



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]



Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

“Law in the Age of Artificial Intelligence: A Fundamental Perspective”

Organised by KES’ Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: <https://doi.org/10.70183/lijdlr.2026.v4si1.33>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE

About the College



KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

KANDIVLI EDUCATION SOCIETY

Established 1936



Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

EDUCATIONAL COMMITMENT

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

A Fundamental Perspective



ABOUT THE INTERNATIONAL CONFERENCE

The International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective” provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

PRINCIPAL'S MESSAGE

KES' Shri. Jayantilal H. Patel Law College



It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective.”

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

DR. VIRAL DAVE

I/c. Principal

KES' Shri. Jayantilal H. Patel Law College

ORGANISING COMMITTEE

International Conference on Law in the Age of Artificial Intelligence



I/c. Principal

Dr. Viral Dave

Convenor

Mr. Mahavir Mandot

Co-Convenors

Dr. Shweta Vijendra Pathak

Ms. Priyanka Khakhadia

Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

*Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of
Doctrinal Legal Research [Volume IV, Special Issue I, 2026]*

SMART CONTRACTS AND ARTIFICIAL INTELLIGENCE IN COMMERCIAL LAW: AN ANALYTICAL STUDY OF EMERGING LEGAL CHALLENGES

Apeksha Sunil Raut¹

I. ABSTRACT

Technological advancement has significantly transformed commercial transactions through the emergence of smart contracts, blockchain-based systems, and Artificial Intelligence (AI). Smart contracts operate through self-executing code deployed on blockchain platforms and automatically perform contractual obligations upon the fulfilment of pre-determined conditions. AI, on the other hand, enhances commercial activity through predictive analysis, automated decision-making, fraud detection, contract management, risk assessment, and data-driven business processes. These technologies have improved speed, transparency, accuracy, and efficiency in commercial dealings. However, their growing use also creates important legal challenges concerning enforceability, consent, liability, jurisdiction, consumer protection, cybersecurity, data privacy, and algorithmic accountability. This paper critically examines the legal implications of smart contracts and AI in commercial law with special reference to India and selected comparative jurisdictions, including the United States, the European Union, the United Kingdom, and Singapore. It analyses the applicability of the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023 to electronic contracts, digital records, and automated commercial transactions. It also considers recent international and domestic developments, including Regulation (EU) 2024/1689, commonly known as the EU Artificial Intelligence Act, India's AI Governance Guidelines, and the RBI's FREE-AI framework. The paper finds that existing Indian laws provide partial recognition to electronic contracts and digital records but do not comprehensively address decentralised execution, coding errors, autonomous decision-making, algorithmic opacity, or cross-border dispute resolution. It recommends a technology-neutral statutory framework, sector-specific AI governance standards, stronger cybersecurity and data-protection

¹ B.Sc.(Micro), LL.B,LL.M,Ph.D. Scholar, Adv. Ramkrishnaji Rath Law College, Washim, Sant Gadge Baba Amravati University, Maharashtra (India).Email: apekshashardasunilraut@gmail.com

safeguards, and specialised online dispute-resolution mechanisms to ensure legal certainty, accountability, consumer protection, and responsible technological innovation in commercial law.

II. KEYWORDS

Smart Contracts; Artificial Intelligence; Commercial Law; Blockchain; Data Protection.

III. INTRODUCTION

The digital economy has fundamentally transformed the structure of commercial transactions across the world. The integration of blockchain technology and Artificial Intelligence (AI) into business operations has created a new era of automated commerce. Smart contracts and AI systems are increasingly used in banking, insurance, e-commerce, international trade, and financial services to improve efficiency and reduce operational costs. These technologies have altered the traditional understanding of contractual relationships and commercial regulation.

Smart contracts are self-executing agreements coded on blockchain platforms that automatically perform contractual obligations upon the fulfillment of predetermined conditions.² Unlike conventional contracts, smart contracts minimize the need for intermediaries and rely upon decentralized digital systems. Artificial Intelligence refers to computer systems capable of performing tasks that generally require human intelligence, including prediction, analysis, and automated decision-making.³ The combination of AI and blockchain technology has significantly expanded the possibilities of digital commerce.

Despite their advantages, these technologies present serious legal challenges. Existing commercial laws are primarily based on human consent, intention, and accountability. Automated transactions generated through coded instructions and algorithmic systems raise questions concerning enforceability, liability, privacy, jurisdiction, and dispute resolution. In India, there is no comprehensive legislation specifically regulating smart contracts or AI-driven commercial activities. Consequently, legal

² Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 18 EXTROPY 2, 2-3 (1996).

³ STUART RUSSELL & PETER NORVIG, *ARTIFICIAL INTELLIGENCE: A MODERN APPROACH* 1-5 (3d ed. 2010).

uncertainty remains regarding the application of traditional contract law principles to automated transactions.

This paper examines the legal implications of smart contracts and AI in commercial law through doctrinal analysis. It critically evaluates the Indian legal framework, comparative international developments, and the need for regulatory reforms.

A. Research Objectives

The present study is guided by the following research objectives:

1. To examine the concept, nature, and commercial significance of smart contracts and Artificial Intelligence in modern business transactions.
2. To analyse the applicability of the Indian Contract Act, 1872 and the Information Technology Act, 2000 to automated digital agreements and electronic commercial transactions.
3. To evaluate the evidentiary relevance of electronic records and blockchain-generated data under the Bharatiya Sakshya Adhiniyam, 2023.
4. To compare India's legal position with selected international regulatory approaches adopted in the United States, European Union, United Kingdom, and Singapore.
5. To identify gaps in the present Indian legal framework and suggest reforms relating to enforceability, liability, cybersecurity, data protection, jurisdiction, and AI accountability.

B. Research Questions

The present study seeks to answer the following research questions:

1. Whether the existing Indian legal framework, particularly the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023, can adequately accommodate smart contracts and blockchain-based commercial transactions?
2. How can traditional principles of offer, acceptance, consent, consideration, enforceability, and intention to create legal relations be applied to automated digital agreements?

3. What liability framework should apply where loss or harm arises from coding errors, system failures, or AI-driven commercial decision-making?
4. What legal and regulatory reforms are required in India to address jurisdictional uncertainty, cybersecurity risks, data protection concerns, and algorithmic accountability in smart contracts and AI-based commercial systems?

C. Research Methodology

This paper adopts a doctrinal and analytical research methodology. It is based on the examination of primary and secondary legal sources relevant to smart contracts, Artificial Intelligence, and commercial law. The primary sources include statutory provisions, judicial decisions, and regulatory instruments, particularly the Indian Contract Act, 1872, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and selected international regulatory developments relating to blockchain technology and AI governance. The secondary sources include books, journal articles, policy materials, institutional reports, and academic commentary on digital contracts, AI accountability, data protection, and commercial regulation.

The scope of the study is primarily confined to the Indian legal framework, with comparative reference to the United States, European Union, United Kingdom, and Singapore. The study does not undertake empirical fieldwork or technical coding analysis of smart contracts. Its focus is limited to the legal enforceability, regulatory challenges, liability concerns, evidentiary issues, and reform requirements arising from the use of smart contracts and AI in commercial transactions.

IV. CONCEPT AND NATURE OF SMART CONTRACTS

Smart contracts are digital agreements that operate automatically through computer programming. The idea of smart contracts was initially proposed by Nick Szabo. In these contracts, the terms and conditions are written in computer code and stored on blockchain technology. Blockchain is a secure digital system that records transactions permanently across multiple computers, making the system decentralized and reliable.

Once the conditions mentioned in the contract are fulfilled, the smart contract automatically performs the agreed actions without requiring human involvement or intermediaries such as banks or lawyers. This helps save time, reduce costs, and increase efficiency in commercial transactions.

Smart contracts have several important features. They are automated, transparent, secure, and difficult to alter once recorded on the blockchain. All parties can verify the transaction details, which increases trust and accountability. They also provide speed, accuracy, and reliability in commercial activities. Due to these advantages, smart contracts are increasingly used in banking, insurance, e-commerce, and other business sectors.

V. ARTIFICIAL INTELLIGENCE IN COMMERCIAL LAW

Artificial Intelligence (AI) has become an important part of modern commercial activities. Many businesses and commercial enterprises currently utilize AI systems to enhance operational efficiency, minimize costs, and support effective decision-making. AI helps companies in areas such as contract management, fraud detection, customer analysis, and business planning. It can process large amounts of information quickly and accurately, which saves both time and human effort. In comparison with conventional methods, AI systems can process and evaluate commercial data more efficiently while delivering quicker outcomes.

AI is widely used in banking and financial services for online transactions, loan approvals, and fraud prevention. In the insurance sector, AI helps in assessing risks and processing claims. Many companies also use AI-powered customer support systems, such as chatbots, to provide quick responses to consumers. AI is further used in supply chain management to track goods and improve delivery systems. Businesses also rely on AI for predictive analysis to understand market trends and consumer behavior.

In commercial law, AI plays an important role in drafting, reviewing, and executing contracts. AI systems can examine legal documents, identify risks, and monitor compliance with contractual terms. However, the increasing use of AI also raises

concerns regarding transparency, accountability, and the fairness of automated decision-making systems.

VI. LEGAL VALIDITY OF SMART CONTRACTS

Traditional contract law is based on certain essential elements such as offer, acceptance, lawful consideration, free consent, and an intention to create legal relations. Smart contracts try to fulfill these legal requirements through electronic and digital methods. In smart contracts, acceptance usually takes place through blockchain verification and coded digital consent instead of physical signatures or written agreements. The terms and conditions of the contract are written in computer code, and the contract automatically performs its functions when the required conditions are fulfilled.

However, the use of smart contracts creates several legal concerns. One major issue is whether all parties properly understand the technical programming language used in these contracts. Many people may agree to the contract without fully understanding how the coded system works. This creates doubts regarding genuine consent and awareness.

Another important concern relates to enforceability. Although smart contracts may technically execute contractual obligations, their legal validity is still uncertain in many countries. Problems such as coding mistakes, software defects, hacking, or system failures may cause incorrect or unintended execution of the contract. In addition, smart contracts are usually irreversible once executed on the blockchain. Therefore, modifying or canceling the contract becomes difficult even in situations involving fraud, mistake, or unfair conduct.

VII. INDIAN LEGAL FRAMEWORK

India does not yet have a binding and comprehensive statute specifically regulating smart contracts or AI-driven commercial transactions. However, the Indian regulatory landscape can no longer be described as a complete vacuum. Existing statutes such as the Indian Contract Act, 1872, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023 provide partial legal support for electronic contracts, digital records, electronic evidence, and

personal-data processing. In addition, recent AI-governance developments indicate that India is gradually moving from general digital regulation toward a more structured AI policy framework. Therefore, the need for comprehensive legislation should be understood as a requirement to build upon and convert the emerging soft-law and sectoral framework into clearer binding legal standards.

1. **Indian Contract Act, 1872:** The Indian Contract Act, 1872 lays down the essential elements of a valid contract, including offer, acceptance, free consent, lawful consideration, and intention to create legal relations. Although the Act was enacted before the development of digital technology, its provisions can still apply to electronic contracts and smart contracts if all the necessary legal requirements are fulfilled.
2. **Information Technology Act, 2000:** The Information Technology Act, 2000 provides legal recognition to electronic records and digital signatures. Sections 4 and 10A of the Act recognize electronic contracts and digital communication, which indirectly supports the validity and enforceability of smart contracts in India. The Act plays an important role in regulating electronic commerce and online transactions.
3. **Bharatiya Sakshya Adhiniyam, 2023:** The discussion on electronic evidence requires statutory updating because the Indian Evidence Act, 1872 has been replaced by the Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024. Under the new framework, electronic and digital records are expressly recognised as documents, and their contents may be proved in accordance with Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. Section 63 substantially retains the evidentiary logic of the former Sections 65A and 65B of the Indian Evidence Act, 1872 by requiring satisfaction of statutory conditions before electronic records can be admitted without production of the original. However, the new provision is more technologically updated in its language, as it refers not only to computers but also to communication devices, computer systems, computer networks, computer resources, intermediaries, and electronic or digital forms of storage. It also requires a certificate to accompany the electronic record whenever such record is submitted for

admission. This certification requirement is particularly important for blockchain-generated records and smart-contract logs, because the party relying on such evidence must identify the electronic record, describe the manner of its production, provide particulars of the device or system involved, and address the integrity and reliability of the record. Thus, while blockchain records may support evidentiary reliability because of their immutability and traceability, their admissibility in Indian courts will still depend upon compliance with the requirements of the Bharatiya Sakshya Adhiniyam, 2023.

4. **Judicial Developments:** Indian courts have also recognized the validity of electronic agreements. In *Trimex International FZE Ltd. Dubai v. Vedanta Aluminum Ltd.*, the Supreme Court held that contracts formed through electronic communication are legally enforceable if the intention to create contractual relations is clearly established. However, Indian law specifically dealing with blockchain-based smart contracts and AI systems is still in the developmental stage.

VIII. INTERNATIONAL PERSPECTIVE

A. United States

The United States follows a technology-neutral and state-driven approach toward smart contracts and blockchain transactions. Several states, including Arizona and Tennessee, have expressly recognised blockchain records, electronic signatures, and smart contracts within their statutory frameworks. This approach supports commercial innovation by clarifying that contracts are not invalid merely because they are created, stored, or executed through blockchain technology. However, the American model remains fragmented because recognition differs from state to state. In commercial practice, this creates uncertainty in cross-border and inter-state digital transactions, particularly where questions of applicable law, consumer protection, and liability for coding errors arise.

B. European Union

The European Union has adopted a more comprehensive regulatory model, particularly through Regulation (EU) 2024/1689, commonly known as the EU

Artificial Intelligence Act. The EU approach is based on risk classification, transparency, accountability, and regulatory supervision of high-risk AI systems. This model is significant for commercial law because AI systems are increasingly used in credit scoring, insurance, consumer profiling, fraud detection, and automated contract management. The EU framework demonstrates that AI regulation must not be limited to innovation policy; it must also include safeguards against opacity, bias, discrimination, and lack of human oversight.

C. United Kingdom

The United Kingdom has adopted a pragmatic common-law approach by recognising that smart contracts may be capable of legal enforcement under existing principles of English contract law. The UK position is important because it shows that traditional doctrines of offer, acceptance, consideration, and intention to create legal relations can be applied to digital and automated agreements, provided that the legal requirements are satisfied. The UK has also recognised crypto-assets as property in appropriate circumstances, which assists in granting legal remedies in disputes involving blockchain-based transactions and digital assets.

D. Singapore

Singapore has adopted an innovation-friendly regulatory approach toward blockchain technology, digital finance, and AI governance. Its framework emphasises responsible innovation, financial-sector supervision, regulatory sandboxes, and practical governance tools. Singapore's model is relevant for India because it demonstrates how commercial innovation can be encouraged while maintaining regulatory control over financial stability, cybersecurity, consumer protection, and technological risk. A similar balanced approach may assist India in promoting digital commerce without compromising legal certainty and accountability.

IX. LEGAL CHALLENGES IN SMART CONTRACTS AND AI

The increasing use of smart contracts and Artificial Intelligence (AI) in commercial transactions has created many legal and practical challenges. Although these technologies provide speed, efficiency, and automation, they also raise serious

concerns relating to jurisdiction, liability, cybersecurity, privacy, and ethics. Existing legal systems often face difficulties in regulating these advanced digital technologies.

1. **Jurisdictional Problems:** One major challenge in smart contracts is determining the proper jurisdiction and applicable law. Blockchain transactions take place on decentralized digital networks that operate across different countries. Since there is no single physical location for these transactions, it becomes difficult to decide which country's laws will apply in case of a dispute. Cross-border commercial transactions involving smart contracts may create conflicts between different legal systems. Courts may also face difficulties in identifying the appropriate forum for resolving disputes arising from blockchain-based agreements.
2. **Liability and Accountability:** Another important issue is determining liability when errors occur in AI systems or smart contracts. Problems may arise due to faulty coding, software defects, or incorrect decisions made by AI systems. In such situations, it becomes difficult to identify who should be legally responsible. Liability may involve software developers, business operators, platform owners, or users of the technology. Since AI systems can operate automatically without direct human involvement, traditional legal principles relating to accountability may not always provide clear solutions.
3. **Cybersecurity Risks:** Smart contracts and AI systems are also exposed to cybersecurity threats. Hackers may attempt to gain unauthorized access to blockchain networks or digital commercial systems. Cyberattacks, malware, and online fraud may lead to financial losses and misuse of confidential information. Weak security systems can affect trust in digital commerce and create risks for businesses and consumers. Therefore, strong cybersecurity protection is necessary for safe commercial transactions.
4. **Data Privacy Concerns:** AI systems usually process large volumes of personal, financial, behavioural, and commercial data. In India, such processing must now be examined with reference to the Digital Personal Data Protection Act, 2023, which establishes a statutory framework for the protection of digital personal data. The Act is particularly relevant to AI-driven commercial

systems because businesses collecting or using personal data may qualify as “Data Fiduciaries” and must process such data only for lawful purposes, generally on the basis of clear and informed consent or other recognised legal grounds. The consent-based framework requires that individuals, referred to as “Data Principals,” should be informed about the purpose for which their data is collected and should have meaningful control over such processing. The Digital Personal Data Protection Rules, 2025, notified in November 2025, further operationalise this framework by requiring clear consent notices, contact information for data-related queries, and phased compliance obligations for Data Fiduciaries. These requirements are important in AI-based commercial activities such as credit assessment, insurance profiling, targeted advertising, fraud detection, and automated customer evaluation, where personal data may be processed at scale. They are also relevant to smart-contract systems where transaction records, wallet-linked identifiers, or commercially sensitive information may be stored or processed through digital platforms. Accordingly, businesses deploying AI or smart-contract technologies must adopt privacy-by-design practices, data-minimisation standards, secure processing systems, consent-management mechanisms, and grievance-redressal procedures. Failure to maintain proper data protection safeguards may result in misuse of personal data, breach of privacy, commercial confidentiality risks, consumer harm, and regulatory liability. Therefore, data protection must be treated as a central component of legal compliance in AI-driven commercial law.

5. **Ethical Issues:** The use of AI in commercial activities also creates ethical concerns. AI systems may produce unfair or biased decisions if they are trained using inaccurate or discriminatory data. In some cases, automated systems may discriminate against certain individuals or groups. Another major issue is the lack of transparency in AI decision-making. Many AI systems function as “black boxes,” where users cannot fully understand how decisions are made. This lack of explainability affects fairness, accountability, and public trust in AI technologies.

6. Consumer Protection Concerns: The use of smart contracts and Artificial Intelligence in commercial transactions also raises significant consumer-protection concerns. Automated platforms, AI-based recommendation systems, algorithmic pricing, digital standard-form contracts, chatbots, and smart-contract execution mechanisms may affect consumers without meaningful negotiation or human intervention. In such transactions, consumers may not fully understand the coded terms, automated consequences, data-use practices, or dispute-resolution limitations embedded in digital systems. This creates risks of unfair contract terms, misleading representations, wrongful automated decisions, denial of refunds, defective digital services, discriminatory pricing, and difficulty in obtaining remedies after automatic execution. In India, these issues must be examined with reference to the Consumer Protection Act, 2019, which provides remedies against unfair trade practices, misleading advertisements, defective goods, deficiency in services, and product liability. The Act is relevant to AI-driven and smart-contract-based commercial transactions because liability may arise where automated systems cause consumer harm through defective digital services, misleading online interfaces, unsafe products, or unfair commercial practices. Its product-liability framework may also become important where AI-enabled products, digital devices, or automated commercial systems cause loss to consumers due to defects in design, manufacture, service, or instructions. The Act further empowers regulatory intervention against unfair trade practices in e-commerce and direct selling. The Consumer Protection (E-Commerce) Rules, 2020 are also directly relevant because they regulate digital and electronic platforms engaged in online commercial transactions. These Rules impose duties on e-commerce entities, including disclosure obligations, grievance-redressal requirements, refund-related responsibilities, and restrictions against unfair trade practices. They apply not only to entities established in India but also to certain foreign e-commerce entities systematically offering goods or services to consumers in India. This is important for smart-contract and AI-based commerce because digital platforms may operate across jurisdictions while affecting Indian consumers.

Accordingly, businesses deploying AI systems or smart-contract platforms in consumer-facing markets should ensure transparency of terms, clear disclosure of automated decision-making, accessible grievance-redressal mechanisms, fair refund and cancellation processes, and safeguards against algorithmic discrimination. Consumer protection must therefore be treated as an essential component of the legal framework governing smart contracts and AI in commercial law.

X. ANALYTICAL FINDINGS AND SUGGESTIONS

1. **Judicial Recognition in India:** Indian courts have gradually recognized the validity of electronic agreements and digital transactions. Existing laws such as the Information Technology Act, 2000 and the Indian Contract Act, 1872 indirectly support electronic contracts if essential contractual elements are fulfilled. In *Trimex International FZE Ltd. Dubai v. Vedanta Aluminum Ltd.*, the Supreme Court accepted that contracts formed through electronic communication are legally enforceable. This shows that Indian courts are willing to adapt traditional legal principles to technological developments. However, judicial recognition specifically relating to blockchain-based smart contracts and AI-driven transactions is still limited in India.
2. **Challenges in India:** India faces several legal and practical challenges in regulating smart contracts and Artificial Intelligence. One major issue is the absence of a specific legal framework governing blockchain technology and AI-based commercial systems. Existing laws were primarily designed for traditional transactions and may not fully address automated digital agreements. Jurisdictional uncertainty also creates difficulties because blockchain transactions often operate across different countries. Determining liability for coding errors, AI-generated decisions, or system failures remains legally complex. In addition, cybersecurity threats, online fraud, and misuse of personal data create serious concerns regarding consumer protection and privacy. Lack of technical awareness and regulatory infrastructure further affects effective implementation.
3. **Legal Reforms and Recommendations:** The rapid growth of smart contracts, blockchain technology, and Artificial Intelligence (AI) in commercial

transactions has created the need for strong legal and regulatory reforms. Existing laws in India are not fully capable of addressing issues relating to automated contracts, digital liability, cybersecurity, and AI-based decision-making. Therefore, proper legal reforms and policy measures are necessary to ensure safe, transparent, and accountable use of these technologies in commercial activities.

- **Comprehensive Legislation:** India should introduce separate and comprehensive legislation specifically regulating smart contracts, blockchain technology, and AI-driven commercial systems. Clear legal recognition will reduce uncertainty and improve business confidence.
 - **Strong Regulatory Framework:** The government should establish specialized regulatory authorities to supervise AI systems, blockchain platforms, and digital commercial activities. Proper monitoring will help ensure compliance with legal and ethical standards.
 - **Online Dispute Resolution Mechanisms:** Specialized Online Dispute Resolution (ODR) systems should be developed to resolve digital commercial disputes quickly and efficiently. This will reduce delays and litigation costs.
 - **Cybersecurity and Data Protection:** Commercial institutions should adopt strong cybersecurity measures and proper data protection systems to prevent hacking, cyber fraud, and misuse of confidential information.
 - **Ethical and Transparent AI Governance:** AI systems should function in a fair, transparent, and accountable manner. The government should encourage ethical AI practices and ensure that automated decisions do not create discrimination or unfair treatment.
- 4. Strengthening Implementation and Accountability:** Effective implementation requires strong regulatory supervision and accountability mechanisms. India should establish specialized regulatory authorities to monitor AI-based commercial activities and blockchain platforms. Businesses using AI systems should ensure transparency, fairness, and explainability in automated decision-making. Strong cybersecurity systems must be adopted to protect commercial transactions and confidential data from cyberattacks and fraud.

Consumer protection measures should also be strengthened to safeguard individuals from algorithmic discrimination and misuse of digital information. Proper accountability mechanisms for developers, operators, and commercial institutions are necessary to ensure responsible use of emerging technologies in commerce.

XI. CONCLUSION

Smart contracts and Artificial Intelligence (AI) have brought major changes to modern commercial law and business transactions. These technologies help businesses perform transactions more quickly, accurately, and efficiently. Smart contracts reduce the need for intermediaries such as banks, brokers, and agents because contractual obligations can be executed automatically through blockchain technology. Similarly, AI systems assist businesses in decision-making, fraud detection, contract management, and data analysis. As a result, commercial transactions have become faster, more transparent, and cost-effective.

However, the growing use of smart contracts and AI also creates several legal and practical challenges. Traditional contract laws were mainly designed for agreements made and controlled by human beings. Automated digital systems and AI-driven transactions often create uncertainty regarding consent, liability, enforceability, jurisdiction, and dispute resolution. Existing legal frameworks in countries such as India are still developing and are not fully prepared to regulate these advanced technologies effectively.

Issues relating to cybersecurity, data privacy, algorithmic bias, and accountability also require immediate legal attention. Therefore, there is a strong need for comprehensive legislation and proper regulatory mechanisms to govern blockchain technology and AI-based commercial systems. Governments, courts, regulatory authorities, and international organizations should work together to create uniform legal standards and ethical guidelines. Effective regulation will help ensure that technological innovation supports economic growth while maintaining fairness, transparency, consumer protection, and accountability in commercial law.

XII. REFERENCES

A. Books

1. STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (3d Ed. 2010).
2. RICHARD SUSSKIND, TOMORROW'S LAWYERS (2017)
3. KEVIN WERBACH & NICOLAS CORNELL, CONTRACTS EX MACHINA (2017).
4. DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION (2016).

B. Journal Articles

1. Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 18 EXTROPY 2 (1996).
2. Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305 (2017).
3. Harry Surden, Artificial Intelligence and Law: An Overview, 35 GA. ST. U. L. REV. 1305 (2019).

C. Statutes

1. Indian Contract Act, 1872.
2. Information Technology Act, 2000.
3. Indian Evidence Act, 1872
4. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7031.

D. Case Laws

1. Trimex International FZE Ltd. Dubai v. Vedanta Aluminum Ltd., (2010) 3 S.C.C. 1 (India).
2. Shamsher Kataria v. Honda Sael Cars India Ltd., Case No. 03/2011.
3. AA v. Persons Unknown, [2019] EWHC 3556 (Comm).

E. Web References

1. [Reserve Bank of India](#)

2. [Ministry of Electronics and Information Technology](#)
3. [European Commission Digital Strategy](#)
4. [World Economic Forum](#)