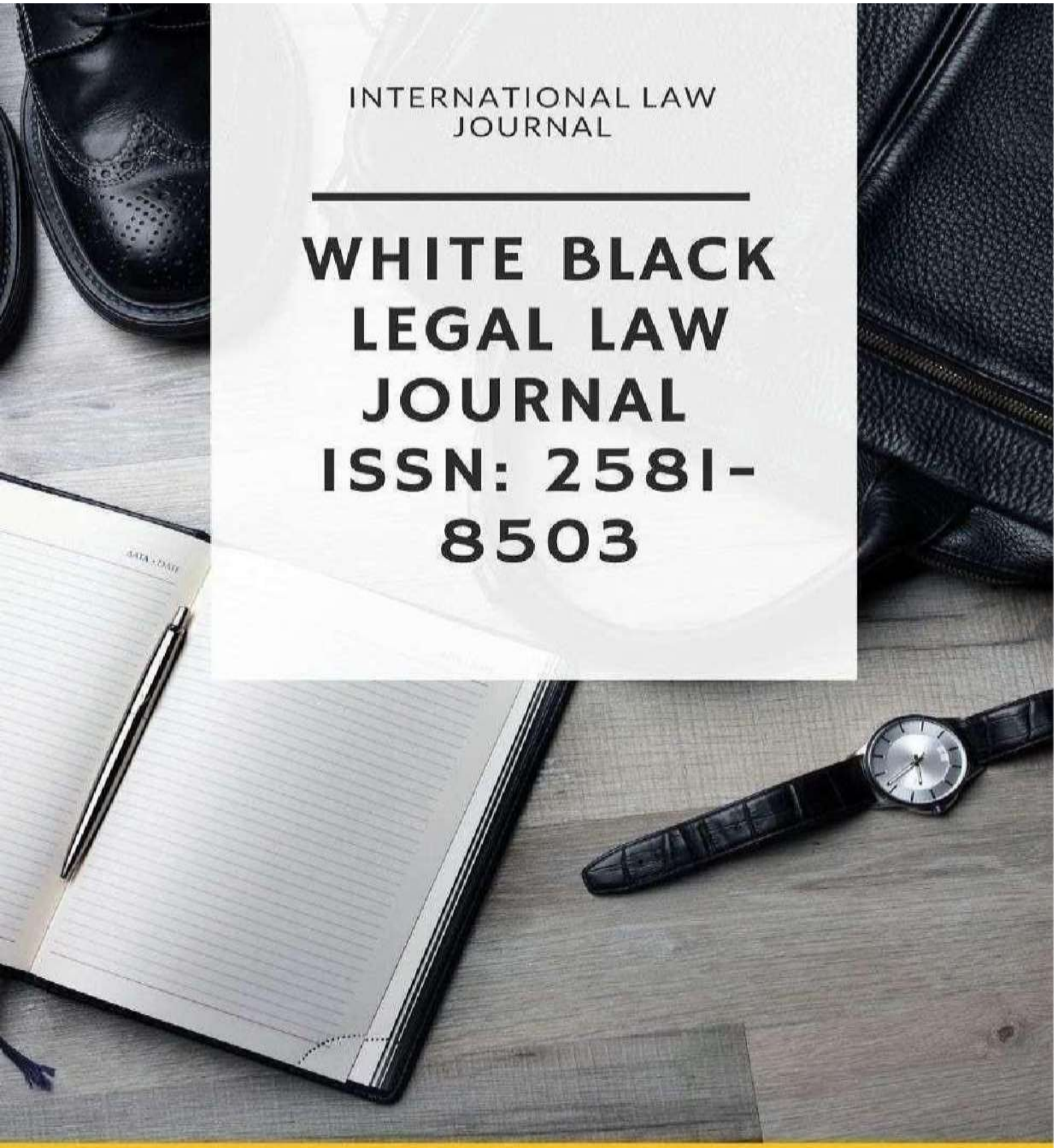

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

BLOCKCHAIN TECHNOLOGY AND THE LEGAL STATUS OF SMART CONTRACTS IN INDIA

AUTHORED BY - P. KAVYANJALI
Trinity Institute of Professional Studies

ABSTRACT

Smart contracts, enabled by blockchain technology, are transforming the manner in which agreements are created and executed in the digital era. This article examines their legal recognition and enforceability within the framework of the Indian Contract Act, 1872 and the Information Technology Act, 2000, while also addressing related issues of evidentiary value and regulatory oversight. It analyses key challenges such as jurisdictional uncertainty, coding risks, and data privacy concerns, along with the limitations of automated execution in accommodating traditional legal principles. The article further considers international approaches and sectoral applications to identify gaps in the Indian legal framework. It concludes that although existing laws provide a foundational basis, a more coherent and adaptive regulatory structure is required for the effective integration of smart contracts in India.

1. INTRODUCTION

Blockchain technology has emerged as a transformative digital innovation with the potential to redefine traditional legal and commercial frameworks. At its core, blockchain is a decentralized and distributed ledger system that ensures transparency, immutability, and security of data without reliance on centralized intermediaries.[1]

A key application of blockchain technology is the emergence of smart contracts—self-executing agreements in which contractual terms are encoded and automatically enforced upon the fulfilment of predetermined conditions.[2] However, the absence of a dedicated statutory framework governing smart contracts creates challenges relating to jurisdiction, dispute resolution, and regulatory clarity, thereby necessitating a careful evaluation of their role within the Indian legal system.[3]

[1] NITI Aayog, *Blockchain: The India Strategy* 3–5 (2020), <https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf>
[2] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 74–76 (2018).
[3] NITI Aayog, Blockchain: The India Strategy (Government of India 2020) <https://niti.gov.in> accessed 17 April 2026; Law Commission of India, Consultation Paper on Digital Economy and Emerging Technologies (Law

2. UNDERSTANDING BLOCKCHAIN

Blockchain is a decentralized digital ledger technology that records transactions across a network of computers in a secure, transparent, and immutable manner. Unlike traditional centralized systems, each transaction is stored in a "block" and linked sequentially to form a "chain," ensuring that once recorded, the data cannot be altered, thereby enhancing trust and integrity.[4]

From a legal and policy perspective, the Information Technology Act, 2000 provides legal recognition to electronic records and digital signatures, forming the foundational basis for blockchain-based transactions.[5] Additionally, regulatory bodies such as the Reserve Bank of India (RBI) have adopted a cautious approach toward virtual assets while acknowledging the potential of underlying blockchain technology.[6] On a broader level, international developments, including the UNCITRAL Model Law on e-commerce and evolving global best practices on digital transactions, further support the recognition of electronic and automated systems, indirectly strengthening the legal acceptance of blockchain-based frameworks.[7] Together, these policies and legal instruments provide a supportive—though still evolving—foundation for the adoption and regulation of blockchain technology in India.

3. THEORETICAL PERSPECTIVE: CODE AS LAW VS TRADITIONAL LEGAL REGULATION

The emergence of blockchain technology and smart contracts has reignited the debate on the relationship between technology and law, particularly through the concept of "code as law." This theory, most prominently articulated by Lawrence Lessig, suggests that in digital environments, code functions as a regulatory mechanism capable of shaping behaviour in ways comparable to legal rules. Unlike traditional law, which operates through ex post enforcement by courts and regulatory institutions, code regulates ex ante by embedding rules directly into technological architecture. In the context of smart contracts, this means that contractual obligations are not merely agreed upon but are automatically executed upon the fulfilment of

Commission of India)

[4] NITI Aayog, *Blockchain: The India Strategy* 3–5 (2020), <https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf>.

[5] Information Technology Act, No. 21 of 2000, s. 4 and s. 5.

[6] Reserve Bank of India, Report of the Working Group on Digital Lending (2021).

[7] UNCITRAL Model Law on Electronic Commerce.

predefined conditions, thereby reducing reliance on external enforcement mechanisms.[8] However, this shift from legal regulation to code-based governance raises important conceptual concerns. Traditional legal systems are inherently interpretative, allowing courts to consider intent, fairness, and contextual factors when resolving disputes. In contrast, code operates on strict logic and binary execution, leaving little room for discretion or equitable considerations.[9] This rigidity can lead to outcomes that, while technically accurate, may be legally or morally undesirable, particularly in cases involving mistake, coercion, or unforeseen circumstances.[10]

From an Indian legal perspective, this tension is particularly significant given the emphasis placed by the Indian Contract Act, 1872 on essential elements such as free consent, lawful consideration, and intention to create legal relations.[11] These elements require interpretative assessment that cannot be fully replicated through code-based execution. While smart contracts may enhance efficiency, they do not inherently account for defects in consent or evolving circumstances that may affect contractual validity, thereby raising concerns regarding their compatibility with traditional doctrines of contract law.[12]

At the same time, it would be reductive to treat code and law as mutually exclusive. A more balanced approach recognises that code can complement legal regulation by enhancing efficiency, reducing transaction costs, and ensuring certainty in performance.[13] This has led to the emergence of hybrid contractual models that combine legal agreements with automated execution mechanisms, allowing parties to benefit from both technological precision and legal flexibility.[14] In this sense, the debate is not whether code should replace law, but how the two can be effectively integrated within a coherent legal framework.

Additionally, international developments reflect a growing acceptance of technology-neutral approaches, where existing legal doctrines are adapted to accommodate digital innovation rather than replaced entirely. Institutions such as the UK Jurisdiction Taskforce and the United Nations Commission on International Trade Law have supported the recognition of automated and electronic contracting systems, reinforcing the relevance of traditional legal principles in technologically advanced environments.[15]

[8] Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 1999) 6–8.
[9] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 73–75.
[10] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 *Duke Law Journal* 313, 335–338.
[11] Indian Contract Act, 1872, s 10.
[12] Ewan McKendrick, *Contract Law: Text, Cases, and Materials* (8th edn, Oxford University Press 2020) 45–47.
[13] Chris Reed, *Making Laws for Cyberspace* (Oxford University Press 2012) 112–115.
[14] Primavera De Filippi and Aaron Wright (n 2) 83–85.
[15] UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (2019).

4. SMART CONTRACTS

Smart contracts are self-executing digital agreements in which contractual terms are embedded in code and automatically executed upon the fulfilment of predefined conditions. Smart contracts on blockchain technology enable direct, peer-to-peer transactions without reliance on intermediaries, thereby increasing efficiency, transparency, and security.[16] The concept was first articulated by Nick Szabo, who described smart contracts as computerized protocols that facilitate, verify, and enforce the performance of contractual obligations.[17] Unlike traditional contracts that depend on written terms and external enforcement, smart contracts operate through automated execution, ensuring that obligations are carried out precisely as programmed.

Technically, smart contracts function on blockchain platforms through distributed networks of nodes that validate transactions using consensus mechanisms and cryptographic techniques. Once deployed, the code is stored on an immutable ledger, making it tamper-resistant and transparent. In the Indian context, although there is no specific legislation governing smart contracts, their legal recognition is assessed under existing frameworks such as the Indian Contract Act, 1872 and the Information Technology Act, 2000, which together provide the foundational basis for determining their validity and enforceability.[18]

5. HYBRID CONTRACTS: INTERFACE BETWEEN CODE AND TRADITIONAL AGREEMENTS

Hybrid contracts represent a pragmatic convergence between traditional legal agreements and blockchain-based smart contracts, combining natural language terms with automated code execution. Unlike purely code-driven smart contracts, hybrid arrangements typically involve a written agreement that outlines the rights and obligations of the parties, while specific operational aspects—such as payment triggers or performance conditions—are executed automatically through code. This dual structure allows parties to retain legal clarity and interpretative flexibility while benefiting from the efficiency and certainty of automation.[19]

From a legal standpoint, hybrid contracts are particularly relevant in jurisdictions like India, where existing frameworks such as the Indian Contract Act, 1872 require clear elements of

[16] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (Harvard University Press 2018).
[17] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996).
[18] Indian Contract Act, 1872; Information Technology Act, 2000.
[19] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (Harvard University Press 2018) 73–75.

offer, acceptance, and free consent for a contract to be valid.[20] The incorporation of a traditional written agreement ensures that these elements are explicitly articulated, thereby reducing ambiguity that may arise from purely coded instructions. At the same time, the automated execution layer enhances performance efficiency by minimizing the need for intermediaries and manual enforcement.[21]

Hybrid contracts also address one of the primary limitations of smart contracts—namely, the rigidity of code. While code operates strictly on predefined logic, legal agreements often require interpretation in light of unforeseen circumstances, such as mistake, fraud, or force majeure.[22] By retaining a parallel natural language contract, hybrid models allow courts to interpret the intent of the parties and apply equitable remedies where necessary, even if the coded component has already been executed. This ensures that traditional doctrines under contract law remain applicable despite technological integration.[23]

Another significant advantage of hybrid contracts lies in their ability to allocate risk and liability more effectively. In purely automated systems, it is often unclear whether liability should rest with the programmer, the user, or the platform.[24] Hybrid contracts mitigate this uncertainty by expressly defining liability clauses, dispute resolution mechanisms, and governing law within the written agreement. This provides a structured legal framework to address issues arising from coding errors, system failures, or external data inaccuracies.[25]

Furthermore, hybrid contracts facilitate better integration with existing regulatory and evidentiary systems. Under the Information Technology Act, 2000, electronic records and digital signatures are granted legal recognition, which supports the enforceability of digitally executed agreements.[26] The presence of a written contract alongside blockchain records strengthens evidentiary reliability, enabling courts to assess both the intent and execution of the agreement.[27]

In practice, hybrid contracts are increasingly being adopted in sectors such as finance, insurance, and supply chain management, where complete automation may not be feasible or legally desirable. They represent a transitional model that bridges the gap between traditional legal systems and emerging technological frameworks. While fully autonomous smart

[20] Indian Contract Act, 1872, s 10.
[21] Chris Reed, *Making Laws for Cyberspace* (Oxford University Press 2012) 112–115.
[22] Indian Contract Act, 1872, ss 13–19.
[23] McKendrick E, Contract Law: Text, Cases, and Materials (8th edn, Oxford University Press 2020) 45–48.
[24] Primavera De Filippi and Aaron Wright (n 1) 83–85.
[25] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 *Duke Law Journal* 313, 340–345.
[26] Information Technology Act, 2000, ss 4–5.
[27] Trimex International FZE Ltd v Vedanta Aluminium Ltd.

contracts may remain limited due to legal and practical constraints, hybrid contracts offer a viable pathway for gradual integration of blockchain technology into mainstream contractual practice.[28]

6. LEGAL VALIDITY OF SMART CONTRACTS UNDER THE INDIAN CONTRACT ACT, 1872

The legal validity of smart contracts in India is primarily assessed under the framework of the Indian Contract Act, 1872, which lays down the essential elements required for a legally enforceable agreement. Under Section 10 of the Act, a valid contract must involve free consent of competent parties, lawful consideration, lawful object, and must not be expressly declared void. Smart contracts, although executed through code, can satisfy these requirements if there is a clear offer and acceptance, lawful consideration embedded within the transaction, and an intention to create legal relations. Thus, in principle, smart contracts are not invalid merely because they are in electronic or coded form.[29]

However, the element of consent may be difficult to interpret where parties interact with automated code rather than negotiated terms, raising questions about informed consent and understanding of obligations. Similarly, issues may arise regarding mistake or coercion, particularly where the execution of the contract is automatic and irreversible. The rigid nature of coded agreements also challenges doctrines such as frustration and modification, as smart contracts lack the flexibility typically available in traditional contracts. Despite these concerns, Indian courts have shown a progressive approach toward electronic agreements. In "Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.", the Supreme Court upheld the validity of contracts formed through electronic communication, affirming that formal written contracts are not always necessary if essential terms are agreed upon.[30]

While the Act does not explicitly refer to smart contracts, it provides a statutory basis for recognizing electronic agreements, thereby indirectly supporting their enforceability. Therefore, although smart contracts can be accommodated within the existing legal framework of the Indian Contract Act, their full legal integration requires clearer statutory recognition and judicial guidance.

[28] UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (2019).
[29] Indian Contract Act, 1872, Section 10.
[30] Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., 2010 SCC OnLine SC 214.

7. RECOGNITION OF ELECTRONIC CONTRACTS UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 constitutes the principal statutory framework governing the legal recognition of electronic contracts in India. Section 10A of the Act explicitly affirms that contracts formed through electronic means shall not be deemed unenforceable solely on the ground that electronic records or communications were used in their formation.[31] This provision reflects a technology-neutral legislative approach, enabling the legal system to accommodate evolving forms of digital contracting, including automated and system-driven agreements. From a doctrinal perspective, it signifies a shift from form-based validity toward substance-based recognition of contractual intent in electronic environments.

However, the absence of explicit reference to blockchain-based agreements or self-executing smart contracts creates interpretational gaps, particularly in relation to automated performance and immutable execution. Consequently, while the existing framework under the Information Technology Act facilitates indirect recognition of such contracts, it remains insufficient to comprehensively address their distinct technical and legal characteristics, thereby underscoring the need for a more specialized and adaptive regulatory approach.

8. ENFORCEABILITY OF SMART CONTRACTS IN INDIA: LEGAL AND PRACTICAL ISSUES

The enforceability of smart contracts in India is shaped by the interplay between traditional contract law principles and emerging technological realities. Under the Indian Contract Act, 1872, a contract is enforceable only if it satisfies essential elements such as offer, acceptance, lawful consideration, and free consent.[32] Smart contracts, though executed through code, may fulfill these requirements where parties demonstrate clear intention to be bound. However, the absence of express statutory recognition of blockchain-based agreements creates uncertainty regarding their legal status.[33] Judicial precedents on electronic contracts provide some guidance; the Supreme Court upheld the validity of agreements formed through electronic communication, thereby indicating a flexible approach toward non-traditional modes of contracting.[34]

[31] Information Technology Act, 2000, s. 10A.
[32] Indian Contract Act, 1872, s. 10.
[33] Id.
[34] Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd., 2010 SCC OnLine SC 214.

Despite this, significant legal challenges arise due to the inherent characteristics of smart contracts. The principle of consent, a cornerstone of contract law, becomes difficult to assess where contractual terms are embedded in complex code rather than comprehensible language.[35] Additionally, doctrines such as mistake, coercion, or misrepresentation may be difficult to invoke once a smart contract is automatically executed, given its immutable nature.[36] From a practical perspective, the irreversibility of blockchain transactions poses a direct conflict with traditional remedies such as rescission or restitution.[37]

Further, issues of jurisdiction and applicable law complicate enforcement, particularly in cross-border transactions where blockchain networks operate across multiple jurisdictions without a centralized authority.[38] Determining the appropriate forum and governing law becomes challenging, thereby creating procedural uncertainty. Policy frameworks such as the National Blockchain Framework introduced by the Government of India acknowledge both the potential and regulatory challenges associated with blockchain deployment.[39] Similarly, industry bodies like the Internet and Mobile Association of India have emphasized the need for a clear and balanced regulatory approach to address risks such as liability, security, and compliance.[40]

Moreover, the issue of liability allocation remains unresolved in cases of coding errors or system vulnerabilities. It is unclear whether liability should attach to the programmer, the contracting parties, or the platform facilitating the transaction.[41]

9. EVIDENCE AND ADMISSIBILITY OF BLOCKCHAIN-BASED TRANSACTIONS

The evidentiary value of blockchain-based transactions in India must be examined within the framework of electronic evidence under the Indian Evidence Act, 1872. Blockchain records, being digitally stored and generated through distributed ledger systems, qualify as "electronic records" under section 2(1)(t) of the Information Technology Act, 2000, and are therefore admissible subject to compliance with statutory requirements.[42] The primary provision governing admissibility is section 65B of the Evidence Act, which mandates that any electronic

[35] 2 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition § 11:2 (5th ed. 2024). (used here for principle of clarity & distinctiveness analogy in contractual understanding)
[36] Indian Contract Act, 1872, s. 13–19.
[37] Id. s. 65–66.
[38] Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 78–82 (2018).
[39] Press Information Bureau, Government of India, National Blockchain Framework: Strengthening Governance through Blockchain Technology (Oct. 2025), https://www.pib.gov.in.
[40] Internet and Mobile Association of India, Blockchain and Crypto Industry Representations (2021).
[41] Primavera De Filippi & Aaron Wright, *supra* note 7, at 83–85.
[42] Information Technology Act, 2000, s 2(1)(t).

record must be accompanied by a certificate confirming the integrity and authenticity of the data.[43] In the context of blockchain, this raises practical questions, as the decentralized and immutable nature of the technology challenges the traditional requirement of identifying a "person in control" who can issue such a certificate.

Judicial interpretation of electronic evidence in India provides important guidance for understanding the admissibility of blockchain records. In *Anvar P V v P K Basheer*, the Supreme Court held that compliance with section 65B is mandatory for the admissibility of electronic evidence, thereby emphasizing the need for procedural safeguards to ensure authenticity.[44] This position was subsequently reaffirmed and clarified in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, where the Court reiterated that the certificate requirement is a condition precedent for admissibility, except in limited circumstances where the original device is produced.[45] These rulings suggest that blockchain-based records, despite their inherent reliability, must still satisfy statutory evidentiary standards to be admissible in Indian courts.

At the same time, the inherent characteristics of blockchain technology—such as immutability, transparency, and cryptographic security—enhance the evidentiary credibility of such records. Once a transaction is recorded on a blockchain, it becomes tamper-resistant and verifiable across multiple nodes, thereby reducing the risk of manipulation.[46] From a legal standpoint, this may strengthen the probative value of blockchain records, even though admissibility remains subject to procedural compliance. Courts may, over time, recognise these technological safeguards as indicators of reliability, potentially influencing the interpretation of evidentiary rules in a digital context.

However, certain challenges persist. The pseudonymous nature of blockchain transactions may complicate the identification of parties, while the absence of a central authority raises questions regarding certification and custody of records. Additionally, issues may arise in demonstrating the chain of custody and linking a particular transaction to a specific individual.[47] These concerns highlight the tension between traditional evidentiary requirements and emerging technological frameworks.

[43] Indian Evidence Act, 1872, s 65B.
[44] Anvar P V v P K Basheer (2014) 10 SCC 473.
[45] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
[46] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 38–40.
[47] Stephen Mason and Daniel Seng, Electronic Evidence (5th edn, Institute of Advanced Legal Studies 2021) 112–115.

10.REGULATORY APPROACH AND POLICY FRAMEWORK IN INDIA

India's regulatory approach to blockchain technology and smart contracts reflects a cautious yet evolving stance, balancing innovation with financial and systemic risk concerns. The Reserve Bank of India has played a central role in shaping the regulatory discourse, particularly in relation to virtual currencies and distributed ledger technologies. While the RBI has consistently highlighted risks such as volatility, consumer protection concerns, and potential misuse for illicit activities, it has also acknowledged the efficiency gains that blockchain can bring to payment systems and financial infrastructure.[48] This dual approach indicates a clear distinction between speculative digital assets and the broader utility of blockchain technology. Concurrently, the Ministry of Electronics and Information Technology has taken a proactive stance in promoting blockchain adoption through policy initiatives and institutional frameworks. The introduction of the National Blockchain Framework reflects the government's intent to create a standardized, secure, and scalable ecosystem for blockchain deployment across sectors such as governance, healthcare, and supply chain management.[49] This initiative is aligned with broader national programs such as Digital India, which aim to leverage emerging technologies to enhance transparency, efficiency, and accessibility in public service delivery.[50] Furthermore, policy discussions emphasize interoperability, data protection, and infrastructure readiness as key pillars for blockchain integration.[51]

Despite these developments, India lacks a comprehensive and unified legal framework specifically governing smart contracts and blockchain-based transactions. The current regulatory approach remains fragmented, relying on general statutes such as the Information Technology Act, 2000 and sector-specific guidelines.[52] This creates uncertainty in critical areas such as cross-border transactions, jurisdiction, liability allocation, and dispute resolution. Industry bodies, including the Internet and Mobile Association of India, have advocated for a balanced regulatory regime that encourages innovation while addressing systemic risks.[53]

[48] Reserve Bank of India, *Report of the Working Group on FinTech and Digital Banking* (2018).
[49] Press Information Bureau, Government of India, National Blockchain Framework: Strengthening Governance through Blockchain Technology (Oct. 2025), <https://www.pib.gov.in>.
[50] Ministry of Electronics & Information Technology, Government of India, Digital India Programme (2015).
[51] Ministry of Electronics and Information Technology, Strategy on Blockchain and Distributed Ledger Technologies (discussion papers).
[52] Information Technology Act, 2000
[53] Internet and Mobile Association of India, *Blockchain and Crypto Industry Representations* (2021).

11.JURISDICTIONAL AND DISPUTE RESOLUTION CHALLENGES IN BLOCKCHAIN TRANSACTIONS

Unlike traditional contracts that are anchored to a specific territorial legal system, blockchain-based agreements may involve parties, nodes, and validating mechanisms spread across multiple jurisdictions. Under Indian private international law principles, jurisdiction is typically determined based on factors such as place of contracting, place of performance, or residence of parties; however, these connecting factors become ambiguous in the context of distributed ledger systems.[54]

Further, dispute resolution in smart contract transactions is complicated by the automated and immutable nature of blockchain execution. Once a smart contract is triggered, it executes automatically without the possibility of intervention, thereby limiting the effectiveness of traditional remedies such as injunctions, rescission, or specific performance.[55] This creates a tension between technological finality and legal flexibility. Additionally, evidentiary issues arise in establishing the intent of parties and interpreting coded terms, particularly where contractual obligations are embedded in complex programming language rather than natural text.[56] The Indian courts, while recognizing electronic records under the Information Technology Act, 2000, may face practical difficulties in assessing technical evidence and attributing liability in such cases.[57]

Moreover, the lack of standardized dispute resolution mechanisms tailored to blockchain transactions further exacerbates enforcement challenges.

Policy discussions at both national and international levels emphasize the need for developing specialized legal frameworks and technological solutions, such as on-chain dispute resolution systems, to address these concerns.[58] In the Indian context, the absence of specific legislative provisions governing cross-border blockchain disputes underscores the necessity for regulatory clarity and institutional innovation to ensure effective dispute resolution in this evolving domain.

12. SECTORAL APPLICATIONS OF SMART CONTRACTS IN INDIA

Smart contracts are increasingly being adopted across multiple sectors in India due to their

[54] Dicey, Morris & Collins, *The Conflict of Laws* 5–10 (15th ed. 2012).
[55] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 78–82 (2018).
[56] Id. at 83–85.
[57] Information Technology Act, 2000, s. 4.
[58] United Nations Commission on International Trade Law, *Technical Notes on Online Dispute Resolution* (2017).

ability to automate transactions, reduce intermediaries, and enhance transparency.

In the field of fintech, blockchain-based smart contracts are being utilized to streamline payment systems, enable faster settlements, and improve compliance mechanisms. Financial institutions are exploring their application in areas such as trade finance, digital lending, and cross-border payments, where automation can significantly reduce operational inefficiencies and transaction costs. Policy discussions by the RBI have acknowledged the role of distributed ledger technologies in strengthening financial infrastructure and improving system resilience.[59]

In the supply chain sector, smart contracts enable end-to-end visibility and traceability by recording each stage of a transaction on a blockchain, thereby reducing fraud and enhancing accountability.[60] Similarly, in the domain of land records, blockchain-based smart contracts are being explored to create tamper-proof property registries, minimizing disputes relating to ownership and title verification. Government initiatives led by the Ministry of Electronics and Information Technology and supported through national policy frameworks have demonstrated the potential of blockchain in modernizing land administration systems.[61]

In the insurance sector, smart contracts facilitate automated claim processing and settlement based on predefined conditions, thereby reducing delays and administrative costs.[62] Claims can be executed automatically upon verification of insured events through external data sources, improving efficiency and reducing the risk of fraud. Industry bodies such as the Internet and Mobile Association of India have emphasized the importance of regulatory clarity to support innovation in such applications.[63] Additionally, global and domestic policy reports highlight that blockchain adoption across these sectors depends on interoperability, data security, and institutional readiness.[64] Despite these advancements, large-scale adoption remains constrained by legal uncertainty, technological limitations, and the absence of standardized regulatory frameworks in India.[65]

13. COMPARATIVE INSIGHTS AND NEED FOR LEGAL REFORM IN INDIA

A comparative analysis of global approaches to smart contracts reveals that several

[59] Reserve Bank of India, *Report of the Working Group on FinTech and Digital Banking* (2018).
[60] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 90–92 (2018).
[61] Ministry of Electronics and Information Technology, *National Strategy on Blockchain* (2020)
[62] World Economic Forum, Blockchain Beyond the Hype (2018).
[63] Internet and Mobile Association of India, Blockchain and Crypto Industry Representations (2021).
[64] NITI Aayog, Blockchain: The India Strategy (2020).
[65] Press Information Bureau, Government of India, Use of Blockchain Technology in Governance (2022), <https://www.pib.gov.in.>

jurisdictions have taken proactive steps toward recognizing and regulating blockchain-based agreements. Countries such as the United States have adopted a technology-neutral approach, allowing existing contract law principles to accommodate electronic and automated agreements, supplemented by legislative developments recognizing blockchain-based records and signatures.[66] Similarly, Singapore has embraced innovation through regulatory flexibility and recognizes the legal validity of electronic contracts within its statutory framework.[67] The United Kingdom, through the UK Jurisdiction Taskforce, has clarified that smart contracts are capable of constituting legally binding agreements, provided traditional contractual elements are satisfied.[68] Academic commentary also supports this adaptive approach toward integrating technology with existing legal doctrines.[69]

In contrast, India's legal approach remains indirect and fragmented, relying primarily on general statutes such as the Indian Contract Act, 1872 and the Information Technology Act, 2000, without explicit statutory recognition of smart contracts.[70] While this technology-neutral framework provides flexibility, it leads to interpretational ambiguity in areas such as automated execution, liability allocation, and cross-border enforcement. Policy assessments by the Reserve Bank of India and the Ministry of Electronics and Information Technology also highlight regulatory gaps and the need for structured governance in emerging technologies.[71]

Accordingly, there is a pressing need for legal reform in India to address the unique challenges posed by smart contracts. International instruments such as the United Nations Commission on International Trade Law Model Law on Electronic Commerce provide guidance for harmonizing digital transaction laws.[72] Domestic policy frameworks, including reports by NITI Aayog, further emphasize the importance of developing a supportive regulatory ecosystem.[73] Comparative scholarship also suggests that jurisdictions adopting clear and adaptive frameworks are better positioned to balance innovation with legal certainty.[74]

[66] Arizona Revised Statutes § 44-7061 (2017) (U.S.).
[67] Singapore Electronic Transactions Act (Cap. 88) (Sing.).
[68] UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (2019).
[69] Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 120–25 (2018).
[70] Indian Contract Act, 1872; Information Technology Act, 2000.
[71] Reserve Bank of India, *Financial Stability Report* (2021).
[72] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce (1996).
[73] NITI Aayog, Blockchain: The India Strategy (2020).
[74] Primavera De Filippi & Aaron Wright, supra note 4, at 126–28.

14.CHALLENGES, RISKS, AND LIMITATIONS OF SMART CONTRACTS

Despite their transformative potential, smart contracts present several legal, technical, and practical challenges that limit their widespread adoption. One of the primary concerns relates to the rigidity of code-based execution, as smart contracts operate strictly according to pre-programmed instructions and lack the flexibility to accommodate unforeseen circumstances.[75] This rigidity conflicts with traditional contract law principles that allow for interpretation, modification, and equitable remedies in cases of mistake, fraud, or frustration. Under the Indian Contract Act, 1872, doctrines such as free consent and voidability require a degree of human interpretation, which is difficult to reconcile with automated execution.[76]

Another significant challenge is the issue of coding errors and vulnerabilities. Since smart contracts are written in software code, any flaw or bug can lead to unintended outcomes, financial losses, or exploitation by malicious actors.[77] The absence of standardized coding practices and regulatory oversight further exacerbates these risks. Additionally, the immutability of blockchain technology means that once a smart contract is deployed, it cannot be easily altered or reversed, even in cases of error or illegality.[78] This creates tension between technological finality and legal remedies such as rescission or restitution.

From a legal standpoint, concerns also arise regarding liability and accountability. In cases where a smart contract fails or produces unintended consequences, it is unclear whether liability should be attributed to the programmer, the contracting parties, or the platform facilitating the transaction.[79] Furthermore, jurisdictional uncertainties and cross-border enforcement issues complicate dispute resolution, particularly in decentralized environments where no single authority governs the transaction.[80] Although the Information Technology Act, 2000 provides a framework for electronic transactions, it does not adequately address the unique features of blockchain-based contracts.[81]

Additionally, smart contracts face limitations in terms of data reliability and external inputs. Many smart contracts rely on external data sources, known as "oracles," to trigger execution. If these data inputs are inaccurate or compromised, the contract may execute incorrectly,

[75] Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 72–75 (2018).
[76] Indian Contract Act, 1872, s. 13–19.
[77] Id. at 80–82.
[78] World Economic Forum, Blockchain Beyond the Hype (2018).
[79] Primavera De Filippi & Aaron Wright, supra note 1, at 83–85.
[80] Gary B. Born, International Commercial Arbitration 89–95 (2d ed. 2014).
[81] Information Technology Act, 2000.

leading to disputes and losses.[82] Moreover, the lack of regulatory clarity and standardized frameworks in India continues to hinder adoption, as emphasized by policy discussions from bodies such as the Reserve Bank of India and the Ministry of Electronics and Information Technology.[83]

In light of these challenges, while smart contracts offer significant efficiency and automation benefits, their practical implementation remains constrained by technological limitations, legal uncertainties, and regulatory gaps. Addressing these issues through clearer legal frameworks, technical standards, and institutional mechanisms is essential for their sustainable integration into the Indian legal system.[84]

15.COMPARATIVE AND INTERNATIONAL PERSPECTIVE

The global regulatory landscape surrounding smart contracts reflects a predominantly technology-neutral approach, wherein existing legal principles are adapted to accommodate emerging digital innovations. In the United States, several states have enacted legislation recognising blockchain-based records and smart contracts, affirming that agreements cannot be denied legal effect solely due to their electronic or automated nature.[85] This approach underscores a broader reliance on traditional contract law doctrines, allowing courts to interpret and enforce such agreements without necessitating entirely new statutory frameworks.[86]

In the United Kingdom, the UK Jurisdiction Taskforce has provided significant clarity by affirming that smart contracts are capable of constituting legally binding agreements under existing principles of English contract law.[87] The UK approach emphasizes flexibility, suggesting that the absence of explicit statutory provisions does not preclude enforceability, provided the essential elements of contract formation are satisfied.[88] This reflects judicial confidence in the adaptability of established legal doctrines to technological advancements.

Singapore has adopted a progressive and innovation-oriented regulatory stance, integrating smart contracts within its broader digital economy and fintech ecosystem. The legal framework in Singapore recognises electronic contracts and supports the use of distributed ledger

[82] Primavera De Filippi & Aaron Wright, supra note 1, at 86–88.
[83] Reserve Bank of India, Financial Stability Report (2021); Ministry of Electronics and Information Technology, National Strategy on Blockchain (2020).
[84] NITI Aayog, Blockchain: The India Strategy (2020).
[85] Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 Georgetown Law Technology Review 305, 310–312.
[86] Kevin Werbach, The Blockchain and the New Architecture of Trust (MIT Press 2018) 95–98.
[87] UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (2019).
[88] Law Commission, Smart Legal Contracts: Advice to Government (Law Com No 401, 2021) 23–26.

technology, thereby facilitating the commercial deployment of smart contracts.[89] This approach balances regulatory oversight with technological advancement, making Singapore a leading jurisdiction in blockchain adoption.

At the international level, frameworks developed by the United Nations Commission on International Trade Law play a crucial role in harmonising legal standards for electronic commerce. Instruments such as the UNCITRAL Model Law on Electronic Commerce and the Model Law on Electronic Transferable Records promote the recognition of electronic communications and automated contracting systems, thereby providing a foundational basis for the legal acceptance of smart contracts in cross-border transactions.[90]

A comparative analysis of these jurisdictions reveals a common trend toward flexibility and technological neutrality, with an emphasis on adapting existing legal principles rather than creating entirely new regimes. Academic scholarship further supports this view, suggesting that rigid regulatory intervention may hinder innovation in rapidly evolving technological domains.[91] In contrast, India's current framework remains indirect and fragmented, relying primarily on general statutes without explicit recognition of smart contracts.[92] This highlights the need for a more coherent and structured legal approach in India, drawing from international best practices while addressing domestic legal and regulatory considerations.

16.CONCLUSION: FUTURE OF SMART CONTRACTS IN THE INDIAN LEGAL SYSTEM

Smart contracts represent a significant shift in contractual architecture, moving from traditional written agreements to automated, code-based execution systems. In India, their future development is situated at the intersection of classical contract principles under the Indian Contract Act, 1872 and the enabling framework for electronic transactions under the Information Technology Act, 2000.[93] While neither statute expressly recognises blockchain-based smart contracts, their technology-neutral design allows courts to interpret such agreements within existing doctrinal boundaries of offer, acceptance, and consideration.

At the policy level, the Government of India has demonstrated increasing engagement with

[89] Singapore Academy of Law, Smart Contracts: Legal and Regulatory Implications (2019) 12–15.
[90] United Nations Commission on International Trade Law, Model Law on Electronic Commerce (1996); UNCITRAL, Model Law on Electronic Transferable Records (2017).
[91] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 180–183.
[92] Roger Brownsword, Law, Technology and Society (Routledge 2019) 102–105.

[93] Indian Contract Act, 1872; Information Technology Act, 2000.

blockchain technology through initiatives led by the Ministry of Electronics and Information Technology, particularly under the National Blockchain Framework aimed at strengthening secure digital infrastructure.[94] Similarly, strategic policy recommendations by NITI Aayog highlight blockchain's potential in governance, financial inclusion, and public service delivery.[95] These developments indicate a gradual institutional acceptance of blockchain as an enabling technology, though not yet a fully regulated legal instrument.

However, regulatory caution continues to be reflected in financial oversight concerns raised by the Reserve Bank of India, particularly regarding systemic risk, consumer protection, and monetary stability.[96] This dual approach—promotion of innovation alongside risk containment—illustrates India's evolving but cautious regulatory posture. Additionally, global standard-setting efforts by the United Nations Commission on International Trade Law support the development of harmonised rules for electronic and automated contracts, which may guide future Indian reforms.[97]

From a doctrinal perspective, judicial recognition of electronic agreements, as seen in Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., suggests that Indian courts are open to enforcing contracts formed through non-traditional means where intention and consensus are clear.[98] Nevertheless, unresolved issues relating to liability allocation, dispute resolution, and code interpretation indicate the need for targeted legislative intervention.[99] Comparative insights from jurisdictions adopting technology-neutral or hybrid regulatory models further reinforce the need for India to evolve a structured framework that balances innovation with legal certainty.[100]

Ultimately, the future of smart contracts in India will depend on a coordinated evolution of law, policy, and technology. A balanced regulatory framework that integrates statutory clarity, judicial adaptability, and technological safeguards will be essential to ensure that smart contracts enhance contractual efficiency without undermining foundational principles of Indian contract law.[101]

[94] Ministry of Electronics and Information Technology, National Blockchain Framework (2025).
[95] NITI Aayog, Blockchain: The India Strategy (2020).
[96] Reserve Bank of India, Financial Stability Report (2021).
[97] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce (1996).
[98] Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., 2010 SCC OnLine SC 214
[99] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* 83–88 (2018).
[100] UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019).
[101] World Economic Forum, *Blockchain Beyond the Hype* (2018).