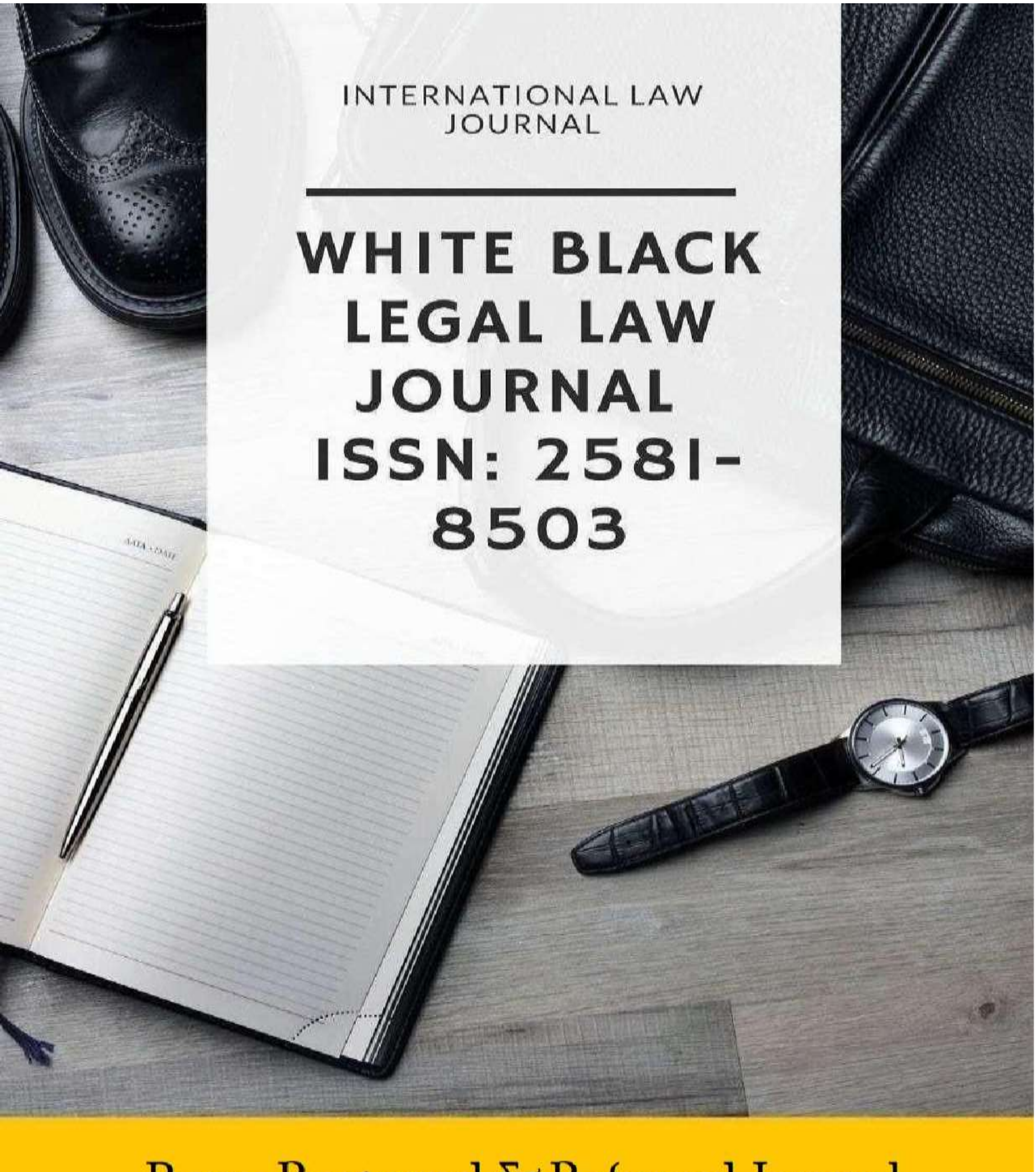

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

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.

LEGAL LANDSCAPE OF SMART CONTRACTS IN DECENTRALIZED BLOCKCHAIN NETWORKS

AUTHORED BY - UJJWAL KUMAR
(Symbiosis Law School)

CO-AUTHOR - ADITI GUPTA
(D.E.S.' Shri. Navalmal Firodia Law College)

Abstract

Smart contracts are an important technological breakthrough in contract creation and contract performance, a combination of contract law principles and cryptography and blockchain technology. Smart contracts, which consist of self-executable software running on decentralised networks, are described as automating the contract process and fulfilling contractual obligations in a deterministic manner (using the logic of if/when-then)[1] that improves efficiency, transparency, and security of transactions conducted by parties. The present paper analyses the conceptual principles and the architecture of smart contracts in blockchain architecture, decentralised consensus, cryptographic authentication, immutability, and integration with oracles. It is a critical analysis of their legal implications, especially the questions of enforceability and jurisdiction, the evidentiary admissibility and liability in decentralised settings.[2] The conflict between blockchain immutability and conventional contractual principles is discussed in detail. The paper also assesses the operational benefits of smart contracts, but at same time recognises the structural weaknesses of the same. It contends that smart contracts cannot be considered as the alternatives to traditional contracts, but as the technologically enhanced means of contractual performance implemented into the current legal frameworks. To enforce the principles of effective integration, technology-neutral statutory status, harmonised digital standards, and hybrid regulation ways that would weigh between innovation and accountability in a changing digital economy are needed.

Keywords: *Smart Contracts, Decentralised Contract Enforcement, Jurisdictional Uncertainty, Algorithmic Liability, Technology-Neutral Regulation*

[1] Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* (2014)
[2] Max Raskin, The Law and Legality of Smart Contracts, 1 Geo. L. Tech. Rev. 305 (2017)

Introduction

Smart contracts are computerized contracts where the conditions of a contract are converted to computer code and automatically executed when the predetermined conditions are met. They work based on the blockchain technology which is a decentralised and distributed registry that documents the transactions in a secure, transparent, and immutable way. In contrast to the traditional contracts where the performance is manually regulated and the enforcement is carried out by the institutions, smart contracts allow the automatic execution of the process without intermediaries, i.e. the banks, brokers or escrow agents.

Smart contracts were initially conceived in the period between 1994-1997[3] as a way of providing computer protocols to support, verify, and enforce the contractual requirements. Nevertheless, it is possible only after the development of blockchain platforms that can facilitate programmable transactions[4] that their practical implementation became a possibility. The nature of these contracts is more of an if-then logic, where once a given condition is met, then the tendency of the contract is automatically carried out. For example, payment may be made automatically on confirmation of delivery, or insurance may be paid out in response to the occurrence of a set event.

Smart contracts are the point of integration between law, technology, and commerce. They are meant to minimise the costs of transactions, improve efficiency, decrease disagreements and improve transparency in contractual relation. They cut out middlemen and automated performance, helping them to simplify commercial procedures and limit the opportunity to commit human error and opportunistic violation. They can be used in a wide range of industries, such as finance, supply chain management, real estate transactions, intellectual property licensing, and insurance.

Even though smart contracts have high technological capabilities, they also pose significant legal and regulatory challenges. The problem of enforceability, jurisdiction, and usage of coded terms as well as applicability of the traditional contract doctrines are still topics of academic discussion.[5] The fixed and irrevocable aspect of agreements based on blockchain is also an unfriendly test to established legal principles permitting the process of modification, rescission,

[3] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996)

[4] Imran Bashir, *Mastering Blockchain* (3rd ed., Packt Publ'g 2020)

[5] U.K. Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 386, 2021)

or equitable relief. Blockchain immutability clashes with equitable flexibility.[6]

Smart contract is not regarded in the modern world of law as a full substitution of the classical contracts. Instead, they are considered to be a technologically advanced system of the contractual performance and enforcement. Their increasing use requires the formulation of relevant legislations, jurisprudence, and regulatory controls to have proper alignment of technological innovation with preexisting stipulations of the law of contract.

Conceptual Framework of Smart Contracts

The convergence of smart contracts is the meeting of the contract theory with cryptography and distributed systems. A smart contract may be defined as a digital protocol that is automated, where the conditions of an agreement are coded, and performed on a blockchain network. This notion was first put forward by Nick Szabo[7] who defined smart contracts as computerised protocols of the transaction that enforce the terms of a contract. Subsequent development of blockchain software, like Ethereum[8], transformed this idea into a model of technology that was popular and applied on a large scale.

The major concept of the framework is that one should apply code to automate. The traditional contracts rely on human interpretation, supervision and enforcement. Conversely, smart contracts store requirements and terms in a deterministic programming language. This is after condition statements which are typically in (if/when-then) form and it is done when predetermined inputs are detected. This implies that the automation will guarantee the lesser utilisation of the intermediaries and reduce the leeway in the performance.

The second building block is the distributed ledger infrastructure. Smart contracts are present in blockchain networks which are replicated copies of a ledger among a number of nodes. This de-centralised system guarantees permanence and openness. The network has an agreement system which confirms the resulting transaction during execution of a smart contract. Integrity is guaranteed by the permanency of blockchain records which prevent unilateral changes to contracts following the executions.

[6] Central London Property Trust Ltd v High Trees House Ltd
[7] Szabo, supra note 6
[8] Buterin, supra note 2

Cryptographic security is another key element of conceptual framework. Smart contracts are based on the principles of public-key cryptography[9] that provides authentication of parties and safeguards transactions. Digital signatures ensure the identity of a participant and cryptographic hashing is used to maintain integrity over the data stored. These come in place to form a trust minimised environment where, no preexisting trust relationships exist between parties; rather mathematical verification and distributed consensus are used.

Another conceptual aspect is the differentiation of on-chain and off-chain aspects. Although smart contracts are implemented on the blockchain, most of the real-life circumstances happen off chain. To address this disparity, external data in the form of oracles are used to provide confirmed off-chain information to the contract.[10] Such an integration increases the scope of practical application of smart contracts but may also come with potential trust and reliability aspects.

Lastly, there is governance and upgradeability, which are part of the broader structure. Since blockchain systems are decentralised, it is complex to make amends to a deployed smart contract. There are frameworks that include upgrade mechanisms or governance protocols that permit changes with predetermined conditions that allow the balance between immutability and flexibility.

In summary, smart contract conceptual framework entails the integration of automation, decentralisation, cryptographic security, deterministic execution, as well as legal theory. Smart contracts introduce a new paradigm of structuring, implementing, and enforcing contracts by incorporating contractual logic into blockchain-based systems and replacing the trust-based structure with the code-based and consensus-driven frameworks.

Smart Contracts in Blockchain Structure

Smart contracts have been accepted as a fundamental innovation in the blockchain design that provides automation, operational efficiency, and confidence in the performance of contractual agreements in various sectors of the industry.

[9] National Institute of Standards and Technology (NIST), Digital Signature Standard (FIPS PUB 186-4) (2013)
[10] Chainlink Labs, *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks (Whitepaper)* (2021)

Within the real-world setting, one may consider smart contracts as the backbone of distributed ledger systems to store and update important records. As an example, title documents of property, corporate governance documents, compliance filings, and any other legal documents can be coded and stored on a blockchain, and as such, a transparent, auditable, and tamper-proof record of ownership and status is generated. These records can be automatically updated with event-related responses including the transfer of ownership or the satisfaction of regulatory requirements with the help of smart contract logic, thus making sure that the records remain up-to-date and verifiable with no human assistance.

The legal profession, specifically, will be benefited by the introduction of smart contracts into the working processes. Traditional legal procedures tend to be resource-based and prone to delays associated with processing of documents, resolution of disputes and enforcing a contract agreement. Most of these activities, e.g. escrow, the completion of compliance steps or corporate governance activities, can be executed automatically by smart contracts, boosting efficiency and reducing the risk of a human error/dispute.

To conclude, smart contracts are an essential element of the modern blockchain architecture that offers automation, security, and trust in the implementation of contracts without intermediaries. Their relevance to the legal and government affairs promises great efficiency and transparency significantly in areas like property documentation, compliance tracking and corporate governance. With the ongoing development of blockchain systems and the adjustment of legal frameworks, smart contracts will take one of the leading positions in the digital transformation of the legal and business infrastructure.

Empirical Evidence and Overview

Smart contracts have evolved into an important digital infrastructure, as it is evidenced by the empirical literature on smart contracts. According to the reports of blockchain analytics in 2022-2024, the deployment of smart contracts on the platforms like Ethereum is in charge of with Total Value Locked (TVL) fluctuating between approximately USD 40 billion and USD 180 billion during 2022–2024.[11] The rise of decentralised applications and automated financial protocols which are growing exponentially is evidence of ubiquitous use in financial and business spheres. Such empirical trend defines the economic validity of smart contract

[11] *DefiLlama*, Total Value Locked (TVL), https://defillama.com (last visited Mar. 2, 2026)

ecosystems and enforces the thesis to introduce their doctrinal legitimacy into the modern justice system.

Security vulnerability audits are an important empirical aspect. Academic studies by Atzei Nicola and Luu Loi and later formal verification findings indicate that there are similar technical shortcomings in deployed smart contracts.[12] These are re-entrancy attacks, uncontrolled external calls, logical programming errors and oracle manipulation. Such vulnerabilities have cost various popular decentralised finance events including losses exceeding USD 3.8 billion in 2022 alone, with individual exploits such as the Ronin Network breach surpassing USD 600 million.[13] The fact that they still contain such defects proves that cryptographic security is not enough without good coding standards and independent audits. Policymaking-wise, the results are in favour of the proposal of mandatory code verification, standardised programming protocols, and regulatory supervision mechanisms.

Judicial recognition and enforceability are still on a transitory stage. According to comparative legal studies, such as the reports of the Law Commission (UK) and the discussion in UNCITRAL, although some jurisdictions have stated that smart contracts may have legal enforceability, there is little case law directly dealing with code-based agreements, as autonomous contractual instruments.[14] This demonstrates a lack of doctrine and justifies the necessity of a technology-neutral statutory reformation capable of incorporating automated contractual performance into the conventional legal doctrine.

On the issue of electronic signatures and the admissibility of evidence under the Information Technology Act 2000 and the Indian Evidence Act 1872, empirical research on blockchain hashes and cryptographic signatures has shown that they can be handled like electronic records. The Supreme Court in Anvar P.V. v P.K. Basheer[15] and later in Arjun Panditrao Khotkar[16] reaffirmed that electronic evidence is admissible only upon compliance with Section 65B certification requirements. Their admissibility is however frequently reliant on expert

[12] Nicola Atzei, Massimo Bartoletti & Tiziana Cimoli, A Survey of Attacks on Ethereum Smart Contracts (SoK), in *Principles of Security and Trust* 164 (2017); Loi Luu et al., Making Smart Contracts Smarter, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* 254 (2016)

[13] See e.g., *Chainalysis*, *The 2023 Crypto Crime Report* (2023), reporting approximately USD 3.8 billion lost to crypto-related hacks in 2022; see also reporting on the Ronin Network exploit (USD 600+ million loss, 2022)

[14] Law Comm'n of Eng. & Wales, *Smart Legal Contracts: Advice to Government*, Law Com No. 398 (2021)

[15] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India)

[16] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India)

testimony because the distributed ledger system is often too technical to be easily understood. The non-existence of the common standards of evidence reveals the need to harmonise judicial principles of blockchain-based contractual evidence.

Lastly, network performance research finds scalability and infrastructural limitations. Fluctuating gas fees (average gas fees ranging from below 20 gwei in low-traffic periods to peaks above 300 gwei during network congestion[17]) and congestion of public blockchains pose a higher cost of execution and finalizing transactions. These drawbacks show that commercial implementation at large scale relies on developments in technology, especially the use of Layer-2 scaling.

Overall, empirical evidence supports the fact that smart contracts can yield substantial efficiency and economic benefits and at the same time create security risks, evidentiary complexities, lack of jurisdiction and scalability issues, which require co-ordinated legal and regulatory change.

Legal Implications and Framework

Smart contracts, computerised contracts with blockchain networks, are very challenging to the common legal construct and provide a range of implications to enforceability, liability, and regulation. Unlike other contracts which are written in natural language, smart contracts are run by fixed code that initiates actions once specific conditions established are met. These agreements are quite technical, which makes it more challenging to identify and handle them in or outside legal frameworks across the globe, with the current laws often preceding blockchain technology and having no particular clause to address the code-based contracts.

In order to deem a contract legally binding[18], it should meet such fundamental requirements as the offer, acceptance, consideration, mutual consent, and the intent to enter into legal relations. Although it is possible that smart contracts are formally able to meet these aspects, since code execution is generally automated and opaque, these concepts might become blurred in reality, creating uncertainties in judicial interpretation of whether or how such arrangements and arrangements qualify to be valid binding contracts. Indian jurisprudence, read with Sections

[17] See historical gas fee data from *Etherscan*, Ethereum Gas Tracker (2021–2024), showing average gas prices ranging from under 20 gwei to peaks exceeding 300 gwei during network congestion periods

[18] Restatement (Second) of Contracts §§ 7, 17 (Am. L. Inst. 1981)

10[19] and 13[20] of the *Indian Contract Act, 1872* and the *Information Technology Act, 2000*[21], and affirmed in *Trimex International FZE Ltd v. Vedanta Aluminium Ltd*[22] and *Shakti Bhog Foods Ltd v. Kola Shipping Ltd*[23], recognises that electronic communications can constitute legally binding contracts where essential elements are satisfied.

Enforcement problems are also enhanced by the complexity of jurisdiction. Since smart contracts are executed on decentralised networks available on national borders, it is difficult to determine in which jurisdiction and at which court of law a dispute resolution will take place. Conventional contracts habitually define the law and jurisdiction to apply, but smart contracts frequently do not contain this, creating uncertainty where the parties operate across different legal systems. Further, in support of the same, the case *Tulip Trading Ltd. V. Bitcoin Association*[24], discusses duties of blockchain developers and the jurisdictional implications of decentralised systems.

Another legal threat is one, of evidence and digital signatures. Though the cryptographic hash used as the signature of a smart contract is recognised as an electronic contract and digital record under many legal regimes[25] (the Information Technology Act and the Evidence Act among others), the hashes are not immediately compatible with the legal definition of the valid digital signature, which could lead to the inadmissibility of such contracts in the court (without expert testimony).

Furthermore, the fact that smart contracts are immutable by default (which is an asset of transparency but a liability of flexibility) means that in case a bug or a vulnerability is introduced into the code, this code cannot be easily corrected after it has been deployed. This situation leads to the liability issues: in case a smart contract does something wrong because of the mistakes in its code, it is not always clear who should be held liable -whether it should be the developer of the contract, the deployer, or the participants of the network.

[19] Indian Contract Act, 1872, § 10, No. 9, Acts of Parliament, 1872 (India)
[20] Id. § 13
[21] Information Technology Act, 2000, §§ 4, 10-A, No. 21, Acts of Parliament, 2000 (India)
[22] Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 S.C.C. 1 (India)
[23] Shakti Bhog Foods Ltd. v. Kola Shipping Ltd., (2009) 2 S.C.C. 134 (India)
[24] *Tulip Trading Ltd. v. Bitcoin Ass'n for BSV*, [2023] EWCA (Civ) 83 (Eng. & Wales)
[25] Information Technology Act, 2000; Indian Evidence Act, 1872 §§ 65A–65B; UNCITRAL Model Law on Electronic Commerce (1996)

There is a growing tendency of regulators to resolve these issues, but the current law system is still disjointed. Digital contract law harmonisation, explanation of digital signature standardisation, and tailored dispute resolution mechanisms are also required to ensure full integration of the smart contracts into the rule of law.

The current research and the wider scholarly investigation highlight a pressing necessity to devise certain statutory frameworks, technology-neutral contract recognition, specific standards of digital signature and hybrid dispute resolutions that combine legal regulation with automated action and thus bridge the gap between code and law.

Institutional Benefits

- **Robotization and Autonomous-ness**

  Smart contracts are automated to run when specified conditions are met. This will do away with the aspect of manual supervision as well as mechanical adherence to contractual terms.
- **Speed and Real Time Settlement**

  Smart contracts can provide the immediate performance of a contract and payment in case the conditions of the contract are met. This real-time performance enhances liquidity, speeds up business process and lowers counterparty risk especially in the cross-border trade where the conventional settlement systems are time consuming.
- **Enhanced Security**

  Smart contracts are encrypted cryptographically and distributed ledger technology, which is very difficult to fight, hack, and unauthorised interruption. The decentralisation of data also lowers the vulnerability to a single point of failure and increases the level of security overall.
- **Immutability and Contractual Certainty**

  After being placed on a blockchain, a smart contract may not be changed unilaterally. This non-revocation upholds the sanctity of the agreement, retrospective modification is barred, and the term of a contract is performed in the very manner it was entered into.
- **Transparency and Trust**

  The history of contract and transaction logic are visible to all the authorised participants on a common ledger. Every transaction is time-stamped and verifiable, and this reduces information asymmetry and builds mutual trust between the parties even in the absence of a previous commercial relationship. The above thus also consists of reduction in disputes.

- **Reliable Digital Evidence**

  Blockchain has an unchanging, time-stamped, and immutable record of all transactions. This establishes a firm evidentiary trail which can be applied in resolving disputes and meeting regulatory requirements enhancing accountability and audit effectiveness.

- **Borderless and Decentralised Operation**

  Smart contracts also run on international decentralised networks which are not territorially specific. This renders them very apt in global trade, transfer of digital assets, and global supply chains.

- **Efficient Accounting and Auditability**

  All operations that have been conducted within a smart contract are indelibly stored in the blockchain to provide an audit trail. This makes it easy to comply with the regulations, financial reporting and monitoring performance besides minimizing the chances of document loss or manipulation.

Regulatory Constraints and Enforcement Challenges

- **Uncertain Legal Status**

  Smart contracts are coded as opposed to natural language, and so they present ambiguity concerning their status in classic contract law. There is no extensive statutory regime or body that expressly regulates smart contracts in most jurisdictions, including emerging legal regimes, calling into question the enforceability of the latter.

- **Jurisdictional and Conflict-of-Laws Problems**

  The smart contracts are run on decentralised blockchain networks including nodes spread all over the world, which complicates the identification of the law to be applied, the court and the forum to use to resolve the dispute.

- **Coding Errors and Software vulnerability**

  Smart contracts can be as trustworthy as the code that they are based on. Unintended execution and huge economic losses can be caused by bugs and logical bugs in programming, as well as security holes. Being automatic, it can be said that there is no possibility to stop the performance when the triggering conditions are fulfilled even when the result is obviously unfair.

- **Oracle Dependency**

  A large portion of smart contracts use external data providers (oracles) to determine whether something has happened in the real world (e.g. delivery of goods, weather, or market price). In case the oracle gives incorrect, slow, or manipulated information, then the smart contract will be executed wrongly. Such dependence brings centralised failure to a decentralised system.

- **Absence of Human Understanding and Fair Solutions**

  Under the traditional contracts, the courts are able to interpret the terms under the circumstances of equity, fairness and commercial intent. Smart contracts are also executed without judicial discretion by strict adherence to coded logic and do not allow good faith considerations, hardship, and equitable remedies when unjust conduct underlies the contract.

- **Proficiency and Knowledge Difficulty**

  In addition to the knowledge of the law, drafting, audit, and interpreting smart contracts require expertise in the programming languages. This presents a hurdle to legal professionals, and a dependency on technical professionals.

- **Cyber Attacks and Security Risks**

  Despite its overall security, smart contracts are prone to the methodology of hacking, including re-entrancy attacks, overflow bugs, and denial-of-service attacks. As blockchain transactions are irreversible the lost assets are incredibly hard to retrieve.

- **Scalability and Limitations of Performance**

  The blockchain networks are usually limited in speed, storage and energy usage. The congestion of the network may contribute to the execution delays, etc., which negatively impacts the effectiveness of smart contracts in large-scale commercial activities.

- **Compliance and Regulatory Issues**

  Smart contract can clash with the current laws in consumer protection, data privacy, taxation, and financial regulation. The pseudonymous identity of blockchain transactions also casts doubt on the anti-money laundering and know-your-customer compliance.

Ethical and Regulatory Considerations

The integration of smart contracts in business and legal processes creates a deep ethical and regulatory repercussion which cuts across technical efficacy.

One of the major issues is the lack of human control and ethical judgement. Smart contracts are enforced by a pre-written programme, thus providing little flexibility in user interpretation or fair modulation. Automated execution in a situation where there was error, a coercive act, undue influence or where there was an asymmetrical bargaining power, may produce technically accurate but substantively unjust results. The absence of discretionary examination goes against the basic tenets of fairness that form part of the contract law.

The problem of accountability and liability is closely related. The decentralised character of blockchain makes responsibility challenging to assign in the case where programming defects, vulnerabilities or systemic failures culminate in the loss of finances. The question of whether the programmer, deployer, platform operator, or network participants have the liability is also a serious regulatory issue that requires more precise doctrinal guidelines.

The conflict between privacy and transparency adds to the complexity of ethics.[26] The enforcement of the immutability of blockchain increases trust and auditability but the irreversible nature of transactional data could violate data protection principles, such as data minimisation and the right to erasure. It is thus important to establish a balance between openness and informational autonomy.

Furthermore, smart contracts are not universally recognised and enforced across the jurisdictions. Issues of legal standing of code as a binding agreement, evidence of consent and applicability of traditional doctrine of fraud or frustration to automated environments remain a subject of questions.

These issues are magnified by jurisdictional uncertainty, since decentralised networks do not respect territorial limits, hence complicating conflict-of-law examination and dispute-resolution procedures.

Regulatory wise, the most important produces are financial and consumer protection. Pseudonymous transactions are also a threat to anti-money- laundering (AML) and know-your-customer (KYC) regulations, and consumers can be prone to abuse since they cannot easily

[26] Regulation (EU) 2016/679 (General Data Protection Regulation)

track transparency behind the pseudonymous codebase or file a complaint.[27]

All of these ethical and regulatory miscellanies underscore the point that technological independence should not be made independent of accountability, equity or the rule of law.

Suggestions and policy recommendations

To deal with the structural and ethical issues of smart contracts, the regulation should go beyond recognition and focus on innovative approaches to governance that are specific to code-based contracts.

In the first place, the paper suggests an idea of a dual-layer contractual architecture as a fundamental change. Based on this model, smart contracts must consist of an executable code (performance layer) and a legally binding natural-language agreement (interpretative layer). This will guarantee that the equitable principles like mistake, coercion, or frustration will not be eradicated through automated execution thus maintaining judicial control without sacrificing efficiency.

Second, a graded liability structure has to be implemented. Instead of a blanket attribution model, the allocation of liabilities should be based on functional control, i.e. a distinction between code developers (design responsibility), deployers (implementation responsibility) and platform operators (infrastructure responsibility). Such functional dispensation would offer doctrinal certainty in decentralised systems.

Third, the paper suggests that high-impact smart contracts that are used in finance market and consumer markets should be subjected to mandatory audits of algorithms and fairness tests. In addition to technical security audits, discriminatory results of coded logic, which are now under-regulated, should also be measured by independent bias assessment.

Fourth, smart contracts must include on-board governance safeguards, such as emergency pause call, upgrading protocols and pre-programmed arbitration conditions. This provides regulated flexibility to otherwise fixed systems, resolve blockchain inflexibility with legal

[27] Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2023)

flexibility.

Fifth, regulators must embrace a privacy-anonymous compliance interface whereby they will promote encrypted levels, storing of personal data off-chain, zero-knowledge verification protocols, as a means of striking balance between transparency and data protection standards. And lastly, to eliminate cross-border enforcement challenges and the jurisdictional uncertainty, international collaboration in the form of model laws and harmonised evidentiary standards is crucial.

Taken together, these suggestions go beyond the customary regulatory adaptation and presents a prospective framework which incorporates technological freedom with legal responsiveness, equity and institutional legitimacy.

Conclusion

Smart contracts represent a shift in designing contractual relations, moving the trust to the institutional enforcement mode to a cryptographic verification and decentralised consensus. They provide cost reduction, unprecedented efficiency, security, transparency and substantial efficiencies in commercial ecosystems across the board by integrating contractual obligations into executable code. The fact that they are integrable into blockchain infrastructures shows that they can simplify property transactions, compliance processes, financial settlements, and corporate governance processes.

Nevertheless, this technological breakthrough also reveals structural strains in the presence of sets of laws. Enforcing the question, the question of jurisdiction, the question of evidentiary admissibility, and the question of the division of liability all demonstrate the incompetence of traditional legal dogmas at the front of autonomous, immutable, and borderless code-based agreements. The inflexibility of blockchain systems poses a challenge to some core concepts of rescission, rectification, frustration, and equitable relief. Additionally, there are weaknesses in coding and oracle stability and cybersecurity that point to a necessity of technical standardisation and obligatory auditing frameworks. The ethical factor of fairness, consumer protection, algorithmic bias, privacy rights and regulatory compliance further highlights the fact that automation cannot surpass normative judgement.

This means that the future of smart contracts is not technologic absolutism, but controlled integration. Technology-neutral awareness of digital contracts, standardised cross-border frameworks, hybrid dispute resolution systems, and institutional regulation should change the legal systems without stifling innovation. Finally, smart contracts must be considered as auxiliary tools that help in improving the performance of the contract and at the same time, they are tied to the principles of the contract law. They are not meant to replace law institutions, but to change the manner in which law is to operate in an economy that is becoming more digital and decentralised.

References

1. **Books**
   - Smart Contract: Building blocks of Digital Markets (1996) Nick Szabo
   - Chris Dannen, Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming (Apress 2017)
   - Imran Bashir, Mastering Blockchain (3rd edn, Packt 2020)

2. **Journal Articles**
   - Max Raskin, The Law and Legality of Smart Contracts (2017) 1 Georgetown Law Technology Review 305
   - Werbach Kevin and Cornell Nicolas, Contracts Ex Machina (2017) 67 Duke Law Journal 313
   - Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation and Governance 505
   - Atzei Nicola, Bartoletti Massimo and Cimoli Tiziana, A Survey of Attacks on Ethereum Smart Contracts (2017)
   - Luu Loi et al., Making Smart Contracts Smarter (2016) ACM CCS

3. **Reports and Policy Documents**
   - Smart Legal Contracts: Government Advice by UK Law Commission (2021)
   - Blockchain and Smart Contracts in the EU Legal Framework (2020) European Parliament
   - UNCITRAL, Legal Frameworks of Electronic Commerce and Digital Trade

4. Statutes (India)

- Indian Contract Act 1872
- Information Technology Act 2000
- Indian Evidence Act 1872

5. Technical and Industry Sources

- Vitalik Buterin (2014), Ethereum White Paper
- Chainlink, Decentralised Oracle Network Whitepaper