The Legal Gazette
OPEN SCHOLARSHIP
www.thelegalgazette.org

Smart Contracts Beyond ‘Code Is Law’: Formation, Attribution, Remedies and Cross-Border Recognition

Yuvraj

Academic article · Published 6 November 2026 · Publication version 1 · OSCOLA edition 4

Article citation: Yuvraj, “Smart Contracts Beyond ‘Code Is Law’: Formation, Attribution, Remedies and Cross-Border Recognition”, The Legal Gazette — Open Scholarship (2026-11-06), version 1, https://www.thelegalgazette.org/scholarship/41a8a48f-608e-406d-9c12-12c22a05d68a.

Downloaded: 6 November 2026 at 14:32 IST (2026-11-06T09:02:49.225Z)

Abstract

Automated performance does not, by itself, make computer code an enforceable contract. This article asks when blockchain-based arrangements satisfy ordinary rules of contractual formation and how legal systems should allocate responsibility when code executes unexpectedly across borders. Using doctrinal and comparative analysis of Indian contract and electronic-transactions law, English legal guidance, selected United States approaches, European Union data regulation and UNCITRAL instruments, it argues that the central problem is not whether a blockchain transaction is technically effective but whether identifiable persons assumed legally enforceable obligations and retained meaningful remedies. The UNCITRAL Model Law on Automated Contracting 2024 offers a significant technology-neutral vocabulary for recognition, attribution and unexpected outputs, but is not a substitute for substantive contract, consumer, property, data-protection or private international law. India can address many ordinary smart-contract disputes through existing principles, although formalities, evidentiary integrity, choice of law and irreversible execution require careful drafting and institutional adaptation. The article proposes a layered framework combining a human-readable legal agreement, a verified executable specification, reliable evidence preservation and a workable dispute-and-remedy mechanism.

Keywords: automated contracting; electronic records; contractual consent; blockchain; attribution; private international law; digital evidence; consumer protection.

I. Introduction: the legal question behind automatic execution

A vending machine illustrates the difference between performance and law. Inserting the correct money may cause a machine to dispense a product, but the mechanical event does not determine whether the seller misrepresented the product, whether the buyer was legally capable of contracting, or what happens if the machine dispenses the wrong item. A blockchain smart contract raises the same distinction at a larger scale. Code can transfer a token without asking a court for permission; it cannot conclusively decide whether that transfer was legally owed.

The research question is therefore: under what conditions can smart-contract code create, evidence or perform binding obligations across jurisdictions, and how should law respond when execution diverges from the parties' legally relevant intentions? Three subsidiary questions follow: (1) how can offer, acceptance, intention, capacity and attribution be identified in automated systems; (2) which mandatory rules survive automation; and (3) how should courts and arbitral tribunals resolve errors and cross-border disputes?

The article advances three propositions. First, ‘smart contract’ is a technical description, not an independent legal category: some programs implement legal contracts, some merely automate transfers, and some form part of a broader relationship. Secondly, legal recognition of electronic communication does not mean blanket validation of every algorithmic outcome. Thirdly, legal interoperability requires more than interoperable code; it requires clear allocation of risk, admissible evidence, jurisdictional design and remedies that can operate even after an irreversible transfer.

The method is doctrinal and comparative. Primary texts receive priority over company announcements or general commentary. Comparisons are functional rather than claims that one jurisdiction's rules automatically apply elsewhere. The inquiry concerns private commercial contracting, not a general legal assessment of cryptocurrency markets or the regulatory status of particular tokens.

II. What a smart contract actually does

A. Code, legal agreement and automated performance

The phrase ‘smart contract’ is used for at least three different objects: a program capable of automatically changing a ledger state; a legal agreement expressed partly in executable logic; and an ordinary agreement whose performance is assisted by software. Conflating these objects produces exaggerated claims about enforceability. The Law Commission of England and Wales expressly focuses on smart legal contracts, namely arrangements in which code defines or performs legally binding obligations.[1]

A typical blockchain workflow has an address, a set of coded conditions, an input transaction and a network that records an output. A program may depend on an external ‘oracle’ for exchange rates, delivery status or weather. The oracle is not a source of legal truth: it is a technical pathway through which a claimed fact enters the program. If the oracle reports an incorrect temperature, the program may perform flawlessly and nevertheless generate the wrong commercial outcome.

B. Why immutability is not legal certainty

An append-only ledger can help establish transaction sequence and integrity, but it does not establish the identity, authority, capacity or intention of the person controlling a private key. A

1. Law Commission of England and Wales, Smart Legal Contracts: Advice to Government, 2021-11-25 <https://lawcom.gov.uk/project/smart-contracts/>.

cryptographic signature is evidence of control over a key; its legal significance depends on the applicable signature, evidence and attribution rules. Likewise, an irreversible on-chain payment does not extinguish a claim for restitution, damages or other relief against an identifiable counterparty.

Technical design affects risk allocation. Upgradeable contracts may be modified through governance arrangements; non-upgradeable contracts may be harder to suspend; administrative keys can create concentration of control. Security audits reduce, but do not eliminate, defects. In an academic legal analysis, the existence of a hash, transaction ID or audit certificate must not be treated as proof that a legal obligation was validly formed.

C. Practical examples and their limits

In supply chains, blockchain records can support provenance claims, but the accuracy of an original physical-world entry still depends on trustworthy inspection and documentation. In property transactions, escrow automation does not dispense with registration or conveyancing requirements. In parametric insurance, automated payment on a measured event may improve speed but does not resolve disputes about the data source, exclusions, regulatory authorisation or unfair terms. These examples illustrate potential applications rather than proving their effectiveness across all jurisdictions.

III. Contract formation: translating intention into executable logic

A. The ordinary requirements remain

An enforceable agreement generally requires applicable elements of contract formation, which differ by legal system. In India, the Indian Contract Act 1872 supplies the principal framework for agreement, consent, capacity, lawful consideration and lawful object.[2] The question is not whether a contract is written in Solidity or ordinary English, but whether the relevant persons entered into an enforceable bargain. A token transfer between anonymous addresses may be evidence of conduct; it is not necessarily proof of every element of a legally binding agreement.

In particular, the transaction may involve a unilateral offer, a standing automated acceptance mechanism or performance under an earlier master agreement. A court must identify which communication constituted an offer, when acceptance became effective and whether the automated action was attributable to a party. Treating all code deployment as an offer is too broad; treating every execution as acceptance is equally unreliable.

B. Electronic recognition in India

Sections 4 and 5 of the Information Technology Act 2000 recognise electronic records and electronic signatures within their statutory conditions; section 10A addresses the validity of

2. Indian Contract Act 1872, ss 2, 10–11, 13–19, 23.

contracts formed through electronic means.[3] These provisions counter a formal objection based solely on electronic form. They do not displace substantive contract requirements, nor do they remove statutory exclusions and transaction-specific formalities. In particular, section 10A should not be paraphrased as a legislative declaration that every self-executing blockchain program is an enforceable contract.

A careful Indian analysis must separate: (i) legal recognition of an electronic record; (ii) proof of an electronic signature or authentication method where one is required; (iii) formation and validity under the Contract Act; (iv) compliance with mandatory form and registration rules; and (v) admissibility and weight of digital evidence. This layered approach is more accurate than asking whether 'India recognises smart contracts' as a binary question.

C. Code–text conflicts

Suppose a written supply agreement says payment follows confirmed delivery, but the executable program releases funds on submission of a tracking number. The tracking number arrives even though the goods do not. The code may have done precisely what its developer intended, while the payment may contradict the parties' bargain. A court needs to know whether the text prevails, whether the code is incorporated as a term, and whether the parties knowingly accepted that technical trigger as conclusive.

Parties should specify a hierarchy among the signed text, technical annexes, deployed code and user-interface representations. A contract that merely states 'code is law' cannot reliably preclude claims based on illegality, fraud, mistake or mandatory consumer protections. Where the code is incomprehensible to an ordinary counterparty, disclosure and incorporation issues become particularly acute.

IV. Automated systems, attribution and unexpected outcomes

A. The UNCITRAL framework

The UNCITRAL Model Law on Automated Contracting (MLAC), adopted on 11 July 2024, is a major recent development.[4] It supplies technology-neutral legal recognition rules for automated transactions, including use of computer code and dynamic information, attribution of automated-system outputs and an optional approach to unexpected outputs. It is model legislation, not a treaty automatically binding on every state. Its adoption by UNCITRAL should not be confused with enactment in India or any other jurisdiction.

3. Information Technology Act 2000, ss 4, 5 and 10A; see also First Schedule (statutory exclusions, as applicable).
4. UNCITRAL, Model Law on Automated Contracting (adopted 11 July 2024) and Guide to Enactment <https://uncitral.un.org/en/mlac> accessed 28 October 2026.

The MLAC builds on the UNCITRAL Model Law on Electronic Commerce 1996 and the United Nations Convention on the Use of Electronic Communications in International Contracts 2005.[5] Article 12 of the latter Convention addresses contracts formed through automated message systems without a natural person's review of each individual action; article 14 addresses certain input errors. Those rules matter because the problem of automation predates blockchain. Their relevance must still be qualified by the Convention's scope and applicability to the transaction.

B. Who is responsible for a machine's output?

Attribution is not equivalent to moral blame. If a business deploys an automated purchasing agent with authority to place orders, legal rules may attribute its messages to the business even if a human did not approve every order. But the answer can change where the system was compromised, exceeded delegated authority, or produced an outcome neither party reasonably contemplated. The MLAC addresses attribution and unexpected outputs as discrete questions; it does not simply presume that every output is binding.[6]

The legal system should ask who configured and controlled the system, what was represented to the other party, whether reliance was reasonable, and what risks were contractually allocated. For generative-AI-assisted contracting, unpredictability adds another layer: a system may produce an unanticipated message rather than merely executing a deterministic instruction. It would be mistaken to treat the software as a separate legal person without a recognised basis in law.

C. Mistake, exploitation and security failures

Consider a pricing bug that offers a high-value digital asset for a negligible sum. Three issues are distinct: whether the displayed price was an offer; whether the counterparty knew or ought to have known of the error; and whether a completed transfer is legally recoverable. Applicable mistake doctrines differ, and code execution alone answers none of them. Similarly, a malicious exploit may involve unauthorised conduct rather than a legitimate exercise of contractual rights. The 2016 DAO incident, discussed in the original manuscript, illustrates governance and technical vulnerability; it is not itself a judicial precedent deciding the law of mistake or restitution.

V. Comparative legal approaches

5. UNCITRAL Model Law on Electronic Commerce (1996); United Nations Convention on the Use of Electronic Communications in International Contracts (adopted 23 November 2005, entered into force 1 March 2013) arts 8, 12 and 14 <https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications> accessed 28 October 2026.
6. UNCITRAL, Model Law on Automated Contracting (adopted 11 July 2024) and Guide to Enactment <https://uncitral.un.org/en/mlac> accessed 28 October 2026.

A. England and Wales: adapting ordinary law

The Law Commission's 2021 advice concluded that the existing law of England and Wales can generally accommodate smart legal contracts, while identifying difficult questions concerning deeds and private international law.[7] This is a nuanced position: it does not declare every program binding, but finds ordinary principles sufficiently flexible for many arrangements. Formation, interpretation, vitiating factors and remedies remain relevant. The Commission's advice is influential analysis, not legislation or a court judgment.

This approach has a practical advantage: it avoids an unnecessarily narrow statutory definition tied to a particular blockchain architecture. Its limitation is that litigation can be expensive when parties must establish code meaning, identity and governing law through technical experts.

B. United States: recognition does not eliminate substantive rules

The original manuscript describes Arizona, Nevada and Wyoming measures. Arizona's legislation expressly addresses blockchain-secured electronic records and smart-contract terms; Nevada adopted provisions concerning blockchain records; Wyoming's digital-asset legislation addresses additional property and commercial-law questions.[8] These examples show targeted legal recognition, but state statutes differ in wording, scope and interaction with federal and uniform commercial law. None supports the sweeping proposition that a coded transfer is enforceable regardless of fraud, capacity, consumer law or conflicting mandatory rules.

For cross-border parties, the key lesson is that statutory validation of a record's electronic form and the enforceability of the underlying bargain are separate issues. A choice-of-law clause may reduce uncertainty but cannot necessarily defeat overriding mandatory protections.

C. European Union: functional regulation of particular uses

The EU Data Act, Regulation (EU) 2023/2854, entered into force in January 2024 and generally began applying in September 2025.[9] Article 36 addresses essential requirements for smart contracts used in executing agreements to make data available, including robustness, access control and mechanisms for safe termination or interruption.[10] It does not amount to a general EU law declaring all smart contracts valid or requiring all blockchain code to contain a universal kill switch. Its subject matter and applicable dates must be read closely.

---

7. Law Commission, Smart Legal Contracts: Advice to Government (Law Com, 2021) <https://lawcom.gov.uk/project/smart-contracts/> accessed 28 October 2026.
8. Ariz Rev Stat § 44-7061; Nevada Senate Bill 398 (2017); Wyoming digital-asset legislation (2019). Editorial verification: verify currently consolidated state provisions and any subsequent amendments before journal submission.
9. Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data [2023] OJ L 2023/2854, arts 50 and 56 <https://eur-lex.europa.eu/eli/reg/2023/2854/oj> accessed 28 October 2026.
10. *ibid* art 36. Editorial verification: confirm the provision-specific transitional application rules against the consolidated EUR-Lex text before publication.

Data-protection law poses a distinct problem. The GDPR's principles of data minimisation and storage limitation, together with rights such as erasure, can be difficult to reconcile with permanent public storage of personal data.[11] Yet the existence of a blockchain does not automatically mean every on-chain item is personal data, nor does the right to erasure apply without exceptions. The better design response is to avoid putting identifiable personal information on-chain where possible, keep sensitive data in controlled off-chain systems and conduct a context-specific compliance assessment.

D. China: evidentiary recognition is not contract validation

The original article invokes the Hangzhou Internet Court's acceptance of blockchain-supported evidence and subsequent Chinese internet-court rules. These developments concern evidentiary authenticity and judicial process. They do not, without more, prove that every blockchain arrangement is substantively enforceable. A revised comparative analysis should verify the official Chinese-language instruments and distinguish court admissibility, contractual validity, cryptocurrency restrictions and sectoral blockchain deployment before making broader claims.

E. Comparative synthesis

The jurisdictions do not occupy a simple spectrum from ‘recognition’ to ‘prohibition’. England and Wales emphasise the adaptability of ordinary contract law; selected US states legislate targeted electronic-recognition rules; the EU regulates specific data-sharing functions and privacy consequences; India relies principally on general contract and electronic-records law; and China has recognised particular evidentiary uses within a different regulatory environment. The decisive question is what exactly is being recognised: code, record, signature, contract, asset, or remedy?

VI. India: enforcement, evidence and formalities

A. Electronic evidence under the current statute

A current Indian manuscript should refer to the Bharatiya Sakshya Adhiniyam 2023 rather than treating the repealed Indian Evidence Act 1872 as the sole contemporary evidence framework. Sections 61–63 address electronic or digital records and proof, including the statutory conditions relevant to electronic-record outputs.[12] A blockchain ledger entry is not self-authenticating for every contested proposition: the party relying on it may need to establish provenance, integrity, device or system details and the evidentiary link between an address and a person. A transaction hash is a useful identifier, not a substitute for compliance with the governing evidence rules.

11. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 5 and 17.
12. Bharatiya Sakshya Adhiniyam 2023, ss 61–63 and sch (certificate) <https://www.indiacode.nic.in/indiacode/bitstream/123456789/20063/1/aa202347.pdf> accessed 28 October 2026.

In a smart-contract dispute, relevant material may include the deployed bytecode, source-code repository, audit trail, compiler version, transaction logs, oracle feeds, user-interface screens, off-chain messages and key-custody arrangements. Evidence preservation should begin before a dispute, because interfaces and off-chain data can change while the on-chain transaction remains fixed.

B. Property and other mandatory formalities

Automation cannot independently transfer a class of property where the law requires a registered instrument or another formal act. In India, the Registration Act 1908 and the Transfer of Property Act 1882 may remain material to transactions involving immovable property.[13] It is therefore misleading to describe a blockchain escrow payment as a completed conveyance of legal title. Similar caution applies to regulated financial services, securities and insurance: the code's technical capability does not itself establish regulatory permission.

C. Consumer protection and standard-form code

The hardest cases may involve consumers who never see, much less understand, the executable terms. A consumer may interact with a simplified application while a complex program governs fees, liquidation, termination or dispute resolution. The Consumer Protection Act 2019 and other mandatory rules may be relevant depending on the nature of the transaction and parties.[14] Where the interface promises one outcome and the code produces another, courts should not treat the program as the only relevant representation.

D. Jurisdiction and remedies

An anonymous address does not provide a conventional place of business. The location of validators or distributed nodes is an unstable proxy for the place of contracting. Courts instead need legally relevant connecting factors: identified parties, the agreement's governing law, performance obligations, consumer location and statutory jurisdictional rules. Parties should specify governing law and a realistic forum, while acknowledging that some disputes and statutory protections cannot be contracted away.

Remedies also require careful design. A court may award damages or restitution even where the original on-chain transfer cannot be reversed. An injunction may operate against an identifiable exchange, custodian or contracting party, but its effectiveness depends on jurisdiction and control. Arbitral awards can provide cross-border enforcement possibilities under the New York Convention, subject to its conditions; a clause embedded only in obscure code may raise serious questions of consent and incorporation.[15]

13. Registration Act 1908, s 17; Transfer of Property Act 1882, s 54 (subject to transaction-specific application).
14. Consumer Protection Act 2019, ss 2(6), 2(9) and 2(46) (definitions relevant to complaints, consumer rights and unfair contracts, as applicable).
15. Convention on the Recognition and Enforcement of Foreign Arbitral Awards (adopted 10 June 1958, entered into force 7 June 1959) 330 UNTS 3, arts II–V.

VII. Digital trade and the limits of harmonisation

UNCITRAL's Model Law on Electronic Transferable Records 2017 (MLETR) is relevant to bills of lading, warehouse receipts and other transferable instruments.[16] Its functional-equivalence approach addresses reliable control and integrity of electronic transferable records. It should not be confused with the MLAC: one concerns transferable records, the other automated contracting. Both can support digital trade, but neither removes the need for the underlying substantive law of documents, carriage, finance or secured transactions.

A shipment could involve an electronic bill of lading, a coded release-of-payment condition and a conventional sales agreement. The records may be interoperable at a technical level while the jurisdictions disagree about title, security interests or dispute resolution. A practical harmonisation agenda therefore requires compatible electronic-commerce laws, reliable identification and signatures, recognition of electronic transferable records, and credible procedures for evidence and remedies.

International harmonisation has limits. Consumer protections, data protection, insolvency priorities and public policy are not merely technical obstacles to be eliminated. They express choices about how risks should be distributed. The objective should be predictable legal interaction among systems, not uniformity at the expense of mandatory safeguards.

VIII. A proposed legal-design framework

A. A human-readable agreement

For commercially significant transactions, parties should record identities, authority, obligations, governing law, forum, disclosures and remedies in language that a non-programmer can understand. This is the first Feynman test: can a person explain what will happen, why, and who bears the loss if it goes wrong? If not, a claim of informed contractual consent is weakened.

B. A technical specification linked to the legal agreement

The agreement should identify the code version, deployed address, oracle sources, upgrade powers and precedence rules. Changes to the program should require an agreed governance procedure. Where legal text and executable logic conflict, the document should say which governs and how discrepancies will be resolved.

C. Safety, monitoring and intervention

Developers and contracting parties should assess foreseeable failures, access controls, oracle manipulation, emergency suspension and recovery options. Not every smart contract should be freely alterable, but neither should immutability be romanticised as a substitute for responsible

16. UNCITRAL, Model Law on Electronic Transferable Records (adopted 13 July 2017) arts 10–12 <https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records> accessed 28 October 2026.

design. A risk-based approach can preserve useful automation while making exceptional intervention transparent and accountable.

D. Evidence and auditability

Systems should retain appropriate logs, source-code snapshots, consent records and independent audit evidence. Preservation methods must comply with data-protection duties and should not disclose confidential information unnecessarily. Parties need a credible chain of evidence connecting code, transactions and legally responsible persons.

E. Remedies beyond the chain

Contracts should specify notification of defects, temporary suspension where technically possible, dispute escalation, independent expert determination for technical issues, and judicial or arbitral recourse. A technical 'reversal' may be impossible; monetary and personal remedies must therefore remain available. Any automated dispute mechanism should satisfy procedural fairness, impartiality and applicable law.

IX. Objections and counterarguments

One objection is that requiring legal wrappers undermines the principal benefit of permissionless systems: interaction without intermediaries. That criticism has force for low-value transfers and protocols deliberately designed without identifiable operators. Yet it cannot answer who bears the loss when a consumer is deceived or a business exploits an obvious error. Where no identifiable counterparty exists, enforceability may be practically limited even if a legal cause of action can be articulated. The honest conclusion is that not all decentralised interactions can be made equivalent to conventional bilateral contracts.

A second objection is that code offers greater certainty than ambiguous prose. Deterministic code can indeed reduce disputes about mechanical calculation. But precision in execution is not precision about legal authority, consent, external facts or fairness. A program can deterministically implement an unlawful or mistaken instruction. The most effective solution is to use code for what it does well while retaining legal interpretation for questions code cannot decide.

A third objection is that model laws risk premature standardisation. The MLAC is technology-neutral and designed to complement existing law, which mitigates this concern. Nevertheless, legislative adoption should follow consultation with commercial users, courts, technologists, consumers and data-protection authorities, and should avoid assuming that all automated systems are blockchain-based.

X. Conclusion

The legal future of smart contracts does not depend on declaring that code is law. It depends on recognising that code is one possible medium through which persons communicate, record and

perform obligations. The governing questions remain recognisably legal: who agreed to what, whether consent and authority were valid, which mandatory rules apply, what evidence proves the transaction, and what remedy follows from error or breach.

UNCITRAL's 2024 Model Law provides a useful international foundation for analysing automated transactions, but its value lies in careful domestic implementation alongside existing contract, evidence, consumer and private international law. For India, the most defensible immediate position is neither wholesale rejection nor automatic validation of blockchain smart contracts. It is a transaction-specific inquiry under the Contract Act, Information Technology Act, current evidence legislation and relevant sectoral rules. Cross-border certainty will improve when technical architecture and legal architecture are designed together.

Bibliography / references

Law Commission of England and Wales, Smart Legal Contracts: Advice to Government, 2021-11-25 <https://lawcom.gov.uk/project/smart-contracts/>.

Kevin Werbach and Nicolas Cornell, ‘Contracts Ex Machina’ (2017) 67 Duke Law Journal 313. Pinpoint passages to be checked against journal version.

Max Raskin, ‘The Law and Legality of Smart Contracts’ (2017) 1 Georgetown Law Technology Review 305. Pinpoint passages to be checked against journal version.

Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (Harvard University Press 2018). Specific page references to be verified before citing discrete propositions.

Eliza Mik, ‘Smart Contracts: Terminology, Technical Limitations and Real World Complexity’ (2017) 9 Law, Innovation and Technology 269. Pinpoint passages to be checked against journal version.

Citation formatting: Common case, legislation, book, journal and web templates; jurisdiction-specific abbreviations, special authorities and complex cross-references require editorial checking. Formatting does not verify a source.

Publication rights

Copyright owner: Yuvraj
Publisher: The Legal Gazette
Licence: Creative Commons Attribution-ShareAlike 4.0 — https://creativecommons.org/licenses/by-sa/4.0/

Publication permissions: The author grants The Legal Gazette a non-exclusive, worldwide, royalty-free permission to host, publish, reproduce, distribute, communicate to the public, preserve, archive and make the substantially revised manuscript available in digital and other agreed formats, subject to the terms of the CC BY-SA 4.0 licence and applicable third-party rights. These permissions extend only to rights owned or lawfully controlled by the author.

Exclusivity: Non-exclusive

Additional author consent for academic republication: Contact the author first

Academic reuse is subject to the article licence, applicable rights and any required consent.
www.thelegalgazette.org/academic-reuse

Research declarations

These disclosures are reproduced from the recorded publication version. They are author declarations, not independent verification by TLG.

Funding and sponsor involvement

No external funding. This research was independently undertaken without financial sponsorship, institutional grants or external sponsor involvement.

Competing interests

The author is associated with The Legal Gazette, the intended publisher of this manuscript. No other financial, professional, institutional or personal competing interests are declared.

Author contributions

Yuvraj was solely responsible for conceptualisation, research design, methodology, investigation, collection and analysis of legal materials, comparative legal analysis, drafting, revision and final approval of the manuscript.

Originality and related publications

This manuscript is a substantially revised and updated version of an article previously published in 2025 under the title “Smart Contracts: A Difference in the Legal Set-Up and International Transactions.”

The earlier version has subsequently been withdrawn from public circulation and removed from the platforms on which it was previously available. The present manuscript has undergone substantial revision, restructuring and updating to incorporate developments in automated contracting, electronic-transactions law, evidentiary frameworks, comparative legal approaches and international legal instruments.

This version is submitted as the substantially revised and updated manuscript for publication in The Legal Gazette. The author acknowledges the prior publication and will provide details of the earlier publication upon editorial request. No concurrent submission of this manuscript to another publication is being made.

Methods and legal currency

This article adopts doctrinal and comparative legal research methods. It examines legislation, judicial decisions, official legal guidance, international instruments, model laws and selected academic literature. Primary legal sources are prioritised over secondary commentary. Comparative analysis draws upon India, the United Kingdom, selected United States jurisdictions, the European Union and China. The legal review is current as of 28 October 2026. No interviews, surveys or original empirical data collection were undertaken.

Limitations

The research primarily examines private commercial contracting and the legal enforceability of automated transactions. Comparative jurisdictions are used for analytical purposes and are not treated as legally interchangeable. The article does not provide a comprehensive assessment of cryptocurrency markets, every category of digital asset or all sector-specific regulatory frameworks. Its findings are doctrinal and normative rather than empirical.

Ethics and participant protections

Not applicable. This is a desk-based doctrinal and comparative legal study relying on publicly available legislation, judicial decisions, official legal materials and academic literature. No human participants, interviews, surveys, personal records or animal subjects were involved.

Data and materials availability

The research is based on publicly accessible legislation, judicial decisions, official publications, international instruments and academic literature cited in the manuscript. No original empirical dataset was generated. Third-party publications and legal materials remain subject to their respective copyright, licensing and access conditions.

AI and writing assistance

Generative AI tools were used to assist with language refinement, editorial organisation and writing assistance during manuscript preparation. The author independently reviewed the manuscript and takes full responsibility for its contents, legal analysis, interpretations, conclusions and source accuracy. No AI system is listed as an author.