regulations, and the Emerging Role of Smart Contract Governance' (2024) Corporate Law Review.
- ¹⁷ Companies Act 2013; Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015.
- ¹⁸ K Krishnamurthy and A Bose, 'Smart Contracts and Corporate Governance: Decentralized Autonomous Organizations, Shareholder Agreements, and Legal Challenges under Indian Company Law' (2024) National Law School Journal.
- ¹⁹ Digital Personal Data Protection Act 2023.
- ²⁰ N Iyer and R Venkataraman, 'Regulatory Approaches to Blockchain-Based Smart Contracts in India: SEBI, RBI, MCA and the Search for a Coherent Legal Framework' (2024) Indian Business Law Journal.
- ²¹ Internet and Mobile Association of India v Reserve Bank of India (2020) 10 SCC 274.
- ²² Ministry of Corporate Affairs, MCA21 Version 3.0 Programme (Government of India).
- ²³ Reserve Bank of India, Concept Note on Central Bank Digital Currency (2022).
- ²⁴ Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 74–89 (Harvard Univ. Press 2018).
- ²⁵ Kevin Werbach, *The Blockchain and the New Architecture of Trust* 121–32 (MIT Press 2018).
- ²⁶ Avik Sarkar, Blockchain Technology and Regulatory Challenges in India, 13 Indian J.L. & Tech. 47, 58–67 (2017).
- ²⁷ Werbach & Cornell, *supra* note 3, at 336–45.
- ²⁸ Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, §§ 61–63 (India).
- ²⁹ Indian Contract Act, 1872, No. 9 of 1872, §§ 2(a), 2(b), 10 (India).
- ³⁰ Max Raskin, *The Law and Legality of Smart Contracts*, 1 Geo. L. Tech. Rev. 305, 323–29 (2017).
- ³¹ Christopher D. Clack, Vikram A. Bakshi & Lee Braine, *Smart Contract Templates: Foundations, Design Landscape and Research Directions* 6–8 (2016),
- ³² Michèle Finck, Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?, 4 Eur. Data Prot. L. Rev. 17, 18–25 (2018).
- ³³ Max Raskin, *The Law and Legality of Smart Contracts*, 1 Geo. L. Tech. Rev. 305, 323–29 (2017).
- ³⁴ Organisation for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance* 45–52 (2023).
- ³⁵ Companies Act, 2013, No. 18 of 2013, § 166 (India); Organisation for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance* 45–52 (2023).
- ³⁶ Unif. Law Comm'n, *Uniform Electronic Transactions Act* (1999).
- ³⁷ *Electronic Transactions Act 2010* (Sing.); Monetary Auth. of Sing., *Project Ubin*.
- ³⁸ Reg (EU) 2023/1114 (MiCA); Reg (EU) No 910/2014 (eIDAS); Reg (EU) 2016/679 (GDPR).
- ³⁹ UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (Nov. 2019),
- ⁴⁰ Law Commission, *Smart Legal Contracts: Advice to Government* (Nov. 2021)