INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

SMART CONTRACTS IN FINTECH LENDING: ARBITRABILITY, EVIDENTIARY CHALLENGES AND THE UNMET NEED FOR A HYBRID DISPUTE RESOLUTION FRAMEWORK IN INDIA

AUTHORED BY - RUPALI PATIL
Independent Legal Researcher; LL.M. Graduate

I. ABSTRACT

The main thrust of the current paper is to consider the legal and procedural challenges associated with smart contract based on-chain fintech lending in India. On one hand, the primary advantages of such contracts lie in speed, certainty, and efficiency of transactions. However, these advantages also give rise to a specific set of disputes involving coding errors, oracle problems, accidental liquidations, and disagreements over the extent to which the code reflects the original bargain reached by the disputing parties. There are three main questions addressed in the course of this research – whether smart contracts based disputes may be considered arbitrable under Indian law, how the existence of the disputed contract and its exact nature could be proven in such arbitrations and whether the existing legal framework may be regarded as sufficient to regulate on-chain lending dispute governance. Based on doctrinal review of Arbitration and Conciliation Act, 1996, Information Technology Act, 2000, Bharatiya Sakshya Adhiniyam, 2023 and some recent jurisprudence in the field, this study concludes that Indian law is directionally favorable to this purpose but doctrinally insufficient. More specifically, it seems that the biggest challenge is not the unavailability of arbitration per se but rather the disjunction between a code-based transaction and a paperwork-based dispute resolution approach. As such, it is proposed that the "Code-Law Hybrid Model" should involve three layers including automated on-chain resolutions, institutional arbitrations and supervision of courts, respectively.

II. INTRODUCTION

However, India's digital lending industry has grown significantly in the past decade, and this growth is far from being limited to any one method. Digital lenders now exist in the form of mobile apps, internet platforms, peer-to-peer models, embedded finance relationships, and

ISSN: 2582-6433

increasingly, protocol-based lending solutions that have little in common with classical contractual lending and more with code-driven lending. The Reserve Bank of India has thus adapted its digital lending regulation, and even SEBI has adopted online arbitration for securities disputes. This suggests that regulators are far from being opposed to innovation per se; what they are rather worried about are consumer harms, opacity, and delegation of discretion.

These worries matter because smart contract lending is not simply about having an automated contract. It executes on its own, sells assets when certain coded triggers occur, releases money once certain conditions are coded into the smart contract, and transfers rights via coded instructions. This seems efficient in good times, but not so much when litigation occurs. Indeed, the question becomes how to assess liability in cases where the borrower was bound by only the code or the code and off-chain elements, whether automatic selling in error constitutes a wrongful act, and whether coding issues themselves are about breach of contract, rectification of errors, restitution, and/or fraud.

But the issue is more than just an academic puzzle. It raises critical questions about arbitrability, evidence and enforcement. Arbitration law in India assumes, explicitly or implicitly, that the parties' agreement can be known by a court in a comprehensible way. Smart contracts challenge that assumption. For instance, it is possible to enter into a loan agreement using a user interface, store it on the blockchain and execute it by way of automated mechanisms, but the question at stake might relate to off-chain disclosures, wallet permissions, code commits, governance votes and oracle feeds. The traditional discourse of contract law does not vanish from the equation; rather, it is superimposed onto technologically sophisticated objects that are hard to interpret without expert help.

For that reason, the purpose of this paper is to address three related research questions. First, are disputes arising out of fintech lending smart contracts arbitrable under the Indian law or they fall within the exception cases involving such matters as fraud, criminal conduct, consumer protection laws, and other issues not arbitrable under the domestic regime? Second, how does one determine evidentiary burdens in the case where the agreement, its performance and breach of the agreement occurred entirely on blockchain? And third, what type of architecture is needed to balance the efficiency gained from smart contracts and compliance with Indian principles? These questions are answered here via a doctrinal method and

ISSN: 2582-6433

comparative analysis.

It is important to note that no attempt is made to prove that it is impossible to regulate smart contracts by the existing Indian laws. Rather, the current legal framework indirectly addresses the problem and leaves something to be desired. Sections 10A and 7 of the Information Technology Act, 2000, and the Arbitration and Conciliation Act, 1996, respectively, provide for agreements entered into electronically and written arbitration agreements, which include electronic means of communication. However, it is clear that they were never thought of in the light of blockchain lending and need certain interpretation. We will now consider the technical background.

III. UNDERSTANDING SMART CONTRACTS IN THE FINTECH LENDING ECOSYSTEM

A. Technical Overview

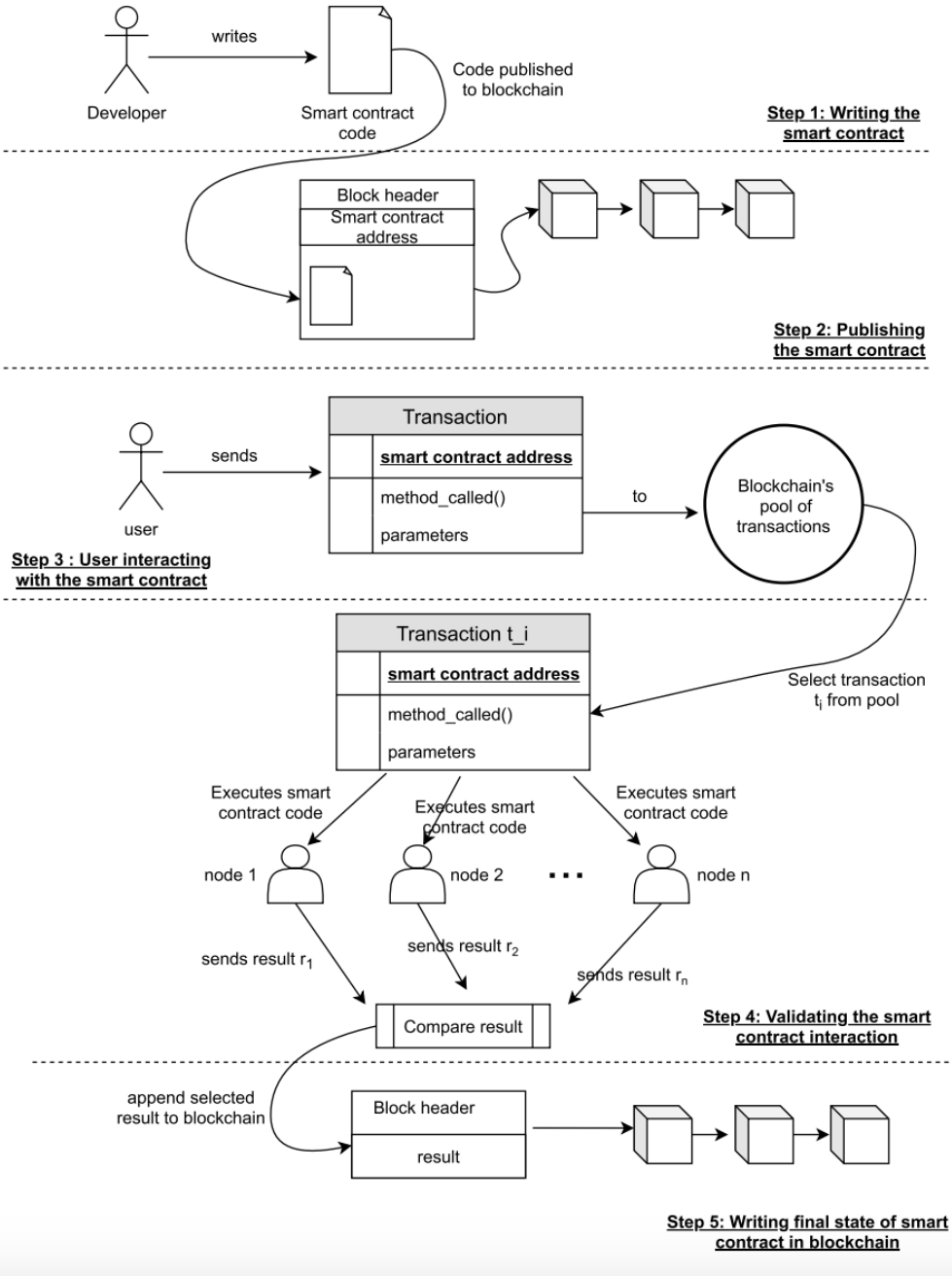
There are many uses of the term 'smart contract' in common parlance but its specific definition is important in this context. From a technical standpoint, a smart contract refers to computer program code deployed in a blockchain or other distributed ledger system to initiate some predefined actions automatically in response to certain conditions being met. Self-executing in nature, such programs do not require human intervention in order to execute asset transfers, trigger payments, lock up collateral and document defaults. From a commercial perspective, however, a smart contract typically forms just one element of a more extensive contractual relationship that encompasses user interfaces, platform terms, off-chain validation measures, wallets, identity verification procedures and oracle-based access to external data.

In the world of fintech, transactions are recorded in interlinked blocks and validated by multiple network nodes, resulting in the creation of tamper-resistant entries. This makes smart contracts very efficient but there is always a risk of executing an erroneous contract since correction might prove difficult due to the underlying architecture. In effect, the code runs almost like a machine and the output is highly certain compared to typical contractual procedures, which can still lead to legal challenges in case the transactions took place without the necessary informed consent, involved errors in implementation, or were executed through deception and fraud.

Smart contract applications in the fintech space are relatively simple despite the impressive-sounding technological solution. Automated payment may become the norm with loans disbursed once risk evaluation based on the digital KYC process is performed. Smart contracts

ISSN: 2582-6433

for collateral management purposes will observe the status of assets of the borrower and proceed with their sale once a certain critical level is reached. Calculations of interest rates and subsequent updating of balances may be performed regularly in real-time. Additionally, peer-to-peer lending platforms can use smart contract-based escrow services to prevent lenders from manipulating clients' funds.



B. Use Cases In Fintech Lending

While the lending sector of fintech in India is different from the decentralized finance sector

ISSN: 2582-6433

that has become prevalent around the world, there has been an increasing level of convergence between these two domains. Digital onboarding and automated funding have been implemented in Peer-to-Peer (P2P) lending services in India. An even more sophisticated system would involve the implementation of smart contracts to lock down borrower money in escrow until certain criteria are met before disbursing funds to multiple creditors on a pro-rata basis.

Another application example is automated collateral management. Suppose that there is a person who takes a loan secured by tokenized assets or cryptos. In such case, the system will automatically check whether the loan-to-value ratio is below or above the certain level. This solution works well during the market volatility as it allows making decisions quickly. However, this feature can be extremely dangerous in the situations where the price feed is not reliable or the threshold for taking action is too low or even set incorrectly, causing huge losses to the borrower. Considering the problems with Indian fintech lending that already exist due to its lack of transparency and predatory approaches, the mentioned issue becomes especially dangerous.

Finally, there is an opportunity for embedded lending. It means that one can get a credit using a digital commerce platform at the point of purchase. This way of lending can help to avoid any disagreements between parties regarding the payment schedule. Nonetheless, in such case, informational asymmetry increases dramatically since the borrower does not realize the technology underlying the process.

C. Smart Disputes

Three types of conflicts commonly arise with smart contracts. These include coding faults where the contract functions exactly as it was designed but fails to work the way it should. The second type is oracle disputes where the contract executes the code perfectly, but the data feed that drives it is faulty. Lastly, there is governance and consent dispute when the users involved cannot agree if the contract was meant to be the entire agreement or just one part of a larger business relationship.

An actual incident of such a conflict can be seen in 2021, where the Compound Protocol had a distribution fault resulting from a bug in the code following an upgrade. This was not merely a problem with technology but rather a dispute about entitlement, restitution and the implications of an executed mistake by a protocol. Users who had received windfall tokens did not have to be considered as “wrongdoers” in the ordinary sense, but nevertheless, the founder of the protocol attempted to request a voluntary repayment from them and initiated changes in its

ISSN: 2582-6433

governance in response to this issue. This is nothing new for any lawyer: the idea that code can make something appear as self-executing does not mean that disputes about fairness and intent will no longer arise.

In the case of oracles giving incorrect market information, similar issues arise. In a lending platform that uses an oracle feed to calculate whether the borrower defaults, even a brief glitch in the data could make a solvent borrower look like a defaulting one. This borrower would have good reasons to contest the decision made by the system, but the lender would be able to refer to the terms of operation that have been set up beforehand.

Table 1. Typology of Smart Contract Disputes in Fintech Lending

Dispute Type	Typical Trigger	Legal Issue	Likely Forum
Coding Error	Bug in reward, interest or liquidation logic	Rectification, restitution, liability	Arbitration with expert evidence
Oracle Failure	Incorrect external price or identity data	Causation, breach, consumer harm	Arbitration or court depending on claim
Fraud/Manipulation	Hidden code change or misleading disclosure	Fraud, inducement, invalid consent	Court or arbitral tribunal with court oversight
Governance Dispute	Upgrade vote, admin key or unilateral change	Authority and legitimacy of execution	Institutional arbitration; possible judicial review

This illustration is for example only, but it serves to highlight the fundamental issue: the legal import of the dispute does not lie simply in what the code did; rather, the legal import is in how the parties interpreted what the code was supposed to do. As long as the legal system emphasizes contracts in text whereas the market stresses code execution, there is a strong likelihood that one party's performance would be another party's breach of contract.

IV. ARBITRABILITY OF SMART CONTRACT DISPUTES UNDER INDIAN LAW

A. Section 7 of the Arbitration Act 1996 and Electronic Agreements

According to Section 7 of the Arbitration and Conciliation Act of 1996, the term “arbitration agreement” refers to the submission of disputes to an arbitrator made through an agreement by

ISSN: 2582-6433

the parties. The section provides that arbitration agreement need not take on any ceremonial form but should only be in writing. In conjunction with Section 10A of the Information Technology Act of 2000, the statute accommodates digital contracting as long as it is not the medium alone which determines the validity of the contract. The issue is thus not whether the parties employed code, emails or interface in their transaction. The key issue is mutual assent as objectively determined from the record of the transaction.12

This is relevant in smart-contract lending because of the multiple locations where arbitration clauses may be situated. The agreement may be contained within the user interface in the form of clickwrap terms; the agreement may be contained within an offline loan agreement; the agreement may be recorded in metadata online; or the agreement may use a combination whereby the computer code refers to a dispute resolution protocol on the platform. No Indian statute forbids these kinds of arrangements. Indeed, according to the combined reading of the Arbitration Act and IT Act, electronic documentation need not prevent the operation of a valid arbitration agreement. It is proving, not prohibition.

One could contend that the smart contract itself is the arbitration agreement provided that the code and documentation demonstrate an intent to arbitrate the dispute. However, this is not always the case. For the smart contract alone does not make for an arbitration agreement when such contracts only automate lending results but do not necessarily refer to submitting to a private arbitration process. If the parties only programmed performance rules, a tribunal cannot infer arbitration by artistic interpretation. The clause must be identifiable as such, even if the identification requires reading the code alongside platform records and disclosures.

B. Are Smart Contract Disputes Commercial and Therefore Arbitrable?

Most conflicts which result from smart contracts used for fintech lending can be characterized as commercial disputes. These relate to lending, repayment, collateral, interest, fraud, breaches of obligations or misallocation of risks between the parties. According to the more liberal Indian approach towards arbitrability, disputes falling within the sphere of private rights in personam may be considered arbitrable and thus amenable to the arbitral process. In this way, the Supreme Court in Vidya Drolia clarified that disputes are generally arbitrable unless they relate to actions in rem, prohibitions under the statute or the need for centralized public resolution. Fintech lending conflicts are not within this last category.4

It follows that if a debtor raises concerns about improper liquidation, or if a creditor claims that the terms of repayment were not adhered to, they will be treated as presumptively arbitrable matters. This would apply equally if a borrower asserts breach of obligations concerning proper

ISSN: 2582-6433

handling of collateral by a platform or non-performance of an agreed upon coded escrow procedure. Coding a particular obligation does not turn the dispute into one of public law significance – it remains a commercial dispute executed digitally.

The problem here is whether an arbitral tribunal might have to rule on matters that fall in between contractual, proprietary, and compliance-related concerns. Disputes can revolve around the legitimacy of a tokenized asset used as collateral, or the legality of a platform's ability to make unilaterally made upgrades. In such cases, while arbitration may still be applicable, the tribunal is required to take into account the statutory limitations involved. There are statutory limitations on using arbitration when the legislature has deliberately left certain matters public in nature. It is not blanket prohibition, but selective screening of the issues that is called for.

C. Non-Arbitrable Subjects and the Borderline Cases

The existing exemptions are still relevant. According to Vidya Drolia and other precedents, fraud might be grounds for considering a claim non-arbitrable if it amounts to an attack on the existence and validity of the arbitration clause, or even of the agreement as a whole. Claims arising from criminal conduct are non-arbitrable since criminal activity affects the sovereign power of the State. Consumer claims are not arbitral if the applicable legislation sets up tribunals or if they relate to compulsive rights. This is critical when dealing with claims based on smart contracts as they tend to encompass all three categories simultaneously.46

Take for instance the borrower alleging that the fintech company hacked into the smart contract code or that the real way it functions is unknown to him. The issue of misinterpretation of the code would be arbitrable. On the other hand, when there is a claim that the loan provider surreptitiously changed the algorithm in order to make opportunistic liquidations possible, falsified deployment logs, or used pseudonymous entities, the case begins to resemble outright fraud. And once the case reaches the point where the issue of whether the whole loan was made under fraudulent pretenses or whether the arbitration agreement itself was obtained through deception must be considered, it would appear that intervention by the court is warranted. Thus, the distinction becomes functional rather than formal.

In any case, it is essential to remember that not all disputes arising in connection with blockchain technologies are necessarily of a purely commercial character. In a smart-contracts lending dispute, the plaintiff may include claims raised by borrowers or consumers which were never negotiated in the course of transactions. If there is significant power imbalance between the parties involved and the dominant concern is consumer protection, then one may raise the

ISSN: 2582-6433

objection that arbitration should not serve as a mechanism that would conceal manipulative practices in the market.

D. The Grey Area and the Significance of Judicial Attitudes Toward Technology

No reported decision by Indian courts exists regarding the arbitrability of disputes arising out of smart contracts in the context of lending agreements. This silence speaks for itself. While the law seems to have become comfortable with e-contracts, it has not quite caught up with smart contracts yet. Judging from the judicial pronouncements in neighboring technology cases, the judiciary is being practical while recognizing its limitations. In the case of Shreya Singhal vs Union of India, the Supreme Court found a broadly defined offense concerning online speech unconstitutional and reiterated the need for standards which are clear and administrable. While this pronouncement can be seen purely as a speech issue, it reflects the judiciary's concern with technologically based standards that are unclear or open-ended.

In the context of smart contract arbitration, the tribunal cannot act as though the facts are self-evident since the blockchain is public. A blockchain record does not take the place of legal characterization; it is simply a source of information which must be interpreted. Judicial conservatism in similar technological cases thus points to an equally balanced course: one that is pro-arbitration yet skeptical.

That same principle emerges through the High Court of Bombay's July 2025 ruling in Radiance Galore v. Yes Bank. The Court was more than ready to consider the appointment process for the online dispute resolution system where algorithms were used for the selection of the arbitrator, and it made it clear that unilateral appointment concerns are not resolved simply by the use of algorithms. This case has two significant implications for smart contract arbitration. Firstly, technology cannot cleanse the appointment process of its flaws. Secondly, India's courts are open to questioning the governance of dispute settlement systems.

V. EVIDENTIARY CHALLENGES IN ARBITRATING SMART CONTRACT DISPUTES

A. Proving Existence And Terms Under The Evidence Regime

"Evidentiary Issues" constitute the most understated issue regarding the arbitration of disputes involving smart contracts. First, one needs to establish that the smart contract was indeed entered into, that it governed the transaction in question, and that its terms were as claimed by the aggrieved party. According to the 2023 Bharatiya Sakshya Adhiniyam, electronic records

ISSN: 2582-6433

can not be excluded on the basis that they are electronic and may be proved in the manner specified under the law. While this might be useful, it is only part of the story.

Even if a block chain entry is admitted, it might be meaningless without proper context. An admission does not necessarily mean understanding. This, obviously, is quite a different task than reviewing a single PDF of a loan agreement. The burden of proof becomes especially significant when there is disagreement about whether the code that was run is indeed the code that was agreed upon. Versioning, permissions, and administration keys take center stage as facts of utmost importance, not some technical details. In other words, what we have here is not just another contract dispute that happens to be automated. We deal here with a dispute over the nature of the evidence in the matter.

This implies a specific outcome. Parties involved, as well as arbitrators, will need forensic help. For example, a dispute might require the services of a blockchain analyst to trace all events in the blockchain, as well as an expert in software engineering to decode the actual code. Then, there will also be the necessity of translating all technical details into legal liability through contractual expertise. All this will inevitably incur extra time and cost. The system which promised quick settlement becomes quite a different one indeed.

B. Expert Testimony And Forensic Code Audits

In all cases where bugs, upgrades, or data feeds figure significantly, expert evidence will almost certainly be required. Among the questions that the court might want to explore through expert evidence are whether the source code had been audited, what precisely had been audited, whether the flaw had been easily observable, whether the upgrade changed the economic assumptions that underlay the smart contract, and whether the flaw was there from the start or inserted subsequently. In conventional financing disputes, expert evidence may add value but is not necessary. In smart contracts, it may be essential. The difference is that where expert evidence becomes vital, the balance of the litigation can depend as much on which party tells the more compelling forensic story as on the underlying law.3

It is important not to understate the cost problem. Borrowers or other retail counterparties may not be able to afford code auditing or expert testimony. Indeed, an advanced claimant may overwhelm the record not due to having the legal case on its side, but because of the format of evidence which simply costs too much for the opponent to counter. Flexibility, so common in arbitration procedure, might turn into exclusion when special expertise is needed to prove a point. This is the reason why the hybrid procedure needs two layers: the first being simple and reserved for ordinary disputes, the second – somewhat more formal and used in contentious

ISSN: 2582-6433

cases.

The involvement of independent experts can make the difference. Some arbitration systems even have provisions that enable hiring of such experts, or tribunals and tribunal secretaries, or emergency procedures for ensuring proper preservation of digital evidence. However, there is no well-developed protocol in India for analyzing smart contract disputes. The absence of it is disturbing since any digital evidence is very vulnerable and blockchain disputes need to be resolved quickly. Code updates, interface changes, and disappearance of oracle information from the public dashboard can happen anytime.

C. Code Is Law, Yet Law Is Not Merely Code

The principle that "code is law" expresses something valuable, but it lacks completeness as a legal rule. While the code may define how the machine will behave, the law still needs to address the question of what should happen when code produces an undesired or unforeseen effect. The intentionality, consent, reasonableness, misrepresentation, unconscionability, and public policy are still matters for the law. Thus, in dealing with a smart contract, the court should decide whether to treat the code alone as the only expression of the parties' agreement or one element of a broader contractual system.

Such questions arise particularly when there is a conflict between off-chain and on-chain data. For example, when a platform termsheet says that a borrower will not be liquidated until the price goes below a certain level, but due to stale oracle updates, the borrower's position was liquidated earlier than promised. The question arises – which document is authoritative – the code, which was executed, or the termsheet, which reflects the business understanding of the parties? In many instances, the answer to the question posed by the scenario will rest on questions of priority, disclosure and assent. In many cases, the reasonable thing to do would be to take the view that both the code and the written terms have to be interpreted together, and that ambiguities should be construed against the drafter of the architecture.

Conversely, there is an opposite situation in which the borrower can argue that he had never intended to provide his assent to such an arrangement through the use of code, and that he had not appreciated that this was the case. He can make this argument, and he cannot easily be ridiculed for doing so. There is a long history in contract law of the distinction between form and substance, and the consequences of making certain arrangements may well be something that the platform will have to think about.

ISSN: 2582-6433

D. Anonymous Parties, Jurisdiction And Identity Proof

Another problem in evidencing disputes relates to pseudonymity in wallets or decentralized platforms. Although the tribunal will be aware that a violation has happened, it does not know from the outset who controlled the wallet, who released the code, or who had authorization to engage in the relevant transaction. In regular lending practices, identifying the other party is part of the procedure. In certain cases related to the blockchain world, identifying the other party may constitute the entire issue of dispute. This, again, results in jurisdictional uncertainties due to lack of knowledge regarding identity.

Although the issues raised above can be addressed by KYC, registering in the relevant platform and proving personal identification upon initial engagement, the more the transaction moves away from the traditional model towards decentralization, the harder it is to prove the conduct involved in the case. Here, the courts will have to deal with circumstantial evidence and platform and exchange records. This difficulty is not specific to India; however, the Indian legal framework of arbitration relies heavily on the premise of an identifiable agreement between parties.

The problem addressed by the Bombay High Court in Radiance Galore regarding the unilateral nomination on an online platform is not just procedural but substantive. Technology should never be used to blur lines of accountability. In matters relating to the nomination of an arbitrator or the execution of a condition of a loan agreement, it must be made clear who instructed what and at what time.

VI. CURRENT LEGAL AND REGULATORY GAPS IN INDIA

A. Reliance On General Contract Law

Currently, India lacks any specific legislation regarding smart contracts. Therefore, the law depends upon general provisions regarding contracts, the Information Technology Act, and other interpretive rules. While this is a sound theoretical basis, there are practical gaps. The Contract Act of 1872 was created at a time when making an offer, acceptance, consideration, and breach all depended on people and language. In short, it sufficiently covers the basic principles of enforceability; however, it fails to address programming deployment, automation, upgrade rights, reliance on oracles, or self-help liquidation.

It is the lack of legislation that poses another concern because it leaves everything in the hands of the judge. The Indian judiciary will certainly develop the issue of smart contracts on a step-by-step basis as it will see more cases in court related to loan defaults, complaints from consumers, fraud cases, or cases regarding arbitrability issues. Such an approach is common

ISSN: 2582-6433

for common law countries, but in this case, the pace of change will be quicker than the pace of legal developments due to the rapid advancement of technology.

B. RBI, SEBI And The Regulatory Mood

The rationale behind the RBI's digital lending guidelines can be seen as part of a larger concern about transparency, data management, and accountability of regulated entities. In its most recent 2025 directions, it reaffirmed the previous guidance and continued focusing on borrower rights, disclosure, and third-party limitations. However, this rationale needs to be understood: the regulators do not ban digital lending. Instead, it mandates that digital intermediation should never be an opportunity for regulatory avoidance. It is difficult to understand where smart contract falls in this regard since it can be decentralised from the technical perspective, yet controlled from the commercial one by some platform, lender or sponsor.10

Similarly, SEBI's master circular regarding online dispute resolution in the securities market reveals that the Indian regulatory state accepts this new tool provided it remains within the context of a regulated structure. This applies to fintech lending as well. Online dispute resolution is not banned in India; however, it must stay within certain boundaries so that it remained legible and compatible with legal requirements. Thus, a smart-contract dispute process would be hard to defend due to lack of notice, reasoning, or review opportunities.

C. The Seated-Arbitration Problem

Jurisdictional problems arise when the underlying blockchain network is distributed on multiple nodes and when the disputing parties are spread out geographically across several states or nations. On what geographical location is the blockchain arbitration seated? Blockchain cannot be the seat of arbitration since it is not a territorial jurisdiction. Each node cannot be a seat either, otherwise territorial laws would cease to operate. In the absence of specific legislation in this respect, it seems likely that the choice of the seat will continue to depend on contractual agreement related to the institution conducting the arbitration, execution place, and law governing the transaction.

Nevertheless, the option to choose a legal seat cannot solve the conceptual problem involved here. While blockchains allow storing documents, automating pre-procedure steps, and distributing decisions, the system for enforcing decisions is still territorial. It requires that courts identify a legal place that gives them jurisdiction to supervise arbitration proceedings. That is yet another reason why a hybrid model would be ideal, where the protocol takes care of logistics while a legal seat of arbitration remains in an identifiable arbitral body and Indian

ISSN: 2582-6433

courts when needed.

D. Enforcement, Property Status And Data Protection

Further, enforcement of awards or orders issued relating to blockchain technology presents another difficulty, where the object itself is crypto or any other digital asset in question. In the 2025 case of Rhutikumari v. Zanmai Labs Pvt. Ltd., the Madras High Court is noteworthy since the court viewed cryptocurrency as an item of property that could be protected through judicial process. The relevance of the judgment in our scenario here lies not in the fact that all crypto issues have been settled, but that the Indian judiciary does not shy away from considering digital assets as legally recognized property instead of being mere legal entities. Such an approach would aid enforcement in the event of any dispute involving smart contracts, especially where the order relates to a digital item or escrow.

The DPDP Act, 2023 provides another requirement for compliance. Lending based on smart contracts often collects identity, repayment records, wallet information, device logs and even behavior scores. Under the Act, data-processing has to be done in a manner that ensures that such processing is lawful, done with the consent of the individual or is a legitimate use. In this case, the institution in charge of the dispute resolution process is required to ensure that there are certain obligations of notice and accountability. This means that in the course of resolving disputes on the blockchain platform, neither party should take for granted the importance of privacy.

It becomes clear from this analysis that at present, India has enough legislation in place to cover both the use of smart contracts for lending, and smart contract dispute resolution, though there is not enough clarity as yet for it to become entirely predictable.

VII. A PROPOSED HYBRID DISPUTE RESOLUTION FRAMEWORK

The basis for the hybrid approach is grounded in the following simple realization: not all disputes related to smart contracts are to be handled using the same level of formality. An insignificant interest calculation problem does not require the same amount of attention from institutions than the one concerning a dispute where there is fraud using hidden admin keys and tampered oracles. This suggests that an appropriate dispute resolution process must be multi-tiered as opposed to being uniform.

A. Layer One: On-Chain Automated Resolution

This layer of dispute resolution is appropriate where the dispute involves low value and

ISSN: 2582-6433

involves rule-based scenarios that can be resolved using software code. Examples include the release of funds held in escrow upon repayment, recalculation of interest based on a predetermined calculation, or automatically issuing refunds when the criteria specified are met. This layer of dispute resolution is essential as it ensures efficiency which forms the basis for the use of smart contracts. Further, this layer of dispute resolution minimizes administrative costs and encourages prompt settlement of disputes as well as preventing human intervention from causing the small-value claims to become unmanageable. Critically, this layer can apply where there is objectivity regarding the rules applicable to the dispute and also where both parties have agreed to the code as the dispute resolution mechanism.13

It will be wise to incorporate a mechanism for addressing any possible technical issues in the code through the creation of a loophole. In the scenario where the updating of the oracle or transactions that surpass the predetermined threshold of risks occur, the system may stop and seek assistance from human intervention.

B. Layer Two: Institutional Arbitration

Layer two deals with higher-value disputes, issues that fall into both law and facts, and matters requiring interpretative skills. The arbitration ought to be institutional and not ad hoc in nature, and such an institution needs to have a pool of arbitrators who are versed in digital finance and blockchain technology. The tribunal must have powers to appoint technical experts, order evidence preservation, and interpret the code in consideration of the contract, platform rules, and regulatory environment. This helps uphold the key qualities of arbitration—autonomy of the parties, expertise, and confidentiality—without leaving room for chances of having a technically intricate matter being arbitrated by a tribunal that lacks the language necessary to deal with the issue at hand.8

Appointment integrity is vital when designing the structure. Radiance Galore indicates that the use of algorithmic selection is not an acceptable way out of the legal requirement of unilateral appointment. Therefore, the hybrid system should incorporate algorithmic assignment only where a valid appointment structure through consent or under Section 11 exists. Algorithm can help in assignment but not in creating jurisdiction. The distinction between the two goes beyond just semantics. It represents the line between procedure and its misuse.

C. Layer Three: Court Fallback For Non-Arbitrable Matters

Thirdly, there is the layer of the safety valve. In cases where there is serious fraud or criminality, statutory consumer right issues, or anything else that is non-arbitrable according

ISSN: 2582-6433

to Indian law, the dispute should revert to the courts or other appropriate public forums. This is crucial, since there cannot be privatization of public wrongs within a hybrid model. Fallback to the courts also plays an important role in the enforcement aspect. This will ensure that emergency reliefs, anti-suit protections, asset preservations, and jurisdictional challenges are available where needed.

Moreover, such a system has the additional benefit of minimizing the need for characterization of every dispute on an initial basis. In the existing Indian model, courts are compelled to resolve the issue of arbitrability even before establishing the facts of the case in technical terms. With a layered approach, the lowest risk cases can be automatically resolved, medium risk cases are referred to arbitration, while the higher risk cases and matters of public interest can be left with the courts.

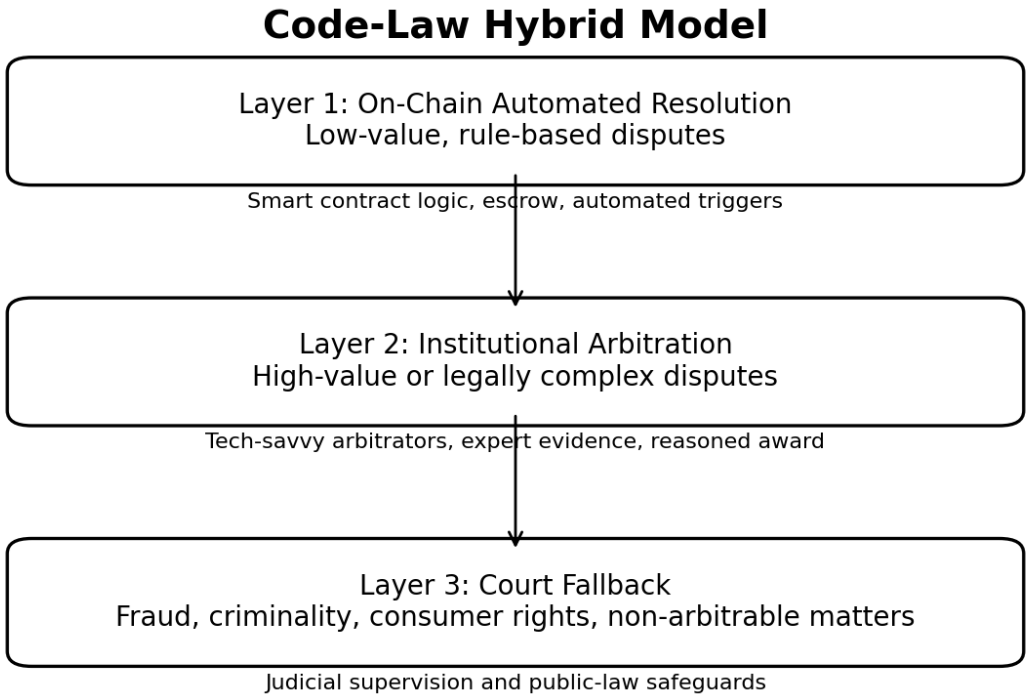
D. How The Hybrid Model Addresses The Existing Gaps

Firstly, the hybrid model deals with the evidentiary problem since it requires preservation of evidence right from the start. The transaction hashes, logs, commit and oracle snapshots must be preserved in a dispute-ready form. It also tackles the arbitrability problem since it leaves the non-arbitrable subject matter for the court while sending all other claims to the arbitration. Thirdly, it solves the access to justice problem since it confines the expertise-laden arbitration to those cases where they are needed. Lastly, it takes care of the regulatory problem since it does leave room for RBI, SEBI, and data protection compliance without falling prey to the regulatory black hole.

Moreover, the model represents an understanding of the greater legal truth. Smart contracts may reduce the role of judgment but cannot eliminate it. Judgment is shifted to different layers of the dispute resolution procedure starting from coding, moving through governance, evidence, characterization, and ending with enforcement. A multi-layered dispute resolution procedure is more realistic because no algorithm can ever take the place of legal judgments. Therefore, the hybrid model is far from being revolutionary. It is just an attempt to render the language of the technology comprehensible by law.

ISSN: 2582-6433

Figure 1. The Code-Law Hybrid Model



VIII. CONCLUSION

As smart contract technology advances, the challenge before Indian law is not entirely new and yet, one that it will need to face anew: while the law recognizes digital transactions, is it capable of regulating disputes arising from such transactions in sufficient detail? To which, there is an affirmative response, albeit qualified: the existing legal framework allows for electronic contracting, electronic evidence and the arbitration of disputes in commerce. However, much remains unclear about coded consent, the admissibility of blockchain evidence, failure of oracles and automation vis-à-vis misconduct.

While the above paper makes the case for the continued arbitrability of the majority of smart-contract lending disputes because such disputes are in personam disputes in commerce, the implications thereof must not be exaggerated. Fraud, criminal activity, consumer protection claims and disputes raising rights that require adjudication in public fora may well be beyond the purview of arbitration. What then matters more is the problem not of arbitrability as such, but the lack of procedural clarity regarding how one would distinguish one dispute from another in this setting.

ISSN: 2582-6433

The Code-Law Hybrid Model presented above represents one way forward. The former will continue being applicable in relation to straightforward, rule-based disputes, while legally complicated disputes will be channeled towards institutional arbitrations involving technical expertise, and everything else will stay in the domain of traditional court litigation. Importantly, this solution is realistic. This approach does not try to suggest that law could somehow be replaced by code. On the contrary, it implies that the only way in which fintech lending can be efficient yet non-opaque and fair is to establish cooperation between law and code. In other words, it means that Indian legislators and jurists have to adopt new procedures regarding the recognition of smart contract data as a part of an arbitration agreement, and rules concerning blockchain transactions as well.

FOOTNOTES

1. Arbitration and Conciliation Act, No. 26 of 1996, § 7 (India).
2. Information Technology Act, No. 21 of 2000, § 10A (India).
3. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 (India).
4. Vidya Drolia v. Durga Trading Corp., (2021) 2 S.C.C. 1 (India).
5. Booz Allen & Hamilton Inc. v. SBI Home Fin. Ltd., (2011) 5 S.C.C. 532 (India).
6. A. Ayyasamy v. A. Paramasivam, (2016) 10 S.C.C. 386 (India).
7. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
8. Radiance Galore v. Yes Bank Ltd., Commercial Arbitration Petition (L) No. 15786 of 2025, order dated July 9, 2025 (Bom. H.C.).
9. Rhutikumari v. Zanmai Labs Pvt. Ltd., O.A. No. 194 of 2025, order dated Oct. 25, 2025 (Mad. H.C.).
10. Reserve Bank of India, Reserve Bank of India (Digital Lending) Directions, 2025 (May 8, 2025).
11. Securities and Exchange Board of India, Master Circular for Online Resolution of Disputes in the Indian Securities Market (Dec. 28, 2023).
12. Digital Personal Data Protection Act, No. 22 of 2023 (India).
13. Compound Proposal 63: Temporary Patch for COMP Distribution Bug (Sept. 30, 2021), COMPOUND GOVERNANCE,
14. Compound Proposal 64: Patch for COMP Distribution Bug (Oct. 2021), COMPOUND GOVERNANCE,
15. Reserve Bank of India, FAQs on Digital Lending Guidelines (updated 2023–2025), https://www.rbi.org.in.

ISSN: 2582-6433

16. Vidya Drolia, (2021) 2 S.C.C. at 35–42.
17. See generally Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305 (2017).

REFERENCE SECTION

STATUTES

Arbitration and Conciliation Act, No. 26 of 1996 (India).

Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).

Digital Personal Data Protection Act, No. 22 of 2023 (India).

Information Technology Act, No. 21 of 2000 (India).

CASES

A. Ayyasamy v. A. Paramasivam, (2016) 10 S.C.C. 386 (India).

Booz Allen & Hamilton Inc. v. SBI Home Fin. Ltd., (2011) 5 S.C.C. 532 (India).

Radiance Galore v. Yes Bank Ltd., Commercial Arbitration Petition (L) No. 15786 of 2025, order dated July 9, 2025 (Bom. H.C.).

Rhutikumari v. Zanmai Labs Pvt. Ltd., O.A. No. 194 of 2025, order dated Oct. 25, 2025 (Mad. H.C.).

Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

Vidya Drolia v. Durga Trading Corp., (2021) 2 S.C.C. 1 (India).

REGULATORY MATERIALS

Reserve Bank of India, Reserve Bank of India (Digital Lending) Directions, 2025 (May 8, 2025).

Reserve Bank of India, FAQs on Digital Lending Guidelines, https://www.rbi.org.in.

Securities and Exchange Board of India, Master Circular for Online Resolution of Disputes in the Indian Securities Market (Dec. 28, 2023).

SECONDARY SOURCES

Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305 (2017).

Werbach & Cornell, Contracts Ex Machina, 67 DUKE L.J. 313 (2017).

Articles and reports concerning blockchain arbitration, decentralized finance (DeFi), electronic evidence, online dispute resolution, and smart contract enforceability under Indian law.