

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

The regulation and enforcement of contracts have always been central to the functioning of any legal system. In Nigeria, as in most common law jurisdictions, contract law is grounded in the principles inherited from English law, notably the doctrines of offer, acceptance, consideration, intention to create legal relations, capacity, and legality of purpose. These elements are reflected in Nigerian judicial decisions and statutory enactments such as the Sale of Goods Act 1893, which continues to apply in various states, and the Contracts Law of some former Eastern Region states.

Traditionally, contracts in Nigeria have been executed through written documents or oral agreements, supported by witnesses and sometimes notarisation. With the advent of information and communication technologies, however, the mode of contracting began to evolve. Electronic contracts, emails serving as evidence of acceptance, and online marketplaces gradually reshaped the landscape of commerce. Nigerian courts, though cautious, eventually recognised the enforceability of electronic evidence under the Evidence Act 2011, which expressly provides for the admissibility of computer-generated records and digital communications in sections 84 and 258. In cases such as *Kubor v. Dickson*, the Supreme Court affirmed that electronically generated documents can be admissible once they meet the statutory conditions.¹

Building upon this foundation, blockchain technology has introduced a new dimension to contractual relations. Unlike conventional contracts, smart contracts are self-executing codes

¹*Kubor v. Dickson* (2013) 4 NWLR (Pt. 1345) 534 (SC).

embedded in a blockchain, which automatically perform the obligations of the parties once pre-determined conditions are satisfied. The concept was first popularised in the 1990s by Nick Szabo, who described smart contracts as digital protocols designed to facilitate, verify, or enforce the performance of an agreement without the need for intermediaries.²

In commercial practice, smart contracts promise significant advantages. They eliminate the costs and delays associated with third-party enforcement, enhance transparency through immutable records, and provide security against manipulation. For example, a supply chain agreement coded into a blockchain could automatically release payments once delivery is confirmed through digital sensors. In the financial sector, decentralised finance (DeFi) platforms already employ smart contracts to facilitate peer-to-peer lending, insurance, and asset swaps without traditional banks.

However, the very features that make smart contracts attractive also raise difficult legal questions within the Nigerian context. Can an agreement expressed entirely in code satisfy the common law requirement of consensus ad idem, a meeting of the minds? How should courts interpret the parties' intentions where no natural language text exists? What happens where a smart contract, once deployed, produces unintended or unjust results due to coding errors or unforeseen circumstances? These questions strike at the heart of Nigerian contract law, which is still grounded in doctrines developed for human-negotiated agreements.

Further, the borderless nature of blockchain transactions creates jurisdictional and enforcement challenges. A smart contract executed on the Ethereum blockchain, for example, may involve a Nigerian buyer, a Kenyan seller, and computer nodes scattered across multiple continents. In the

²Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets" (1996) available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html accessed 3 September 2025

event of a dispute, which country's courts have jurisdiction, and which substantive law applies? Nigerian private international law, governed by common law rules and judicial precedents, was never designed to address such decentralised and automated relationships.

The background therefore reveals a tension: while smart contracts offer opportunities for commercial innovation in Nigeria, their enforceability under existing legal principles remains uncertain. This uncertainty poses risks for businesses, consumers, and the Nigerian economy at large. Unless the law adapts to provide clarity, Nigeria may find itself ill-equipped to regulate, adjudicate, or benefit from this emerging frontier of digital commerce.

1.2 Statement of the Problem

Contract law in Nigeria is founded on principles that emphasise human intention, communication, and mutual assent. The classical elements, offer, acceptance, consideration, capacity, legality, and intention to create legal relations, have been tested and refined in countless judicial decisions.³ These principles assume that contracts are formed through natural language (spoken or written words) and that disputes may be resolved by examining documentary or oral evidence of the parties' intentions.

Smart contracts challenge this traditional model. By design, they are not written in natural language but in programming code that is automatically executed when certain conditions are met. For example, a smart contract between two parties could be written to automatically transfer ownership of a digital asset once payment is received in cryptocurrency. Once deployed on a

³African Reinsurance Corp. v. AIM Consultants Ltd (2004) 11 NWLR (Pt. 883) 1 (SC).

blockchain, the code executes itself, often without human oversight. This automation raises several legal problems under Nigerian law.

First, there is the problem of consensus ad idem, the meeting of the minds. Nigerian courts have consistently held that for a contract to be binding, there must be clear evidence that the parties intended to enter into legal relations. In *Orient Bank (Nig.) Plc v. Bilante International Ltd*, the Court of Appeal stressed that a binding contract is formed only when offer and acceptance correspond and there is a genuine intention to be bound.⁴ With smart contracts, however, it is not always clear whether the parties understand or even read the underlying code. If a party assents to a smart contract through a digital platform without comprehending the technical details, can it be said that genuine consent exists?

Second, there is the issue of contract interpretation. Traditional contracts, though sometimes ambiguous, allow courts to interpret words, clauses, and intentions based on established rules of construction. With smart contracts, interpretation is limited to the code itself, which may not always reflect the commercial reality the parties envisioned. A coding error could, for example, release funds prematurely or permanently lock assets in an inaccessible blockchain address. Nigerian courts, untrained in computer programming, may struggle to determine liability or correct such mistakes.

Third, Nigerian law requires that contracts not founded on illegality or fraud are enforceable.⁵ Yet smart contracts are susceptible to being used for illicit purposes such as money laundering, terrorism financing, or fraudulent initial coin offerings (ICOs). The borderless and pseudonymous nature of blockchain transactions makes it difficult for regulators and law

⁴ *Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

⁵ *UBA Plc v. Ogundokun* (2009) 6 NWLR (Pt. 1138) 450 (CA).

enforcement agencies to trace parties' identities. This raises concerns about whether courts will enforce smart contracts tainted by illegality or fraud, and whether such enforcement would inadvertently legitimise unlawful activity.

Fourth, the rules of evidence pose practical problems. The Evidence Act 2011 permits the admission of computer-generated evidence under certain conditions.⁶ However, blockchain-based contracts raise questions of authenticity, authorship, and admissibility. If a dispute arises, who bears the burden of proving that a blockchain record is genuine, unaltered, and attributable to the parties? Nigerian courts have yet to address such questions directly, leaving a gap in judicial guidance.

Fifth, there is the jurisdictional challenge. Smart contracts are executed on decentralised platforms without regard to geographical boundaries. A contract between a Nigerian and a foreign party could be coded and executed on a blockchain platform hosted across thousands of nodes worldwide. Nigerian private international law, derived largely from common law precedents, was developed to address disputes involving identifiable territories, governing laws, and jurisdictions. It is uncertain whether these doctrines are flexible enough to accommodate disputes where no centralised place of contracting or performance exists.

Finally, there is regulatory uncertainty. While jurisdictions like the United States and the United Kingdom have begun to clarify the legal status of smart contracts, Nigeria has not enacted any specific legislation on the subject. The Central Bank of Nigeria (CBN) has issued circulars restricting cryptocurrency transactions in the banking sector, but it has not directly addressed the

⁶ Evidence Act 2011, ss. 84, 258

legal recognition of blockchain-based contracts. This regulatory vacuum creates uncertainty for businesses and investors seeking to leverage smart contracts for commercial activities in Nigeria.

In summary, the problem this study seeks to address is whether smart contracts, with their unique technological characteristics, can be reconciled with the requirements of Nigerian contract law and enforced by Nigerian courts. If enforceability is doubtful, what reforms, doctrinal, statutory, or regulatory, are necessary to provide certainty, promote innovation, and protect commercial actors in Nigeria?

1.3 Research Questions

Every meaningful legal inquiry is anchored on specific questions that guide the direction of analysis. In examining the enforceability of smart contracts under Nigerian law, the central concern is whether such contracts can fit within the established doctrinal framework of Nigerian contract law, and if not, how the law might evolve to accommodate them. From this central concern, a number of subsidiary questions arise.

The first question is whether smart contracts, which are written and executed entirely in computer code, can satisfy the fundamental elements of a valid contract as recognised in Nigeria. Offer, acceptance, consideration, intention to create legal relations, capacity, and legality are cornerstones of enforceability. Nigerian courts have repeatedly emphasised these elements as indispensable. For instance, in *B. J. Export & Chemical Co. Ltd v. Kaduna Petro-Chemical Co. Ltd*, the Court of Appeal affirmed that a valid contract cannot exist in the absence of consensus between the parties.⁷ The issue, therefore, is whether clicking an icon, initiating a blockchain

⁷*B. J. Export & Chemical Co. Ltd v. Kaduna Petro-Chemical Co. Ltd* (2003) 13 NWLR (Pt. 837) 305 (CA).

transaction, or deploying a coded agreement constitutes the kind of consensus contemplated by Nigerian law.

A second research question is whether Nigerian evidentiary rules are sufficient to support the enforcement of smart contracts. Although the Evidence Act 2011 recognises electronic records, its application to blockchain data remains untested in Nigerian jurisprudence. Would Nigerian courts accept blockchain ledgers as self-authenticating records, or would additional proof be required to establish their validity? This question is critical because, without reliable evidentiary foundations, even a theoretically valid smart contract may prove unenforceable in practice.

The third question concerns the extent to which Nigerian regulatory institutions are prepared to address the peculiar risks of smart contracts. The Central Bank of Nigeria (CBN), the Securities and Exchange Commission (SEC), and the Nigerian Communications Commission (NCC) are all stakeholders in the digital economy. Yet their policies often focus narrowly on cryptocurrencies or fintech operations without explicitly addressing the broader question of blockchain-based contracts. The research must therefore ask whether existing regulations provide adequate consumer protection, fraud prevention, and dispute resolution mechanisms for smart contracts in Nigeria.

Another research question relates to the jurisdictional dimension. Because smart contracts operate on decentralised platforms across multiple borders, disputes arising from them often defy conventional rules of private international law. Nigerian courts may be confronted with cases involving parties in different countries, coded agreements deployed on global platforms, and obligations performed digitally without a territorial nexus. The question is whether Nigerian

conflict-of-law rules are adaptable enough to handle such disputes or whether legislative intervention is required.

Finally, the study must ask what lessons Nigeria can learn from comparative jurisdictions such as the United States, the United Kingdom, and the European Union. These jurisdictions have begun to experiment with legal recognition of blockchain records and smart contracts. By studying their approaches, Nigeria may find a basis for legal reform that balances innovation with consumer protection.

Taken together, these questions aim to uncover the extent to which Nigerian law is prepared, or unprepared, to recognise and enforce smart contracts, and what reforms are necessary to close the identified gaps.

1.4 Objectives of the Study

The purpose of this study is to critically examine the enforceability of smart contracts within the Nigerian legal framework, with a particular emphasis on their commercial and jurisdictional implications. The overarching objective is to determine whether the principles of Nigerian contract law, as currently applied by courts and recognised by statutes, are capable of accommodating the novel features of smart contracts, or whether reform is required to ensure legal certainty.

One objective of the study is to evaluate the compatibility of smart contracts with the traditional elements of contract formation under Nigerian law. This requires a close examination of whether automated agreements, written and executed entirely in code, can meet the requirements of offer, acceptance, consideration, capacity, intention to create legal relations, and legality of purpose.

By interrogating these elements in the context of blockchain transactions, the study seeks to establish whether Nigerian courts are likely to recognise such agreements as binding and enforceable.

A second objective is to assess the adequacy of existing evidentiary rules in Nigeria in relation to smart contracts. While the Evidence Act 2011 makes provision for the admissibility of electronic records, the practical application of these provisions to blockchain data remains uncertain. This study aims to determine whether blockchain records, given their immutability and decentralised nature, can be reliably admitted in Nigerian courts, and what additional safeguards may be necessary to ensure fairness and accuracy in adjudication.

A further objective is to analyse the regulatory environment in Nigeria as it relates to smart contracts. The Central Bank of Nigeria, the Securities and Exchange Commission, and other relevant institutions have adopted cautious approaches towards blockchain and cryptocurrency transactions. However, they have not provided a comprehensive framework for smart contracts. This study therefore aims to explore whether the current regulatory posture adequately addresses issues of consumer protection, fraud, illegality, and technological determinism, or whether specific reforms are required.

Another objective is to investigate the jurisdictional and conflict-of-law challenges that smart contracts pose for Nigerian courts. Given the global and decentralised nature of blockchain transactions, the study seeks to determine whether Nigeria's existing rules of private international law are sufficient to resolve cross-border disputes involving smart contracts, or whether legislative innovation is needed to address these jurisdictional complexities.

Finally, this study aims to draw lessons from comparative jurisdictions that have made progress in recognising and regulating smart contracts. By analysing approaches in the United States, the United Kingdom, and the European Union, the research intends to provide Nigeria with possible models for reform. These comparative insights will be used to develop concrete recommendations for improving the enforceability of smart contracts under Nigerian law.

Taken together, these objectives are directed not only at resolving theoretical questions of enforceability but also at providing practical guidance for policymakers, courts, businesses, and consumers who will inevitably interact with smart contracts as digital commerce continues to expand in Nigeria.

1.5 Significance of the Study

The significance of this study lies in its potential to bridge a critical gap between emerging technological realities and the Nigerian legal system. As commerce continues to migrate from traditional paper-based transactions to digital platforms, the law must adapt to provide certainty, predictability, and fairness. Smart contracts, self-executing agreements embedded in blockchain technology, represent the next phase of this evolution, yet Nigerian law has not squarely confronted their implications.

Academically, the study contributes to the growing body of literature on the interface between law and technology in Nigeria. Much of the existing scholarship has focused narrowly on cryptocurrency regulation, fintech innovation, or data protection. Very little attention has been devoted to the specific question of whether smart contracts are legally enforceable under Nigerian contract law. By addressing this gap, the study not only enriches Nigerian legal

scholarship but also provides a foundation for further academic research on digital contracts, blockchain governance, and cyber-law.

For the judiciary, the study is significant because Nigerian courts will inevitably be called upon to adjudicate disputes arising from smart contracts. Judges trained in classical contract doctrines may find it difficult to apply traditional principles to coded agreements, especially where technical issues like coding errors, automated performance, or blockchain immutability arise. By identifying the doctrinal and evidentiary challenges posed by smart contracts, this study will equip judges with analytical frameworks that can guide decision-making and ensure consistency in the administration of justice.

From the perspective of policymakers and regulators, the study provides critical insights into the gaps and ambiguities in Nigeria's current legal and institutional framework. The Central Bank of Nigeria, for instance, has taken a restrictive stance towards cryptocurrency transactions, directing financial institutions to avoid dealing in virtual currencies.⁸ The Securities and Exchange Commission has issued guidelines on digital assets and initial coin offerings, but these focus on investor protection rather than on the enforceability of smart contracts as legal agreements. This study highlights the need for a coherent regulatory response that balances innovation with consumer protection and provides certainty for businesses engaging with smart contracts.

The commercial significance of the study is equally profound. Nigerian businesses, particularly in the banking, insurance, supply chain, and fintech sectors, stand to benefit immensely from the efficiency and transparency of smart contracts. Yet without clear legal rules, companies may be

⁸Central Bank of Nigeria, "Letter to Deposit Money Banks, Non-Bank Financial Institutions and Other Financial Institutions on Cryptocurrency Operations in Nigeria" (CBN/GEN/DIR/INT/CIR/001/013, 5 February 2021).

reluctant to adopt such technologies for fear that disputes will not be enforceable in Nigerian courts. By clarifying the enforceability question, the study promotes commercial confidence, encourages investment, and enhances Nigeria's competitiveness in the global digital economy.

For consumers, the study is significant because it addresses issues of trust, fairness, and protection in digital transactions. Smart contracts, while efficient, are vulnerable to coding errors, fraud, and exploitation. A clear legal framework ensures that consumers are not left at the mercy of technological determinism but are instead safeguarded by accessible remedies and effective enforcement mechanisms.

Finally, the significance of this study extends to Nigeria's aspiration to integrate into the global digital economy. Comparative jurisdictions such as the United States, United Kingdom, and European Union have already begun to recognise and regulate smart contracts. Unless Nigeria takes proactive steps to clarify their enforceability, it risks being left behind in the global race for technological innovation. By recommending reforms grounded in comparative insights, this study seeks to position Nigeria as a jurisdiction that is both open to innovation and committed to the rule of law.

In sum, the study is significant for academics, the judiciary, regulators, businesses, consumers, and the Nigerian economy at large. It offers both theoretical contributions to the understanding of contract law in the digital age and practical solutions for ensuring that Nigeria can harness the opportunities of smart contracts while mitigating their risks.

1.6 Scope and Limitations

The scope of this study is defined by its focus on the enforceability of smart contracts within the Nigerian legal system, with particular emphasis on commercial and jurisdictional challenges.

The research is primarily doctrinal in nature, interrogating statutes, judicial decisions, and scholarly writings to determine whether smart contracts can be reconciled with the fundamental principles of Nigerian contract law.

Substantively, the study is limited to the law of contract, evidence, and related aspects of private international law. It examines how Nigerian courts, applying doctrines of offer, acceptance, consideration, and intention to create legal relations, would approach disputes involving smart contracts. It also considers the evidentiary challenges that arise when parties attempt to rely on blockchain-based records in court. Furthermore, the study evaluates the jurisdictional implications of smart contracts, given their decentralised and borderless nature, and assesses whether Nigerian conflict-of-law rules are capable of addressing these complexities.

Geographically, the research is limited to Nigeria, though comparative references will be made to other jurisdictions such as the United States, the United Kingdom, and the European Union. These comparative insights are employed not for their own sake but to provide Nigeria with possible models for reform. For example, the UK Jurisdiction Taskforce's legal statement on smart contracts and crypto-assets offers an instructive example of how common law principles may be adapted to technological innovations. Similarly, the legislative experiments of U.S. states such as Arizona and Nevada illustrate possible approaches to statutory recognition.

The study is also limited in its treatment of blockchain technology. While blockchain has numerous applications, ranging from digital currencies and decentralised finance (DeFi) to supply chain tracking and voting systems, this research confines itself to its application in smart

contracts as a legal phenomenon. It does not attempt to provide a comprehensive technical account of blockchain systems but instead engages with them only to the extent necessary for legal analysis.

In terms of commercial scope, the study concentrates on areas most likely to be affected by the adoption of smart contracts in Nigeria, including banking, insurance, supply chain management, and digital commerce. However, it does not delve into highly specialised sectors such as securities tokenisation, decentralised autonomous organisations (DAOs), or cross-border taxation, except insofar as they illustrate broader legal principles.

Methodologically, the research is limited by the scarcity of Nigerian judicial decisions directly addressing smart contracts. As of the date of this writing, Nigerian courts have not been called upon to resolve disputes arising specifically from blockchain-based agreements. Consequently, the analysis is necessarily speculative in certain respects, drawing on analogous cases in contract and evidence law, as well as comparative jurisprudence. This limitation underscores the importance of the study, as it highlights the urgent need for doctrinal clarity and legislative reform before such disputes arise in practice.

Another limitation lies in the rapidly evolving nature of technology. Blockchain protocols, programming languages, and regulatory responses change at a pace that often outstrips legal scholarship. This study therefore represents a snapshot in time and cannot claim to anticipate every future development. Nevertheless, by grounding its analysis in enduring principles of contract law and comparative insights, the study seeks to provide guidance that remains relevant even as technology advances.

In summary, the scope of this study is confined to Nigerian contract law, evidence law, and private international law as they relate to smart contracts, with a focus on commercial applications. Its limitations include the absence of Nigerian case law on smart contracts, the exclusion of non-contractual applications of blockchain, and the dynamic nature of technological developments. These boundaries are necessary to maintain analytical clarity and ensure that the study's objectives are realistically achievable within the confines of a final-year research project.

1.7 Research Methodology

Every research project is shaped by its methodology, which determines how data is gathered, analysed, and interpreted. In legal research, methodology is particularly important because the law is both a normative and interpretative discipline: it not only describes existing rules but also evaluates their adequacy and recommends reforms. This study adopts a doctrinal and comparative legal methodology, supplemented by elements of normative analysis, in order to address the enforceability of smart contracts under Nigerian law.

The doctrinal approach, sometimes described as “black-letter law” methodology, focuses on the systematic exposition of legal rules and principles. In the context of this research, the doctrinal method involves a close reading and analysis of Nigerian statutes, case law, and regulatory instruments relevant to contract formation, evidence, and jurisdiction. For instance, the Evidence Act 2011 is examined to determine how digital records may be admitted in Nigerian courts, while judicial decisions such as *Kubor v. Dickson* are analysed to illustrate how Nigerian courts have dealt with electronically generated evidence.⁹ Similarly, case law on contract formation, such as *Orient Bank (Nig.) Plc v. Bilante International Ltd*, is interrogated to determine whether

⁹ *Kubor v. Dickson* (2013) 4 NWLR (Pt. 1345) 534 (SC).

automated agreements can satisfy the requirements of consensus ad idem and intention to create legal relations.¹⁰

The doctrinal method is particularly suitable for this study because smart contracts, though technologically novel, must ultimately be assessed against the existing framework of Nigerian law. By systematically analysing statutes and judicial precedents, the research seeks to answer whether smart contracts can be enforced under current legal principles, or whether reform is necessary.

Alongside doctrinal analysis, the study employs a comparative methodology. Given the absence of Nigerian case law directly addressing smart contracts, it is necessary to look to other jurisdictions for guidance. The United States provides a rich laboratory of legislative experiments, with states such as Arizona, Nevada, and Tennessee enacting laws that explicitly recognise blockchain records and smart contracts as legally enforceable. The United Kingdom, through the UK Jurisdiction Taskforce's Legal Statement on Crypto-assets and Smart Contracts (2019), has affirmed that English common law is capable of recognising such agreements. The European Union, meanwhile, has developed regulatory frameworks for blockchain applications through initiatives such as the European Blockchain Services Infrastructure. By examining these comparative experiences, the study identifies possible models that Nigeria can adapt to its own legal and commercial environment.

In addition, the study incorporates elements of normative and policy analysis. While doctrinal research clarifies what the law is, normative analysis asks what the law ought to be. This dimension is important because, in the absence of direct Nigerian authority on smart contracts,

¹⁰ *Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

the study must evaluate whether existing doctrines are adequate or whether reforms are necessary. For instance, should Nigeria adopt specific legislation recognising blockchain-based agreements? Should the Evidence Act 2011 be amended to expressly provide for blockchain records? Should regulators such as the Central Bank of Nigeria and the Securities and Exchange Commission issue guidelines addressing consumer protection in smart contracts? These are normative questions that go beyond mere doctrinal description.

The study relies primarily on secondary sources, including textbooks, journal articles, policy papers, and online legal resources. Statutory texts such as the Evidence Act 2011 and relevant judicial decisions provide the foundation for doctrinal analysis. Comparative materials are drawn from statutes, reports, and case law in other jurisdictions, while normative insights are developed from academic commentary and policy-oriented literature.

The methodology is subject to certain limitations. First, there is limited Nigerian judicial authority on smart contracts, which means the study must rely heavily on analogies from traditional contract and evidence law. Second, the fast-evolving nature of blockchain technology means that the analysis represents a snapshot in time and may require updating as technology and regulation develop. Third, as a library-based research project, the study does not employ empirical methods such as interviews or field surveys, although it occasionally draws on policy statements from regulators such as the Central Bank of Nigeria.

Despite these limitations, the combination of doctrinal, comparative, and normative methodologies ensures that the study is both rigorous and forward-looking. It provides an accurate account of the current position of Nigerian law, situates that position within a broader international context, and offers policy recommendations for reform.

1.8 Structure of the Study

This study is divided into five chapters, each logically building upon the other to provide a comprehensive analysis of the enforceability of smart contracts under Nigerian law. The structure is deliberately designed to move from general conceptual discussions to specific legal analysis, and finally, to conclusions and recommendations.

Chapter One introduces the study. It sets out the background to the research, identifies the problem to be addressed, and frames the research questions, objectives, significance, and limitations. It also explains the methodology adopted and outlines the structure of the work. In this way, the first chapter lays the foundation for the entire research.

Chapter Two provides a review of relevant literature and establishes the conceptual and theoretical framework of the study. It begins with an exposition of the concept of smart contracts, their historical development, and key features. It then examines scholarly debates on the legal nature of smart contracts, identifying the theories that have been advanced to explain their enforceability. The chapter concludes by highlighting gaps in existing literature, thereby situating the contribution of this research within the broader academic discourse.

Chapter Three turns to the Nigerian legal and regulatory framework. It begins with an overview of Nigerian contract law and examines how existing legal doctrines apply to smart contracts. Particular attention is paid to the statutory requirements for enforceability under Nigerian law, including offer, acceptance, and consideration. The chapter also analyses the Evidence Act 2011 on the admissibility of digital evidence, and considers comparative perspectives from the UK, US, and EU. It concludes by assessing how Nigerian institutions and courts have begun, if at all, to respond to the rise of blockchain-based agreements.

Chapter Four examines the commercial and jurisdictional challenges associated with smart contracts in Nigeria. It analyses tensions between contractual autonomy and technological determinism, and evaluates practical problems such as dispute resolution, cross-border jurisdiction, privity of contract, and identity verification. Issues of fraud, mistake, illegality, regulatory uncertainty, and consumer protection are also addressed. The chapter then considers existing and proposed enforcement mechanisms, both judicial and technological, to determine how disputes arising from smart contracts may be effectively resolved.

Chapter Five summarises the key findings of the research and draws conclusions. It highlights the practical and doctrinal challenges that hinder the enforceability of smart contracts under Nigerian law, and makes recommendations for reform. These include legislative interventions, judicial approaches, and regulatory measures to ensure that Nigerian law is capable of accommodating the realities of blockchain-based agreements. The chapter also identifies areas for further research, given the evolving nature of technology and regulation in this field.

By structuring the study in this way, the research ensures a logical flow: beginning with a general introduction, moving to conceptual foundations, analysing Nigerian law, addressing specific challenges, and finally, offering conclusions and recommendation.

CHAPTER TWO

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

2.1 Concept of Smart Contracts

The term smart contract is one of the most frequently invoked yet often misunderstood concepts in discussions about blockchain technology and the future of digital commerce. At its simplest, a smart contract is a computer code designed to automatically execute, control, or document legally relevant events and actions according to the terms of a contract. The concept was first introduced by Nick Szabo in the 1990s, who described smart contracts as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises.”¹¹ His vision was to harness computer protocols to enforce contractual obligations, thereby reducing reliance on intermediaries such as lawyers and courts.

In practice, smart contracts are typically deployed on blockchain platforms, most notably Ethereum, where self-executing code can automatically transfer digital assets once specified conditions are met. For example, a smart contract may be programmed to release payment once goods are delivered and verified on the blockchain. This feature has led many to describe smart contracts as “trustless” systems, in the sense that they reduce or eliminate the need for trust between contracting parties.¹²

However, despite their name, smart contracts are not necessarily “contracts” in the strict legal sense. The “smart” component refers to their automation and technical sophistication, while their

¹¹ Nick Szabo, “Smart Contracts” (1994) available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html accessed 3 September 2025.

¹² Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018) 71.

“contractual” nature depends on whether they meet the traditional legal requirements of contract formation, offer, acceptance, consideration, and intention to create legal relations.¹³ In some cases, smart contracts may operate merely as pieces of software code with no legal significance unless embedded within or linked to a traditional written agreement. In other cases, particularly where parties intend the code itself to constitute their agreement, the issue arises as to whether courts can and should enforce such arrangements.

Scholars have identified multiple forms of smart contracts.¹⁴ Some are embedded contracts, where the smart contract is linked to a traditional contract that governs the parties’ relationship but automates performance of certain aspects. Others are stand-alone smart contracts, where the entire agreement is expressed and executed in code. Still others are hybrid models, combining legal prose with automated code to capture both human and machine-readable obligations. The significance of these distinctions is that enforceability may vary depending on whether the code is intended to supplement, replace, or coexist with traditional contractual documents.

The literature also distinguishes between the technological concept of smart contracts and the legal concept. From a technological perspective, a smart contract is simply a piece of blockchain code designed to execute automatically when certain conditions are met. From a legal perspective, however, a smart contract is enforceable only if it satisfies the doctrines of contract law in the relevant jurisdiction. This duality explains why commentators such as Werbach and Cornell argue that “smart contracts are neither particularly smart nor necessarily contracts,” but instead represent a new mechanism for enforcing promises.¹⁵

¹³ Chikosa Banda, “Smart Contracts and Contract Law: Reconciling Code with Legal Principles” (2020) 44(2) *Journal of African Law* 123, 127.

¹⁴ Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 69–73.

¹⁵ Kevin Werbach and Nicolas Cornell, “Contracts Ex Machina” (2017) 67(2) *Duke Law Journal* 313, 322.

Importantly, the concept of smart contracts cannot be divorced from the broader theory of contract as an instrument of private ordering. The law of contract has long been understood as the mechanism by which individuals create binding obligations between themselves, with the state providing enforcement through courts. Smart contracts, by contrast, attempt to bypass or supplement the role of the state by making performance automatic. This creates both opportunities (in terms of efficiency, certainty, and cost reduction) and challenges (in terms of fairness, consent, and remedies).

In the Nigerian context, the concept of smart contracts is still nascent. There is little doctrinal or judicial commentary, and regulators have largely focused on cryptocurrencies rather than blockchain applications in general. Nevertheless, the conceptualisation of smart contracts is critical for Nigerian legal scholars and policymakers, since the extent to which such agreements are enforceable will depend on how they are understood: as mere software tools, as evidence of a contract, or as legally binding contracts in themselves.

2.2 Historical Development and Evolution of Smart Contracts

The idea of smart contracts did not emerge fully formed with the advent of blockchain technology. Rather, it has developed gradually over the past three decades, shaped by advances in computer science, cryptography, and digital commerce. Understanding this historical trajectory is essential because it highlights the intellectual roots of smart contracts, as well as the technical and legal challenges that continue to define their enforceability.

The earliest articulation of smart contracts is credited to Nick Szabo, a computer scientist and legal theorist, who in the 1990s envisaged a future where contractual performance could be

automated through computer protocols.¹⁶ Szabo drew an analogy with everyday mechanisms such as vending machines, which execute a simple form of self-enforcing agreement: once money is inserted and verified, the machine automatically dispenses goods, without requiring human intervention or legal enforcement.¹⁷ He theorised that digital technologies could enable more complex forms of such automated agreements, thereby reducing reliance on courts and intermediaries.

Despite Szabo's visionary proposal, the implementation of smart contracts in the 1990s was constrained by technological limitations. The internet at the time lacked secure decentralised systems capable of ensuring trust between anonymous parties. Centralised platforms could automate certain transactions, but they could not guarantee immutability or resistance to manipulation. Consequently, smart contracts remained largely theoretical until the emergence of blockchain technology.

The launch of Bitcoin in 2009 marked a turning point. While Bitcoin itself was designed primarily as a peer-to-peer electronic cash system, its underlying blockchain architecture provided a decentralised and tamper-resistant ledger that could potentially host programmable agreements.¹⁸ However, Bitcoin's scripting language was deliberately limited, restricting its use for more complex contracts.

The real breakthrough came with the development of Ethereum in 2015, a blockchain platform specifically designed to support decentralised applications and smart contracts. Ethereum introduced the Ethereum Virtual Machine (EVM), a decentralised computing environment

¹⁶ Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets" (1996) available at http://szabo.best.vwh.net/smart_contracts_2.html accessed 3 September 2025.

¹⁷ Ibid.

¹⁸ Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) available at <https://bitcoin.org/bitcoin.pdf> accessed 3 September 2025.

capable of executing code across thousands of nodes. This allowed developers to write self-executing contracts in programming languages such as Solidity, enabling complex agreements to be automated without reliance on a central authority.¹⁹ Ethereum thus transformed smart contracts from an abstract concept into a practical reality, sparking a wave of experimentation in areas such as decentralised finance (DeFi), supply chain management, and digital identity.

Since then, the evolution of smart contracts has been closely tied to broader developments in blockchain technology. The emergence of second- and third-generation blockchains, such as Cardano, Polkadot, and Solana, has sought to improve scalability, interoperability, and energy efficiency. These advancements expand the potential uses of smart contracts but also introduce new legal challenges, particularly with respect to jurisdiction, regulatory oversight, and consumer protection.

At the same time, smart contracts have increasingly attracted the attention of governments, regulators, and scholars. In the United States, several states, including Arizona and Nevada, have enacted legislation recognising smart contracts and blockchain records as legally enforceable.²⁰ In the United Kingdom, the UK Jurisdiction Taskforce issued its 2019 Legal Statement on Crypto-assets and Smart Contracts, affirming that English common law is sufficiently flexible to accommodate such agreements.²¹ In the European Union, initiatives such as the Markets in Crypto-assets Regulation (MiCA) and the European Blockchain Services

¹⁹ Gavin Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger” (2014) Ethereum Project Yellow Paper <https://ethereum.github.io/yellowpaper/paper.pdf> accessed 3 September 2025.

²⁰ Arizona Revised Statutes §44-7061 (2017); Nevada Revised Statutes §719.090 (2017)

²¹ UK Jurisdiction Taskforce, *Legal Statement on Crypto-assets and Smart Contracts* (2019) 5–6.

Infrastructure reflect a policy-level commitment to integrating blockchain technologies into commerce and governance.

In Nigeria, however, the development has been much slower. Regulatory attention has focused primarily on cryptocurrencies, particularly with the Central Bank of Nigeria's (CBN) circulars restricting financial institutions from facilitating cryptocurrency transactions.²² While these measures reflect caution about financial stability and consumer risks, they also indirectly affect the environment in which smart contracts may be adopted. Nigerian legal discourse on smart contracts remains sparse, underscoring the need for academic engagement with both the theoretical foundations and practical challenges of their enforceability.

In summary, the historical development of smart contracts can be divided into three phases: (1) Szabo's early theoretical conception in the 1990s; (2) the emergence of blockchain technology through Bitcoin, which provided the infrastructure for decentralised trust; and (3) the practical implementation of smart contracts through platforms like Ethereum, followed by continuing innovation and regulatory responses worldwide. Each phase reveals both the potential and the limitations of smart contracts, and together they provide the backdrop against which Nigerian law must now grapple with their enforceability.

2.3 Key Features and Types of Smart Contracts

Smart contracts are defined not only by their theoretical foundations or historical development, but also by their unique features that distinguish them from traditional contracts. Understanding

²² Central Bank of Nigeria, "Letter to Deposit Money Banks, Non-Bank Financial Institutions, and Other Financial Institutions on Cryptocurrency Transactions" (5 February 2021) Ref. BSD/DIR/GEN/LAB/14/001.

these features is essential because they illuminate both the benefits and risks of smart contracts, as well as the reasons why their enforceability under Nigerian law raises commercial and jurisdictional challenges.

A. Key Features of Smart Contracts

1. **Automation and Self-Execution:** The most fundamental feature of a smart contract is that it is self-executing. Once programmed conditions are satisfied, the contract automatically performs the agreed-upon action without further input from the parties. For example, a smart contract governing a loan may automatically transfer collateral to the lender if the borrower fails to repay on time. This reduces reliance on courts or third-party enforcers.²³
2. **Immutability:** Because smart contracts are typically deployed on blockchains, they inherit the immutability of the ledger. Once recorded, the code cannot easily be altered or tampered with. While this promotes certainty and security, it also raises problems: if the contract contains an error, or if circumstances change, modifying the code is difficult and sometimes impossible without creating a new contract.²⁴
3. **Decentralisation:** Smart contracts operate on decentralised networks, meaning no single authority controls execution. This reduces risks associated with centralized intermediaries but also complicates questions of jurisdiction and legal accountability. Parties in different

²³ Aaron Wright and Primavera De Filippi, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia” (2015) 5 *SSRN Electronic Journal* 1, 12.

²⁴ Max Raskin, “The Law and Legality of Smart Contracts” (2017) 1 *Georgetown Law Technology Review* 305, 311.

jurisdictions may interact through code without clear legal oversight.²⁵

4. **Transparency and Verifiability:** Most public blockchains allow participants to inspect smart contract code and verify execution. This transparency can enhance trust, but it also raises privacy concerns, especially where commercially sensitive information is exposed on public ledgers.²⁶
5. **Trust Minimisation:** A recurring theme in blockchain discourse is that smart contracts reduce the need for trust between contracting parties. Instead of relying on the integrity of individuals or institutions, parties rely on code and cryptography. This has been described as shifting from “trust in people” to “trust in technology.”²⁷
6. **Borderlessness:** Smart contracts are inherently transnational, operating across borders without regard to territorial boundaries. While this expands commercial opportunities, it simultaneously generates complex jurisdictional issues regarding applicable law, forum selection, and enforcement.²⁸

B. Types of Smart Contracts

Scholars and practitioners have categorised smart contracts into different types based on their structure and function.

²⁵ Henry Gabriel, “Smart Contracts and Their Application in International Commercial Transactions” (2019) 24(1) *Uniform Law Review* 155, 160.

²⁶ Michele Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2019) 89.

²⁷ Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018) 84.

²⁸ Larry A. DiMatteo, “Smart Contracts and Contract Law: Reconciling Innovation and Tradition” (2019) 21(2) *SMU Science and Technology Law Review* 277, 280.

1. Basic Smart Contracts

These are simple “if-then” coded agreements that execute straightforward instructions (e.g., releasing payment once goods are delivered). They mirror Szabo’s original conception and are widely used in decentralised finance (DeFi).²⁹

2. Hybrid Smart Contracts

Hybrid contracts combine traditional legal agreements with blockchain-based automation. For instance, the main contract may be expressed in natural language, while a smart contract automates certain performance aspects such as payment or verification. This dual nature ensures legal enforceability while taking advantage of automation.³⁰

3. Decentralised Autonomous Organisation (DAO) Contracts

At the more complex end of the spectrum are DAOs, which operate entirely through smart contracts and allow decentralised governance by token-holders. DAOs represent an attempt to replace traditional corporate structures with blockchain-based governance. However, they raise serious regulatory and legal challenges, as illustrated by the collapse of “The DAO” in 2016 following a code exploit.³¹

4. Smart Legal Contracts

The UK Jurisdiction Taskforce and subsequent literature distinguish between smart

²⁹ Nick Szabo, “Smart Contracts: Building Blocks for Digital Markets” (1996) available at http://szabo.best.vwh.net/smart_contracts_2.html accessed 3 September 2025.

³⁰ Christopher Clack, Vikram Bakshi, and Lee Braine, “Smart Contract Templates: Foundations, Design Landscape and Research Directions” (2016) 5 *arXiv preprint arXiv:1608.00771* 7.

³¹ Philipp Paech, “The Governance of Blockchain Financial Networks” (2017) 80 *Modern Law Review* 1073, 1082.

contracts in general and smart legal contracts.³²The latter are agreements that satisfy traditional legal requirements of contract formation but are expressed, in whole or in part, through computer code. This concept is particularly important in bridging the gap between legal enforceability and technical execution.

C. Relevance of Features and Types for Enforceability

The features and types of smart contracts have direct implications for enforceability under Nigerian law. Their automation challenges the traditional judicial role in enforcing performance, since disputes may arise after execution has already occurred. Their immutability conflicts with contract doctrines allowing for rescission or variation. Their decentralisation and borderless nature complicate jurisdiction and applicable law, particularly under Nigeria's rules of private international law. Similarly, the distinction between basic, hybrid, DAO, and smart legal contracts highlights that not all smart contracts will raise the same enforceability challenges: hybrid and smart legal contracts may align more closely with Nigerian legal principles, while purely code-based agreements may be harder to reconcile.

2.4 Legal Nature and Recognition of Smart Contracts

A central question in the discourse on smart contracts is whether they qualify as legally binding contracts or whether they should be treated as mere technological tools. The answer to this question is critical for their enforceability under Nigerian law because only agreements that

³² UK Jurisdiction Taskforce, *Legal Statement on Crypto-assets and Smart Contracts* (2019) 6.

satisfy the requirements of contract formation and validity can attract judicial recognition and enforcement.

A. The Doctrinal Debate: Are Smart Contracts “Contracts”?

There is considerable scholarly debate over whether smart contracts, by their very nature, can be considered “contracts.” On one hand, proponents argue that smart contracts are capable of embodying the essential elements of contract law: offer, acceptance, consideration, and intention to create legal relations.³³ For example, a party may code an offer into a smart contract, another party may manifest acceptance by interacting with the code, consideration may be provided in the form of cryptocurrency or other digital assets, and intention to create legal relations may be inferred from the nature of the transaction.

On the other hand, critics argue that many smart contracts are simply pieces of computer code without the normative force of a legal agreement.³⁴ For instance, when an agreement is expressed solely in code, parties may lack a clear understanding of its terms, raising concerns about informed consent. Furthermore, the rigid automation of smart contracts may prevent recognition of doctrines such as mistake, duress, or frustration, which are central to contract law’s concern with fairness.

B. Legal Recognition in Common Law Jurisdictions

Common law jurisdictions have generally taken a functional approach, suggesting that smart contracts can be legally recognised provided they meet the ordinary requirements of contract law.

In the United States, for example, the Uniform Electronic Transactions Act (UETA) and the

³³Larry A. DiMatteo, “Smart Contracts and Contract Law: Reconciling Innovation and Tradition” (2019) 21(2) *SMU Science and Technology Law Review* 277, 283.

³⁴Kevin Werbach and Nicolas Cornell, “Contracts Ex Machina” (2017) 67(2) *Duke Law Journal* 313, 322.

federal Electronic Signatures in Global and National Commerce Act (E-SIGN Act) provide that contracts should not be denied legal effect merely because they are in electronic form.³⁵ Several states, including Arizona, Nevada, and Tennessee, have gone further by enacting statutes explicitly recognising the enforceability of blockchain-based contracts.³⁶

In the United Kingdom, the UK Jurisdiction Taskforce issued a landmark Legal Statement on Crypto-assets and Smart Contracts (2019), affirming that smart contracts are capable of forming valid contracts under English law.³⁷ It concluded that the common law's flexibility enables it to adapt to technological innovations, provided that the traditional requirements of contract formation are satisfied.

Similarly, courts in some jurisdictions have implicitly recognised the enforceability of blockchain-based arrangements. In *AA v. Persons Unknown* (2019), the English High Court treated Bitcoin as property capable of being the subject of a proprietary injunction, thereby implicitly acknowledging the legal significance of blockchain transactions.³⁸

C. Nigerian Law and Smart Contracts

In Nigeria, there is currently no statute or judicial decision that expressly addresses smart contracts. However, the recognition of electronic agreements under existing law provides a doctrinal pathway. Section 84 of the Evidence Act 2011 expressly provides for the admissibility of electronically generated evidence, while the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 affirms the legal validity of electronic signatures and records.³⁹ In *Kubor v. Dickson*, the

³⁵Uniform Electronic Transactions Act 1999 (UETA); Electronic Signatures in Global and National Commerce Act 2000 (E-SIGN Act).

³⁶Arizona Revised Statutes §44-7061 (2017); Tennessee Code Annotated §47-10-202 (2018).

³⁷UK Jurisdiction Taskforce, *Legal Statement on Crypto-assets and Smart Contracts* (2019) 8–9.

³⁸*AA v. Persons Unknown* [2019] EWHC 3556 (Comm).

³⁹Evidence Act 2011, s.84; Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s.17.

Supreme Court recognised the admissibility of computer-generated evidence, thereby reinforcing the principle that digital transactions are not excluded from legal recognition.⁴⁰

The broader question is whether Nigerian contract law, rooted in common law principles, can accommodate agreements expressed entirely or partially in code. Nigerian courts have traditionally applied the doctrines of offer, acceptance, consideration, and intention to create legal relations strictly.⁴¹ Thus, the enforceability of a smart contract will likely depend on whether the court is satisfied that these elements are present. For hybrid smart contracts, where legal prose is combined with automated code, this requirement may be easier to satisfy. For purely code-based agreements, however, the lack of human-readable terms may complicate judicial recognition.

D. Theories of Legal Nature

Three main theories have been advanced to explain the legal nature of smart contracts:

1. The Code as Contract Theory

This view holds that the code itself constitutes the contract.⁴² The parties agree to be bound by whatever outcome the code produces, and the legal system should recognise this intention. This theory emphasises autonomy and technological determinism but risks ignoring doctrines of fairness.

2. The Code as Performance Theory

According to this theory, the legal contract exists in prose, while the smart contract

⁴⁰*Kubor v. Dickson* (2013) 4 NWLR (Pt. 1345) 534 (SC).

⁴¹*Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

⁴²Raskin (n 14) 310.

merely automates its performance.⁴³ This aligns with hybrid contracts, where the legal agreement governs the relationship and the code executes specific obligations.

3. The Dual-Character Theory

A middle-ground view posits that smart contracts may have both legal and technological dimensions.⁴⁴ The code is not always a complete contract in itself but can form part of the contractual relationship, supplemented by traditional legal principles where necessary. This approach has gained traction among scholars and regulators because it balances innovation with legal certainty.

E. Implications for Nigerian Recognition

For Nigeria, the dual-character theory appears most appropriate. It recognises that while some smart contracts may be enforceable as contracts in their own right, others function only as mechanisms of performance. Nigerian courts are likely to prefer this flexible approach, given the judiciary's historical reliance on common law reasoning and analogical interpretation.

Furthermore, statutory provisions on electronic signatures and digital evidence suggest that Nigerian law is already positioned to recognise at least certain forms of smart contracts.

Nevertheless, recognition will require judicial creativity and possibly legislative clarification. Without express statutory or judicial authority, uncertainties remain, particularly regarding jurisdiction, consumer protection, and remedies in the event of fraud or mistake.

⁴³Clack, Bakshi, and Braine (n 20) 7.

⁴⁴De Filippi and Wright (n 4) 74.

2.5 Theoretical Framework

The enforceability of smart contracts under Nigerian law cannot be fully appreciated without situating the discussion within broader theoretical perspectives. Theoretical frameworks provide analytical tools for understanding how law interacts with emerging technologies and help in evaluating the commercial and jurisdictional challenges posed by smart contracts.

A. Legal Positivism and the Command Theory

Legal positivism, as articulated by John Austin and later refined by H.L.A. Hart, holds that the validity of law is determined by its sources rather than its moral content.⁴⁵ From this perspective, the enforceability of smart contracts under Nigerian law depends strictly on whether they can be situated within existing statutory and common law frameworks. Nigerian courts, operating under a positivist tradition, will therefore focus on whether smart contracts meet the requirements of contract formation under the Contracts Act, judicial precedents, and related legislation, such as the Evidence Act 2011 and the Cybercrimes Act 2015.

The positivist approach explains why Nigerian courts may be reluctant to recognise purely code-based agreements in the absence of legislative or judicial authority, as there is no formal rule of recognition that extends to blockchain-based instruments.

B. The Law and Economics Perspective

The law and economics school emphasises efficiency, transaction costs, and market facilitation.⁴⁶ Smart contracts are celebrated within this framework because they reduce transaction costs by

⁴⁵H.L.A. Hart, *The Concept of Law* (2nd edn, Clarendon Press 1994) 97.

⁴⁶Richard A. Posner, *Economic Analysis of Law* (9th edn, Wolters Kluwer 2014) 15.

eliminating intermediaries, ensuring automatic execution, and enhancing trust through blockchain verification. In theory, this increases market efficiency and access to commerce.

However, the Nigerian legal environment complicates this picture. While smart contracts promise efficiency, the underdeveloped regulatory infrastructure, weak consumer protection mechanisms, and the prevalence of fraud in digital transactions raise concerns about whether efficiency can be achieved without sacrificing fairness.⁴⁷ The law and economics perspective thus highlights the tension between efficiency-driven innovation and the need for institutional safeguards in Nigeria's commercial landscape.

C. Socio-Legal Theory and Legal Realism

Socio-legal theorists and American legal realists emphasise that the law is not merely a set of abstract rules but a living institution shaped by social, economic, and political forces.⁴⁸ From this standpoint, the enforceability of smart contracts in Nigeria will be influenced not only by doctrinal principles but also by factors such as judicial attitudes toward technology, infrastructural readiness, and the role of regulatory agencies like the Central Bank of Nigeria (CBN) and the Nigerian Communications Commission (NCC).

For example, the CBN's cautious stance on cryptocurrencies, including restrictions on banks facilitating cryptocurrency transactions, demonstrates how regulatory culture can affect the legal status of blockchain-based innovations, including smart contracts.⁴⁹ Thus, socio-legal theory

⁴⁷A.O. Adekoya, "The Challenges of Regulating Digital Transactions in Nigeria" (2020) 6(1) *Nigerian Journal of Commercial Law* 45, 53.

⁴⁸Karl Llewellyn, *The Bramble Bush* (Oceana Publications 1930) 13.

⁴⁹Central Bank of Nigeria (CBN), "Letter on Cryptocurrency Transactions" (5 February 2021).

suggests that the evolution of smart contract enforceability will depend heavily on institutional behaviour and societal acceptance, not just legal doctrine.

D. Technological Determinism vs. Contractual Autonomy

Another theoretical lens is the debate between technological determinism and contractual autonomy. Technological determinism posits that technology evolves according to its own logic and compels social adaptation.⁵⁰ In the context of smart contracts, this means that the self-executing nature of code may constrain parties' ability to modify or avoid performance, even in cases of fraud or mistake.

By contrast, contractual autonomy, a foundational principle of Nigerian contract law , emphasises that parties are free to determine their rights and obligations, provided they are not illegal or contrary to public policy.⁵¹ From this view, the rigidity of smart contracts threatens autonomy by limiting judicial discretion and parties' ability to renegotiate terms. The Nigerian legal order, steeped in common law traditions, is likely to favour contractual autonomy over technological determinism.

E. Regulatory Theories: Paternalism vs. Self-Regulation

Finally, regulatory theory provides another useful framework. One perspective is regulatory paternalism, which argues that the state must intervene to protect vulnerable parties, especially consumers, from unfair or harmful practices in emerging technologies.⁵² This resonates strongly in Nigeria, where consumer awareness of blockchain technology is limited and digital fraud is prevalent.

The opposing view is self-regulation, where industry participants establish norms and technical standards without heavy-handed government intervention. This model has been

⁵⁰Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 6.

⁵¹*Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

⁵²Cass R. Sunstein, *After the Rights Revolution: Reconceiving the Regulatory State* (Harvard University Press 1990) 72.

advanced in some blockchain communities but may be unsuitable for Nigeria given weak institutional trust and the absence of effective enforcement mechanisms. The balance between state regulation and self-regulation will significantly shape the enforceability of smart contracts.

Together, these theoretical frameworks provide the intellectual foundation for analysing the enforceability of smart contracts under Nigerian law, while anticipating the commercial and jurisdictional challenges to be discussed in later chapters.

2.6 Identified Gaps in Existing Studies

Despite the growing body of scholarship on smart contracts and blockchain technology, a number of gaps remain in the literature, particularly from the Nigerian perspective. These gaps highlight why a focused study on the enforceability of smart contracts under Nigerian law is both timely and necessary.

A. Limited Nigerian Scholarship

Most existing studies on smart contracts are rooted in foreign jurisdictions such as the United States, the United Kingdom, and the European Union.⁵³ Nigerian legal scholarship has engaged with issues such as electronic commerce, digital signatures, and cybercrime, but few works have addressed smart contracts directly or in a comprehensive doctrinal manner.⁵⁴ As a result, there is limited guidance for Nigerian courts and policymakers on how to approach the enforceability of smart contracts in line with domestic realities.

⁵³Werbach and Cornell, “Contracts Ex Machina” (2017) 67(2) *Duke Law Journal* 313.

⁵⁴O.A. Adeoye, “E-Commerce and Contract Law in Nigeria” (2018) 2(1) *Journal of Business Law and Practice* 121.

B. Doctrinal Ambiguities in Nigerian Law

Another gap lies in the uncertainty surrounding how Nigerian law applies to blockchain-based transactions. While the Evidence Act 2011 and the Cybercrimes Act 2015 recognise electronic documents and digital signatures, they do not specifically address self-executing agreements coded into blockchain platforms.⁵⁵ Nigerian case law, such as *Kubor v. Dickson*, has acknowledged the admissibility of electronic evidence, but there is still no direct judicial pronouncement on whether smart contracts can constitute enforceable legal contracts.⁵⁶ This doctrinal silence leaves significant uncertainty in commercial practice.

C. Overemphasis on Technological Aspects

Much of the global literature on smart contracts has focused on their technological innovation, often at the expense of detailed legal analysis.⁵⁷ While computer scientists discuss how blockchain ensures immutability and decentralisation, fewer studies engage with questions of contract law doctrines such as mistake, illegality, duress, and frustration in the context of self-executing code. This creates a gap in understanding how traditional legal principles interact with emerging technologies.

D. Inadequate Exploration of Jurisdictional Issues

Smart contracts are borderless by design, operating across decentralised networks without respect to national boundaries. Yet, there is limited scholarly work exploring the jurisdictional challenges this poses for enforcement, particularly within the Nigerian legal system where

⁵⁵Evidence Act 2011, s.84; Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s.17.

⁵⁶*Kubor v. Dickson* (2013) 4 NWLR (Pt. 1345) 534 (SC).

⁵⁷Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 56.

jurisdiction is closely tied to territorial boundaries.⁵⁸ Questions remain unresolved as to which courts have competence to adjudicate disputes arising from blockchain-based agreements and how Nigerian courts will interact with foreign judgments or arbitral awards in this area.

E. Insufficient Focus on Consumer Protection

Another underexplored area is consumer protection. In Nigeria, consumer awareness of blockchain technologies is low, and regulatory agencies such as the Federal Competition and Consumer Protection Commission (FCCPC) have not developed tailored policies to address risks associated with smart contracts.⁵⁹ Most scholarly works assume that parties to smart contracts are sophisticated commercial actors, neglecting the possibility of asymmetry of knowledge and bargaining power.

F. Absence of Empirical Research

Finally, there is a dearth of empirical research on how Nigerian businesses and consumers perceive or use smart contracts. While global reports suggest that smart contracts are increasingly being deployed in sectors like finance, supply chain management, and real estate,⁶⁰ Nigerian-specific data remains scarce. Without such empirical insights, the academic discourse risks being too abstract and disconnected from commercial realities.

⁵⁸Ugochukwu O. Ugwuodike, “Jurisdictional Dilemmas in Cyberspace Transactions: Implications for Nigerian Law” (2021) 10(2) *Nigerian Journal of Public and Private Law* 89.

⁵⁹FCCPC, “Guidelines on Digital Commerce” (2022).

⁶⁰Deloitte, “Blockchain and the Future of Smart Contracts” (2020) <https://www2.deloitte.com> accessed 15 September 2025.

These gaps justify the present study, which aims to provide a doctrinally grounded, Nigerian-focused analysis of the enforceability of smart contracts while addressing their commercial and jurisdictional challenges.

CHAPTER THREE: LEGAL AND REGULATORY FRAMEWORK IN NIGERIA

3.1 Overview of Nigerian Contract Law

The Nigerian law of contract forms the bedrock for determining the enforceability of smart contracts. Rooted in English common law, it provides the principles and doctrines against which any novel contractual mechanism, including blockchain-based agreements, must be assessed.

A. Historical Foundations

Nigerian contract law is primarily derived from English common law, equity, and statutes of general application received into Nigeria through the Interpretation Act and colonial legal instruments.⁶¹ The Supreme Court and Court of Appeal have consistently applied English contract principles, subject to statutory modifications. This reception has ensured that Nigerian contract law largely mirrors the doctrines of English law, particularly in areas concerning offer, acceptance, consideration, capacity, intention to create legal relations, and privity of contract.

B. Sources of Nigerian Contract Law

The key sources of Nigerian contract law include:

1. Judicial Precedents – Nigerian courts, drawing on common law, have developed a body of binding case law. For example, in *Orient Bank (Nig.) Plc v. Bilante International Ltd*, the Court of Appeal reaffirmed the orthodox requirement of consensus ad idem (meeting

⁶¹Interpretation Act, Cap I23 Laws of the Federation of Nigeria (LFN) 2004, s.32.

of the minds) for contract formation.⁶²

2. Statutes – While Nigeria does not have a codified Contracts Act like India, various statutes influence contractual relations. These include:

- The Statute of Frauds 1677 (as a statute of general application, applicable in limited circumstances, e.g., contracts for sale of land).
- The Sale of Goods Act 1893 (received into Nigerian law and still applicable in some states).
- The Evidence Act 2011, which regulates the proof and admissibility of contracts, including electronic agreements.
- Special statutes such as the Consumer Protection Act 2018 and the Cybercrimes Act 2015.

3. Customary and Islamic Law – In certain circumstances, customary law contracts (e.g., bride price, land pledges) are recognised, provided they are not repugnant to natural justice, equity, and good conscience. Islamic commercial contracts (e.g., murabaha) are also valid within Sharia jurisdictions.⁶³

⁶²*Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

⁶³J.O. Orojo and A. Ajomo, *Law of Contract in Nigeria* (Mbeyi & Associates 2001) 25.

C. Essential Elements of a Valid Contract

Under Nigerian law, a contract is enforceable if it satisfies the following elements:

1. Offer and Acceptance – There must be a definite offer and an unequivocal acceptance, creating consensus ad idem. In *Carlill v. Carbolic Smoke Ball Co.*, applied in Nigeria, the court held that an advertisement promising reward constituted an offer capable of acceptance.⁶⁴ Nigerian courts follow the same principle.
2. Consideration – A valid contract must be supported by consideration. Nigerian law adheres to the rule that consideration need not be adequate, but must be sufficient. In *Orient Bank v. Bilante*, the court stressed that promises unsupported by consideration are unenforceable.⁶⁵
3. Intention to Create Legal Relations – Social or domestic agreements are presumed not to create legal obligations, while commercial agreements carry the presumption that parties intended to be bound.
4. Capacity – Parties must have legal capacity to contract. Minors, persons of unsound mind, and undischarged bankrupts may face restrictions.
5. Legality of Object – Contracts must not be illegal, immoral, or contrary to public policy. In *Niger Insurance Co. Ltd v. Abed Brothers Ltd*, the Supreme Court held that contracts

⁶⁴*Carlill v. Carbolic Smoke Ball Co.* [1893] 1 QB 256.

⁶⁵*Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

tainted with illegality are unenforceable.⁶⁶

6. Certainty of Terms – Courts will not enforce vague or uncertain agreements.

These requirements are equally applicable to digital or technology-driven contracts, including smart contracts.

D. Special Doctrines Relevant to Smart Contracts

Nigerian contract law also recognises doctrines that may impact the enforceability of smart contracts:

- Privity of Contract – Only parties to a contract can sue or be sued on it. This may present difficulties where blockchain transactions involve multiple, anonymous, or pseudonymous participants.
- Mistake, Misrepresentation, and Fraud – Courts may set aside contracts induced by mistake or fraud. The question arises whether self-executing code allows sufficient room for such equitable reliefs.
- Frustration – Under Nigerian law, a contract may be discharged if unforeseen events render performance impossible. Smart contracts, by contrast, tend to rigidly enforce performance regardless of supervening impossibility.

⁶⁶*Niger Insurance Co. Ltd v. Abed Brothers Ltd* (1976) 7 SC 35.

E. Nigerian Courts and Technological Adaptability

While Nigerian courts are yet to directly address smart contracts, their willingness to adapt to technological change is evident in decisions concerning electronic evidence. In *Kubor v. Dickson*, the Supreme Court upheld the admissibility of electronically generated materials, emphasising that the law must keep pace with technology.⁶⁷ Similarly, the Evidence Act 2011 accommodates digital transactions by recognising electronic signatures and records.

Thus, the existing contract law framework in Nigeria is not inherently hostile to technological innovation, but significant interpretive and regulatory challenges remain in applying these traditional principles to smart contracts.

3.2 Application of Existing Laws to Smart Contracts

While Nigerian law has not yet enacted legislation specifically governing blockchain or smart contracts, existing statutory and common law frameworks remain applicable. The central issue is whether these frameworks are sufficiently adaptable to cover the unique characteristics of self-executing agreements. This section examines how Nigerian legal doctrines on contract formation, electronic transactions, admissibility of evidence, and substantive contractual doctrines apply to smart contracts, before highlighting regulatory attitudes and the limitations of the current framework.

A. Contract Formation in Smart Contracts

⁶⁷*Kubor v. Dickson* (2013) 4 NWLR (Pt. 1345) 534 (SC).

Under Nigerian law, a contract is valid if it satisfies the four traditional elements: offer, acceptance, consideration, and intention to create legal relations.⁶⁸ These requirements are equally applicable to smart contracts, though their manifestation differs from traditional written agreements.

1. Offer and Acceptance: Nigerian courts recognise that contracts can be formed without formal documentation, provided there is a clear offer and unequivocal acceptance.⁶⁹ In the context of smart contracts, the code deployed on a blockchain may represent an offer, while a counterparty's execution of a corresponding transaction (such as transferring cryptocurrency to trigger performance) constitutes acceptance. For instance, in a decentralised finance (DeFi) arrangement, a borrower requesting a loan from a smart contract protocol makes an "offer," which is automatically "accepted" once the coded conditions are satisfied. The blockchain ledger records this interaction immutably, creating evidence of consensus. However, Nigerian courts may face difficulty interpreting whether parties genuinely consented to contractual terms that are embedded in code, which may be incomprehensible to non-technical users. This raises a potential challenge of consensus ad idem, a principle emphasised in *Orient Bank (Nig.) Plc v. Bilante International Ltd*, where ambiguity in consent undermined contractual validity.⁷⁰
2. Consideration: Nigerian law recognises consideration as an essential element, requiring only sufficiency, not adequacy.⁷¹ Consideration in smart contracts may take the form of

⁶⁸*Carlill v. Carbolic Smoke Ball Co.* [1893] 1 QB 256; applied in *Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

⁶⁹*Odutola v. Papersack (Nig.) Ltd* (2006) 18 NWLR (Pt. 1012) 470 (SC).

⁷⁰*Orient Bank (Nig.) Plc v. Bilante International Ltd* (1997) 8 NWLR (Pt. 515) 37 (CA).

⁷¹*Thomas v. Thomas* (1842) 2 QB 851; followed in *Union Bank of Nigeria v. Ajabule* (2011) 18 NWLR (Pt. 1278) 152 (SC).

cryptocurrency, tokens, or other digital assets. Since value can be attributed to digital currency, the requirement of consideration should not pose doctrinal barriers. However, volatility of cryptocurrencies may raise issues about whether consideration is real or illusory, particularly in contracts for future performance.

3. Intention to Create Legal Relations: Commercial contracts enjoy a presumption of legal enforceability.⁷² Smart contracts used for business transactions, such as supply chain finance or automated insurance pay-outs, would likely benefit from this presumption. Nevertheless, where smart contracts are used for experimental or social transactions within blockchain communities (e.g., airdrops or “gas fee tipping”), Nigerian courts may need to determine whether the presumption holds.

Thus, contract formation doctrines are flexible enough to encompass smart contracts, but evidentiary and interpretive issues may complicate enforcement.

B. Electronic Transactions and Digital Signatures

The Nigerian legal framework expressly accommodates electronic contracts and signatures, which strengthens the enforceability of smart contracts. Some of these regulations are discussed below.

The Nigerian Evidence Act 2011 recognises the admissibility of computer-generated evidence under Section 84, provided that proper certification is supplied to demonstrate the reliability of

⁷²*Balfour v. Balfour* [1919] 2 KB 571; applied in *Rose & Frank Co. v. JR Crompton & Bros Ltd* [1925] AC 445.

the electronic record.⁷³ In principle, blockchain transaction records, which are immutable and verifiable, could fall within the ambit of this provision. However, practical challenges arise due to the decentralized nature of blockchain technology, which lacks a central authority capable of issuing conventional certification. Consequently, courts may need to rely on expert testimony or forensic verification methods to establish the authenticity and integrity of blockchain records, consistent with the provisions of Section 68 of the Evidence Act, which allows for the admissibility of expert evidence to explain or validate technical data.⁷⁴ This demonstrates that while Nigerian law provides a legal pathway for the recognition of blockchain evidence, judicial adaptation and technical expertise are crucial to ensuring enforceability in practice.

Cybercrimes (Prohibition, Prevention, etc.) Act 2015 also plays a significant role in the legal framework for smart contracts in Nigeria. Section 17 of the Act validates the use of electronic signatures in transactions, although certain exceptions apply, including wills, immovable property transactions, and negotiable instruments.⁷⁵ Smart contracts typically rely on private keys and digital signatures to authenticate the parties involved and to trigger automated execution of contractual obligations. Under Nigerian law, such digital signatures are recognised as functionally equivalent to traditional “wet ink” signatures, thereby providing a statutory basis for the legal enforceability of smart contracts in commercial transactions. The alignment of blockchain-based digital signatures with Section 17 demonstrates the growing capacity of Nigerian legislation to accommodate emerging technologies.

Additionally, regulatory guidance from the Nigerian Communications Commission (NCC) affirms that electronic contracts possess the same legal force as paper-based agreements.⁷⁶ This

⁷³ Evidence Act 2011 (No 6) s 84.

⁷⁴ Ibid, s 68.

⁷⁵ Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 17.

⁷⁶ Nigerian Communications Commission, *Guidelines on Electronic Transactions* (NCC Policy, 2019) 4–6.

policy recognition reinforces the validity of smart contracts as legally binding instruments and provides regulatory support for their adoption in commercial and financial sectors. By combining statutory provisions with regulatory recognition, Nigeria has established a framework that enables the legal recognition of smart contracts, though practical implementation may require judicial interpretation and technical expertise to navigate issues such as evidentiary certification and cross-border execution.

Comparatively, jurisdictions such as the UK (under the Electronic Communications Act 2000) and the EU (under the eIDAS Regulation) also recognise electronic signatures, including advanced and qualified digital signatures. Nigeria's statutory stance aligns with these international trends, even though blockchain-specific recognition is absent.

C. Admissibility and Evidential Challenges

The admissibility of blockchain records raises several practical challenges:

- **Certification Requirement** – Nigerian courts have stressed the necessity of certification under s.84 in cases such as *Kubor v. Dickson*, where uncertified electronic evidence was rejected.⁷⁷ Applying this to blockchain, certification may be impractical, as no central authority controls the ledger.
- **Expert Testimony** – Courts may need to rely on expert evidence under s.68 of the Evidence Act to establish the authenticity of blockchain records. This parallels the approach in US courts, where blockchain evidence has been admitted through expert

⁷⁷*Kubor v. Dickson* (2013) 4 NWLR (Pt. 1345) 534 (SC).

witnesses explaining cryptographic proof.

- Evidential Weight – Blockchain records, being immutable, may enjoy higher probative value compared to other electronic evidence. However, this does not resolve questions about whether the underlying contract terms were legally valid or void for uncertainty, mistake, or illegality.

D. Substantive Doctrines of Nigerian Contract Law

Smart contracts must also comply with substantive doctrines, which may present obstacles:

1. Privity of Contract

Nigerian law adopts a strict doctrine of privity, meaning only parties to a contract can sue or be sued.⁷⁸ In blockchain transactions, where multiple parties are indirectly affected (e.g., developers, miners, oracles), privity may prevent redress for non-parties.

Comparative developments, such as the UK's Contracts (Rights of Third Parties) Act 1999, provide statutory exceptions to privity, but no equivalent exists in Nigeria.

2. Capacity

Capacity issues are accentuated in blockchain transactions due to anonymity. Nigerian law bars minors and persons of unsound mind from contracting.⁷⁹ If a pseudonymous participant is later found to lack capacity, enforcement of a smart contract could be

⁷⁸*Dunlop Pneumatic Tyre Co. Ltd v. Selfridge & Co. Ltd* [1915] AC 847 (HL).

⁷⁹Sale of Goods Act 1893 (received English law), ss. 2–3; *Labinjoh v. Abake* (1924) 5 NLR 33

voidable.

3. Illegality and Public Policy

Nigerian courts will not enforce contracts contrary to public policy or tainted with illegality, as reaffirmed in *Akinsanya v. UBA Ltd.*⁸⁰ Smart contracts used for money laundering, pyramid schemes, or illegal gambling would therefore be unenforceable, regardless of blockchain immutability.

4. Mistake and Frustration

Doctrines of mistake and frustration are central to Nigerian contract law. Yet their application to smart contracts is uncertain. For instance, if a coding error leads to unintended performance, can a party plead unilateral or mutual mistake? The automated nature of blockchain complicates judicial intervention, since performance may have already occurred irreversibly.

E. Institutional and Regulatory Stance

Regulatory attitudes significantly influence judicial treatment of smart contracts. The Central Bank of Nigeria's 2021 directive prohibiting banks from dealing in cryptocurrency transactions⁸¹ reflects caution, though it does not outlaw blockchain or smart contracts. Conversely, the introduction of the eNaira demonstrates willingness to harness blockchain technology.

⁸⁰*Akinsanya v. UBA Ltd* (1986) 4 NWLR (Pt. 35) 273 (CA).

⁸¹Central Bank of Nigeria (CBN), "Letter on Cryptocurrency Transactions" (5 February 2021).

The Securities and Exchange Commission (SEC) has also issued guidelines classifying certain digital assets as securities, implying that smart contracts governing such assets may fall within its regulatory oversight. This layered regulatory environment introduces uncertainty, as courts may hesitate to enforce smart contracts that intersect with proscribed cryptocurrency activities.

F. Limits of Existing Legal Framework

While existing Nigerian laws provide a doctrinal basis for recognising smart contracts, critical limitations persist:

- **Ambiguity in Consensus** – The requirement of consensus ad idem may be undermined where parties cannot interpret or understand the code.
- **Remedial Inflexibility** – Common remedies such as rescission or injunction may be ineffective once a blockchain transaction is executed irreversibly.
- **Jurisdictional Uncertainty** – Nigerian courts lack statutory guidance on handling disputes where parties, nodes, and servers are scattered across multiple jurisdictions.
- **Regulatory Ambivalence** – The CBN's restrictive stance on cryptocurrency undermines confidence in the enforceability of smart contracts that involve digital tokens.

In conclusion, Nigerian law can theoretically enforce smart contracts under general contract and electronic transaction principles, but significant **commercial, evidential, and jurisdictional**

challenges remain unresolved. Judicial and legislative innovation will be required to bridge these gaps.

3.3 Legal Requirements for Contract Enforceability

For a smart contract to be enforceable under Nigerian law, it must satisfy the traditional requirements of contract formation, capacity, legality, and certainty. These principles, drawn from common law, statutes, and Nigerian judicial decisions, remain the framework through which novel technologies like blockchain agreements are evaluated.

A. Offer and Acceptance

At the core of contractual enforceability lies the principle that there must be a clear offer and a corresponding acceptance. In *Labinjo v Abake*,⁸² the court invalidated an alleged marriage contract because there was no proof of consensus ad idem, emphasising that a binding agreement requires a definite offer and unequivocal acceptance. The same reasoning applies to smart contracts: the coded terms must represent an intelligible offer, while a counterparty's digital action (e.g., transferring cryptocurrency) must reflect acceptance.

In English law, *Ashbury Railway Carriage & Iron Co v Riche*⁸³ demonstrates the strictness of acceptance rules, where the House of Lords held a contract void because it was ultra vires the company's objects clause, notwithstanding consent between the parties. Nigerian courts have adopted this orthodoxy, reinforcing the necessity of mutual assent as a precondition to enforceability.

⁸²*Labinjo v Abake* (1924) 5 N.L.R. 33 (Nig.).

⁸³*Ashbury Railway Carriage & Iron Co v Riche* (1875) LR 7 H.L. 653 (H.L.).

B. Consideration

Nigerian law, following English common law, requires consideration, though it need only be sufficient and not adequate. In *Odutola v Papersack Nigeria Ltd*,⁸⁴ the Supreme Court affirmed that a contractual promise unsupported by consideration could not be enforced. Likewise, in *Orient Bank (Nig.) Plc v Bilante International Ltd*,⁸⁵ the Court of Appeal stressed that the presence of some form of reciprocal value was indispensable.

By comparison, the English decision in *Thomas v Thomas*⁸⁶ illustrates the principle of sufficiency: even nominal rent was held to be valid consideration. In the Nigerian context, digital tokens or cryptocurrencies exchanged under a smart contract would likely satisfy the requirement, even if their real-world value is uncertain.

C. Intention to Create Legal Relations

The presumption of intention in commercial agreements has been consistently upheld by Nigerian courts. In *Union Bank of Nigeria Plc v Ajabule*,⁸⁷ the Supreme Court reiterated that courts must consider whether the parties intended their arrangement to give rise to legal obligations. Conversely, English law in *Balfour v Balfour*⁸⁸ drew a line between domestic arrangements (non-binding) and commercial contracts (binding), a principle echoed in Nigerian jurisprudence.

⁸⁴*Odutola v Papersack Nigeria Ltd* (2006) 18 N.W.L.R. (Pt. 1012) 470 (S.C.).

⁸⁵*Orient Bank (Nig.) Plc v Bilante International Ltd* (1997) 8 N.W.L.R. (Pt. 515) 37 (C.A.).

⁸⁶*Thomas v Thomas* (1842) 2 Q.B. 851 (C.A.).

⁸⁷*Union Bank of Nigeria Plc v Ajabule* (2011) 18 N.W.L.R. (Pt. 1278) 152 (S.C.).

⁸⁸*Balfour v Balfour* [1919] 2 K.B. 571 (C.A.).

In *Rose & Frank Co v J.R. Crompton & Bros Ltd*,⁸⁹ the House of Lords held that an explicit “honourable pledge” clause could exclude legal enforceability. This suggests that even in the digital context, parties to a smart contract could, in principle, exclude legal consequences by coding disclaimers into the agreement.

D. Capacity to Contract

A party must possess legal capacity for a contract to be enforceable. In *Akinsanya v United Bank for Africa Ltd*,⁹⁰ the Court of Appeal reaffirmed that minors and persons of unsound mind cannot be bound by contractual obligations, except for necessities. Statutory law, such as the Infants Relief Act 1874,⁹¹ invalidates certain contracts entered into by minors.

For companies, the Companies and Allied Matters Act 2020 (CAMA) grants corporate entities capacity to contract within their objects and powers.⁹² In practice, blockchain transactions raise serious capacity issues, since pseudonymous addresses on a distributed ledger may conceal whether a counterparty is legally competent to contract.

E. Certainty of Terms

A contract must be sufficiently certain to be enforceable. In *Taylor v Caldwell*,⁹³ the court refused to enforce a contract for a music hall hire that had been destroyed by fire, holding that the agreement was frustrated. Similarly, in *Araka v Monier Construction Co (Nig) Ltd*,⁹⁴ the

⁸⁹*Rose & Frank Co v J.R. Crompton & Bros Ltd* [1925] A.C. 445 (H.L.).

⁹⁰*Akinsanya v United Bank for Africa Ltd* (1986) 4 N.W.L.R. (Pt. 35) 273 (C.A.).

⁹¹*Infants Relief Act* 1874 (37 & 38 Vict. c. 62).

⁹²Companies and Allied Matters Act 2020, ss.42–43.

⁹³*Taylor v Caldwell* (1863) 3 B. & S. 826 (C.A.).

⁹⁴*Araka v Monier Construction Co (Nig) Ltd* (1978) All N.L.R. 219 (S.C.).

Supreme Court stressed that vagueness or indefiniteness in contractual terms would render an agreement unenforceable.

The House of Lords in *Scammell v Ouston*⁹⁵ reaffirmed that contracts lacking clarity in essential terms cannot stand. Applying this to smart contracts, code-based agreements must articulate obligations clearly enough for courts (and not just machines) to interpret. Ambiguity in coding may therefore frustrate enforcement.

F. Formalities and Evidence

While Nigerian law recognises oral contracts, certain agreements require compliance with statutory formalities. The Statute of Frauds 1677,⁹⁶ as part of received English law, requires contracts relating to land to be in writing. Similarly, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 recognises the validity of electronic signatures except in relation to wills, immovable property, and negotiable instruments.⁹⁷

The Evidence Act 2011 (s.84) further provides for the admissibility of computer-generated documents, thereby enabling blockchain transaction records to be produced in evidence.⁹⁸

However, the Supreme Court in *Kubor v Dickson* stressed the need for strict compliance with evidential rules in electronic records, underscoring that blockchain-based evidence must still meet certification standards.

Conclusively, smart contracts, though technologically innovative, remain subject to the orthodox rules of Nigerian contract law. Offer, acceptance, consideration, intention, capacity, certainty, and

⁹⁵*Scammell v Ouston* [1941] A.C. 251 (H.L.).

⁹⁶Statute of Frauds 1677 (29 Cha. II c. 3).

⁹⁷Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s.17.

⁹⁸Evidence Act 2011, s.84.

compliance with statutory formalities are all indispensable. Nigerian courts will likely apply these principles with caution, balancing technological novelty against doctrinal stability.

3.4 Digital evidence and admissibility under Nigerian law

A. Why this matters for smart-contract disputes

Smart contracts run on distributed ledgers and produce inherently digital outputs (transaction records, block confirmations, event logs, on-chain state). When a dispute arises about a smart-contract transaction (whether performance occurred, who invoked a function, whether funds were transferred), the court will be asked to treat blockchain data as evidence. That raises familiar (but technically demanding) issues: (a) admissibility (is the material legally receivable?), (b) authentication (is it what it claims to be and who produced it?), and (c) weight (how persuasive is it once admitted?). Nigerian law treats electronic evidence as documentary evidence but subjects it to statutory foundational rules intended to guarantee reliability and authenticity.

B. Key statutory framework

1. Evidence Act 2011, section 84:

- Section 84 is the primary gateway for statements contained in documents produced by a computer: such statements are admissible if the conditions in s.84(2) are shown. The subsection sets out the familiar four-part foundation test (use of computer for regular activities, data supplied in ordinary course, computer operating properly or defects not affecting accuracy, and that the information

reproduces or is derived from information supplied in the ordinary course).

Subsection (4) then permits a certificate (signed by a responsible person) that identifies the document, explains how it was produced and gives particulars about any device involved; that certificate is admissible as evidence of the matters stated in it. The Act also treats a chain or combination of computers as a “single computer” for purposes of s.84.

2. Definitions and expansion, s.258 and the Evidence (Amendment) Act 2023:

- The Interpretation section (s.258 as amended) defines “computer”, “document” and , after the 2023 Amendment, now specifically defines “electronic record”, “digital signature”, “cloud computing”, etc. The 2023 Amendment inserted new subsections (84A–84D) and clarifications designed to accommodate cloud, printed copies of electronic records, and digital signatures; this materially affects how courts should treat electronic records (including certain forms of blockchain outputs). Practitioners must read s.84 together with the 2023 amendments because the Amendment explicitly modernised the category of admissible “electronic records” and recognises digital signature techniques.⁹⁹

Practical consequence: s.84 remains the gateway: to admit a blockchain/smart-contract record you must either (a) call oral foundation evidence (an appropriately qualified witness who can

⁹⁹ Evidence (Amendment) Act 2023: Nigerian Evidence Law Accommodates Technological Advancements https://www.templars-law.com/app/uploads/2023/08/Evidence-Amendment-Act-2023-2.pdf?utm_source=chatgpt.com accessed 17 September 2025.

testify to the s.84(2) facts) or (b) produce a properly framed certificate under s.84(4) (or both).

The Amendment 2023 gives additional tools (electronic record/digital signature routes) but does not eliminate the need to authenticate provenance and integrity.

C. Technical terms explained

- **Computer-generated document / electronic record:** under s.258 (and the 2023 amendment) a “document” includes any data or matter expressed or stored by electronic means, and “electronic record” is now expressly defined to include data/images/sound stored or sent in electronic form. A **computer-generated** item is one produced by a device that stores or processes information.
- **Certificate of compliance / authentication (s.84(4)):** a written statement identifying the document, describing how it was produced, and giving particulars of the device or system involved , signed by somebody in a responsible position , which the Act treats as evidence of the matters stated.
- **Chain of custody:** the documented, chronological record (who handled the data, when and how) that shows the evidence was preserved without tampering. For digital materials this includes hashes, write-protected images, timestamps and export logs.
- **Hash (cryptographic digest):** a short fixed-length string derived from a larger data set (e.g., a transaction or file). Hashes are used in forensics to prove that a file has not changed: the same file will always produce the same hash; any change produces a

different hash.

- **Public key / private key / signed message:** blockchain transactions are authorized with digital signatures. A party who can **sign an arbitrary message** with the private key corresponding to a blockchain address provides strong proof that the party controls that address (helpful to show who transmitted a transaction). However, control of an address $\neq$ legal identity (addresses are pseudonymous), so identity issues remain.
- **Immutability vs. mutability in practice:** while blockchain ledgers provide a tamper-resistant, replicated record, “immutability” is not absolute , forks, chain reorganisations, or compromised private keys may complicate the evidentiary story. For adversarial litigation, a court will examine not only whether the chain record shows a transaction, but whether the record reliably links to the human/legal actor claimed to have acted. For smart-contract disputes, the on-chain record may be powerful proof of what code executed and when , but not always proof of parties’ legal consent to the contract terms. For admissibility and weight, both provenance and context matter.¹⁰⁰

D. What these rules mean for blockchain / smart-contract evidence (practical problems)

1. What counts as “the computer” or the “device” that produced the document?

¹⁰⁰Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes
https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2024.1306058/full?utm_source=chatgpt.com
accessed 17 September 2025.

- For blockchain evidence the “computer” may be a full node, a cluster of nodes, the block-explorer service, or even an exchange’s internal ledger. Section 84(5) treats combinations of computers as a single computer, but that statutory comfort does not resolve the cross-jurisdictional problem when key nodes or custodians sit overseas. The 2023 Amendment’s inclusion of cloud records helps with evidence in cloud or distributed contexts, but international cooperation will still be necessary for custody and certificates.
2. Proving identity or control (privity): blockchain addresses are pseudonymous. A transaction shows that some private key authorized the transaction, but linking that key to a named person or corporate actor requires extra proof (e.g., exchange records, KYC documents, signed messages with the private key, wallet-management logs). Courts will treat on-chain records as probative of what happened on-chain, but proof of who acted usually requires off-chain corroboration.¹⁰¹
 3. Tampering and immutability myths: although blockchains are tamper-resistant, forks or reorganisations can change which transactions ultimately appear in the canonical chain for a short time; more practically, private keys can be stolen and transactions made by third parties. A court will ask about how the transaction was created, when, and whether anyone had motive/opportunity to manipulate keys or metadata. Forensic explanations

¹⁰¹ “SMART CONTRACTS” & LEGAL ENFORCEABILITY
https://cardozo.yu.edu/sites/default/files/2020-01/smart_contracts_report_2_0.pdf?utm_source=chatgpt.com
accessed 17 September 2025.

(hashes, node logs, broadcast receipts) are essential.¹⁰²

4. Cross-border evidence production: many custodians (exchanges, custodial wallet providers, node-operators) are outside Nigeria. The certificate route under s.84(4) can be used but may need cooperation (letters rogatory, MLATs) to obtain a responsible-person certificate. The Court of Appeal's Stanbic IBTC line of authorities signals judicial sensitivity to practical difficulty, but expects judges to press for the best attainable foundation, not perfection.¹⁰³

E. Courtroom and Pre-Trial Considerations for Tendering Smart-Contract Evidence in Nigeria

The admissibility of blockchain and smart-contract evidence in Nigerian courts requires careful preparation to satisfy both procedural and evidentiary standards under the Evidence Act 2011. A foundational step involves meticulously inventorying the relevant on-chain proof. Practitioners should document the transaction hash, block number, timestamp, smart contract address, function call logs, including input parameters and return values, and associated event logs. Wallet addresses involved in the transaction must also be recorded, while preserving screenshots and native exports, such as JSON representations of transaction receipts. It is essential to note the

¹⁰² BLOCKCHAIN EVIDENCE: HOW SMART LITIGATORS CAN KEEP IT OUT AT TRIAL https://fordhamlawreview.org/wp-content/uploads/2024/05/Sahara-042-059.pdf?utm_source=chatgpt.com accessed 17 September 2025.

¹⁰³ OALP DISPUTE RESOLUTION PRACTICE https://www.olaniwunajayi.net/blog/wp-content/uploads/2021/12/OALP-DISPUTE-RESOLUTION-PRACTICE-QUARTERLY-NEWSLETTER-4th-QUARTER-2021-Final-30.12.2021.pdf?utm_source=chatgpt.com accessed 17 September 2025.

precise node or blockchain explorer used and the exact date and time of the snapshot, as these details establish the authenticity and provenance of the data.

In addition to preserving raw data, counsel must produce cryptographic proof of integrity. This involves computing a trusted hash, for example using the SHA-256 algorithm, of the exported transaction files. The computed hash should be stored in a time-stamped, write-protected format, such as in a court file or notarised record, while the original export is preserved on read-only media. Documenting the hashing algorithm used and the process of computation ensures that the integrity of the record can be independently verified, thereby strengthening its evidentiary value.¹⁰⁴

Where identity verification is material to the dispute, it is crucial to demonstrate control over the blockchain address. This can be achieved by having the alleged actor sign an arbitrary message using the private key associated with the relevant address. Verification of the signed message against the on-chain public key serves as strong evidence of control. In cases where the key is held by a custodian or exchange, it is necessary to obtain Know-Your-Customer (KYC) records and a formal certificate from the custodian linking the address to the client.¹⁰⁵

The statutory foundation for tendering computer-generated evidence in Nigeria is primarily Section 84 of the Evidence Act 2011, which provides two principal routes. First, an oral foundation may be laid by calling a competent witness, such as a developer, node custodian, IT expert, or exchange compliance officer, who can swear to the facts under Section 84(2). The witness must confirm that the blockchain or node routinely stored and processed the relevant

¹⁰⁴Evidence Act 2011, s 84.

¹⁰⁵Ibid, s 68; see also Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (No 21) s 17 on recognition of digital signatures.

data, that the system was functioning correctly, and that the on-chain data reproduces or derives from ordinary-course inputs. Alternatively, Section 84(4) permits tendering a certificate from a person in a responsible position, detailing the document, its production process, and particulars of the devices involved. In cases involving foreign nodes or operators, Nigerian courts may accept such foreign certificates, supplemented by corroborating local oral evidence, particularly where cross-border cooperation is difficult, as illustrated by the Court of Appeal in *Stanbic IBTC*.¹⁰⁶

Maintaining a chain-of-custody log is critical to demonstrate procedural integrity. Counsel should document who exported the transaction, when it was exported, the tools used, and the node or IP address accessed. Where feasible, forensic copies of relevant media should be obtained, accompanied by expert hash logs. For third-party custodians or exchanges, obtaining litigation hold notices and server logs can further bolster the evidentiary record. Expert testimony is frequently required to explain blockchain mechanics, hashing procedures, and the reliability of the exported data, enabling the court to understand the technical processes underlying the evidence. Section 68 of the Evidence Act provides the framework for admitting expert opinions, including the qualifications and limits of expert inference.¹⁰⁷

Practitioners should also anticipate counterarguments regarding admissibility versus weight. Opposing parties may challenge the chain-of-custody, argue that screenshots are fabricated, or question the reliability of certificates. It is essential to distinguish between procedural admissibility under Section 84 and the evidential weight that the court ultimately assigns. Even

¹⁰⁶*Stanbic IBTC Bank Ltd v. Chief Femi Osibona & Ors* (Court of Appeal, Lagos, 2019) CA/L/234/2018.

¹⁰⁷Evidence Act 2011 (No 6) s 68.

where the statutory foundation is satisfied, the court will evaluate the overall reliability and probative value of the evidence in context.

Cross-border and jurisdictional considerations present additional challenges. When nodes, exchanges, or certificate-issuers are located abroad, counsel may need to employ international assistance mechanisms, such as letters rogatory or mutual legal assistance treaties (MLATs), or rely on local witness testimony paired with public, verifiable on-chain data. The *Stanbic IBTC* decision indicates that Nigerian courts are willing to consider such evidence even when certificates originate from foreign jurisdictions, provided that counsel can demonstrate the steps taken to obtain cooperation and the practical limitations encountered.

In conclusion, the admissibility of blockchain-based smart-contract evidence in Nigeria is achievable under Section 84, whether through oral foundation or certification. Courts have demonstrated practical flexibility where rigid compliance would otherwise exclude vital proof. However, admissibility does not equate to legal characterization: even when a smart-contract record is admitted, the court must still determine whether the code or on-chain activity constitutes a contract at law, whether parties manifested sufficient assent, and how remedies should be framed, such as specific performance, freezing crypto assets, or other equitable relief. The legal resolution of these issues relies heavily on the same digital-evidence foundation established under Section 84. Practically, commercial litigators handling smart-contract disputes should combine technical evidence, such as hashes, node exports, and signed messages, with a sound legal foundation, including Section 84 certificates or sworn oral testimony, while documenting cross-border custody steps to satisfy both admissibility and evidentiary weight requirements.

3.5 Comparative Perspective: UK, US and EU Approaches

Understanding how leading common-law and regional systems have confronted the legal status of smart contracts helps to identify pragmatic options for Nigeria. This comparative review focuses on: (a) legislative recognition and electronic-signature regimes; (b) judicial treatment of blockchain records and crypto-assets; and (c) regulatory measures that address consumer protection, market integrity and cross-border enforcement. For each jurisdictional strand I provide short factual summaries of key decisions or policy documents, explain their legal effect, and draw out lessons relevant to Nigeria.

A. United Kingdom: doctrinal flexibility and authoritative private-sector guidance

The UK has approached smart contracts principally through the lens of adaptation rather than legislation: English contract law's established principles are treated as sufficiently flexible to capture contractual relations expressed or performed by code, provided the classical requirements (offer, acceptance, intention, consideration) are satisfied.

The most influential non-statutory instrument is the Legal Statement on Crypto-assets and Smart Contracts issued by the UK Jurisdiction Taskforce (a private-sector body of senior practitioners). The Statement analysed whether English law recognises crypto-assets as property and whether smart contracts can form enforceable legal obligations. It concluded that crypto-assets can be property in English law and that smart contracts may be legally binding when their terms satisfy ordinary contract requirements. The Statement's reasoning is practical: it treated smart contracts as capable of being either (i) evidence of contractual intention, (ii) constituting part of a legally

binding contract where code is the medium of offer/acceptance, or (iii) as performance mechanisms governed by an underlying legal contract.¹⁰⁸

English courts have increasingly signalled receptiveness. A notable instance is the High Court's decision in *AA v Persons Unknown* (2019), where the court recognised Bitcoin as property capable of being the subject of injunctive relief and accepted on-chain tracing evidence as a basis for relief in fraud cases. The practical effect is that English courts will treat blockchain records as probative of transfers and ownership, and they will fashion equitable remedies (freezing orders, proprietary injunctions) to secure on-chain assets.¹⁰⁹

The UK has favoured a sectoral regulatory approach (Financial Conduct Authority for regulated activities), and has emphasised innovation-friendly guidance coupled with consumer protection. The Taskforce's Statement, while not binding, has been influential in aligning market practice and encouraging use of arbitration clauses and specialist tribunals for crypto disputes.

The UK model shows that a combination of authoritative guidance (from respected legal bodies) and doctrinal adaptation can provide near-term legal certainty without wholesale statutory reform. For Nigeria, this suggests that a well-argued, locally-authored legal statement (e.g., from the Nigerian Bar Association or a judicial taskforce) could help judges and practitioners interpret smart contracts against existing doctrines while legislators consider long-term reforms.

B. United States: patchwork of federal statutes, state experiments and case law

The US approach is multi-layered such that federal statutes (notably the E-SIGN Act) and the Uniform Electronic Transactions Act (UETA) establish the legal parity of electronic records and

¹⁰⁸UK Jurisdiction Taskforce, *Legal Statement on Crypto-assets and Smart Contracts* (2019).

¹⁰⁹*AA v Persons Unknown* [2019] EWHC 3556 (Comm).

signatures; at the state level, a number of legislatures have enacted blockchain-friendly provisions that expressly recognise smart contracts and blockchain records.

The E-SIGN Act (2000) and UETA (1999) provide that electronic records and signatures cannot be denied legal effect solely because they are electronic. They provide a sturdy legal basis for enforcing digital agreements and have been relied on in commercial disputes to validate electronic consent and records.¹¹⁰ Similarly, several US states have gone further. For example, Arizona enacted provisions recognising blockchain signatures and smart contracts as having legal effect; Tennessee and Nevada similarly enacted statutes to expressly validate blockchain records and smart contracts. These state laws typically declare that a “smart contract” is not invalid solely because it is in electronic or coded form.¹¹¹

Federal and state courts also admits blockchain evidence in criminal and civil contexts. In *United States v Ulbricht*, the Southern District of New York admitted blockchain records and used them for tracing illicit proceeds tied to the Silk Road marketplace; the case illustrates how on-chain records can be integrated into evidentiary narratives, subject to foundation and authentication.¹¹²

Therefore, US regulators apply sectoral rules, that is, the SEC evaluates token offerings under securities law; the CFTC treats certain tokens as commodities; banking and consumer-protection regulators apply existing laws to crypto activities. This results in a complex regulatory environment where enforceability of smart contracts may depend on the regulatory classification of the underlying asset/activity.

¹¹⁰Electronic Signatures in Global and National Commerce Act 2000 (E-SIGN Act); Uniform Electronic Transactions Act (UETA) (1999).

¹¹¹Arizona Revised Statutes §44-7061 (2017); Tennessee Code Annotated §47-10-202 (2018).

¹¹²*United States v Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

Hence, the US demonstrates the power of existing electronic-signature statutes to underpin enforceability, and the utility of state-level experimentation to test statutory language before nationwide uptake. For Nigeria, strengthening or clarifying the legal effect of electronic signatures and explicitly recognising blockchain records in evidence statutes would give immediate doctrinal support for smart-contract enforcement while regulators decide classification issues.

C. European Union: regulatory harmonisation and emphasis on trust services

The EU has pursued harmonised regulation emphasizing trust and interoperability through instruments such as the eIDAS Regulation (which creates legal effects for electronic signatures and trust services) and, more recently, focused frameworks for crypto-assets (for example, the Markets in Crypto-assets Regulation , MiCA) that address market integrity, consumer protection and governance. The EU's approach is comparatively prescriptive and regulatory.

Key instruments

- **eIDAS Regulation (Regulation (EU) No 910/2014):** provides legal recognition for electronic identification and trust services (qualified electronic signatures, seals, timestamps). Qualified signatures under eIDAS are afforded a high evidential value and legal equivalence to handwritten signatures. This helps ensure that electronic agreements have predictable legal standing.¹¹³

¹¹³Regulation (EU) No 910/2014 (eIDAS).

- **MiCA and broader DLT initiatives:** aim to regulate issuers of crypto-assets, stablecoins, and service providers, creating clearer compliance regimes and investor protections across member states. These rules are still being rolled out, but their thrust is to place blockchain markets inside a harmonised regulatory framework.

Also, EU courts and national courts within member states increasingly accept electronic records where backed by qualified trust services, and regulators have the power to require disclosures and safeguard mechanisms. The EU's emphasis is on combining technical trust measures (qualified signatures, timestamps, qualified trust service providers) with robust consumer protections.

Hence, the EU model highlights how technical standards (e.g., recognised electronic signatures; accredited trust service providers) can reduce evidentiary friction and increase judicial confidence in electronic records. Nigeria could benefit from adopting national standards for trusted electronic signatures and an accreditation regime for trust providers to improve the evidentiary quality of blockchain-related records.

D. Synthesis: comparative lessons and pragmatic paths for Nigeria

Drawing these strands together suggests a three-track strategy Nigeria could adopt to improve enforceability and reduce commercial uncertainty:

1. Doctrinal clarity through authoritative guidance, encourage the development of a Nigerian legal statement or taskforce report (similar to the UK Jurisdiction Taskforce) that interprets how existing contract and evidence rules apply to smart contracts and

crypto-assets.

2. Statutory modernization of electronic evidence and signatures. This will involve amending or clarifying the Evidence Act and related statutes to explicitly recognise cryptographic signatures, blockchain hashes, and distributed records as admissible and, in certain circumstances, self-authenticating evidence , while preserving judicial discretion to scrutinise provenance.
3. Regulatory coordination and technical standards. Empower a lead regulator (or a coordinated regulatory forum) to issue technical standards for wallet custodians, exchanges, and trust service providers (digital identity/KYC, certified timestamping, accredited custody). This reduces cross-border friction and provides courts with clearer routes to provenance evidence.

Taken together, these comparative lessons show that Nigeria need not choose between a laissez-faire approach and heavy-handed prohibition. Careful doctrinal adaptation, targeted statutory reform, and sensible technical standards can provide a workable legal environment that supports the enforceability of smart contracts while protecting consumers and preserving public policy.

3.6 Institutional and Judicial Responses in Nigeria (with Comparative Perspectives)

The enforceability of smart contracts under Nigerian law is not simply a doctrinal question of contract formation. It depends on how courts and regulatory institutions respond to technological

innovation. So far, Nigerian courts have been cautious, focusing on electronic evidence without pronouncing on smart contracts directly. Regulators have also taken fragmented approaches, oscillating between caution and promotion. To appreciate Nigeria's position, it is instructive to contrast its institutional and judicial responses with those of jurisdictions such as the United Kingdom, the United States, and the European Union, which have more advanced frameworks.

A. Judicial Responses in Nigeria

(i). Recognition of Electronic Evidence

The judiciary's openness to digital records forms the bedrock of smart contract enforceability. In *Kubor v Dickson*,¹¹⁴ the Supreme Court admitted computer-generated evidence from Sahara Reporters in an election petition, provided the requirements of section 84 of the Evidence Act 2011 were satisfied. This was significant because it marked the Court's recognition that electronic documents can serve evidential purposes in high-stakes disputes.

Similarly, in *Dickson v Sylva*,¹¹⁵ the Supreme Court reaffirmed that electronically generated records are admissible if properly certified. The Court, however, emphasised procedural compliance, an indication that while the judiciary is flexible, it remains cautious. These decisions suggest that blockchain records, immutable transaction logs generated by smart contracts, would be admissible, provided certification requirements are met.

(ii). Silence on Smart Contracts and Probable Trajectory

¹¹⁴*Kubor v Dickson* (2013) 4 N.W.L.R. (Pt. 1345) 534 (S.C.).

¹¹⁵*Dickson v Sylva* (2016) 8 N.W.L.R. (Pt. 1515) 427 (S.C.).

Nigerian courts have yet to pronounce directly on the validity or enforceability of smart contracts. However, their reliance on comparative jurisprudence suggests they may follow developments in English law. In *AA v Persons Unknown*,¹¹⁶ the English High Court recognised cryptocurrencies as property capable of being the subject of injunctions. Nigerian courts, historically inclined to adopt English common law where local precedents are lacking,¹¹⁷ could be persuaded to extend property or contractual status to digital assets and blockchain agreements.

(iii). Comparative Perspective: Judicial Responses Abroad

The UK has taken deliberate steps to provide judicial and institutional clarity. In 2019, the UK Jurisdiction Taskforce (UKJT) issued a Legal Statement affirming that smart contracts can be enforceable under English law, provided they satisfy the ordinary requirements of contract formation.¹¹⁸ This proactive stance provides commercial actors with certainty. Similarly, in the US, courts have recognised smart contracts in cases involving blockchain-based agreements, with the New York legislature going further to amend statutes to expressly recognise smart contracts as legally valid.¹¹⁹ The EU, through the proposed Regulation on Markets in Crypto-Assets (MiCA), also acknowledges the legal force of blockchain-based transactions, creating a harmonised regime across member states.¹²⁰

By contrast, Nigerian courts remain reactive, awaiting disputes rather than issuing interpretive guidance. This judicial silence limits commercial certainty, as parties cannot predict how self-executing agreements will be treated.

¹¹⁶*AA v Persons Unknown* [2019] EWHC 3556 (Comm).

¹¹⁷See *Okonkwo v Okagbue* (1994) 9 N.W.L.R. (Pt. 368) 301 (S.C.).

¹¹⁸UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (2019).

¹¹⁹New York State Senate, Bill S8839 (2022), recognising smart contracts as legally valid.

¹²⁰Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA).

B. Regulatory Responses in Nigeria

(i). Central Bank of Nigeria (CBN)

The CBN has oscillated between caution and adoption. In its 2021 circular, it directed banks to cease cryptocurrency transactions, citing volatility, consumer risks, and financial crime.¹²¹ While this move curtailed the integration of cryptocurrencies into financial systems, it did not criminalise individual ownership. Yet, paradoxically, the CBN launched the eNaira in October 2021, a central bank digital currency (CBDC).¹²²

The implication is twofold: first, smart contracts that rely on cryptocurrencies for performance are practically hindered; second, there is potential for integration if the eNaira is embedded into blockchain platforms. However, without explicit regulation, this remains speculative.

Comparative Perspective

In the UK, the Financial Conduct Authority (FCA) regulates crypto-assets by classifying them as e-money or securities, ensuring that blockchain-based platforms are brought within existing financial regulation.¹²³ In the US, the SEC and the Commodity Futures Trading Commission (CFTC) assert jurisdiction over digital assets, with the SEC focusing on securities classification and the CFTC on derivatives.¹²⁴ Unlike Nigeria's outright prohibitionist posture, these regulators adopt a risk-based approach, permitting innovation under supervision.

¹²¹Central Bank of Nigeria, Circular No. CBN/GEN/DIR/INT/CIR/001/002 (5 February 2021).

¹²²Central Bank of Nigeria, Design Paper for the eNaira (2021).

¹²³Financial Conduct Authority (UK), "Guidance on Cryptoassets" (2020).

¹²⁴US SEC, "Framework for 'Investment Contract' Analysis of Digital Assets" (2019); US CFTC, "Digital Assets Primer" (2020).

The EU has gone further by adopting the MiCA Regulation (2023),¹²⁵ which provides a harmonised framework for crypto-assets, including rules on disclosure, licensing, and investor protection. The Nigerian approach is therefore restrictive and fragmented, limiting innovation while failing to create a comprehensive risk-based regime.

(ii). Securities and Exchange Commission (SEC)

The SEC Nigeria has issued statements recognising digital assets as securities when they resemble investment contracts.¹²⁶ It requires registration of offerings and imposes disclosure obligations. This is significant because smart contracts often facilitate investment schemes and tokenised platforms. By asserting jurisdiction, the SEC offers clarity to investors and issuers, even though its enforcement remains nascent.

Comparative Perspective

In the US, the SEC applies the Howey Test¹²⁷ to determine whether a digital asset constitutes an investment contract. Courts have upheld this approach, as seen in *SEC v W.J. Howey Co.*,¹²⁸ which defined securities broadly to cover investment schemes with an expectation of profit derived from others' efforts. Under this approach, many smart contract-based tokens fall within securities regulation.

By contrast, Nigeria's SEC lacks detailed jurisprudence or litigation, relying instead on broad guidelines. This limits predictability for commercial actors, leaving enforcement patchy compared to the US.

¹²⁵Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA).

¹²⁶Securities and Exchange Commission (Nigeria), "Statement on Digital Assets" (14 September 2020).

¹²⁷*SEC v W.J. Howey Co.* 328 U.S. 293 (1946).

¹²⁸*Ibid.*

(iii). National Information Technology Development Agency (NITDA)

NITDA has adopted a facilitative stance. Its 2023 National Blockchain Policy recognises blockchain as a tool for digital transformation in governance, finance, and supply chains.¹²⁹

Although non-binding, this policy reflects institutional recognition of blockchain's potential and hints at future regulatory sandboxes.

Comparative Perspective

The EU's approach, through the European Blockchain Services Infrastructure (EBSI), supports experimentation with blockchain in cross-border services, including notarisation and supply chain monitoring.¹³⁰ Similarly, Singapore has launched Project Ubin to test blockchain in payment settlements.¹³¹ NITDA's policy is a step in this direction but lacks legislative backing, rendering its initiatives more aspirational than binding.

(iv). Federal Competition and Consumer Protection Commission (FCCPC)

The FCCPC's 2022 Guidelines on Digital Commerce¹³² promote transparency and consumer remedies in online contracts. Although they do not mention smart contracts, their principles could apply to blockchain-based consumer transactions. The key challenge is rigidity: coded contracts may automatically execute terms without providing opportunities for redress, conflicting with statutory consumer protections.

Comparative Perspective

¹²⁹National Information Technology Development Agency, National Blockchain Policy (2023).

¹³⁰European Blockchain Services Infrastructure (EBSI), launched 2018.

¹³¹Monetary Authority of Singapore, "Project Ubin: Central Bank Digital Money Using Distributed Ledger Technology" (2020).

¹³²Federal Competition and Consumer Protection Commission, Guidelines on Digital Commerce (2022).

In the UK, consumer protection laws apply to digital contracts irrespective of technology, ensuring rights such as withdrawal from distance contracts.¹³³ Similarly, EU directives mandate consumer rights in digital transactions, which override automated contractual enforcement.¹³⁴ Nigeria's FCCPC could extend its guidelines in the same way, but lack of judicial or legislative clarification creates uncertainty.

C. Institutional Silence and Fragmentation

Nigeria's regulatory landscape is fragmented. The CBN restricts cryptocurrencies, the SEC regulates them as securities, NITDA promotes blockchain, and FCCPC oversees consumer rights, often without coordination. This creates conflicting obligations. For example, a blockchain-based investment scheme may be recognised as valid by SEC but simultaneously frustrated by CBN's banking restrictions.

In contrast, the UK and EU emphasise regulatory coordination. The UKJT's Legal Statement aligns judicial reasoning with regulatory clarity, while the EU's MiCA harmonises rules across member states. The US adopts a dual-regulatory model, with both SEC and CFTC asserting jurisdiction, though even here, debates about overlap persist. Nigeria, however, has neither harmonisation nor judicial guidance, amplifying uncertainty.

D. Implications for Enforceability

From this comparative analysis, several implications for Nigeria emerge:

¹³³Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (UK).

¹³⁴Directive 2011/83/EU on Consumer Rights.

1. Judicial readiness but lack of precedent. Nigerian courts are open to digital evidence but silent on smart contracts. By contrast, the UK and US have begun clarifying legal status through judicial or quasi-judicial pronouncements.
2. Regulatory ambivalence hinders certainty. The CBN's restrictive stance undermines SEC and NITDA's progressive policies, unlike the coordinated frameworks in the EU.
3. Consumer protection is underdeveloped. FCCPC guidelines lack the detailed enforcement structures of UK and EU consumer law, leaving coded contracts unchecked.
4. Comparative lag. Nigeria risks being left behind in digital commerce if judicial and regulatory institutions fail to provide certainty, as commercial actors may prefer jurisdictions with clearer frameworks.

Conclusively, Institutional and judicial responses in Nigeria reveal an uneasy tension between technological innovation and legal conservatism. Courts have cautiously adapted evidentiary rules to digital realities but have yet to pronounce on smart contracts directly. Regulators oscillate between prohibition (CBN), facilitation (NITDA), and partial regulation (SEC, FCCPC). By contrast, the UK, US, and EU have moved towards harmonisation and certainty, providing judicial guidance, regulatory frameworks, and consumer protection. For Nigeria, the lesson is clear: without a coordinated institutional response and judicial leadership, the enforceability of smart contracts will remain precarious, deterring innovation and undermining commercial confidence.

CHAPTER FOUR: COMMERCIAL AND JURISDICTIONAL CHALLENGES

4.1 Contractual Autonomy vs. Technological Determinism

A. Introduction

The central feature of contract law in Nigeria, as elsewhere in common law jurisdictions, is the doctrine of contractual autonomy , the principle that parties are free to determine the content of their agreements, provided such agreements do not contravene law or public policy. This principle is codified under common law doctrines of offer, acceptance, consideration, and intention to create legal relations. It reflects the liberal philosophy that contracting parties are rational agents best placed to regulate their own affairs.

However, the advent of smart contracts introduces an entirely new dimension , technological determinism. In this context, technological determinism refers to the idea that the terms of a contract, once translated into code and deployed on a blockchain, execute automatically without the possibility of human intervention or discretion. Unlike traditional contracts, where performance may be negotiated, deferred, or excused, smart contracts are self-enforcing and rigidly determined by the technological architecture. This tension between autonomy and determinism lies at the heart of commercial and jurisdictional challenges surrounding smart contracts in Nigeria.

B. Contractual Autonomy under Nigerian Law

The Nigerian legal system, influenced by English common law, has consistently upheld the principle of freedom of contract. In *Union Bank of Nigeria v Ozigi*,¹³⁵ the Court of Appeal reaffirmed that parties are generally bound by the terms of their voluntary agreements. Courts are reluctant to rewrite contracts freely entered into by consenting adults. Similarly, in *Orient Bank (Nig.) Plc v Bilante Int. Ltd*,¹³⁶ the Court held that it was not the function of courts to relieve a party of the burden of an unfavourable contract, emphasising sanctity of contract.

This jurisprudence underscores that Nigerian law prioritises autonomy: individuals and corporations can decide how they allocate risks, specify obligations, and agree on remedies. The corollary is that courts intervene sparingly, except where contracts are illegal, fraudulent, unconscionable, or contrary to statute.

C. Technological Determinism in Smart Contracts

Smart contracts challenge this doctrinal framework by embedding contractual performance into self-executing code. Once deployed, the blockchain ensures that performance occurs automatically when conditions are met, regardless of subsequent human intentions. For example, in a smart contract governing the sale of cryptocurrency, once payment is sent to the contract's wallet, the coded protocol automatically releases the agreed tokens to the buyer.

This differs radically from traditional contracts where parties might renegotiate, invoke doctrines of frustration, or plead non est factum in cases of mistake. In a smart contract, performance is technologically predetermined: if the code says “if A pays B, then transfer asset X,” the blockchain executes it without regard to fairness or unforeseen circumstances.

¹³⁵*Union Bank of Nigeria v Ozigi* (1994) 3 N.W.L.R. (Pt. 333) 385 (C.A.).

¹³⁶*Orient Bank (Nig.) Plc v Bilante Int. Ltd* (1997) 8 N.W.L.R. (Pt. 515) 37 (C.A.).

Scholars describe this as a shift from “**legal enforcement**” to “**technological enforcement.**”¹³⁷

The contract enforces itself, bypassing judicial supervision until disputes arise after execution.

The legal system is, therefore, confronted with agreements whose operation leaves little room for doctrines such as waiver, estoppel, or equitable relief.

D. The Tension Between Autonomy and Determinism

The key question is whether contractual autonomy is truly preserved when performance is predetermined by code. On the one hand, parties exercise autonomy when drafting the code: they freely decide which obligations and conditions to translate into self-executing scripts. On the other hand, once deployed, the parties lose control, since the blockchain will enforce the contract automatically regardless of subsequent will.

This tension raises doctrinal challenges. For example:

- **Mistake and Rectification:** In traditional contracts, if both parties are mistaken as to a fundamental term, courts may rectify or void the contract. In smart contracts, however, the blockchain executes irrespective of mistake, leaving courts with the difficult task of unwinding transactions already performed irreversibly.
- **Equitable Doctrines:** Nigerian law recognises doctrines such as undue influence, unconscionability, and frustration. Yet, how can these doctrines be applied to an agreement already executed by code? By the time a party approaches the court, the

¹³⁷Primavera de Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 76.

performance may be complete and irreversible.

- Party Autonomy vs Code Autonomy: True autonomy requires ongoing capacity to make decisions. Smart contracts transfer autonomy from human agents to computer code. This “code is law” phenomenon, famously articulated by Lessig,¹³⁸ sits uneasily with the Nigerian tradition of human-centred adjudication.

E. Nigerian Legal Responses and Comparative Lessons

While Nigerian courts have yet to confront this tension directly, they may draw guidance from comparative jurisdictions. In the UK, the UK Jurisdiction Taskforce (UKJT) Legal Statement on Cryptoassets and Smart Contracts (2019) affirmed that smart contracts are capable of creating binding legal obligations, whether expressed in natural language or code.¹³⁹ The UKJT emphasised that autonomy remains preserved at the point of drafting, even if execution is automatic.

In Nigeria, the principle of freedom of contract suggests that courts may adopt a similar approach, recognising that autonomy lies in the initial coding choice. However, Nigerian courts are also known for strong equitable intervention, as seen in *Akinsanya v UBA Ltd*,¹⁴⁰ where the Court of Appeal refused to enforce a contract tainted by unconscionability. This equitable tradition suggests that courts may attempt to override technological determinism in extreme cases, perhaps by ordering restitution even after blockchain execution.

¹³⁸Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 24.

¹³⁹UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019) para 36.

¹⁴⁰*Akinsanya v UBA Ltd* (1986) 4 N.W.L.R. (Pt. 35) 273 (C.A.).

F. Implications for Enforceability

The autonomy-determinism tension carries several implications for smart contract enforceability in Nigeria:

1. **Rigid Enforcement:** Nigerian courts may uphold self-executing outcomes as reflecting the autonomy of parties, even where performance is harsh.
2. **Judicial Intervention:** In equity, courts may override technological determinism by awarding restitutionary remedies, though practical enforcement against irreversible blockchain transfers remains problematic.
3. **Drafting Burden:** Lawyers and coders must anticipate contingencies at the drafting stage, since post-deployment modifications are difficult.
4. **Regulatory Impact:** Nigerian regulators, especially the SEC and FCCPC, may insist on disclosure and fairness requirements, tempering the determinism of code with protective oversight.

The Nigerian law of contract is built upon the edifice of autonomy, but smart contracts, through technological determinism, threaten to displace human control with automated execution. The courts are thus faced with the task of balancing respect for contractual freedom with the need for equitable intervention in the face of rigid code. The tension between autonomy and determinism

is not merely theoretical; it has profound commercial implications for enforceability, fairness, and jurisdictional competence in Nigeria.

4.2 Dispute Resolution and Cross-Border Jurisdiction

A. Introduction

Dispute resolution lies at the heart of contract law because parties require certainty that breaches will be remedied and rights enforced. In traditional contracts, this function is easily fulfilled by domestic courts and arbitral tribunals, since contracts are often localised within a particular jurisdiction. Jurisdiction is determined through connecting factors such as the place of contracting, the domicile or residence of the parties, and the locus of performance. Nigerian courts have consistently underscored the primacy of jurisdiction, with the Supreme Court in *Madukolu v Nkemdilim* stating that a court is competent to adjudicate only where it has jurisdiction over the subject matter, parties, and proper constitution.¹⁴¹

Smart contracts, however, upset this traditional paradigm. Because they are coded agreements executed on decentralised blockchain networks, they rarely have a physical location. A smart contract may involve a Nigerian buyer purchasing digital assets from a German seller via a blockchain platform operated by developers in Singapore. The transaction is verified across nodes scattered globally. This decentralisation raises fundamental questions:

- Where is the contract deemed to be formed?

¹⁴¹*Madukolu v Nkemdilim* (1962) 2 S.C.N.L.R. 341.

- Which jurisdiction's laws govern its performance?
- How are disputes to be resolved where no human discretion exists within the execution process?

The absence of answers creates serious risks for Nigerian commercial actors engaging with blockchain-based contracts.

B. Jurisdictional Challenges in Smart Contracts

(i) Place of Formation

Nigerian law generally determines jurisdiction partly by the place of formation of the contract. Under common law principles, a contract is concluded where acceptance is communicated. In cases like *Entores Ltd v Miles Far East Corporation*,¹⁴² courts have applied the “postal rule” and its electronic variations to determine when and where acceptance occurs.

But with smart contracts, acceptance occurs algorithmically, the contract is executed automatically when certain coded conditions are met. There is no “communication” of acceptance in the traditional sense, but a machine-triggered transaction on a blockchain ledger. Thus, applying existing rules to locate the “place of formation” is problematic. For instance:

- If a Nigerian enters a contract coded and deployed on a U.S.-based blockchain, is the place of formation Nigeria (where the user clicked “confirm”), the U.S. (where the

¹⁴²*Entores Ltd v Miles Far East Corporation* [1955] 2 QB 327.

blockchain was deployed), or global (since nodes are distributed across jurisdictions)?

- This ambiguity creates potential for conflicting jurisdictional claims, leading to forum shopping and uncertainty for Nigerian litigants.

(ii) Place of Performance

Performance in traditional contracts is tied to physical acts such as delivery of goods or payment of money. Nigerian law, as in *Nika Fishing Co. Ltd v Lavina Corporation*,¹⁴³ allows courts at the place of performance to assume jurisdiction. But in smart contracts, performance occurs digitally, often through instantaneous transfer of cryptocurrency or automated release of digital tokens. Since these transactions are validated simultaneously across multiple blockchain nodes worldwide, there is no singular “place of performance.”

This borderless performance erodes the applicability of Nigerian territorial jurisdiction rules. If a dispute arises, courts will struggle to pin down where the breach or performance occurred, complicating enforcement.

(iii) Multiplicity of Laws and Forum Non Conveniens

Smart contracts are inherently transnational. A single transaction may engage several jurisdictions simultaneously. Nigerian courts, following private international law, attempt to resolve conflicts by applying the doctrine of proper law of the contract or by invoking forum non

¹⁴³*Nika Fishing Co. Ltd v Lavina Corporation* (2008) 16 N.W.L.R. (Pt. 1114) 509 (S.C.).

conveniens. But without a clearly expressed governing law clause in the smart contract, determining the “proper law” becomes a Herculean task.

For example, in *Sonmez Denizcilik ve Ticaret A.S. v The MV “Bloomberg”*,¹⁴⁴ Nigerian courts emphasised that the choice of law governs validity and enforceability of contractual terms. In the absence of express provisions in a smart contract, the court may fall back on presumptions, such as law of the place of performance or formation, both of which are nebulous in blockchain transactions.

This uncertainty deters commercial actors from relying fully on smart contracts, as they cannot predict how Nigerian courts will approach jurisdictional conflicts.

C. Dispute Resolution Mechanisms

(i) Litigation in National Courts

Litigation in Nigerian courts offers a familiar dispute resolution pathway, but it suffers critical shortcomings for smart contracts. Firstly, jurisdictional uncertainties mean courts may decline competence, particularly where foreign parties are involved. Secondly, even if jurisdiction is established, enforcement of judgments is another challenge. For example, if damages are awarded against a defendant holding assets only in cryptocurrency wallets, Nigerian sheriffs cannot seize such assets without access to private keys, raising practical enforcement obstacles.

Furthermore, the technical complexity of blockchain transactions means judges and lawyers may lack the expertise to interpret the underlying code, leading to reliance on expert testimony, thereby prolonging litigation.

¹⁴⁴*Sonmez Denizcilik ve Ticaret A.S. v The MV “Bloomberg”* (2005) 1 N.W.L.R. (Pt. 940) 370.

(ii) Arbitration

Arbitration is traditionally preferred for cross-border commercial disputes, offering flexibility and enforceability under the New York Convention 1958, which Nigeria has ratified. The new Arbitration and Mediation Act 2023¹⁴⁵ strengthens the arbitral framework by incorporating emergency arbitration and modern recognition procedures.

Smart contracts can be programmed to include arbitration clauses. For instance, a coded instruction may specify that disputes be referred to arbitration in Lagos under the rules of the Lagos Court of Arbitration. This reduces uncertainty. However, questions remain:

- Do parties understand and consent to arbitration clauses written in programming languages?
- Can arbitrators interpret self-executing code, or must disputes be translated into natural language?
- What if the contract executes irreversibly before arbitration is triggered?

Unless these issues are addressed, arbitration may be undercut by the very automation it seeks to regulate.

(iii) Decentralised Dispute Resolution (DDRs)

¹⁴⁵ *Arbitration and Mediation Act 2023*, ss. 1–3.

Blockchain communities have experimented with decentralised dispute resolution systems such as Kleros, where jurors selected randomly from token holders decide disputes and record outcomes on-chain.¹⁴⁶ These systems are efficient and low-cost, but they lack state recognition. Under Nigerian law, only arbitration awards recognised by the Arbitration and Mediation Act or judgments of competent courts are enforceable. Thus, DDRs cannot presently substitute for legally binding dispute resolution.

D. Comparative Perspectives

The United States, through cases like *Zippo Manufacturing Co. v Zippo Dot Com, Inc.*,¹⁴⁷ developed the “sliding scale” test for internet jurisdiction, linking jurisdiction to the interactivity of online platforms. Nigerian courts could adapt this reasoning to blockchain contracts, assessing jurisdiction based on the degree of involvement of Nigerian parties or assets.

The European Union’s Brussels Regulation (Recast)¹⁴⁸ provides harmonised rules on jurisdiction and recognition of judgments, reducing forum-shopping. Nigeria could emulate this by developing statutory guidance for blockchain disputes.

The UK Jurisdiction Taskforce (UKJT), in its Legal Statement on Smart Contracts,¹⁴⁹ affirmed that smart contracts are capable of being valid, enforceable contracts under English law and can include express choice-of-law and jurisdiction clauses. This offers clarity Nigeria lacks, showing a path for reform.

¹⁴⁶Wessel Reijers et al, “Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies” (2018) 10 Technology Innovation Management Review 20.

¹⁴⁷*Zippo Manufacturing Co. v Zippo Dot Com, Inc.* 952 F Supp 1119 (WD Pa 1997).

¹⁴⁸Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and recognition of judgments in civil and commercial matters (Brussels I Recast).

¹⁴⁹UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019).

E. Implications for Nigerian Law

The jurisdictional and dispute-resolution issues arising from smart contracts have significant implications:

1. **Erosion of Territorial Jurisdiction:** Traditional Nigerian rules based on formation and performance are ill-suited to borderless transactions.
2. **Risk of Forum Shopping:** Without clarity, parties may deliberately structure transactions to avoid Nigerian jurisdiction, disadvantaging domestic commerce.
3. **Weak Enforcement Mechanisms:** Even where Nigerian courts assume jurisdiction, enforcing judgments against decentralised digital assets remains problematic.
4. **Need for Modernisation:** Nigeria must adopt legislative or judicial innovations, recognising coded arbitration clauses, promoting digital asset seizure frameworks, and clarifying jurisdictional rules in blockchain contexts.

Hence, dispute resolution and jurisdictional certainty are indispensable for the growth of commerce. Smart contracts, by their decentralised and autonomous nature, challenge the very foundations of these legal doctrines in Nigeria. Litigation is limited by jurisdictional vagueness, arbitration faces hurdles of code interpretation, and decentralised mechanisms lack state recognition. Unless Nigeria reforms its dispute resolution framework to accommodate technological change, its legal system risks obsolescence in the face of digital commerce.

4.3 Privity of Contract and Identity Verification Issues

The doctrine of privity of contract is one of the cornerstones of Nigerian contract law. Rooted in the English common law principle, it posits that only parties to a contract can sue or be sued upon it. The locus classicus is *Dunlop Pneumatic Tyre Co. Ltd v Selfridge & Co. Ltd*,¹⁵⁰ where Lord Haldane established that contractual rights and obligations cannot be conferred upon or enforced by strangers. Nigerian courts have consistently applied this doctrine. In *Ikpeazu v ACB Ltd*,¹⁵¹ the Supreme Court held that only the parties who have furnished consideration and assented to the terms of a contract have locus to enforce it.

Smart contracts, however, disrupt this doctrinal certainty. They are created, executed, and enforced through computer code on decentralised platforms. The parties often appear only as alphanumeric addresses without corresponding legal identities. Execution may also involve third parties such as miners, validators, and developers whose involvement is indispensable but who are not “parties” in the traditional sense. Thus, Nigerian law faces two fundamental challenges: (a) identifying who the “parties” are for the purposes of privity, and (b) determining whether contractual obligations and rights can be enforced in the absence of verified identities.

A. The Doctrine of Privity in Nigerian Law

Nigerian jurisprudence adopts the strict common law position that strangers to a contract cannot sue or be sued. The principle has been affirmed in cases such as *Ikpeazu v ACB Ltd*¹⁵² and *Afolabi v Polymera Industries (Nig.) Ltd*,¹⁵³ where courts refused to extend contractual benefits

¹⁵⁰*Dunlop Pneumatic Tyre Co. Ltd v Selfridge & Co. Ltd* [1915] AC 847.

¹⁵¹*Ikpeazu v ACB Ltd* (1965) N.M.L.R. 374 (S.C.).

¹⁵²*ibid.*

¹⁵³*Afolabi v Polymera Industries (Nig.) Ltd* (1967) N.M.L.R. 144 (S.C.).

to outsiders. While equity and agency principles sometimes mitigate the rigidity of privity, Nigerian courts have not embraced statutory reforms similar to the UK's Contracts (Rights of Third Parties) Act 1999, which allows expressly designated third parties to enforce certain contractual rights.

This rigidity presents a difficulty for smart contracts, where execution often involves actors beyond the immediate counterparties. For instance, if a blockchain developer embeds faulty code that leads to losses, can an aggrieved user sue the developer? Under privity, the answer is negative, as the developer was not a contracting party. The effect is to deny remedies to parties injured by actors who play critical roles in the transaction ecosystem.

B. Identifying Contracting Parties in Smart Contracts

In conventional transactions, the identity of parties is established through names, signatures, addresses, and registration numbers (for companies). Nigerian courts insist on certainty of parties; in *Okwejinor v Gbakeji*,¹⁵⁴ the Court of Appeal held that a valid contract must be certain as to the parties.

Smart contracts, however, are executed between pseudonymous blockchain addresses. A wallet address does not disclose the person behind it. Thus, if a Nigerian company contracts with a counterparty whose wallet belongs to an anonymous individual in another jurisdiction, the “identity” of the contracting party is obscure. Without verifiable identity, courts may struggle to enforce the agreement.

¹⁵⁴*Okwejinor v Gbakeji* (2008) 5 NWLR (Pt. 1079) 172 (C.A.).

Consider this hypothetical: a Nigerian fintech company enters a smart contract with what it believes to be a Swiss investor for cryptocurrency-based services. Later, the investor defaults. When the Nigerian company seeks enforcement, it discovers the “Swiss investor” is an anonymous actor based in another jurisdiction. Under Nigerian law, the contract could be deemed void for uncertainty of parties, undermining enforceability.

C. The Problem of Third Parties in Blockchain Transactions

Smart contracts often involve participants who are neither “parties” nor total strangers. These include:

- Developers who design the contract code;
- Validators/miners who confirm transactions on the blockchain; and
- Platform operators who host decentralised applications.

Under strict privity, such actors owe no contractual duties to end-users. However, their actions can directly impact outcomes. A coding error by a developer or network manipulation by a validator could lead to massive losses. Nigerian courts, applying traditional doctrine, would exclude liability since there is no privity. Yet this approach may be unjust in blockchain contexts, where the distinction between parties and facilitators is blurred.

In comparative perspective, English law has gradually allowed exceptions to privity, especially through statutory intervention. The UK’s Contracts (Rights of Third Parties) Act 1999 allows

contracting parties to confer enforceable rights on third parties if expressly stated.¹⁵⁵ Nigeria lacks such statutory reform, leaving privity as an obstacle to fair outcomes in smart contract disputes.

D. Identity Verification and Consent

Another obstacle to enforceability is the requirement of consensus ad idem (meeting of the minds). For a valid Nigerian contract, there must be genuine agreement between identifiable parties. In *Sule v Aromire*,¹⁵⁶ the court held that lack of consensus renders a contract void. Where parties are pseudonymous blockchain addresses, it is debatable whether there is true consensus.

Identity verification is essential not only for establishing contractual parties but also for preventing fraud and illegality. Nigerian law, through the Central Bank of Nigeria (CBN) Know Your Customer (KYC) Regulations,¹⁵⁷ requires financial institutions to verify customer identities. However, smart contracts executed on decentralised platforms bypass such frameworks, allowing transactions without institutional oversight. This increases risks of impersonation, fraud, and money laundering, which courts may consider contrary to public policy.

E. Fraud, Mistake, and Illegality from Identity Ambiguity

The absence of verified identities creates fertile ground for fraud and mistake. Nigerian courts recognise that mistake as to identity can vitiate a contract. In *Solle v Butcher*,¹⁵⁸ the English Court of Appeal acknowledged that fundamental mistakes, including about the identity of a

¹⁵⁵Contracts (Rights of Third Parties) Act 1999 (UK), ss. 1–2.

¹⁵⁶*Sule v Aromire* (1964) N.M.L.R. 94.

¹⁵⁷Central Bank of Nigeria, *AML/CFT Regulations* (2013).

¹⁵⁸*Solle v Butcher* [1950] 1 KB 671.

party, may invalidate consent. If a Nigerian company unknowingly contracts with a fraudulent actor masked behind a blockchain address, the contract could be void ab initio.

Similarly, contracts with anonymous or pseudonymous parties could facilitate criminal activities such as money laundering or terrorist financing. Nigerian courts may refuse enforcement on the grounds of illegality. In *Niger Insurance Co. Ltd v Abed Brothers Ltd*,¹⁵⁹ the Supreme Court held that courts will not enforce contracts tainted with illegality, even where innocent parties suffer loss. This poses risks for smart contracts executed without adequate identity verification.

F. Comparative Perspectives

- United States: Courts have demonstrated willingness to pierce pseudonymity. In *United States v Ulbricht*,¹⁶⁰ the operator of Silk Road was unmasked and prosecuted despite pseudonymous transactions. Nigerian authorities could adopt similar approaches, relying on cybercrime legislation to trace blockchain identities.
- European Union: The EU's 5th Anti-Money Laundering Directive (AMLD5)¹⁶¹ mandates crypto-exchanges and wallet providers to verify customer identities, indirectly linking blockchain addresses to real-world individuals. This enhances enforceability by ensuring contracting parties can be legally identified.
- United Kingdom: The UK Jurisdiction Taskforce (UKJT) confirmed that smart contracts are enforceable under English law, provided that contractual elements, including

¹⁵⁹*Niger Insurance Co. Ltd v Abed Brothers Ltd* (1976) 7 S.C. 35.

¹⁶⁰*United States v Ulbricht* 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

¹⁶¹Directive (EU) 2018/843 (5th Anti-Money Laundering Directive).

identification of parties, are satisfied.¹⁶² This reflects a pragmatic approach, balancing doctrinal principles with technological realities.

Nigeria, however, lacks a statutory framework harmonising blockchain transactions with contract and financial regulation, leaving gaps in identity verification and third-party rights.

G. Implications for Nigerian Law

The intersection of the doctrine of privity and the problem of identity verification in smart contracts raises profound implications for the Nigerian legal system. These implications are doctrinal, regulatory, and commercial in nature, and if left unaddressed, they could hinder Nigeria's ability to harness the economic and technological benefits of blockchain.

(i) Doctrinal Rigidity and Outdated Common Law Principles

The strict adherence of Nigerian courts to the traditional doctrine of privity means that third-party actors in smart contracts, such as developers, miners, oracles, and validators, are excluded from contractual rights and obligations. This rigidity contrasts sharply with the multi-actor ecosystem of blockchain transactions. For example, if a coding error embedded by a developer results in financial loss, Nigerian courts applying strict privity would bar the injured party from claiming damages against the developer since no contractual nexus exists between them. This situation reflects the limits of importing early twentieth-century common law principles (like *Dunlop Pneumatic Tyre*¹⁶³) into twenty-first-century technologies. Unless

¹⁶²UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019).

¹⁶³*Dunlop Pneumatic Tyre Co. Ltd v Selfridge & Co. Ltd* [1915] AC 847.

reformed, privity will continue to insulate critical blockchain actors from liability, producing outcomes that undermine justice and commercial certainty.

(ii) Uncertainty of Parties and Enforceability Problems

The Nigerian law of contract requires certainty as to parties, offer, acceptance, and consideration.¹⁶⁴ Pseudonymous transactions, where parties are identified only by alphanumeric wallet addresses, create difficulty in proving who exactly assumed contractual obligations. Courts may declare such contracts void for uncertainty, as they did in *Okwejiminor v Gbakeji*,¹⁶⁵ where the lack of clarity about parties defeated contractual enforceability. In the blockchain context, an anonymous wallet address cannot satisfy the legal requirement for identifiable parties, unless regulatory frameworks like Know Your Customer (KYC) procedures are integrated. This uncertainty undermines the enforceability of smart contracts under Nigerian law, creating significant risks for businesses.

(iii) The Gap between Private Law and Regulatory Compliance

Nigeria's financial regulatory framework, spearheaded by the Central Bank of Nigeria (CBN), insists on robust identity verification through KYC and Anti-Money Laundering (AML) requirements.¹⁶⁶ Smart contracts on public blockchains bypass institutional intermediaries and regulatory checks, facilitating anonymous transactions. This creates tension between private law enforcement of contracts and the state's public law objective of preventing financial crimes. Where transactions appear to circumvent KYC obligations, Nigerian courts may refuse enforcement on grounds of illegality or public policy, as seen in *Niger Insurance Co. Ltd v Abed*

¹⁶⁴*Sule v Aromire* (1964) N.M.L.R. 94.

¹⁶⁵*Okwejiminor v Gbakeji* (2008) 5 NWLR (Pt. 1079) 172 (C.A.).

¹⁶⁶Central Bank of Nigeria, *AML/CFT Regulations* (2013).

Brothers Ltd.¹⁶⁷ Thus, identity verification in blockchain is not only a matter of contractual certainty but also of compliance with financial regulation.

(iv) Risk of Fraud, Mistake, and Illegality

The inability to verify counterparties' identities exposes parties to heightened risks of fraud and mistake. Nigerian law recognises that mistake as to identity can void a contract *ab initio*.¹⁶⁸

Similarly, contracts tainted by illegality, such as those facilitating money laundering or terrorist financing, will not be enforced.¹⁶⁹ In practice, this means many smart contracts in Nigeria could be unenforceable even if technically valid, because they fail to meet the threshold requirements of legality and consensus *ad idem*. This risk discourages businesses from adopting smart contracts for high-value or sensitive transactions.

(v) Commercial Risks and Inhibiting Innovation

The combination of privity, identity uncertainty, and regulatory gaps discourages Nigerian businesses from embracing blockchain-based smart contracts. Fintech firms, start-ups, and even traditional corporations may be reluctant to adopt such tools without legal assurance of enforceability. This hesitancy could stifle innovation and prevent Nigeria from fully participating in the global digital economy, especially in sectors like decentralised finance (DeFi), cross-border remittances, and supply-chain tracking where blockchain offers efficiency gains. Meanwhile, jurisdictions such as the United Kingdom (through the UK Jurisdiction Taskforce's statement¹⁷⁰) and the European Union (via AMLD5¹⁷¹) are already aligning law with technology,

¹⁶⁷*Niger Insurance Co. Ltd v Abed Brothers Ltd* (1976) 7 S.C. 35.

¹⁶⁸*Solle v Butcher* [1950] 1 KB 671.

¹⁶⁹*ibid.*

¹⁷⁰UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019).

¹⁷¹Directive (EU) 2018/843 (5th Anti-Money Laundering Directive).

thereby attracting investment and innovation. Nigeria risks being left behind if reforms are not introduced.

(vi) Need for Legal Reform and Doctrinal Flexibility

These challenges highlight the urgent need for legislative and judicial innovation in Nigeria.

Possible reforms include:

1. Adopting a Nigerian equivalent of the UK's Contracts (Rights of Third Parties) Act 1999, allowing third parties explicitly conferred rights in smart contracts to sue or be sued.
2. Developing statutory recognition of digital identities, ensuring blockchain addresses are tied to verifiable legal persons or entities.
3. Integrating smart contracts into financial regulatory frameworks, obligating platforms and exchanges operating in Nigeria to implement robust KYC/AML measures.
4. Judicial pragmatism, where Nigerian courts adopt purposive interpretations of privity, recognising the functional roles of blockchain intermediaries without waiting for statutory reform.

Such reforms would modernise Nigerian contract law, harmonise it with regulatory needs, and foster a more enabling environment for innovation.

The combined effects of doctrinal rigidity, uncertain identities, regulatory non-alignment, and fraud risks mean that smart contracts presently face serious enforceability challenges in Nigeria. Unless Nigerian law adapts by reforming the doctrine of privity and establishing mechanisms for identity verification, smart contracts will remain legally precarious. This could isolate Nigeria from the benefits of blockchain-driven commerce, placing it at a competitive disadvantage globally. The implications therefore extend beyond mere doctrinal debates: they affect Nigeria's economic growth, technological competitiveness, and the integrity of its legal system in the digital age.

4.4 Fraud, Mistake, and Illegality in Smart Contracts

The enforceability of contracts under Nigerian law rests not only on their compliance with the requirements of offer, acceptance, intention to create legal relations, and consideration, but also on the absence of vitiating elements such as fraud, mistake, and illegality.¹⁷² Nigerian jurisprudence has consistently held that contracts tainted by these elements are either void or voidable. In the context of smart contracts, self-executing agreements encoded on blockchain, these doctrines assume new significance, given the unique challenges posed by automation, pseudonymity, and immutability.

A. Fraud in Smart Contracts

(i) Nigerian Legal Position on Fraud

Fraud, under Nigerian contract law, is a species of misrepresentation that goes to the root of consent. In *Adeniji v Adeniji*,¹⁷³ the court defined fraud as a “false representation of fact made

¹⁷²*Sule v Aromire* (1964) N.M.L.R. 94.

¹⁷³*Adeniji v Adeniji* (1972) 1 All NLR (Pt. 1) 298.

knowingly, without belief in its truth, or recklessly, careless whether it be true or false.” In *Oba Adebayo & Sons Ltd v National Bank of Nigeria Ltd*,¹⁷⁴ the Supreme Court stressed that fraud invalidates a contract ab initio.

(ii) Fraud in the Smart Contract Context

Smart contracts, despite their promise of transparency, are susceptible to fraud:

- Identity fraud: Parties transact under pseudonymous blockchain addresses, making it easy for fraudsters to misrepresent themselves as trusted entities.
- Coding fraud: Developers may deliberately embed hidden instructions or “backdoors” that transfer assets without the counterparty’s consent.
- Ponzi and “rug-pull” schemes: Investors are induced to fund smart contracts with the promise of returns, only for project promoters to abscond with the assets.

For example, if a Nigerian investor enters a decentralised lending contract under the belief that the counterparty is a registered financial institution, but later discovers the address belonged to an impostor, the investor may claim fraud. However, unlike in traditional contracts where rescission restores parties to their pre-contractual positions, blockchain’s immutability means that once the contract executes, funds may be irretrievable without intervention by courts or regulators.

¹⁷⁴*Oba Adebayo & Sons Ltd v National Bank of Nigeria Ltd* (1962) 1 All NLR 113.

(iii) Remedies and Limitations

While Nigerian courts may declare such contracts voidable for fraud, practical enforcement remains problematic. Even if rescission is ordered, blockchain systems lack a central authority to reverse transactions. Unless funds are frozen in custodial wallets or the fraudster is unmasked, remedies may be ineffective. This tension illustrates the gulf between doctrinal principles and technological realities.

B. Mistake in Smart Contracts

(i) Nigerian Law on Mistake

Mistake undermines the consensus ad idem required for valid contracts. Nigerian courts distinguish between common mistake (both parties share the same mistaken belief), mutual mistake (both are mistaken but about different things), and unilateral mistake (one party is mistaken, the other is not). In *Okonkwo v Kpajie*,¹⁷⁵ the Supreme Court recognised that where mistake goes to the root of the agreement, the contract is void.

(ii) Mistake in Smart Contracts

Smart contracts are particularly prone to mistakes because of their technical nature:

- Coding errors: If the code incorrectly reflects the parties' true intention, it may execute unintended outcomes. A misplaced decimal point in a loan agreement could transfer 1000 tokens instead of 100.

¹⁷⁵*Okonkwo v Kpajie* (1992) 2 NWLR (Pt. 226) 633 (S.C.).

- Oracle errors: Smart contracts often rely on “oracles” for external data (e.g., exchange rates). If incorrect data is fed, transactions may execute on false premises.
- Misunderstanding code terms: Non-programmer parties may mistakenly believe the contract does one thing when, in fact, the code specifies another.

These raise complex questions: should the code be treated as the sole embodiment of the parties’ intention, or should courts look beyond the code to the subjective agreement? The principle in *Solle v Butcher*¹⁷⁶ suggests courts may void contracts for fundamental mistakes. But in practice, proving mistakes in a smart contract may require expert technical evidence.

(iii) Implications

If Nigerian courts adopt a strict “code is law” approach, mistakes in code would bind the parties, undermining fairness. If they adopt a purposive approach, recognising mistakes where code deviates from intention, courts may have to craft remedies, such as restitution or reformation of the contract.

C. Illegality in Smart Contracts

(i) Nigerian Law on Illegality

Contracts prohibited by statute or contrary to public policy are void ab initio. In *Niger Insurance Co. Ltd v Abed Brothers Ltd*,¹⁷⁷ the Supreme Court held that courts will not enforce contracts tainted with illegality, reaffirming the maxim *ex turpi causa non oritur actio*.

¹⁷⁶*Solle v Butcher* [1950] 1 KB 671.

¹⁷⁷*Niger Insurance Co. Ltd v Abed Brothers Ltd* (1976) 7 S.C. 35.

(ii) Illegality in Smart Contracts

Smart contracts may facilitate:

- Money laundering and terrorist financing, prohibited under the Money Laundering (Prohibition) Act 2011.¹⁷⁸
- Gambling contracts, where platforms facilitate decentralised betting in breach of the National Lottery Act.
- Sanctions evasion, where parties use blockchain to circumvent government restrictions.

Such contracts would not only be void but also expose parties to criminal liability.

(iii) Comparative Lessons

The U.S. prosecution of *United States v Ulbricht*¹⁷⁹ (Silk Road case) demonstrated how illegal marketplaces can operate through smart contracts, with courts ready to override claims of technological neutrality. Similarly, EU regulations (AMLD5)¹⁸⁰ compel identification in crypto transactions to prevent illegal use. Nigeria, however, lacks equivalent blockchain-specific safeguards, making courts likely to strike down such contracts when detected.

D. Implications for Nigerian Law

¹⁷⁸Money Laundering (Prohibition) Act 2011 (as amended).

¹⁷⁹*United States v Ulbricht* 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

¹⁸⁰Directive (EU) 2018/843 (5th Anti-Money Laundering Directive).

1. Doctrinal Continuity: Fraud, mistake, and illegality remain relevant to smart contracts; Nigerian courts will apply them as they do in traditional contracts.
2. Practical Limits of Enforcement: Even where fraud or mistake is proven, irreversibility of blockchain transactions weakens judicial remedies.
3. Regulatory Gaps: Without statutory reforms mandating digital identity verification and blockchain compliance, illegality will remain difficult to police.
4. Risk to Commercial Adoption: Businesses in Nigeria may avoid smart contracts for fear of unenforceability or exposure to illegal dealings, stifling fintech innovation.

Conclusively, fraud, mistake, and illegality in smart contracts highlight the tension between traditional doctrines of Nigerian contract law and the technological peculiarities of blockchain systems. While courts may rely on established precedents to address fraud and mistake, and refuse to enforce illegal contracts, the practical enforceability of remedies remains doubtful given the decentralised and immutable nature of blockchain. Unless reforms address these gaps, through digital identity frameworks, statutory recognition of smart contracts, and regulatory oversight, Nigerian parties will continue to face significant legal and commercial risks in adopting blockchain-based agreements.

4.5 Regulatory Uncertainty and Consumer Protection in Smart Contracts

One of the most pressing challenges posed by smart contracts in Nigeria is the absence of a clear regulatory framework coupled with insufficient consumer protection mechanisms. Unlike traditional contracts, which are shaped by centuries of judicial precedent and statutory refinement, smart contracts operate in a largely unregulated technological environment. This results in significant uncertainty as to their enforceability, the institutions with oversight powers, and the remedies available to consumers in cases of fraud, mistake, or unfair practices.

In Nigeria, regulation of financial and contractual transactions lies primarily in the hands of the Central Bank of Nigeria (CBN), the Securities and Exchange Commission (SEC), and the Federal Competition and Consumer Protection Commission (FCCPC). However, these institutions approach blockchain and digital assets with caution, often focusing on cryptocurrency while leaving smart contracts largely unaddressed.

4.5.1 Regulatory Uncertainty in Smart Contracts

(a) Absence of Smart Contract Recognition

Unlike traditional contracts, which Nigerian courts enforce based on the common law of contracts and the Contracts Act 1917 (applicable in parts of the country), smart contracts lack express statutory recognition. No Nigerian legislation currently stipulates whether a contract executed exclusively through blockchain code can be admitted in evidence as a valid legal instrument.

By contrast, U.S. jurisdictions such as Arizona and Tennessee expressly provide that smart contracts shall not be denied legal validity solely because of their blockchain nature.¹⁸¹ The

¹⁸¹Arizona Revised Statutes §44-7061 (2017); Tennessee Senate Bill 1662 (2018).

absence of similar statutory clarity in Nigeria leaves parties uncertain as to whether judges will enforce blockchain-based agreements without an accompanying written document.

(b) Jurisdictional Challenges

The borderless nature of blockchain technology raises profound jurisdictional issues. Nigerian courts determine jurisdiction by reference to territorial nexus and the parties' intentions, as established in *Nika Fishing Co Ltd v Lavina Corp.*¹⁸² However, smart contracts are typically coded without jurisdiction or governing law clauses, leaving courts to grapple with conflict-of-laws rules.

For instance, a Nigerian entrepreneur might execute a loan agreement through a smart contract coded on the Ethereum blockchain, with the counterparty domiciled in London and the server nodes distributed globally. If a dispute arises, should the Nigerian court apply domestic contract law, the law of England and Wales, or international arbitration principles? Without statutory or judicial guidance, the answer remains unsettled.

(c) Fragmented Regulatory Stance: CBN and SEC

The CBN's 2021 circular prohibiting banks from dealing in cryptocurrencies¹⁸³ created significant uncertainty for blockchain-based transactions in Nigeria. Although the directive was softened in 2023 with guidelines allowing licensed Virtual Asset Service Providers (VASPs), the CBN's cautious stance sends mixed signals to businesses exploring smart contract applications.

¹⁸²*Nika Fishing Co Ltd v Lavina Corp* (2008) 16 NWLR (Pt. 1114) 509.

¹⁸³CBN Circular to Deposit Money Banks, OFIs and Payment Service Providers, "Re: Transactions in Cryptocurrencies" (5 February 2021).

In contrast, the SEC’s 2020 Statement on Digital Assets classified certain digital tokens as securities under the Investment and Securities Act 2007.¹⁸⁴ However, the statement is silent on smart contracts, leaving questions as to whether self-executing agreements fall under securities regulation, financial services regulation, or remain in a regulatory vacuum. This fragmentation undermines investor confidence and hinders innovation.

4.5.2 Consumer Protection Challenges

(a) Weakness of Traditional Safeguards

The FCCPA 2018 establishes extensive protections for consumers, including prohibitions on unfair contract terms (section 120) and misleading trade practices (sections 115–117).¹⁸⁵ Yet these safeguards presuppose contracts drafted in plain language and executed through identifiable parties. Smart contracts, by contrast, present difficulties because:

- They execute automatically and irreversibly, even where consumers allege misrepresentation or mistake.
- Parties are frequently pseudonymous, making it impossible to identify who should bear liability.
- They rarely incorporate statutory terms implied by law, such as merchantability or fitness for purpose.

¹⁸⁴SEC Nigeria, “Statement on Digital Assets and their Classification and Treatment” (14 September 2020).

¹⁸⁵Federal Competition and Consumer Protection Act 2018, ss. 115–120.

Thus, while the FCCPA theoretically protects consumers, its provisions are hard to apply to automated blockchain transactions.

(b) Information Asymmetry and Technical Complexity

The average Nigerian consumer lacks the technical expertise to audit blockchain code.

Developers and coders therefore occupy a position of superior bargaining power, able to embed hidden fees, exploitative terms, or even backdoors into smart contracts.

For example, in decentralised finance (DeFi) protocols, contract codes may contain “kill switches” allowing developers to freeze user funds. If a Nigerian consumer falls victim to such a mechanism, the courts may invoke equity or the FCCPA to provide relief. Yet enforcement remains difficult when the developer is anonymous or located outside Nigeria.

(c) Absence of Built-in Dispute Resolution

Unlike traditional contracts, which often include arbitration clauses or recourse to consumer protection tribunals, most smart contracts are silent on dispute resolution. Once executed, the contract code governs the transaction with no room for negotiation or remedial mechanisms.

Some blockchain projects experiment with decentralised dispute resolution platforms, such as Kleros (an on-chain arbitration mechanism). However, these platforms have not been recognised under the Arbitration and Mediation Act 2023 in Nigeria. Nigerian courts are therefore unlikely to enforce awards issued by such bodies, leaving consumers without recourse.

4.5.3 Comparative Perspectives

(a) United Kingdom

The United Kingdom has taken a pragmatic approach toward smart contracts, relying on its flexible common-law system. In 2021, the Law Commission published “Smart Legal Contracts: Advice to Government”, concluding that existing common-law principles are sufficiently adaptable to accommodate smart contracts without requiring comprehensive statutory reform.¹⁸⁶ The Commission categorised smart contracts into three forms: hybrid contracts, which combine natural-language terms with automated code; fully code-based contracts, where obligations are executed entirely by code; and agreements that integrate digital signatures to authenticate intent.¹⁸⁷ It affirmed that the fundamental elements of contract formation, including offer, acceptance, consideration, and intention to create legal relations, remain applicable to smart contracts.¹⁸⁸ Courts are therefore expected to treat such agreements as binding if these elements are satisfied.¹⁸⁹

The Commission further highlighted the admissibility of electronic records and cryptographic signatures, noting that blockchain transaction logs could be used as evidence where authenticity and reliability are established.¹⁹⁰ This allows smart contracts to satisfy writing or signature requirements in contexts where the law demands formality, such as under the Statute of Frauds. Nevertheless, challenges persist, particularly concerning smart contracts intended to take effect as deeds and private international law, where the question of jurisdiction and applicable law may be complex due to the decentralised and borderless nature of blockchain.¹⁹¹ These concerns are especially relevant for transactions involving tokenised assets or cross-border parties, where the physical location of parties or nodes may not align with the governing law.

¹⁸⁶UK Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 25 November 2021) paras 3.4–3.6.

¹⁸⁷*Ibid*, paras 4.12–4.18.

¹⁸⁸*Ibid*, paras 4.12–4.18.

¹⁸⁹*Ibid*, paras 4.24–4.25.

¹⁹⁰ *Ibid*, paras 4.68–4.72.

¹⁹¹*Ibid*, paras 5.1–5.8.

(b) United States

In the United States, the legal framework recognises electronic agreements and signatures through federal and state legislation. The Electronic Signatures in Global and National Commerce Act (E-SIGN, 2000) establishes that electronic contracts, records, and signatures are legally equivalent to paper-based counterparts.¹⁹² At the state level, most jurisdictions have adopted the Uniform Electronic Transactions Act (UETA, 1999), which similarly validates electronic records and signatures and provides statutory certainty for digital agreements.¹⁹³

Legal scholars have argued that these statutes extend naturally to smart contracts executed electronically, including blockchain-based agreements, provided they satisfy traditional contract law requirements such as offer, acceptance, consideration, and lawful purpose.¹⁹⁴ Courts have generally treated certain smart contract transactions as enforceable when parties can demonstrate consent and execution through identifiable digital signatures.¹⁹⁵ Practical challenges remain, however, including interpreting consent in fully automated contracts, compliance with state-specific statute-of-frauds provisions, and verifying identity when parties interact via pseudonymous blockchain addresses.¹⁹⁶ These issues illustrate that while statutory frameworks exist to support enforceability, practical considerations related to digital identification, security, and accountability must be addressed to ensure full legal recognition.

(c) European Union

¹⁹² Electronic Signatures in Global and National Commerce Act 2000 (E-SIGN), 15 USC §§ 7001–7031.

¹⁹³ Uniform Electronic Transactions Act 1999 (UETA), ss 1–14.

¹⁹⁴ N. Szabo, “Smart Contracts: Background and Legal Status,” in *Smart Contracts – Law, Practice and Technology* (2018) 5–12.

¹⁹⁵ *Ibid.*

¹⁹⁶ *Ibid.*, 12–15.

Within the European Union, the eIDAS Regulation (EU Regulation 910/2014) provides a harmonised framework for electronic identification and trust services. It recognises electronic signatures, including advanced and qualified types, as legally equivalent to handwritten signatures.¹⁹⁷ This recognition allows contracts executed electronically, including smart contracts, to satisfy formal requirements for enforceability across member states. Although eIDAS does not explicitly mention smart contracts, its recognition of electronic identification and trust services creates a framework within which smart contracts can be legally effective, particularly where they incorporate secure digital signatures and verifiable records.¹⁹⁸

EU authorities have emphasised compliance with consumer protection laws, data protection regulations, and general contract law, signalling that enforceability is contingent not only on technical execution but also on broader regulatory compliance.¹⁹⁹ This ensures that smart contracts, even when executed automatically, respect the rights of contracting parties and adhere to principles of fairness, transparency, and accountability. Regulatory guidance also addresses cross-border enforcement, highlighting the importance of harmonised legal standards in multi-jurisdictional contexts.

Synthesis and Implications for Nigeria

A comparative examination of these jurisdictions reveals several insights for Nigeria. The UK demonstrates that enforceability can be achieved through judicial adaptation of existing contract principles.²⁰⁰ The US model highlights the advantages of technology-neutral legislation that

¹⁹⁷ Regulation (EU) 910/2014 on electronic identification and trust services (eIDAS), Art 25.

¹⁹⁸ European Commission, *Distributed Ledger Technology and Blockchain: Legal and Regulatory Overview* (2020) 14–18.

¹⁹⁹ *Ibid*, 19–22.

²⁰⁰ UK Law Commission, *Smart Legal Contracts: Advice to Government* (n 1) paras 6.1–6.4.

validates electronic contracts broadly.²⁰¹ The EU shows the benefits of harmonised electronic signature frameworks combined with regulatory oversight.²⁰² Across all three jurisdictions, enforceability depends not only on legal recognition but also on evidentiary standards, identity verification, and the careful integration of automated code with human-readable contract terms.

For Nigeria, these comparative lessons suggest that smart contracts could be integrated into the legal system through adaptation of existing laws, technology-neutral statutory reforms, or a combination of both. Lawmakers may adopt statutory recognition of electronic agreements, guidance on evidentiary requirements, and mechanisms for dispute resolution, while also allowing judicial interpretation to handle unforeseen scenarios. Such reforms would enhance commercial certainty and support the growth of blockchain-based transactions and fintech innovation within the Nigerian legal framework.

4.6 Enforcement Mechanisms in Practice

Enforcement of smart contracts under Nigerian law represents a novel challenge, testing the capacity of both judicial and regulatory institutions to adapt traditional legal doctrines to modern technological realities. While the Nigerian legal system provides extensive mechanisms for enforcing contractual obligations, through litigation, arbitration, or statutory regulation, these mechanisms assume that the contract is a human-readable document executed between identifiable parties. Smart contracts, by contrast, are self-executing codes, often anonymous, decentralised, and borderless, raising unique practical difficulties for enforcement.

²⁰¹ N. Szabo (n 9) 10–12.

²⁰² European Commission (n 13) 20–22.

This section examines these mechanisms, the limits of judicial intervention, and how Nigerian courts, regulators, and legal practitioners can approach the enforcement of smart contracts in practice.

(a) Judicial Enforcement and the Problem of Code as Law

Smart contracts execute automatically once pre-set conditions are met, leaving little room for judicial discretion. In a traditional contract, a party may approach the court for specific performance, injunction, or damages for breach. However, in a blockchain-based agreement, performance occurs automatically through the operation of code, often rendering judicial intervention *ex post facto*.

The jurisprudential debate on “code as law,” advanced by Lawrence Lessig, posits that in the digital realm, software dictates behaviour in the same way that law does.²⁰³ Nigerian courts, however, are not equipped to “reverse” the code once it executes. This limitation raises the question: how can courts enforce, rescind, or modify a contract that has already executed itself without central authority?

An instructive analogy can be drawn from *Okoli v. Morecab Finance (Nig.) Ltd*,²⁰⁴ where the Court of Appeal reiterated that equity will not allow a statute or instrument to be used as an engine of fraud. Applied to smart contracts, this suggests that if a smart contract operates unjustly or fraudulently (for instance, if the code is designed to divert funds to an unintended address), a court could intervene equitable reliefs, such as restitution or tracing. However,

²⁰³L. Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 6.

²⁰⁴*Okoli v. Morecab Finance (Nig.) Ltd* (2007) 14 NWLR (Pt. 1053) 37.

technical enforcement , such as reversing transactions , remains practically difficult since blockchain records are immutable.

(b) Admissibility of Smart Contract Evidence

The enforceability of smart contracts also depends on whether digital records and blockchain data are admissible as evidence in Nigerian courts. The Evidence Act 2011, sections 84 and 258, recognises the admissibility of electronic records provided that the party tendering such evidence satisfies the conditions for reliability and authenticity.

In *Kubor v. Dickson*,²⁰⁵ the Supreme Court held that electronically generated documents (such as computer printouts) are admissible once compliance with section 84 is demonstrated. Similarly, in *FRN v. Fani-Kayode*,²⁰⁶ the court admitted digital evidence where the integrity of the electronic device was established.

Applying these principles, a party seeking to enforce a smart contract could tender blockchain transaction data , such as timestamps, wallet addresses, or execution logs , as proof of performance or breach. However, practical challenges persist:

- Blockchain addresses are pseudonymous, making it difficult to tie a transaction to a legal person.
- Parties may dispute the reliability of blockchain records, particularly if forks or smart contract bugs occur.

²⁰⁵*Kubor v. Dickson* (2012) 12 NWLR (Pt. 1315) 230.

²⁰⁶*FRN v. Fani-Kayode* (2010) LPELR-4140(CA).

- Expert witnesses with technical competence would be required to interpret the code and validate its execution.

Thus, while the Evidence Act theoretically accommodates smart contracts, Nigerian procedural law has yet to develop protocols for authenticating blockchain evidence in commercial disputes.

(c) Arbitration and Alternative Dispute Resolution

Given the technological nature of smart contracts, arbitration and ADR mechanisms may offer a more practical enforcement path than litigation. The Arbitration and Mediation Act 2023 expressly allows electronic agreements to constitute valid arbitration clauses,²⁰⁷ suggesting that a smart contract coded with an arbitration trigger could give rise to a valid arbitral submission.

However, a problem arises when the arbitration clause itself is embedded within the smart contract code and executes automatically without explicit human consent. Would Nigerian courts enforce such a clause? While no Nigerian precedent yet exists, persuasive English authority in *HLB Kidsons (A Firm) v. Lloyd's Underwriters*²⁰⁸ suggests that courts will interpret contractual intent liberally where the parties' intention to arbitrate can be inferred. Nigerian courts, following similar reasoning, could uphold arbitration clauses embedded within smart contracts, provided there is evidence of consent.

Furthermore, blockchain-based arbitration models such as Kleros or Aragon Court propose on-chain dispute resolution using token-based juries. However, since these mechanisms lack statutory recognition under Nigerian law, their awards would not qualify as arbitral awards under

²⁰⁷ Arbitration and Mediation Act 2023, s. 3(3)(a).

²⁰⁸ *HLB Kidsons (A Firm) v. Lloyd's Underwriters* [2008] EWCA Civ 1206.

section 57 of the Arbitration and Mediation Act. Consequently, such outcomes would remain unenforceable in Nigeria unless validated by a formal arbitral institution.

(d) Enforcement of Foreign Judgments and Awards

Smart contracts are often executed across borders, meaning that disputes arising therefrom may involve foreign parties or courts. Nigeria's regime for enforcing foreign judgments derives from the Foreign Judgments (Reciprocal Enforcement) Act,²⁰⁹ which allows the recognition of judgments from countries with reciprocal arrangements.

However, enforcement remains uncertain where the contract exists purely on a blockchain without clear territorial connection. If, for example, a Nigerian investor secures a judgment in the UK enforcing a smart contract, a Nigerian court might refuse recognition on the ground that the subject matter, being a cryptocurrency transaction, contravenes Nigerian public policy, as implied in the CBN circular of 2021.

For arbitral awards, the New York Convention (1958), to which Nigeria is a party, facilitates enforcement of foreign arbitral awards.²¹⁰ Nonetheless, awards arising from decentralised blockchain arbitration mechanisms would not qualify, since they are not "arbitrations" within the meaning of the Act.

(e) Available Remedies

Under Nigerian contract law, a successful claimant may obtain damages, restitution, rescission, or specific performance. In the context of smart contracts:

²⁰⁹Foreign Judgments (Reciprocal Enforcement) Act, Cap. F35, Laws of the Federation of Nigeria 2004.

²¹⁰Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958).

- Damages may be the most practical remedy, as courts cannot reverse blockchain transactions.
- Rescission may be impossible where the contract has already executed.
- Restitution could apply where unjust enrichment occurs due to coding errors or fraud.
- Specific performance would be impracticable since performance occurs automatically.

Courts may also rely on constructive trust principles to recover misdirected digital assets, following the reasoning in *AA v Persons Unknown*,²¹¹ where crypto-assets were treated as property capable of being held on trust. This reasoning, though English, could influence Nigerian courts as they adapt equitable doctrines to new technological contexts.

(f) Institutional Enforcement and Regulatory Oversight

The role of regulators is also pivotal in practical enforcement. The CBN, SEC, and FCCPC may enforce compliance through administrative sanctions or regulatory guidance. The CBN's 2023 Guidelines for Virtual Asset Service Providers signal a shift towards inclusion by requiring registration and due diligence for crypto-related businesses. Once formalised, these institutions could serve as enforcement gateways, allowing consumers to lodge complaints against service providers who deploy faulty or fraudulent smart contracts.

²¹¹*AA v Persons Unknown* [2019] EWHC 3556 (Comm).

However, coordination among these bodies remains limited. Regulatory silos hinder uniform enforcement, and no statutory mechanism currently mandates collaboration between the CBN, SEC, and FCCPC in handling blockchain-related disputes.

(g) Conclusion

In practical terms, enforcing smart contracts under Nigerian law is both technically and institutionally complex. While existing legal frameworks, contract law, evidence law, arbitration, and consumer protection, provide conceptual tools, they were designed for human-readable agreements, not autonomous code. Nigerian courts can, in principle, enforce smart contracts where consent, legality, and performance can be established, but the immutable nature of blockchain and the anonymity of parties limit judicial remedies.

The future of enforcement in Nigeria will depend on judicial innovation, capacity building in digital forensics, and legislative intervention to recognise smart contracts formally. Until these reforms occur, enforcement will remain a blend of legal theory and technical improvisation.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 SUMMARY OF KEY FINDINGS

This research set out to critically evaluate the enforceability of smart contracts under Nigerian law, focusing on the commercial and jurisdictional challenges that hinder their practical application. The study reveals that while blockchain technology has introduced a new era of efficiency, transparency, and decentralization in commerce, Nigerian law has yet to fully integrate this innovation into its legal architecture. The findings across the preceding chapters may be summarized as follows:

First, the study established in Chapter One that Nigeria's legal system, founded upon English common law principles, defines a contract through the traditional elements of offer, acceptance, consideration, and intention to create legal relations. These foundational principles are reflected in judicial authorities such as *Carlill v Carbolic Smoke Ball Co.* (1893) 1 QB 256 and *Orient Bank (Nig.) Ltd v Bilante Int'l Ltd* (1997) 8 NWLR (Pt. 515) 37, where courts emphasised that the formation of a valid contract is predicated on consensus and intention. However, in smart contracts, these elements are often executed through algorithmic commands rather than human expression. The implication is that although such transactions satisfy functional equivalence, they do not fit neatly into the conceptual framework of intention recognised by Nigerian courts.

Secondly, Chapter Two showed that smart contracts evolved from early discussions in the 1990s led by Nick Szabo, who envisioned computer protocols capable of automatically enforcing contractual terms. The chapter further established that smart contracts are self-executing agreements, deployed on blockchain systems like Ethereum, and triggered by conditions encoded

in digital scripts. It was also observed that the theoretical frameworks , notably Legal Positivism (as expounded by H.L.A. Hart), Law and Technology Theory, and the emergent Lex Cryptographica , provide competing perspectives on how technology interacts with law. While positivism demands statutory recognition, the Lex Cryptographica suggests a self-governing code-based order. Nigerian legal development remains more aligned with positivism, which explains the absence of direct enforceability for smart contracts until the legislature intervenes.

Thirdly, Chapter Three examined the Nigerian legal and regulatory framework governing contracts and found that although existing statutes like the Evidence Act 2011, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, and the Nigerian Communications Act 2003 indirectly accommodate electronic transactions, they do not expressly regulate blockchain-based agreements. In particular, section 84 of the Evidence Act provides for the admissibility of electronic evidence, yet blockchain data does not fit squarely within its evidentiary standards due to the distributed nature of blockchain storage. Additionally, the Contract Act does not contemplate self-executing agreements, leaving judicial interpretation as the primary means through which smart contracts might be assimilated into Nigerian law.

Comparatively, jurisdictions like the United Kingdom and United States have demonstrated adaptability. The UK Law Commission's 2021 report affirmed that existing principles of contract law are capable of accommodating smart contracts without legislative overhaul, while the Uniform Electronic Transactions Act (UETA) in the U.S. recognises electronic signatures and records as legally binding. This comparative progress underscores the need for Nigerian reform.

Fourthly, Chapter Four identified and analysed the commercial and jurisdictional challenges confronting smart contract enforcement. These include conflicts between technological

determinism and legal autonomy, problems of cross-border jurisdiction, issues of privity and digital identity, as well as difficulties relating to fraud, illegality, mistake, and consumer protection. The study found that while smart contracts can self-enforce, they lack the remedial flexibility of traditional contracts , courts cannot easily undo a transaction once blockchain immutability takes effect. Furthermore, jurisdictional uncertainty persists because smart contracts often operate across borders without a centralised location, complicating the determination of applicable law or competent forum.

Finally, the research concluded that Nigerian institutions such as the National Information Technology Development Agency (NITDA), Securities and Exchange Commission (SEC), and Central Bank of Nigeria (CBN) have not yet established a unified regulatory position on blockchain-based contracts. Consequently, parties rely largely on the technical enforceability of smart contracts rather than their legal enforceability, leaving disputes in a grey zone. The findings thus reveal a duality between technological capability and legal adaptability , a gap that must be bridged through targeted legislative, judicial, and institutional reform.

5.2 CONCLUSION

The advent of smart contracts represents one of the most transformative innovations in contemporary commercial relations. This study has demonstrated that while the technological potential of smart contracts is profound, enabling automation, transparency, and trustless transactions, their legal enforceability within the Nigerian context remains uncertain and largely untested. The law, as it stands, is still tethered to traditional contract doctrines that presuppose human intention, written documentation, and centralized enforcement mechanisms.²¹²

²¹²R. E. Scott and P. G. Triantis, *Contract Law and Theory* (6th edn, Foundation Press 2021) 87.

The conceptual framework of contract law, as established under both English common law and Nigerian jurisprudence, rests on four essential elements: offer, acceptance, consideration, and intention to create legal relations.²¹³ However, in the case of smart contracts, these elements are often expressed through lines of computer code rather than human declarations. For instance, the “offer” and “acceptance” in a blockchain-based transaction are executed automatically by predefined algorithms, while “consideration” is digitally represented in cryptocurrency or tokenised assets. The Nigerian legal system, rooted in textual interpretation and human agency, has not yet fully adapted to accommodate such machine-mediated exchanges.²¹⁴

Furthermore, smart contracts challenge established notions of consent and intention, two of the cornerstones of classical contract formation. Nigerian courts, as seen in *Carlill v Carbolic Smoke Ball Co.*²¹⁵ and *Orient Bank (Nig.) Ltd v Bilante Int’l Ltd*,²¹⁶ have historically insisted on clear evidence of mutual assent and the presence of legal intention. Yet, in smart contracts, the very concept of intention is diffused within coded logic rather than explicit communication between human parties. This renders traditional judicial tools of interpretation inadequate in dealing with code-based expressions of will.

Equally significant is the challenge of jurisdiction and governing law. Smart contracts, by their very nature, are decentralized and borderless, often operating across multiple nodes situated in various countries. This decentralization undermines traditional jurisdictional principles that rely on territorial connection. In Nigeria, where the *lex loci contractus* (law of the place of contract)

²¹³See *Currie v Misa* (1875) LR 10 Ex 153; also *Orient Bank (Nig.) Ltd v Bilante Int’l Ltd* (1997) 8 NWLR (Pt. 515) 37 at 75.

²¹⁴A. O. Eze, “Smart Contracts and the Future of Commercial Transactions in Nigeria” (2022) 14 *Nigerian Law and Practice Journal* 45, 53.

²¹⁵*Carlill v Carbolic Smoke Ball Co.* (1893) 1 QB 256.

²¹⁶*Orient Bank (Nig.) Ltd v Bilante Int’l Ltd* (1997) 8 NWLR (Pt. 515) 37.

and *lex loci solutionis* (law of the place of performance) remain guiding doctrines,²¹⁷ determining which law governs a blockchain transaction becomes problematic. The global nature of blockchain thus disrupts the spatial logic upon which conventional private international law is built.

From a regulatory perspective, Nigeria's current framework, comprising the Evidence Act 2011, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, and the Nigerian Communications Act 2003, has proven insufficient to regulate blockchain-based transactions. Section 84 of the Evidence Act, though progressive in admitting electronically generated evidence, was designed for static digital records, not dynamic blockchain ledgers.²¹⁸ The Cybercrimes Act, while criminalising online fraud, does not address contract formation, enforceability, or dispute resolution in smart environments. This legislative vacuum places Nigerian users and businesses at risk, as they rely solely on the technical execution of smart contracts without the protective intervention of the courts in cases of fraud, mistake, or unjust enrichment.

Comparative analysis reveals that other jurisdictions have begun to bridge this gap. The United Kingdom Law Commission concluded that existing contract law principles are sufficiently flexible to encompass smart contracts,²¹⁹ while the United States, through the Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN), explicitly recognises electronic contracts and signatures as legally valid.²²⁰ These developments show that legal systems can evolve to reflect technological realities without

²¹⁷*British Nylon Spinners Ltd v Imperial Chemical Industries Ltd* [1953] Ch 19; *Re Missouri Steamship Co.* (1889) 42 Ch D 321.

²¹⁸Evidence Act 2011, s 84.

²¹⁹UK Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) para 26.

²²⁰Uniform Electronic Transactions Act 1999 (UETA); Electronic Signatures in Global and National Commerce Act 2000 (E-SIGN).

abandoning fundamental principles. Nigeria, however, remains in the early stages of this adaptation.

The study thus concludes that for smart contracts to achieve legal parity with traditional agreements in Nigeria, several key reforms are required. First, legislative intervention should expressly recognise blockchain-based contracts as valid and enforceable under Nigerian law. Second, judicial training should be enhanced to equip judges with the technological literacy necessary to interpret and adjudicate disputes arising from coded agreements. Third, regulatory harmonisation among agencies such as the Central Bank of Nigeria (CBN), the National Information Technology Development Agency (NITDA), and the Securities and Exchange Commission (SEC) is crucial for creating a consistent policy framework.

Ultimately, the enforceability of smart contracts in Nigeria depends not merely on technological advancement but on the law's capacity for innovation. The rule of law must evolve to accommodate emerging digital realities without compromising its fundamental values of justice, fairness, and accountability. In this sense, the true test of legal modernity lies not in rejecting new technologies but in reimagining jurisprudence to reflect the complexities of a digital economy.

5.3 RECOMMENDATIONS FOR LEGAL REFORM

The legal enforceability of smart contracts under Nigerian law remains an evolving and unsettled subject. This research has established that while the technological and commercial potential of blockchain is undeniable, the absence of a clear legal framework leaves participants exposed to uncertainty and potential injustice. Therefore, concrete and pragmatic legal reforms are essential to harmonise technological innovation with existing contract principles.

(a) Legislative Recognition of Smart Contracts

The first and most pressing recommendation is for legislative recognition of smart contracts as valid and enforceable legal instruments. While Nigerian contract law is derived from English common law principles and the Contract Act 1917, it remains silent on the recognition of electronic and automated contracts. This lacuna can be bridged through the enactment of a Digital Transactions (Regulation) Act, modelled after the UK Electronic Communications Act 2000 and the US Uniform Electronic Transactions Act (UETA).

Such an Act should expressly define smart contracts as “agreements whose terms are recorded and executed, in whole or in part, by means of distributed ledger technology,” and stipulate that such contracts shall not be denied legal validity solely because they exist in digital or code-based form.²²¹ This statutory recognition would provide the foundation for judicial interpretation, similar to how the Evidence Act 2011 validated electronic evidence through section 84.

Furthermore, the National Assembly should empower the National Information Technology Development Agency (NITDA) and the Securities and Exchange Commission (SEC) to issue implementing guidelines, clarifying standards for digital signatures, authentication, and the allocation of liability between programmers, contracting parties, and platform providers.²²²

(b) Reform of Judicial and Institutional Capacity

²²¹M. S. Ezeani, “Digital Contracts and the Nigerian Legal System: Bridging the Gap between Law and Technology” (2021) 5 *Nigerian Journal of Commercial Law* 113, 118.

²²²National Information Technology Development Agency (NITDA) Act 2007, ss 6–8; Securities and Exchange Commission (SEC) Rules 2022, Part F.

A key impediment to smart contract enforcement is the technological illiteracy of the judiciary and enforcement agencies. Nigerian judges and legal practitioners are still accustomed to paper-based documentation and human-mediated transactions. Consequently, disputes arising from code-based transactions are often misunderstood or dismissed on procedural grounds.

To address this, the National Judicial Institute (NJI) should introduce continuing professional development programmes on blockchain technology, cryptocurrency regulation, and digital evidence.²²³ Courts must also develop specialised technology benches, similar to the Technology and Construction Court in the UK, which can adjudicate complex technological disputes. These courts could sit within the Federal High Court system, which already has jurisdiction over cybercrime and ICT matters under the Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

The Nigerian Bar Association (NBA) should also play a role by integrating LegalTech education into its training curriculum by ensuring law faculties and postgraduate programmes introduce courses on smart contract law, blockchain governance, and artificial intelligence in commercial law. This academic reform is essential for cultivating a generation of lawyers capable of interpreting contracts coded in algorithmic syntax rather than ink.

(c) Establishment of a Smart Contract Regulatory Framework

Beyond judicial adaptation, Nigeria requires a comprehensive regulatory framework for smart contracts. The Central Bank of Nigeria (CBN), NITDA, and SEC currently issue fragmented directives on blockchain and virtual assets, leading to regulatory inconsistency. For instance, while the CBN restricts cryptocurrency transactions by financial institutions, the SEC

²²³National Judicial Institute, *Handbook on the Adjudication of Cyber and Digital Evidence Cases* (NJI Press 2022) 12.

simultaneously issues guidelines for virtual asset service providers. This incoherence must be resolved through inter-agency coordination and the creation of a National Blockchain Regulatory Council (NBRC). The Council should be mandated to develop unified policies governing the deployment of smart contracts in financial services, e-commerce, insurance, and real estate. It should also set minimum standards for coding integrity, data privacy, and consumer protection. In addition, the Cybercrimes Act 2015 should be amended to include provisions on digital fraud, hacking, and manipulation of smart contracts, recognising that malicious actors may exploit vulnerabilities in blockchain code to subvert contractual intent.

(d) Adoption of Hybrid Dispute Resolution Mechanisms

Given the transnational nature of blockchain transactions, disputes involving smart contracts often span multiple jurisdictions, hence traditional court litigation, with its territorial limitations and procedural delays, is ill-suited to resolving such issues. Therefore, the introduction of hybrid dispute resolution mechanisms, particularly Online Dispute Resolution (ODR) and Blockchain Arbitration is recommended.

Also, arbitration institutions such as the Lagos Court of Arbitration (LCA) and the Regional Centre for International Commercial Arbitration (RCICA) should develop model smart contract arbitration rules. These rules should allow for automated evidence presentation, digital identity verification, and enforceable awards recognised under the Arbitration and Mediation Act 2023. The Arbitration Act should also be amended to explicitly validate arbitration agreements embedded in code or expressed through digital signatures, following the approach adopted in Singapore's International Arbitration (Amendment) Act 2020. This will ensure that

blockchain-related disputes can be resolved efficiently, with minimal interference from conflicting national jurisdictions.

(e) Strengthening Data and Consumer Protection Laws

Smart contracts, though automated, are not immune to errors, fraud, or abuse. Code may execute transactions in ways that contradict the parties' real intentions, especially where input data (so-called "oracles") are manipulated. Therefore, consumer protection and data integrity are critical to maintaining public confidence. Hence, The Federal Competition and Consumer Protection Commission (FCCPC) should issue sector-specific guidelines requiring smart contract platforms to disclose algorithmic terms in plain language, enabling users to understand their obligations. Moreover, the Nigerian Data Protection Act 2023 should be expanded to impose liability on service providers for data breaches arising from blockchain vulnerabilities.

In cases of proven fraud, courts should be empowered to suspend or reverse transactions executed by smart contracts, mirroring the equitable remedies of rescission and restitution available under traditional contract law.

(f) International Cooperation and Harmonisation

Finally, Nigeria should collaborate with regional and international organisations to harmonise blockchain and smart contract laws. Participation in frameworks such as the African Continental Free Trade Area (AfCFTA) Digital Protocol and the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce will ensure compatibility between Nigerian law and global standards. Such alignment would enhance

investor confidence, facilitate cross-border transactions, and position Nigeria as a competitive player in the emerging digital economy.

5.4 SUGGESTIONS FOR FURTHER RESEARCH

The enforceability of smart contracts under Nigerian law remains a developing area of study, shaped by rapid technological advancements and evolving jurisprudence. As the legal landscape continues to adapt to the complexities of blockchain and decentralised finance (DeFi), this research recognises several critical areas where further scholarly and empirical exploration is needed to deepen understanding and guide effective reform.

(a) The Intersection of Smart Contracts and Artificial Intelligence (AI)

One of the most promising yet least explored areas is the interaction between smart contracts and artificial intelligence. Current smart contracts are static in nature, they execute predefined commands without learning or adapting, however, future iterations may incorporate AI-driven “smart agents” capable of interpreting changing circumstances and renegotiating contractual terms autonomously. This raises novel legal questions about agency, liability, and consent. For instance, if an AI algorithm modifies the terms of a smart contract without explicit human authorisation, who bears responsibility for breach or mistake, the programmer, the user, or the AI system itself? Future research could examine the extent to which existing doctrines of agency and vicarious liability under Nigerian law can be extended to autonomous digital agents. It could also explore comparative models from jurisdictions such as the EU, which have begun to consider the concept of “electronic personhood” for autonomous systems.

(b) The Role of Blockchain in Public Governance and Legal Infrastructure

Beyond private commercial contracts, blockchain technology holds potential for transforming public law and governance systems, for instance, through smart contract-based land registries, procurement systems, and tax administration. Research into the public law implications of such deployment in Nigeria remains sparse. A future study could investigate the legal feasibility of integrating smart contracts into public registries managed by agencies like the Corporate Affairs Commission (CAC) or the Federal Inland Revenue Service (FIRS), questions of transparency, accountability, and data sovereignty would need to be addressed, especially under the Nigerian Data Protection Act 2023.

(c) Judicial Interpretation and Case Law Development

Another significant research gap lies in the absence of judicial precedent on smart contracts in Nigeria. As courts begin to confront disputes arising from blockchain-based agreements, it will be critical to observe how judges interpret , consent, and evidence within coded transactions.

Future researchers could conduct doctrinal and empirical analyses of Nigerian case law as it emerges, assessing how courts balance the rigidity of code with the flexibility of equitable principles. They could also examine whether section 84 of the Evidence Act 2011, originally designed for static electronic documents, adequately accommodates dynamic blockchain evidence, or whether a Digital Evidence Reform Bill is needed. Such work would contribute meaningfully to both judicial education and legislative refinement in the digital era.

(d) Comparative Studies on Transnational Enforcement of Smart Contracts

Given the borderless nature of blockchain transactions, the enforcement of smart contracts across jurisdictions remains a complex challenge, hence future research could explore private

international law dimensions, including issues of choice of law, recognition of judgments, and arbitral award enforcement in the context of decentralised systems.

Particular attention should be given to the role of conflict-of-laws doctrines under the Rome I Regulation (EU) and the Hague Principles on Choice of Law in International Commercial Contracts, and how these frameworks could inspire reforms to Nigeria's own Private International Law (Recognition and Enforcement of Foreign Judgments) Bill. Such research would assist policymakers in developing bilateral and regional treaties to facilitate blockchain-based trade under frameworks like the African Continental Free Trade Area (AfCFTA).

(e) Socio-Economic and Ethical Implications

Finally, future research should consider the broader socio-economic and ethical implications of smart contract adoption, this is because while technological efficiency and cost reduction are often emphasised, there is a risk of exclusionary effects if small and medium enterprises (SMEs), rural traders, and the unbanked population lack access to digital literacy and blockchain infrastructure, moreover, ethical concerns surrounding algorithmic fairness, data ownership, and privacy require further interdisciplinary inquiry involving legal scholars, ethicists, and technologists, hence, an equitable digital economy must ensure that automation enhances, rather than undermines, human dignity and distributive justice.

In sum, this research contributes to the foundational understanding of smart contracts under Nigerian law but recognises that it only scratches the surface of a vast, rapidly changing field. The path forward lies in collaborative, interdisciplinary, and comparative scholarship that bridges the gap between law, technology, and policy. Only through such integrated research can Nigeria

build a forward-looking legal framework that not only validates smart contracts but also aligns them with the constitutional ideals of justice, equity, and technological progress.