# SMART CONTRACTS: THE NEED OF LEGAL IMPLICATIONS IN INDIA

Mitali Aditya Patil, DES Navalmal Firodia Law College[1]

## ABSTRACT

"Code it, Trust it, Seal it: Smart Contracts simplify everything". Smart contracts are automated, self-executing electronic contracts that are maintained on a blockchain and will automatically enforce and carry out the terms and conditions of an agreement when specific criteria are satisfied. Smart contracts have emerged as a key component of the blockchain ecosystem, encouraging innovation across industries by automating agreements and transactions in a safe, transparent, and decentralized manner. Currently, platforms such as Ethereum, Binance Smart Chain, Polkadot, and Cardano host millions of smart contracts, which power decentralized finance (DeFi), non-fungible tokens (NFTs), supply chain solutions, and more. DeFi, in particular, has experienced tremendous growth, with smart contracts allowing for decentralized lending, borrowing, trading, and staking without the use of intermediaries. Despite their popularity, smart contracts confront obstacles such as scalability, security flaws, and a lack of defined legal frameworks. Smart contracts are not explicitly recognized and regulated under the Indian legal framework, leading to their enforceability ambiguity under laws like the Indian Contract Act,1872. The lack of specific regulations governing blockchains affects the validity of smart contracts under Indian law. The incorporation of laws and regulations regarding smart contracts in the Indian legal system efficiently enhances the governance of enforceability and legal validity of smart contracts. With an emphasis on their enforceability under current laws, this research attempts to investigate the legal and regulatory obstacles to smart contract adoption in India. It aims to evaluate sector-specific applications, find gaps in the current legal framework, and suggest changes to bring it into line with emerging technologies. Recommending solutions for consumer protection, legal recognition, and effective dispute resolution while encouraging innovation and compliance is the goal.

**Keywords:** Apps, Automated, Blockchains, Codes, Contracts, programs, Decentralized Finance, Non-fundable Tokens, Smart contracts, Self-executing.

[1] L.L.M Student [DES NFLC]

## 1. INTRODUCTION TO SMART CONTRACTS: BLOCKCHAIN TECH AND AUTOMATION

Smart contracts are an innovative application of blockchain technology and are considered a game-changer in the digital economy. With these contracts in place, transactions are automatically executed and enforced when certain conditions are met. This eliminates the need of an intermediary and minimizes the risk of human errors.[2] At their foundation, these contracts operate on blockchain technology, which provides the infrastructure for smart contracts by storing all transactions in an immutable manner, allowing for trustless interactions. It also ensures that only valid transactions are stored and executed. These contracts operate on decentralized networks, which eliminates the need for intermediaries such as the bank, notary, or lawyer. By using the security and transparency of blockchain, these contracts guarantee trust, automation, and efficiency in transactions across industry verticals.[3] Smart contracts will automatically execute once the conditions are met. Typically, traditional agreements bring a lot of intermediaries, which causes a longer time and much cost and risk. Moreover, there more chances to be cheated, lost or counterfeited with the help of such agreements as they are centralized. The formation and execution of smart contracts involve a systematic process governed by blockchain technology.

First, the terms and conditions of the contract, such as payment conditions, property transfer or completion of the service, are expressed in a code composed in a programming language like Rust (for Solana), or Vyper programming language. This code indicates the rules and procedures conducted by the smart contract. After the creation of this code, the smart contract is loaded into a blockchain network. They cannot be altered, and everyone with access will be able to see them. The execution of the smart contract is triggered when the system recognizes certain conditions. For example, for every e-commerce transaction, the smart contract can release money for the seller if the buyer has confirmed the receipt of the purchased item. Therefore, it is possible to guarantee that the buyer does not receive the item or the seller of the money. After the execution of the transaction, it is immortalized in the blockchain, ensuring auditability of the transactions.

[2] [Primavera De Filippi & Aaron Wright], [*Blockchain and the Law: The Rule of Code],* [45], [Harvard University Press], [2018]

[3] [World Economic Forum], [*The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services* ], [12],
[2016], http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

## 2. LEGITIMACY OF SMART CONTRACTS IN INDIA

These Smart Contracts being a dependable tool yet hinges legal binding on their compliance with the essential elements of a contract defined under the Indian Contract Act, 1872. A contract is considered to be valid only when it satisfies the essential elements of offer, acceptance, consideration, and the intention to create legal relations outlined in Section 10 of the Act.[4] For example, the "offer" and "acceptance" are written in the code and "consideration" is frequently digital currency [crypto currency] or other digital assets. These contracts can satisfy these fundamental requirements, provided that the involved parties have consented to their terms and conditions in a legally recognizable manner. Nevertheless, a valid signature for smart contracts is a difficult task to legally enforce it in India, as prescribed under the Information Technology Act, 2000.[5] While electronic and digital signatures are valid under the Act, it is uncertain whether blockchain-based cryptographic signatures conform with the standards of electronic execution under Indian law. However, the absence of human intervention in the creation and execution of smart contracts raises doubts about whether there is "intention to create legal relations," a subjective element that courts have traditionally considered.[6] It remains unclear whether smart contracts can be deemed as legally binding under Indian law due to this ambiguity.".

Additionally, the judicial enforceability of smart contracts poses certain issues regarding dispute resolution mechanism, jurisdiction, and interpretation of contractual clauses. When it comes to smart contracts, conventional contract remedies like specific performance, injunctions, or damages can be a task to enforce during disputes. Further, it leads to the territorial jurisdiction of Indian courts which may turn out to be a point of conflict in cross-border smart contract transactions, as blockchain technology transcends national borders. While arbitration and other forms of alternative dispute resolution (ADR) could potentially provide remedies, the absence of regulatory certainty on the legal status of smart contracts in India continues to pose a challenge. The Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have issued guidelines on cryptocurrencies and blockchain, but these do not directly address smart contracts.[7] These issues demand for legislative

[4] [Indian Contract Act], [No. 9], [2(h)], [Acts of Parliament], [1872]
[5] [The Information Technology Act], [No. 21], [3A], [India Code] [2000]
[6] [Avtar Singh], [*Law of Contract and Specific Relief],* [45], [Eastern Book Company], [13th ed.], [2020]
[7] [Reserve Bank of India], [*Statement on Developmental and Regulatory Policies],* [2018], https://www.rbi.org.in

clarification to address smart contracts as "contracts" for purposes of Indian law and for establishing a regulatory framework in order to enforce them.[8]

## 3. ENFORCING SMART CONTRACTS: A LEGAL CHALLENGE

One of the most significant challenges in enforcing smart contracts is the ambiguity in dispute resolution. Unlike traditional contracts, which rely on human interpretation and judicial discretion, smart contracts are self-executing and operate based on pre-programmed code.[9] This lack of human intervention makes it difficult to resolve disputes when the outcome of a smart contract is unclear or unintended. For example, if the terms of a smart contract are ambiguous or the code contains errors, courts may struggle to interpret the parties' intentions or modify the contract's outcome. Additionally, the decentralized nature of blockchain technology complicates jurisdictional issues, as it is often unclear which court or legal system has the authority to resolve disputes involving cross-border smart contracts.[10]

Another major challenge is the irreversibility of transactions and the potential for errors in code. Once a smart contract is deployed on a blockchain, it cannot be altered or reversed, even if the outcome is unintended or harmful.[11] This immutability is a core feature of blockchain technology but poses significant risks in cases of coding errors or fraudulent activity. For instance, in 2016, a coding error in the DAO (Decentralized Autonomous Organization) smart contract led to the theft of over $50 million worth of cryptocurrency. Despite the clear unintended outcome, the immutability of the blockchain made it impossible to reverse the transaction without resorting to a controversial "hard fork" of the Ethereum network.[12] Such incidents highlight the challenges of enforcing remedies in cases of errors or fraud, as traditional legal mechanisms like rescission or restitution are difficult to apply to immutable smart contracts.

Determining liability in case of breaches or malfunctions is another significant challenge. Smart contracts involve multiple parties, including developers, users, and platform providers,

[8] [Ministry of Electronics and Information Technology], [*National Strategy on Blockchain],* [12], [2021], https://www.meity.gov.in/writereaddata/files/National_Strategy_on_Blockchain.pdf

[9] [Wright], *Supra* note, 1

[10] [Arvin Abraham], [*Smart Contracts in India: Legal and Regulatory Challenges]*, [12 Indian J.L. & Tech.] [78], [85], [2020]

[11] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 4 (2008), https://bitcoin.org/bitcoin.pdf

[12] [Nathaniel Popper], [*A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency]*, [N.Y. Times] [June 17], [2016], https://www.nytimes.com

each of whom may contribute to errors or failures.[13]

For instance, a developer may write faulty code, a user may input incorrect data, or a platform may experience a technical failure. However, existing laws do not provide clear guidelines on who should be held liable in such scenarios. Should the developer be responsible for coding errors, even if the user agreed to the terms? Should the platform hosting the smart contract bear liability for technical failures?[14] These questions remain unanswered, creating uncertainty for all parties involved and complicating the enforcement of smart contracts.[15] Proving intent and consent in automated systems also presents unique challenges. For a contract to be legally enforceable, parties must demonstrate intent to create legal relations and free consent to the terms of the agreement.[12] However, smart contracts are often written in complex programming languages that may not be easily understood by non-technical users.[13]

As a result, a user may claim that they did not fully comprehend the terms of the contract or that they were unaware of certain conditions encoded in the agreement.[14] For example, a user may unknowingly agree to a smart contract that automatically transfers funds to another party under specific conditions, only to later dispute the transaction.[16] In such cases, courts may struggle to determine whether the user genuinely consented to the terms, especially if the contract's code is not transparent or accessible. This lack of clarity undermines the enforceability of smart contracts and highlights the need for clearer legal standards.

Finally, the enforcement of smart contracts is further complicated by regulatory gaps and technological limitations. For instance, India's Information Technology Act, 2000, does not explicitly address smart contracts or blockchain technology, leaving their legal status uncertain.[17] Similarly, the Indian Evidence Act, 1872, allows electronic records to be used as evidence but does not provide specific guidelines for handling disputes involving smart contracts.[18] On the technological front, the scalability and interoperability of blockchain platforms remain limited, making it difficult to integrate smart contracts into existing legal and business systems.[19] These challenges underscore the need for comprehensive legal and

[13] [Wright], *supra* note 1, [at 102]
[14] [Abraham], *supra* note 9
[15] *Ibid*. [at 93]
[16] Id. [at 104]
[17] [Abraham], *supra note* 9, [at 92]
[18] Id. [At 95]
[19] [World Economic Forum], *Supra* note 2

technological reforms to ensure the effective enforcement of smart contracts.

## 4. INTELLECTUAL PROPOERTY AND SMART CONTRACTS

The code used in smart contracts raises important questions about intellectual property (IP) ownership and protection. Under Indian law, software code is generally protected under the Copyright Act, 1957, which grants the creator exclusive rights to reproduce, distribute, and adapt the work.[20] However, determining ownership of smart contract code can be complex, especially when multiple developers or organizations collaborate on its creation. For instance, if a developer writes code for a smart contract as part of their employment, the employer may own the copyright under the "work made for hire" doctrine.[21]mConversely, if the code is created independently, the developer retains ownership unless explicitly transferred.[22] This ambiguity can lead to disputes over who owns the rights to the code and whether it can be used or modified without permission. Additionally, the decentralized nature of blockchain platforms complicates enforcement, as once the code is deployed, it becomes publicly accessible and difficult to control.[23]

### Licensing Issues and Open-Source Smart Contract Platforms

Many smart contracts are built on open-source platforms like Ethereum, which encourage collaboration and innovation but also create licensing challenges. Open-source software is typically governed by licenses such as the GNU General Public License (GPL) or the MIT License, which dictate how the code can be used, modified, and distributed.[24] For example, if a developer uses open-source code to create a smart contract, they may be required to release their derivative work under the same license, potentially limiting their ability to commercialize it. This can create conflicts between the principles of open-source development and the proprietary interests of businesses. Furthermore, the lack of clear licensing terms for smart contracts deployed on blockchain platforms can lead to unintentional violations of IP rights, as users may not fully understand the legal implications of using or modifying the code.[25]

[20] [Copyright Act, 1957],[ No. 14], [Acts of Parliament], [1957] [India]

[21] *Ibid*

[22] [Abraham], *supra note* 9, [at 98]

[23] [Wright], *supra note* 1, [at 112]

[24] [GNU General Public License], [Version 3], [2007], https://www.gnu.org/licenses/gpl-3.0.en.html

[25] [Kevin Werbach], [*The Blockchain and the New Architecture of Trust],* [145], [MIT Press], [2018]

### Potential IP Disputes Arising from Smart Contract Execution

The execution of smart contracts can also give rise to IP disputes, particularly when the contract involves the transfer or licensing of intellectual property. For example, a smart contract may automatically transfer ownership of a digital asset (e.g., an NFT or copyrighted work) when certain conditions are met. If the terms of the contract are unclear or if the parties disagree on the scope of the rights transferred, disputes may arise over ownership or infringement.[26] Additionally, the immutability of smart contracts can exacerbate these disputes, as the terms cannot be easily modified once deployed.[27] For instance, if a smart contract inadvertently grants broader rights than intended, the parties may face lengthy legal battles to resolve the issue. These challenges highlight the need for clear contractual terms and robust IP protections to prevent disputes and ensure the enforceability of smart contracts.

## 5. CONSUMER PROTECTION AND SMART CONTRACTS

The Consumer Protection Act, 2019, provides a robust framework for safeguarding consumer rights in India, but its application to smart contracts remains uncertain. The Act defines a consumer as any person who purchases goods or services for personal use and grants them rights such as protection against unfair trade practices, the right to information, and the right to seek redressal for grievances.[28] However, smart contracts, which are often executed automatically and without human intervention, may not always align with these protections. For example, if a consumer enters into a smart contract without fully understanding its terms or if the contract contains hidden clauses encoded in the software, it may violate their right to information and fair treatment. This raises questions about whether smart contracts can be held accountable under the Act and how consumer rights can be enforced in such cases.[29]

### Transparency and Fairness in Automated Contracts

Transparency and fairness are critical components of consumer protection, but they pose significant challenges in the context of smart contracts. While smart contracts are designed to be transparent in terms of their execution on the blockchain, the underlying code may not

[26] [Abraham], *supra* note 9, [at 102]
[27] [Wright], *supra* note 4, [at 115]
[28] [Consumer Protection Act], [2019], [No. 35], [Acts of Parliament], [2019]
[29] [Abraham], *supra* note 9,[ at 106]

always be accessible or understandable to the average consumer.[30] For instance, a consumer may agree to a smart contract without realizing that it includes unfavorable terms or automatic deductions from their digital wallet. This lack of transparency undermines the principle of informed consent, which is essential for fair contractual relationships. Additionally, the automated nature of smart contracts leaves little room for negotiation or flexibility, which can disadvantage consumers in cases where exceptions or modifications are needed.[31] To address these issues, there is a need for greater standardization and clarity in the design of smart contracts, ensuring that consumers can easily understand and agree to their terms.[32]

### Redressal Mechanisms for Consumers in Case of Disputes

One of the most significant challenges in applying consumer protection laws to smart contracts is the lack of effective redressal mechanisms for disputes. Under the Consumer Protection Act, 2019, consumers can file complaints with consumer forums or commissions, but these mechanisms are not well-suited to handle disputes involving blockchain-based contracts.[33] For example, if a consumer disputes a transaction executed by a smart contract, it may be difficult to identify the responsible party or reverse the transaction due to the immutability of the blockchain. Furthermore, the decentralized nature of smart contracts complicates jurisdictional issues, as it is often unclear which authority has the power to resolve the dispute.[34] To address these challenges, experts have proposed the use of online dispute resolution (ODR) mechanisms, which can provide faster and more efficient solutions for disputes involving smart contracts.[35] However, the implementation of such mechanisms requires significant legal and technological reforms to ensure their effectiveness and accessibility for consumers.[36]

## 6. TAXATION AND FINANCIAL IMPLICATIONS

The tax treatment of transactions executed through smart contracts is a complex and evolving area, as existing tax laws were not designed to address the unique characteristics of blockchain-based agreements. In India, the Income Tax Act, 1961, governs the taxation of income,

[30] [Wright], *supra* note 1, [at 113]
[31] [Werbach], *Supra* note [24], [at 156]
[32] [Ministry of Electronics and Information Technology], Supra note 7
[33] [Consumer Protection Act], [2019], [Id 35, No. 35]
[34] [Abraham], *supra* note 9, [at 109]
[35] [World Economic Forum], *Supra* note 2
[36] [Abraham], supra note 9, [at 109]

including profits and gains from business or profession, capital gains, and other sources.[37] However, the automated and decentralized nature of smart contracts raises questions about how taxable events are identified and assessed. For example, if a smart contract automatically transfers cryptocurrency or digital assets as part of a transaction, it may be unclear whether this constitutes a sale, exchange, or barter for tax purposes.[38] Additionally, the anonymity of blockchain transactions complicates the tracking and reporting of income, making it difficult for tax authorities to enforce compliance.[39] To address these challenges, there is a need for clear guidelines on the tax treatment of smart contract transactions, including the classification of income and the determination of taxable events.

The Goods and Services Tax (GST) regime in India, governed by the Central Goods and Services Tax Act, 2017, applies to the supply of goods and services, including digital transactions.[40] However, the application of GST to blockchain-based transactions executed through smart contracts is not explicitly addressed in the law. For instance, if a smart contract facilitates the supply of digital goods or services, it may be unclear whether GST is applicable and, if so, at what rate.[41] Furthermore, the cross-border nature of many blockchain transactions complicates GST compliance, as it raises questions about the place of supply and the applicability of integrated GST (IGST).[42] To ensure clarity and compliance, businesses using smart contracts must carefully analyze the GST implications of their transactions and seek guidance from tax authorities where necessary.[43] Businesses using smart contracts face significant challenges in meeting their reporting and compliance requirements under Indian tax laws. The decentralized and immutable nature of blockchain technology makes it difficult to maintain traditional accounting records, which are essential for tax reporting and audits.

For example, businesses must ensure that all transactions executed through smart contracts are accurately recorded and reported in their financial statements, including details of income, expenses, and taxes paid.[44] Additionally, the use of cryptocurrencies in smart contracts adds another layer of complexity, as businesses must comply with the Reserve Bank of India

[37] [Income Tax Act, 1961], [No. 43], [Acts of Parliament], [1961]

[38] [Abraham], *supra* note 9, [at 112]

[39] *Ibid*

[40] [Reserve Bank of India], *Supra* note 6

[41] [Central Goods and Services Tax Act], [2017], [No. 12], [Acts of Parliament], [2017]

[42] [Abraham], *supra* note 9, [at 115]

[43] [Goods and Services Tax Council], [*Clarifications on GST for Digital Transactions],* [2021], https://www.gstcouncil.gov.in

[44] [Wright], *supra* note 1, [at 135]

(RBI) guidelines on virtual currencies and report their holdings and transactions accordingly.[45] To address these challenges, businesses may need to invest in specialized accounting software and seek professional advice to ensure compliance with tax laws and regulations.

## 7. GLOBAL COMPARATIVE ANALYSIS

### Legal Recognition of Smart Contracts In The United States

In the United States, smart contracts have gained significant legal recognition, particularly in states like Arizona and Tennessee, which have enacted specific legislation to validate their use. For instance, Arizona passed the Electronic Transactions Act in 2017, explicitly recognizing smart contracts as legally enforceable agreements. Similarly, Tennessee amended its Uniform Electronic Transactions Act to include blockchain-based signatures and smart contracts, ensuring they are treated on par with traditional contracts.[46] These legislative efforts provide clarity on the enforceability of smart contracts and establish a framework for resolving disputes. However, challenges remain in areas such as liability for coding errors and the integration of smart contracts with federal laws.[47] The U.S. approach highlights the importance of proactive legislation to foster innovation while addressing potential legal uncertainties**.**

### Legal Recognition of Smart Contracts in the European Union

The European Union (EU) has also taken steps to recognize and regulate smart contracts, particularly under the eIDAS Regulation (Electronic Identification and Trust Services Regulation), which provides a legal framework for electronic transactions.[48]

While the eIDAS Regulation does not explicitly mention smart contracts, it supports the use of blockchain technology for secure and transparent transactions.[49] Additionally, the EU has been exploring the development of a comprehensive regulatory framework for blockchain and smart contracts through initiatives like the European Blockchain Partnership.[50] These efforts aim to harmonize regulations across member states and promote the adoption of smart contracts in various sectors, including finance and supply chain management. The EU's emphasis on cross-

[45] [Reserve Bank of India], Supra note 6

[46] Tennessee Code Annotated, Title 47, Chapter 10, § 47-10-201 (2018)

[47] [Abraham], supra note 9, [at 120]

[48] [Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market], [2014] [O.J.] (L 257) 73

[49] [European Blockchain Partnership], [*Blockchain Strategy for Europe],* [2019], https://ec.europa.eu

[50] *Ibid*

border collaboration and standardization offers valuable insights for India's regulatory approach.

### Legal Recognition of Smart Contracts in Singapore

Singapore is widely regarded as a global leader in blockchain and smart contract regulation. The city-state has adopted a progressive approach under its Electronic Transactions Act (ETA), which was amended in 2021 to explicitly recognize smart contracts as legally binding agreements.[51] The amended ETA provides clarity on issues such as the formation, validity, and enforceability of smart contracts, ensuring they are treated similarly to traditional contracts.[52] Additionally, Singapore's Monetary Authority of Singapore (MAS) has issued guidelines on the use of blockchain technology in financial services, further supporting the adoption of smart contracts.[53] Singapore's regulatory framework demonstrates the benefits of clear and forward-looking legislation in fostering innovation and building trust in emerging technologies.

### Lessons India Can Learn from Global Regulatory Frameworks

India can draw valuable lessons from the regulatory frameworks of the U.S., EU, and Singapore to develop a robust legal environment for smart contracts. First, India should consider enacting specific legislation to recognize smart contracts as legally enforceable agreements, similar to the approach taken by Arizona and Singapore. This would provide much-needed clarity and encourage businesses to adopt smart contracts. Second, India can learn from the EU's emphasis on cross-border collaboration and standardization, particularly in addressing jurisdictional challenges and promoting interoperability. Finally, Singapore's proactive approach to regulating blockchain technology highlights the importance of clear guidelines and stakeholder engagement in building trust and fostering innovation. By incorporating these lessons, India can create a balanced regulatory framework that supports the growth of smart contracts while addressing potential legal and technical challenges.

## 8. CONCLUSION AND SUGGESSIONS

The future of smart contracts in India holds immense potential, driven by the rapid adoption of blockchain technology and the government's push toward digital transformation. With

[51] [Electronic Transactions Act], [Chapter 88], [Id 16A], [2021], (Singapore)

[52] [Id.16B]

[53] [Monetary Authority of Singapore], [*Guidelines on Digital Token Offerings],* [2020, https://www.mas.gov.sg

initiatives like the National Blockchain Strategy and the Digital India campaign, India is laying the groundwork for the integration of smart contracts into various sectors, including finance, supply chain, healthcare, and real estate. However, realizing this potential requires addressing key challenges, such as regulatory ambiguity, lack of technical expertise, and concerns over data privacy and security. For instance, while the Information Technology Act, 2000, provides a foundation for electronic contracts, it does not explicitly address the unique features of smart contracts, creating uncertainty about their legal enforceability. To overcome these hurdles, India must enact specific legislation to recognize smart contracts as legally binding agreements, similar to the approach taken by jurisdictions like Singapore and the United States.

To fully harness the potential of smart contracts, India must adopt a proactive and forward-looking approach to regulation. This includes enacting specific legislation to recognize smart contracts as legally binding agreements, similar to the frameworks established in jurisdictions like Singapore and the United States. Additionally, the development of standardized guidelines for smart contract development and deployment will be crucial in ensuring transparency, fairness, and security. Collaboration between the government, industry, and academia will also play a vital role in fostering innovation and addressing the technical and legal challenges posed by smart contracts. For instance, the establishment of specialized bodies or task forces to oversee blockchain and smart contract regulation could provide much-needed clarity and guidance. Moreover, India can draw valuable lessons from global best practices to create a balanced regulatory framework that encourages innovation while safeguarding consumer rights and legal certainty.

By embracing a holistic approach that balances innovation with consumer protection and legal certainty, India can unlock the transformative potential of smart contracts and pave the way for a more efficient, transparent, and inclusive digital future. The journey ahead is complex, but with the right policies and collaborative efforts, India can emerge as a global leader in the adoption and regulation of smart contracts.