CHOICE OF LAW IN CROSS-BORDER E-CONTRACTS AND SMART CONTRACTS

Thenmozhi G, LL.B. (Hons.), Vinayaka Mission's Law School (VMLS), Chennai

Mahendiran V, LL.B. (Hons.), Vinayaka Mission's Law School (VMLS), Chennai

ABSTRACT

The rapid growth of digital commerce and blockchain technology has transformed the way commercial agreements are formed and executed in different jurisdictions across the borders. The electronic contracts (e-contracts) and smart contracts are making transactions easier between the two parties who are in different jurisdictions. However, the e-contracts and smart contracts are much easier to use compared to the traditional method, but this digital transaction raises more complex legal questions like relating to jurisdiction, governing law, enforceability, and evidentiary validity of the contract. Traditional legal frameworks developed related to territorial transactions, whereas modern electronic agreements often operate simultaneously across multiple legal systems of different countries. Consequently, determining which country's law applies to cross-border electronic contracts and smart contracts has become a critical issue in Private International Law.

The research paper examines the doctrine of choice of law in cross-border electronic contracts and smart contracts. It analyzes how the courts were determining the applicable law governing agreements formed through digital platforms, automated systems, and blockchain technology based protocols. While most of the countries legally recognized electronic contracts under the existing contract laws.

The study further explores the situations in which no governing law is expressly specified in an electronic agreement. In those situations, courts rely on existing conflict of law principles and the proper law of the contract. However, finding these connecting factors becomes difficult in online environments because contract formation, performance, and digital infrastructure may span multiple jurisdictions. Furthermore, the evidentiary value of electronic data records and blockchain entries is examined in the context of cross border disputes.

An international comparative study of the legal system highlights diverse regulations concerning electronic and blockchain, based contracting. The

study also looks at the role of international instruments, particularly UNCITRAL model laws, in promoting harmonization of electronic commerce. The research finds that even though the existing contract law and private international law recognized electronic contracts (e-contracts) and smart contracts, clearer rules on applicable domestic law, jurisdiction, and enforceability, there is a need for more provisions to ensure legal certainty in cross border digital transactions and contract disputes.

Keywords: Choice of Law - Electronic Contract (e-contract) - Smart Contract - Block Chain Technology - Private International Law - Jurisdiction - Electronic Evidence - Cross border Digital Transactions.

1) INTRODUCTION

The contract plays a vital role in every day-to-day life from human evolution. But now technologies have evolved more advanced, as a human being needs to adapt to it. Otherwise, humans can't survive in the fast moving technological world. So, by technological development the traditional method of contract using the paper for agreement started to enter the new method of electronic contract (e-contract) and smart contract which is paperless. The growth of digital technology has fundamentally changed the manner how contracts made and performed in modern commerce. Transactions that once required physical presence and paper documentation are now commonly done through electronic form. Electronic contracts (hereinafter referred to as e-contracts) have made it possible for the contractual parties who are in different parts of the world to enter into agreements without geographical limitations. This change has significantly contributed to the growth of cross border trade and digital economies. On the other hand, the development of blockchain technology has introduced a new type of agreement which is known as smart contracts. It is a type of digital and automatic contract where the performance of the contractual parties is regulated by the computer code and executed immediately once certain conditions are fulfilled. While such contracts are bringing efficiency and reduce dependency on intermediaries, they also challenge the legal fundamentals of contracts like intention, consent and enforcement.

The growing adoption of e-contracts and smart contracts in cross border transactions has raised complex legal challenges. In the case of traditional contracts, which are usually connected to a single territory and therefore have a clear legal jurisdiction. But digital contracts often operate across multiple jurisdictions simultaneously. This situation produces several questions such as governing law of contract, which court has jurisdiction in case of disputes

and enforceability of the contract. These issues become even more complicated when the blockchain-based transactions are involved, since the very decentralized nature of the technology makes it difficult to identify a single legal framework.

Although many legal systems including India, recognized the validity of the e-contracts under the same existing contract law principles, there is still a lack clarity in the operation of cross-border contracts. Especially the absence of a specific regulatory framework for smart contracts makes the situation more uncertain. Consequently, courts have no other choice, but are required to rely on traditional principles of private international law, such as party autonomy and the proper law of the contract, to resolve disputes arising from digital transactions.

This research paper deals with the choice of law in cross border e-contracts and smart contracts. It also explores the suitability of existing law for digital contracts and the to identify legal challenges in deciding the law applicable to such transactions. By analyzing statutory provisions, court rulings, and international legal developments, the research will present a clear understanding of the legal system and suggests the need for change in this evolving area of law.

2) EVOLUTION OF ELECTRONIC CONTRACTS

The concept of electronic contracts did not develop suddenly but rather evolved with improvements in communications technology and the internet. Initially, the commercial agreements were concluded through traditional written documents requiring signatures and physical presence. However, with the growth of electronic communication, especially email and online platforms, the contract making process started to move towards digital methods. The reason behind this was the need for speed, efficiency, and ability to conduct transactions across geographical boundaries. In the early stages, there was uncertainty regarding whether agreements formed through electronic means could be considered legally valid. Traditional contract law was built around the idea of written documents and physical signatures, which created doubts about the recognition of electronic communications. However gradually, the courts and legislation started adopting a different perspective, focusing on the intention of the contractual parties rather than the form of the contract. This change in viewpoint made it possible for electronic communications, such as emails and online acceptances, to be treated as legally binding means of offer and acceptance.

As internet usage expanded, different forms of electronic contracts became common in commercial practice. Click-wrap agreement, which requires users to click the "I Agree" button to stipulate their acceptance of the terms and conditions before accessing a service or completing a transaction. Another form that is common is the browser-wrap agreement, where the terms are displayed on the website and the user's ongoing use of the site is considered the acceptance of those terms. There are also shrink-wrap agreements, typically used in software transactions, where the terms become binding once the packaging is opened, or the software is installed. These standard forms of contracts have become an essential part of digital commerce, particularly in e-commerce platforms, software licensing, and online services.

One major element that has impacted the legal recognition of the agreements has been the readings of courts. Usually, judgements have been in favor of such online agreements where users are notified in a clear way about the terms and their consent is given by an affirmative action. In Specht v. Netscape communications corp., the court held that users could not be bound by terms that were nit reasonably communicated or easily accessible.[1] This case highlighted the importance of informed consent in electronic contracting. Similarly, in the case of Rudder v. Microsoft Corp., the court upheld the enforceability of an online agreement, including its jurisdiction clause, the court indicated that such contracts are enforceable when users knowingly and voluntarily accept the terms.[2] These decisions demonstrate that while electronic contracts are recognized, their enforceability depends on the manner in which consent is obtained.

In India, the growth of electronic contracts has been supported by both judicial interpretation and legislative intervention. It was recognized by the courts that the contract could be formed through modern means of communication such as emails and electronic communications. The enactment of the Information Technology Act, 2000 plays a major role in the recognition of electronic transactions. It gave a legal status to electronic records and communications, thus ensuring digital contracts the same legal treatment as that of conventional agreements. The evolution of electronic contracts has also laid the foundation for more advanced forms of digital agreements, such as smart contracts. Traditional e-contracts still require some level of human interpretation and enforcement, smart contracts are designed to run the entire process independently by just using computer code. This represents the next

[1] Specht v. Netscape Communications Corporation, 306 F .3d 17 (2d Cir. 2002).
[2] Rudder v. Microsoft Corporation [1999] O.J. No. 3778 (Ont. Sup. Ct. J.).

stage in the development of digital contracting because now technology is not only helping in making contracts but also in carrying out those contract terms. E-contracts have grown from being an innovative concept to an integral part of business transactions. This has been possible because legal systems are dynamic in nature, as seen in the development of E-contracts. Although most legal systems have been quite effective in recognizing the validity of e-contracts, the increasing complexity of cross border transactions and emerging technologies are continuously creating new legal issues. These issues become even more significant, especially in the context of smart contracts, which confuse the boundary line between technology and law.

3) SMART CONTRACTS AND BLOCKCHAIN TECHNOLOGY

3.1 Blockchain Technology

To understand smart contracts, you first need to understand the technology supports them. A blockchain is a digital record book, but unlike a normal record book that one person or organisation controls, a blockchain is stored simultaneously across thousands of computers spread across the world.[3] Each group of new transactions is bundled into a "block" and linked to the chain of previous blocks. Once a block is added, it essentially cannot be changed, because altering it would require simultaneously changing every copy on every computer in the network, which is practically impossible.

This creates what people call an immutable record. Nobody can quietly go back and alter past transactions. And because no single person or organization controls the entire network, there is no central authority that can be pressured or corrupted into changing the records. The system enforces itself through its distributed architecture. There are two broad kinds of blockchains. A public blockchain, such as Ethereum or Bitcoin, is open to anyone, anyone can join the network, and anyone can read the transactions.[4] A private or permissioned blockchain is controlled by a specific set of organisations with restricted access. Most commercial smart contract applications use public blockchains, though banks and large enterprises are increasingly experimenting with private ones for regulated financial

[3] World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note No. 1, at 2–3 (2017).
[4] Vitalik Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, ETHEREUM WHITE PAPER 1, 3 (2013).

transactions.

3.2 Smart Contract

Szabo described a smart contract as a set of promises in digital form, with protocols through which the parties perform on those promises.[5] In plain terms, it is a piece of code sitting on a blockchain that automatically does something when certain conditions are verified. The logic is very simple, if X happens, then Y executes automatically. A practical example helps make this concrete. Say a buyer and seller agree that payment will be released from escrow once a shipment is confirmed as delivered. Instead of the buyer manually approving payment after checking delivery, a smart contract monitors the shipment tracking data through an external data feed is called an oracle and releases the payment the moment delivery is confirmed. Nobody has to do anything. The code handles it entirely. One thing that makes smart contracts legally significant and legally complicated is their immutability. Once the code is deployed on a blockchain, it cannot easily be changed or corrected.[6] If there is an error in the code, or if the code produces an unexpected result, you generally cannot simply fix it the way you would correct a mistake in a written contract. The code runs, and the result stands. This is both the strength and the fundamental weakness of smart contracts from a legal perspective.

3.3 Types of Smart Contracts

Legal scholars and practitioners distinguish between what they call strong and weak smart contracts.[7] A strong smart contract operates entirely within the blockchain, all the conditions it needs to verify can be checked from within the network itself. A weak smart contract depends on external data fed in through oracles, delivery confirmations, weather readings, market prices, or other off-chain information to trigger its execution. Most of the real world commercial smart contracts fall into the weak category, because real world events simply cannot be verified from inside a blockchain on their own. There is also a growing category called Ricardian contracts, hybrid instruments that pair a human readable legal agreement with a machine executable smart contract, both covering the same underlying transaction.[8] The legal

[5] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, EXTROPY: J. TRANSHUMANIST THOUGHT, no. 16, 1996, at 1.
[6] Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305, 309–10 (2017).
[7] Jeremy M. Sklaroff, Smart Contracts and the Cost of Inflexibility, 166 U. PA. L. REV. 263, 270–72 (2017).
[8] Ian Grigg, The Ricardian Contract, in PROCEEDINGS OF THE FIRST IEEE INTERNATIONAL WORKSHOP ON ELECTRONIC CONTRACTING 25 (2004).

text can be read and interpreted by lawyers and courts. The code automates the performance. This is actually a very practical approach, and many Indian businesses are already informally using something like this, placing smart contract payment automation within broader written agreements that include governing law clauses and dispute resolution provisions.

3.4 Smart Contracts differ from Ordinary E-Contracts

The essential difference is simple. In a regular e-contract, somebody still has to actually perform their obligations after the contract is formed. In a smart contract, the performance itself is automated, the code carries it out without any human trigger. This creates genuinely new legal questions that existing Indian law does not answer. If performance is automatic, who breaches the contract when the code does something wrong? If neither party controlled the execution, who is responsible for an unintended result? Can a court grant meaningful relief when execution has already happened on an immutable ledger and cannot be reversed?[9] These questions point to real gaps in the current legal framework.

4) LEGAL FRAMEWORK GOVERNING E-CONTRACTS IN INDIA

Electronic contracts were legally recognized not by creating new legal principles, but rather by modifying the existing contract law to make it relevant to the technological developments. Most legal systems, including India, have taken the technology neutral approach, that they apply the traditional contract formation to electronic agreements However, to address the issues related to authentication, validity, and enforceability, separate statutory provisions have been enacted to support electronic transactions. In India, the basis of all contractual arrangements still rests on the Indian Contract Act, 1872 which lays down the essential elements of a valid contract. The fundamental elements to the contract are, offer, acceptance, lawful consideration, intention to create legal relations, and free consent.[10] E-contracts are not treated as a separate category of contracts, rather they are assessed on whether these fundamental elements are fulfilled. Hence, a contract made through electronic form like clicking “I Agree” or accepting terms through email can be legally valid if it meets these requirements. In the case of Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., Supreme Court of India held that a contract done through exchange of emails can be a legally

[9] Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305, 310-11 (2017).
[10] Indian Contract Act, No. 9 of 1872, Section 10.

binding contract even without the formal written agreement.[11] The court observed that the intention of the parties and existence of consensus ad idem are more important than the form in which the contract was made. This decision reflects the broader judicial approach of adapting traditional contract principles to modern communication methods.

In India the e-contracts was governed by the Information Technology Act, 2000. Section 4 grants legal recognition to electronic records and Section 5 does the same for electronic signatures.[12] Section 10A of the Act explicitly provides that contracts formed through electronic means cannot be considered unenforceable solely because it is formed by electronic communications.[13] This provision plays an important role as it supports the legality of e-contracts by eliminating uncertainties about their legal recognition. By this way, electronic contracts are given equal status and are on the same footing as paper based contracts. The IT Act also addresses issues relating to authentication and security in e-contracts through provisions dealing with electronic and digital signatures. These mechanisms are essential for establishing the identity of parties and ensuring the integrity of electronic records. Nevertheless, in international business transactions, differences in the level of acceptance of digital signatures among the different countries may create challenges, particularly where one or both parties use different kinds of technology or rely on their respective certification authorities. The Act is technology neutral, which means it does not list specific technologies and therefore does not exclude blockchain systems, even though blockchain was not contemplated when the Act was originally drafted. There is a gap, though. The IT Act does not deal with automated execution, immutability, pseudonymous parties, or decentralised networks. It was written for emails and digital signatures, not for self-executing blockchain programs. This is where the law starts to show its age.

Another important aspect of the legal framework governing e-contracts is the evidentiary recognition of electronic records. Section 65B of the Indian Evidence Act, 1872 governing the admissibility of electronic evidence in legal proceedings. In the case of Anvar P.V. v. P.K. Basheer & Ors, the supreme court held that electronic records can be accepted as evidence only if they have a valid certificate under Section 65B.[14] This requirement ensures the authenticity and trustworthiness of electronic evidence, which is crucial in disputes

[11] Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1. (India)
[12] Information Technology Act, No. 21 of 2000, Section 4, 5 (India).
[13] Information Technology Act, No. 21 of 2000, Section 10A (India).
[14] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473 (India).

involving digital contracts. The Bharatiya Sakshya Adhiniyam, 2023, which replaced the old Evidence Act, made some adjustments to how courts deal with electronic records.20 Whether those adjustments are sufficient for blockchain evidence is something courts will work out through litigation. The new law moves in the right direction but does not specifically address the problem of decentralised records.

When e-contracts involve ordinary consumers, the Consumer Protection Act, 2019 becomes important.[15] It protects consumers against unfair contract terms, which is especially relevant for click-wrap and browse-wrap agreements where the consumer cannot negotiate anything. The Supreme Court in LIC of India v. Consumer Education and Research Centre observed that contracts involving a serious imbalance of bargaining power between the parties call for closer judicial scrutiny.[16] That principle applies directly to the standard form digital contracts that platforms routinely impose on users who have no real choice.

On the international level, the development of electronic contracts has been affected by the effort to create uniform legal standards. The UNCITRAL Model Law on Electronic Commerce (1996) played a vital role in promoting the acceptance of electronic communications in commercial transactions. It introduced the concept of functional equivalence, which ensures that electronic records and signatures will be treated as legally valid counterparts of paper based documents when the provided certain conditions are met.[17] This model law has led to creation of legal frameworks in many countries and has contributed to the harmonization of e-commerce laws across jurisdictions.

In addition to UNCITRAL Modern Law, different countries have enacted their own laws to regulate electronic contracts. For example, the United States enacted two laws, namely the Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (E-Sign Act), that both declare electronic documents and signatures as valid. Similarly, the European Union's eIDAS Regulation provides a comprehensive legal framework for electronic identification and trust services, making sure that secure and reliable electronic transactions throughout the Member States. Such regulations reflect the worldwide move towards identifying electronic contracting as a legitimate and essential component of

[15] Consumer Protection Act, No. 35 of 2019, Section 2(47), 47 (India).
[16] LIC of India v. Consumer Education & Research Centre, (1995) 5 SCC 482, 499 (India).
[17] UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, U.N. Doc. A/51/49 (1996).

modern commerce. Despite this legal recognition, the challenges have remained in the context of cross border e-contracts. Differences in national laws regarding electronic signatures, data protection, and consumer rights can create uncertainty for the parties entering into international agreements. For instance, a contract that is valid in one jurisdiction may face enforcement issues in another jurisdiction due to the different system of legal standards. This issue becomes even more important if the parties did not or have not explicitly specified the governing law in their contract.

Another issue is that various studies raise as a significant one is the usage of standard form contracts especially in the case of digital transactions. Most users often accept terms and conditions without fully understanding them, which raises questions about the validity of consent. Courts have been pointing out the need for clear communication about the terms of contracts and genuine acceptance by users. This is particularly significant in cross border transactions, where consumer protection laws may override contractual provisions, including those related to choice of law provision. The legal framework governing e-contracts has been established on the combination of the long-standing contract law principles and the newly enacted legislation that recognize electronic transactions. Even though significant progress has been made in validating electronic agreements, the international aspect of digital commerce still raises many issues. The interaction between domestic laws, international instruments/treaties, and technological developments makes it necessary to develop more uniform and legal standards for electronic contracting.

5) ADVANTAGES OF ELECTRONIC AND SMART CONTRACTS

5.1 Advantages of Electronic Contracts (E-Contracts)

Speed is the most obvious advantage. Before e-contracts, getting a signed agreement in place meant drafting, printing, posting, waiting, receiving it back. That could take a week or more. Now the same process happens in minutes.[18] For any business dealing with large numbers of contracts, this speed is genuinely transformative. The cost savings are also real and significant. No printing, no couriering, no physical storage, much less administrative work.[19] For a small business in India trying to deal with international buyers, reducing the transaction

[18] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, at 17 (1999).
[19] World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note No. 1, at 4 (2017).

cost of each deal makes cross-border trade financially viable in a way it simply was not before. This is not a minor point, it has opened international markets to businesses that previously had no realistic access to them.[20] Record keeping is better too. A digital contract properly stored does not get lost, does not deteriorate, and can be retrieved immediately when needed. When a dispute comes up years later, having a clear, timestamped record of exactly what was agreed is far more useful than trying to reconstruct events from memory or paper copies. United Nations Commission on International Trade Law providing that electronic records satisfy any legal requirement for a document to be in writing. There is also the benefit of standardisation at scale. A company that needs the same agreement with hundreds of customers can create one template and deploy it consistently. This reduces errors, keeps terms uniform, and makes compliance management simpler.[21]

5.1 Advantages of Smart Contracts

Smart contracts build on all the above and add something qualitatively new automated performance. The contract is not just formed electronically, the performance also happens electronically, without anyone needing to trigger it manually. The removal of intermediaries is one of the most commercially significant advantages. Many transactions require third parties like banks, escrow agents, clearing houses are purely to verify that both sides have performed.[22] A smart contract can replace many of these intermediaries by building the verification and execution logic directly into the code. These cuts cost and remove the human element that introduces delay, error, and sometimes deliberate fraud. Trust between parties who do not know each other is a genuine benefit. With a conventional contract, there is always a risk that one side will not follow through voluntarily. With a smart contract, once the triggering condition is verified, execution happens automatically, the other party simply cannot stop or delay it.[23] This is particularly valuable in cross-border dealings where the parties are in different legal systems and cannot easily enforce their rights against each other through courts.

The tamper-resistance of blockchain records also matters. Because the record of every transaction is held simultaneously across thousands of independent computers, nobody can

[20] United Nations Convention on the Use of Electronic Communications in International Contracts, opened for signature Jan. 16, 2006, U.N. Doc. A/60/515.
[21] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162, U.N. Doc. A/51/628, art. 6 (1996)
[22] Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 305, 315-16 (2017).
[23] Jeremy M. Sklaroff, Smart Contracts and the Cost of Inflexibility, 166 U. PA. L. REV. 263, 267-68 (2017).

secretly alter it after the fact.[24] Disputes about what actually happened, who paid what, when, and under what conditions are becoming very difficult to sustain when there is an objective, independently verifiable record on the ledger. For cross-border transactions, smart contracts partially solve the enforcement problem. Getting a court in India to enforce a judgment against a foreign defendant is slow, expensive, and uncertain. A smart contract that holds funds in escrow and releases them only when conditions are satisfied does not need court enforcement, the contract enforces itself.[25] The evidentiary quality of blockchain records is another genuine benefit. Every transaction leaves a permanent, time-stamped, cryptographically secured record on the ledger. In litigation or arbitration, having this kind of objective record is far more reliable than depending on documents that a party could potentially have altered or destroyed. In practice, these benefits are already being realised. Trade finance, insurance, and supply chain management. Institutions across these sectors are already piloting or deploying smart contract applications globally. India's own financial sector regulators have shown interest in distributed ledger technology for exactly these efficiency reasons.[26]

6) CHOICE OF LAW IN CROSS-BRODER E-CONTRACTS

When a contract involves parties from different countries and something goes wrong, one of the first questions to be answered is whose law governs it. Different countries have very different rules on contract validity, breach, and remedies. The answer to this question can change the entire outcome of a dispute. The starting point in private international law is the principle of party autonomy, the idea that parties should generally be free to choose which legal system governs their contract.[27] In practice, this means including a governing law clause in the contract. Indian courts generally respect these clauses in commercial disputes between businesses and apply the chosen law. The Hague Principles on Choice of Law in International Commercial Contracts, adopted in 2015, represent the current international consensus on how party autonomy should operate in cross-border commercial contracting.[28] India has not formally adopted these Principles, but they reflect sound practice that Indian courts broadly

[24] World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note No. 1, at 3 (2017)
[25] Convention on the Recognition and Enforcement of Foreign Arbitral Awards art. III, June 10, 1958, 330 U.N.T.S. 38.
[26] Vitalik Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, ETHEREUM WHITE PAPER 5-7 (2013).
[27] Hague Conference on Private International Law, Principles on Choice of Law in International Commercial Contracts, Article 2 (2015).
[28] Hague Conference on Private International Law, Principles on Choice of Law in International Commercial Contracts, Article 1-3 (2015).

follow through their common law heritage.

The harder situation arises when the parties have not chosen a governing law, which is common in consumers, facing digital transactions where the terms are drafted entirely by the platform, and most users never read them. When there is no choice of law clause, Indian courts fall back on common law connecting factors, the place where the contract was formed, the place where it is to be performed, and the legal system with which the contract has its closest and most real connection.[29] None of these factors are easy to identify in an online transaction. Where was the contract formed, where the user clicked, where the company's servers are hosted, or where the company's headquarters are located? Courts have given different answers to this, which creates unpredictability. Section 13 of the Information Technology Act gives some limited help by defining where an electronic record is considered dispatched and received, the originator's principal place of business for dispatch, the addressee's principal place of business for receipt.[30] But this provision helps only with simple bilateral communications. It does not tell you much about governing law in multi-party or automated digital transactions.

Even where parties have agreed on a governing law, that choice has limits when one party is a consumer. Indian consumer protection law contains mandatory rules that operate regardless of contractual stipulations.[31] A platform that uses a governing law clause to strip an Indian consumer of their statutory rights will find that clause challenged and likely set aside on public policy grounds. The European Union's approach in Article 6 of the Rome I Regulation is worth examining here. It provides that a consumer always retains the protection of their home country's mandatory rules, regardless of any governing law clause in the contract.[32] India has no codified equivalent of Article 6. The principle is recognised through the Consumer Protection Act and through judicial interpretation of public policy, but its application to cross-border digital disputes is not settled and consistent.

7) CHOICE OF LAW FOR SMART CONTRACTS

If choice of law is already complicated for ordinary e-contracts, smart contracts make

[29] . DICEY, MORRIS & COLLINS ON THE CONFLICT OF LAWS r. 202–203 (Lord Collins of Mapesbury et al. eds., 15th ed. 2012).
[30] Information Technology Act, No. 21 of 2000, Section 13 (India).
[31] Consumer Protection Act, No. 35 of 2019, Section 47 (India).
[32] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I), Article 6, 2008 O.J. (L 177) 6 (EU).

it significantly harder. The reason is that they remove or obscure most of the connecting factors that private international law traditionally relies on. In a conventional e-contract, the parties may be online, but you can still identify them. A company registered in Mumbai, a buyer based in Frankfurt, each with a traceable domicile and principal place of business. In a smart contract on a public blockchain, the parties may be entirely pseudonymous, identified only by a cryptographic wallet address with no name, country, or physical location attached.[33] Without knowing who the parties are, standard connecting factors simply cannot operate. Three approaches have been proposed. The first is sometimes called the "code is law" approach, the idea that the smart contract itself is the governing norm and whatever the code produces is the final and binding answer.[34] This might sound clean and logical, but it removes the possibility of any judicial review or legal correction. Courts have not accepted this position, and rightly. So, it would effectively exempt smart contracts from any external legal oversight.

The second approach applies to the law of the place where the contract was deployed, essentially where the developer who wrote the code is domiciled. This at least provides a concrete connecting factor, but it fails entirely when the developer is also pseudonymous, or when the contract was deployed by a Decentralised Autonomous Organisation (DAO) with no identifiable person behind it. The third approach and in practical terms the most workable is to use a Ricardian contract alongside the smart contract. The human-readable legal agreement includes a governing law clause, and that clause governs the relationship between the parties. The smart contract automates performance. The legal agreement provides the framework for dispute resolution. Many commercial entities in India already informally follow this hybrid model by embedding blockchain payment mechanisms within conventional Master Service Agreements. Where none of these approaches gives a clear answer, which is the case in many truly decentralised transactions, private international law simply has no ready solution. This is the honest position, and it points directly to the need for legislative reform.

8) JURISDICTIONAL CHALLENGES IN ONLINE TRANSACTIONS

Jurisdiction and choice of law are related but distinct questions. Choice of law asks which legal system applies. Jurisdiction asks which court gets to hear the case. They need to

[33] Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 75–76 (Harvard Univ. Press 2018).
[34] Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 78-80 (Harvard Univ. Press 2018).

be kept conceptually separate even though they often arise together in cross-border digital disputes. Under the Code of Civil Procedure, 1908, an Indian civil court has territorial jurisdiction where the defendant resides or carries on business, or where the cause of action wholly or partly arises.[35] In an online dispute, identifying where the cause of action "arose" is genuinely difficult. The buyer may be in Delhi, the seller in London, the server in Singapore, and payment executed across a global blockchain network. The cause of action does not have one clear territorial home. The old Supreme Court principle from Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas, held that a contract is completed at the place where acceptance is communicated, does not translate meaningfully to automated blockchain execution.[36] The Arbitration and Conciliation Act, 1996, combined with India's accession to the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, means that arbitral awards can usually be enforced across borders with reasonable predictability.[37] For cross-border digital disputes, arbitration is a far more practical route than litigation. The jurisdictional problem becomes almost unmanageable when a DAO is involved. A DAO has no registered office, no directors, no legal personality under Indian law.[38] If a smart contract operated by a DAO causes financial loss, there may simply be no identifiable legal entity to sue. Wyoming in the United States addressed this directly through its DAO LLC Act of 2021, which gives DAOs formal legal status equivalent to limited liability companies.[39] India has nothing comparable, and this gap will cause real problems as decentralised finance platforms grow in the Indian market.

9) EVIDENTIARY VALUE OF BLOCKCHAIN AND ELECTRONIC RECORDS

One area where blockchain technology is genuinely an advantage in legal proceedings is evidence. When a smart contract dispute comes to court or arbitration, the record of what happened is usually very clear, what the code was programmed to do, what conditions were verified, what was executed, and when. That record is distributed across thousands of independent computers and practically cannot be altered after it is written. That is a significantly stronger evidentiary property than almost any paper document or centralised

[35] Code of Civil Procedure, No. 5 of 1908, Section15–20 (India).
[36] Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas & Co., AIR 1966 SC 543, 548 (India).
[37] Arbitration and Conciliation Act, No. 26 of 1996, Section 44-52 (India); Convention on the Recognition and Enforcement of Foreign Arbitral Awards art. III, June 10, 1958, 330 U.N.T.S. 38
[38] Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 97-99 (Harvard Univ. Press 2018).
[39] DAO LLC Act of 2021, Section 1, Article 1, 17-31-101 to 17-31-115 (2021) (State of Wyoming)

database system. The difficulty in India lies in admissibility. Section 65B of the Indian Evidence Act requires a certificate from the responsible person at the organisation that manages the computer system which produced the record. For a normal company server, the IT manager or system administrator can sign this certificate. For a public blockchain with no central administrator, there is nobody who can sign it. This procedural requirement was clearly designed for a different era.

The UNCITRAL Model Law on Electronic Transferable Records of 2017 provides internationally recognised guidance on this front. It says electronic records should be treated the same as paper documents when their integrity can be independently verified through a reliable method.[40] India has not adopted this instrument. Doing so or using it as the basis for updating Indian evidence rules, would go a long way toward fixing the current problem.

10) COMPARATIVE INTERNATIONAL STUDY

10.1 United Kingdom (UK)

The UK's position is that existing English contract law is flexible enough to accommodate smart contracts without needing any new legislation. The UK Jurisdiction Taskforce published a detailed Legal Statement in 2019 confirming that smart contracts can satisfy offer, acceptance, consideration, and intention to create legal relations just like any other contract and are therefore enforceable. The UK Law Commission reaffirmed this in its 2021 report on Smart Legal Contracts.[41] The most detailed judicial engagement with smart contract law anywhere in the common law world is probably the Singapore Court of Appeal's decision in Quoine Pte Ltd. v. B2C2 Ltd.[42] That case arose from a coding error on an automated trading platform that caused trades to execute at prices nowhere near market rates. The court examined whether the doctrine of unilateral mistake could void these automated transactions and concluded that it could, on the facts. That is a significant finding because it shows that classical contract law doctrines can reach into automated, coded performance and override it where justice demands. The code did not get the final say.

[40] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records, U.N. Doc. A/CN.9/WG.IV/WP.142 (2017)
[41] UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (Nov. 2019).
[42] Quoine Pte Ltd. v. B2C2 Ltd., [2020] SGCA(I) 02 (Singapore Ct. App. 2020).

10.2 Singapore

Singapore assesses smart contracts under ordinary contract principles without needing special legislation.[43] The Electronic Transactions Act 2010 provides a broad framework for digital contracting.[44] More importantly, Singapore has built genuine institutional capacity to handle technology disputes, its courts, arbitral institutions, and regulators have developed real expertise in these areas. Singapore has become the preferred seat for cross-border digital commercial arbitration across Asia because of this combination of good law and strong institutions. India, which is developing its own arbitration infrastructure, could learn directly from this model.

10.3 United States (US)

The United States has primarily handled smart contracts at the state level. Arizona, Tennessee, Nevada, and Wyoming have all passed statutes explicitly recognising smart contracts as legally valid.[45] Wyoming's DAO LLC Act of 2021 went furthest by giving decentralised autonomous organisations formal legal status as limited liability companies, they can be sued, can hold property, and can enter into contracts in their own name. This directly and practically solves the defendant-identification problem that makes DAO litigation impossible elsewhere. At the federal level, the Electronic Signatures in Global and National Commerce Act and the Uniform Electronic Transactions Act provide an electronic contracting framework broadly comparable to India's IT Act.[46]

10.4 European Union

The EU has the most developed codified framework for choice of law in contracts. The Rome I Regulation sets out clear rules, commercial parties can freely choose their governing law, but consumers always retain the protection of their home country's mandatory rules regardless of any governing law clause in the contract.[47] Article 6 of Rome I, which codifies this consumer protection guarantee, is precisely what India's private international law is missing. The EU's

[43] Electronic Transactions Act 2010, Section 4 (Singapore).
[44] Electronic Transactions Act 2010, Section 4,11 (Singapore).
[45] Tennessee Code, Title 47, Section 47-10-201 (2018); Arizona Revised Statutes, Title 44, Section 44-7061 (2017); Nevada Revised Statutes, Section 719.230, 719.310 (2017).
[46] Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001–7006 (2000); Uniform Electronic Transactions Act Section 1–21 (Unif. Law Comm'n 1999).
[47] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I), Articles 3, 4, 6, 2008 O.J. (L 177) 6 (EU).

Markets in Crypto-Assets Regulation, enacted in 2023, is the most comprehensive piece of digital asset legislation in the world.[48] It addresses smart contracts indirectly through its provisions on decentralised finance and crypto-asset issuers. India cannot simply copy this framework, but it demonstrates what a serious, committed legislative response to digital commerce looks like. Looking at all four jurisdictions together, one thing is unmistakable, the countries that have made the most progress are those that made a deliberate decision to engage with the problem rather than waiting for courts to develop the law case by case. The UK published its Legal Statement. Wyoming enacted its DAO statute. The EU adopted Rome I and then MiCA. Each was a deliberate institutional act. India has not yet made that kind of move, and the gap is widening as digital commerce expands. There is also a lesson about institutional capacity. Singapore works well not just because of its laws but because its judges, arbitrators, and regulators genuinely understand the technology. India has capable institutions, but building technical expertise within them to handle blockchain evidence and smart contract disputes will need deliberate investment over time.

11) LEGAL GAPS AND REMAINING CHALLENGES

After going through all of this, a few important gaps in Indian law stand out. The biggest one is that India has no law dealing specifically with smart contracts. The IT Act and the Contract Act apply in a general way, but neither was written for self-executing, immutable code. When a smart contract malfunctions or produces an unintended result, there is no clear statutory answer for who is liable or what a court can actually do about it. India also lacks a codified private international law framework for contracts. There is no statute clearly setting out how to find the governing law in a cross-border digital dispute.[49] Courts work it out case by case, which creates inconsistency. Businesses cannot plan cross-border transactions with any real confidence when the answer depends on which judge hears the case. The evidence problem is also unresolved. Section 65B needs a certificate from whoever manages the computer system. For a public blockchain, nobody manages it centrally, so the certificate cannot exist. This needs a direct fix. DAOs have no legal identity under Indian law, which means nobody can practically be sued when a DAO operated smart contract causes harm.[50]

[48] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA), 2023 O.J. (L 150) 1 (EU).
[49] DICEY, MORRIS & COLLINS ON THE CONFLICT OF LAWS r. 202 (Lord Collins of Mapesbury et al. eds., 15th ed. Sweet & Maxwell 2012).
[50] Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 97-99 (Harvard Univ. Press 2018).

And the bargaining power gap in standard-form digital contracts is real, most users click agree without reading, which makes calling that free consent somewhat fictional.[51]

12) CONCLUSION AND RECOMMENDATIONS

What this paper has argued, put simply, is that Indian law handles conventional e-contracts reasonably well. The Contract Act and the IT Act give courts enough to work with for most situations. But smart contracts and genuinely decentralised cross-border transactions expose structural gaps that courts cannot fill. The UK, Singapore, US, and the EU all made deliberate legislative choices to address these problems. India has relied on judicial development, and that approach is no longer keeping pace. Five reforms would make a real difference. The IT Act should be amended to recognise and govern smart contracts, including preserving judicial power to award compensation where code produces unintended results. A codified choice of law statute for cross-border contracts is needed, drawing on the Hague Principles for commercial transactions[52] and the Article 6 consumer protection model from the Rome I Regulation.[53] The evidence rules need updating to make blockchain records practically usable in court, either through expert certification or by adopting the UNCITRAL Model Law on Electronic Transferable Records.[54] DAOs need a recognized legal form, so they can actually be held accountable.[55] And an online dispute resolution system for small cross-border digital claims would make consumer protection law work in the real world, not just in theory.[56] India's digital economy is growing fast. The legal infrastructure around it needs to grow with it. None of these reforms are drastic or untested, they are all built on things other countries have already done. What is needed now is simply the will to do them.

[51] LIC of India v. Consumer Education & Research Centre, (1995) 5 SCC 482, 499 (India); Consumer Protection Act, No. 35 of 2019, Section 47 (India).
[52] Hague Conference on Private International Law, Principles on Choice of Law in International Commercial Contracts, Article 1-3 (2015).
[53] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I) Article 6, 2008 O.J. (L 177) 6 (EU).
[54] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records, U.N. Doc. A/CN.9/WG.IV/WP.142 (2017).
[55] DAO LLC Act of 2021, Section 1, Article 1, 17-31-101 to 17-31-115 (2021) (State of Wyoming).
[56] United Nations Commission on International Trade Law, UNCITRAL Technical Notes on Online Dispute Resolution 5-7 (2017),

REFERENCES

- Anjali Sharma & Karan Singh Gaur, E-Contracts in the Commercial World, 9 INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES, 1473, 1473–1497 (2026), https://ijlmh.com/wp-content/uploads/E-Contracts-in-the-Commercial-World.pdf (last visited Mar. 28, 2026, 09:55 PM).

- Swarup Chatterjee & Rajvardhan, Evolution and Challenges of Cross-Border Electronic Contracts, 13 INTERNATIONAL JOURNAL OF CURRENT ADVANCED RESEARCH, 2938, 2938–2942 (2024), https://journalijcar.org/sites/default/files/issue-files/14390F.pdf (last visited Mar. 28, 2026, 09:56 PM).

- Rab, Ajar Partner of Law Firm (2020) "Smart Contracts and Blockchain: The Panacea to the Unequal Bargaining Power of Consumers?," International Journal on Consumer Law and Practice: Vol. 8, Article 3, https://repository.nls.ac.in/ijclp/vol8/iss1/3 (last visited Mar. 28, 2026, 09:58 PM).

- Vidhisastras, How Smart Contracts Work Under Indian Law: Enforceability, Evidence and Compliance, VIDHISASTRAS (Dec. 26, 2025), https://vidhisastras.com/blog/how-smart-contracts-work-under-indian-law-enforceability-evidence-and-compliance/ (last visited Mar. 28, 2026, 09:59 PM).

- Architha Manikantan, Cross-Border E-Contracts: Jurisdictional Challenges in Online Transactions, PRIME LEGAL BLOG (Dec. 13, 2025), https://blog.primelegal.in/cross-border-e-contracts-jurisdictional-challenges-in-online-transactions/ (last visited Mar. 28, 2026, 10:00 PM).

- Aravindh, Smart Contracts in India - An Overview, KING STUBB & KASIVA (Sept. 9, 2024), https://ksandk.com/corporate/smart-contracts-in-india-an-overview/ (last visited Mar. 28, 2026, 10:00 PM).

- R. Thirushya, Electronic Contracts: Legal Frameworks and Challenges in the Digital Age, MANUPATRA ARTICLES (Oct. 09, 2024), https://articles.manupatra.com/article-details/Topic-ELECTRONIC-CONTRACTS-LEGAL-FRAMEWORKS-AND-CHALLENGES-IN-THE-DIGITAL-AGE (last visited Mar. 28, 2026, 10:02 PM).

- Aanchal Trivedi & Shilpi, Smart Contract: A New Paradigm of Contracts in the Digital Era, S&A LAW OFFICES, https://sandalawoffices.com/smart-contract-a-new-paradigm-of-contracts-in-the-digital-era/ (last visited Mar. 28, 2026, 10:04 PM).

- Dalila Djamane, Smart Contracts: Global Perspectives and Legal Realities — Part 2, DAILY JUS (Aug. 6, 2025), https://dailyjus.com/legal-tech/2025/08/smart-contracts-

global-perspectives-and-legal-realities-part-2 (last visited Mar. 28, 2026, 10:07 PM)

- Smart Contracts & Legal Disputes: Key Issues Explained, YOURTECHLEGAL, https://yourtechlegal.com/blog/138-2/ (last visited Mar. 28, 2026, 10:10 PM)

- Shunfang, Understanding Governing Law and Jurisdiction in International Contracts, ESIGN GLOBAL (Dec. 6, 2025), https://www.esignglobal.com/blog/determining-governing-law-jurisdiction-contract (last visited Mar. 28, 2026, 10:11 PM).

- IBL Partners, Legal Challenges in Defining and Regulating Smart Contracts, LINKEDIN PULSE (Nov. 5, 2024), https://www.linkedin.com/pulse/legal-challenges-defining-regulating-smart-contracts-iblpartners-qg6mc (last visited Mar. 28, 2026, 10:12 PM).

- Shaan Shaikh, Smart Contracts in the Eyes of the Law: Emerging Trends in India and Across Borders, LAWFUL LEGAL (June 22, 2025), https://lawfullegal.in/smart-contracts-in-the-eyes-of-the-law-emerging-trends-in-india-and-across-borders/ (last visited Mar. 28, 2026, 10:14 PM).

- Vartika, Smart Contract Laws in Different Countries: A Global Overview, NADCAB LABS (Jan. 22, 2026), https://www.nadcab.com/blog/smart-contract-laws-explained (last visited Mar. 28, 2026, 10:14 PM).