



Research Article

Digital Jurisprudence in the Albertine Graben: A Critical Appraisal of Smart Contracts and Blockchain Technology in Optimizing Petroleum Revenue Management under Uganda's Legal Framework

SSENGENDO JULIUS*Faculty of Law, Cavendish University, Uganda*

Abstract: This paper undertakes a critical appraisal of the potential integration of blockchain technology and smart contracts into Uganda's petroleum revenue management framework, with specific focus on the Albertine Graben region. Against the backdrop of persistent challenges in revenue transparency, contract accountability, and community benefit realization, the study examines whether distributed ledger technology (DLT) can offer legally viable solutions within the existing regulatory landscape. Employing a doctrinal legal methodology complemented by comparative analysis and a "deconstructive integrationist" theoretical lens, the research engages with three theoretical paradigms in digital jurisprudence: coherentism, reformism, and integrationism to assess the scope for technological innovation without destabilizing foundational legal principles.

The article introduces novel legal concepts, including "Interplanetary Legality" to resolve jurisdiction issues for permissioned cross-border ledgers and the "Tribunal as an Oracle" doctrine to bridge the divide between decentralized execution and state-centric adjudication. It analyses Uganda's upstream legal framework, including the Petroleum (Exploration, Development and Production) Act, the Public Finance Management Act, and relevant environmental regulations, alongside emerging international practice from Nigeria and Venezuela. The study finds that while blockchain technology presents compelling capabilities for enhancing fiscal transparency and automating revenue distribution through smart contracts, significant obstacles persist regarding evidentiary weight under Ugandan law, data privacy compliance, and the absence of statutory recognition for decentralised ledgers.

The paper concludes that a reformist pathway preserving core legal structures while introducing targeted amendments to accommodate blockchain-based revenue management offers the most prudent and legally coherent approach.

Keywords: *Blockchain, Smart Contracts, Petroleum Revenue Management, Albertine Graben, Digital Jurisprudence, Uganda, Deconstructive Integrationism*

1. INTRODUCTION

The Albertine Graben, Uganda's western rift valley basin holds an estimated 6.5 billion barrels of oil, with 1.4 billion barrels classified as recoverable.^[1] Following the Final Investment Decision in 2022 and first oil anticipated by 2025, petroleum revenues are projected to exceed USD 3 billion annually by 2030.^[2] This fiscal windfall presents both an opportunity for transformative development and a risk of perpetuating the 'resource curse', a phenomenon historically observed in resource-rich African economies where opaque production sharing agreements, discretionary revenue allocation, and weak institutional oversight precipitate corruption and conflict.^[3]

Uganda has responded legislatively with what appears, on its face, to be a robust governance framework. However, the administrative implementation of these statutes reveals persistent vulnerabilities: manual reconciliation processes creating temporal gaps of 90-120 days between production verification and revenue disbursement;^[4] limited real-time audit capabilities for the Auditor General; and restricted civil society oversight of petroleum fund flows. These challenges invite consideration of digital solutions.

This article undertakes a critical appraisal of two interconnected digital technologies; blockchain and smart contracts as potential tools for optimising petroleum revenue governance in Uganda.

1.1 CONCEPTUAL FOUNDATIONS: BLOCKCHAIN AND SMART CONTRACTS

1.1.0 Smart contracts

A smart contract is a computer protocol, a set of conditional 'if-then' functions written in code that automatically executes contractual obligations when predetermined conditions are satisfied, without human intervention.^[5] The term was coined by cryptographer Nick Szabo in 1994, but practical implementation became possible only with the emergence of blockchain platforms such as Ethereum in 2015.^[6]

Simplistic Illustration: Consider a vending machine. You insert money (condition), and the machine releases a soda (execution). There is no human decision-maker; the machine executes automatically based on programmed rules. Now apply this logic to petroleum revenue: If production meter X confirms 100,000 barrels lifted (condition), then automatically disburse 20% to the Consolidated Fund, 50% to the Petroleum Fund, and 30% to local governments (execution). That is a smart contract self-executing, transparent, and irreversible.^[7]

1.1.2 Blockchain Technology

Blockchain is a decentralised digital ledger in which transactions are recorded chronologically and publicly across a distributed network of computers (nodes). Each transaction is grouped into a 'block' that is cryptographically linked to the preceding block, forming an immutable 'chain.' Once recorded, data cannot be altered retroactively without altering all subsequent blocks. It is therefore a computationally infeasible enterprise requiring consensus of the network majority.

Simplistic Illustration: Imagine a shared notebook, photocopied and distributed simultaneously to the Ministry of Energy, the Bank of Uganda, the Auditor General, and twenty civil society organisations. Every time a petroleum transaction occurs, everyone writes it down simultaneously. No one can erase or change an entry without everyone else immediately seeing the alteration and rejecting it. This is blockchain, a shared, synchronized, immutable record.

1.1.3 The Petroleum Use-Case

Right now, if a barrel of oil moves from Hoima to Tanga (Tanzania), five different offices have to sign manual papers. However, with the Blockchain; a sensor on the pipe-EACOP called (The "Oracle") sends signals to the Blockchain pertaining the Volume of crude oil running through the pipeline and the ledger updates automatically. Hence, the government sees the exact volume of oil in real time, and the oil company cannot claim they have shipped less to avoid taxes.

Blockchain operates in three primary variants: public (Permissionless), private (permissioned), and consortium (hybrid). For petroleum revenue governance, under a permissioned or consortium blockchain where the state grants access to verified nodes (URA, Auditor General,

selected IOCs, Parliamentary Committee on Natural Resources) offers optimal balance between transparency and confidentiality of proprietary production data.

A blockchain is, therefore, a type of decentralized ledger technology. This allows anyone to verify data included on the blockchain while preventing its unilateral modification, as each information 'block' is chained to the others. Any alteration or modification of data entered into the network first requires achieving consensus from a vast number of computers (nodes), before the alteration to the recorded information can be propagated.

As a rule, the records created are immutable. As previously noted, the popularization of Blockchain technology occurred from 2008 onward, rendering it a relatively recent innovation in terms of legal regulation. Although several years have since elapsed, the fundamental nature and technological novelty of Blockchain continue to present significant challenges for its definitive characterization, legal classification, and governance. The pace of technological innovation complicates the task of keeping legal frameworks apace, as it continuously gives rise to novel, valid legal questions that are inherently difficult to resolve. One such question concerns the precise legal qualification of the Blockchain itself.

1.2.0 Statement of the Problem: The Four Deficits

Uganda's legal framework for petroleum revenue management exhibits four interconnected deficiencies that create the space for technological intervention:

1.2.1 The Transparency Deficit

Production Sharing Agreements (PSAs) between the Government of Uganda and international oil companies (Total Energies, CNOOC, and Tullow Oil prior to its exit) are classified as confidential. The Petroleum (Exploration, Development and Production) Act, 2013, imposes criminal penalties for disclosure of "proprietary information" obtained under the Act.^[11] While Section 76 provides limited exceptions for parliamentary oversight and audit, civil society^[12] As a result, the fiscal terms including royalty rates, cost recovery limits, and profit oil splits are not subject to public scrutiny. This opacity creates opportunities for negotiation outcomes that may not serve the public interest, and it undermines the accountability of both government negotiators and company officials.

1.2.2 The Verification Deficit

The architecture of revenue collection is fragmented across multiple institutions. The Uganda Revenue Authority (URA) collects tax revenues; the Petroleum Authority of Uganda (PAU) monitors production and verifies company reports; the Ministry of Finance, Planning and Economic Development (MoFPED) receives the revenues and allocates them through the budget process. No single entity has a complete, real-time view of the revenue chain from production to allocation. This fragmentation creates opportunities for

delay, misallocation, and error. Audits conducted by the Auditor General are retrospective, often lagging by several years, and they rely on sampling rather than full-population analysis.

1.2.3 The Inclusion Deficit

The Petroleum (Exploration, Development and Production) (Local Content) Regulations^[13], require oil companies to give preference to Ugandan goods and services and to report annually on their local content performance. However, local communities particularly those in the Albertine Graben affected by petroleum operations have no access to these reports and no mechanism to verify that the companies are complying with their local content obligations. Furthermore, the regulations do not establish a clear legal framework for community benefit agreements or revenue sharing with local governments. The result is a perception, widely documented in civil society reports, that petroleum wealth is being extracted from local communities without commensurate benefits flowing back to them.

1.2.4 The Environmental Deficit

^[14] highlights the complete absence of a real-time, cross-border verification mechanism for environmental compliance. While Uganda's National Environment Act^[15], requires Environmental and Social Impact Assessments (ESIA) for petroleum activities, and the East African Community has adopted Transboundary Environmental Impact Assessment (TESIA) guidelines, there is no shared data infrastructure that would allow Uganda, the DRC, and affected communities to verify compliance in real time. Environmental monitoring data is collected by the oil companies themselves, reported to NEMA on a periodic basis, and not shared across the border. This creates an evidential deficit: when transboundary harm is alleged, as in the EACJ case, the parties lack a shared factual foundation for dispute resolution.

The central problem, therefore, is that the features making blockchain attractive for petroleum revenue management (immutability, transparency, automation) generate direct legal conflicts with existing legislation, while the absence of these features perpetuates the four deficits. The challenge is to determine whether, and how, Uganda's legal framework can be reformed to accommodate blockchain technology without destabilizing foundational legal principles.

2. METHODOLOGY

The Article employs a doctrinal legal methodology as its primary approach, supplemented by comparative legal analysis and, where appropriate, theoretical legal scholarship.

2.1.0 Doctrinal Analysis

The core of the paper is a systematic analysis of Ugandan legislation (the Constitution, the Petroleum Act, the PFMA, the Evidence Act, the Contracts Act, the

Data Protection Act) and case law (where available). The doctrinal method involves identifying relevant legal rules, analyzing their internal coherence, and identifying gaps, ambiguities, and conflicts.

2.1.1 Comparative Analysis

The paper adopts a comparative method, analyzing how other jurisdictions have addressed similar legal questions. The selection of comparator jurisdictions (Nigeria, Venezuela, Kenya, Ghana, the EU) is justified by their relevance to the Ugandan context: Nigeria as a fellow African petroleum producer with common law heritage; Venezuela as a cautionary tale of petroleum-backed digital assets; Kenya and Ghana as East African and West African comparators with similar legal traditions; and the EU as a source of sophisticated digital asset regulation.

2.1.2 Theoretical Legal Scholarship

The paper further engages with legal theory, particularly in literature review and its novel doctrinal contributions. The theoretical framework deconstructive integrationism draws on Hartian legal positivism (via Reyes, Tosato, and Hinkes) and regulatory theory (via Lessig and Finck).

The dissertation does not employ empirical methods (surveys, interviews, case studies of actual blockchain deployment) because no such deployment exists in Uganda's petroleum sector at the time of writing.

3. LITERATURE REVIEW

3.1 Introduction to the Literature Review

This Literature Review undertakes a systematic and critical examination of the existing scholarly discourse across three intersecting domains: (1) digital jurisprudence and the theoretical foundations of blockchain regulation; (2) the application of distributed ledger technology to petroleum revenue management in resource-dependent economies; and (3) the specific legal framework governing Uganda's nascent oil and gas sector. The review serves a dual purpose: first, to situate the present research paper within the broader landscape of legal scholarship on technology and governance; second, to identify the lacunae theoretical, doctrinal, and empirical that this research seeks to address.

The central argument advanced through this review is that existing literature suffers from a binary polarization that this paper terms the "coherentist-integrationist divide." On one hand, "coherentist" scholarship, often emanating from traditional legal circles, insists that existing legal rules are sufficient to address blockchain technology without modification. This position, most forcefully articulated by Judge Frank Easterbrook in the context of cyber law generally, holds that creating specialized rules for blockchain is as foolish as creating "Law of the Horse." General principles of contract, evidence, and tort suffice.^[16]

On the other hand, "integrationist" scholarship, represented most prominently by De Filippi and Wright, argues that blockchain is not merely a tool for traditional law but a competing legal system *Lex Cryptographia* that operates independently of state authority.^[17]

This research paper charts a third path: deconstructive integrationism. "Deconstructive" in its critical engagement with *Lex Cryptographia*'s overreach, drawing on Reyes, Tosato, and Hinkes to expose the ontological gap between code and law.^[18] "Integrationist" in its insistence that blockchain technology can be rendered legally coherent through deliberate acts of "legal investiture" targeted amendments to existing statutes that attach legal consequences to specific code-based states, while preserving the ultimate authority of positive law and state courts.

3.2 Theoretical Paradigms in Digital Jurisprudence

3.2.1 Lessig and the Architectural Regulation Thesis

The modern scholarly inquiry into the relationship between code and law traces its origins to Lawrence Lessig's seminal work, *Code and Other Laws of Cyberspace*.^[19] Lessig's central insight was deceptively simple yet profoundly generative: software code functions as a regulator of behavior, operating alongside and sometimes in tension with law, social norms, and markets. As Lessig famously argued, "Code is law" in the descriptive sense that the architecture of cyberspace constrains what users can do, just as legal rules constrain what they may do. A speed bump on a residential street, like a firewall on a computer network, enforces compliance through technical architecture rather than through the threat of state sanction.

Lessig's framework identified four modalities of regulation; 1. law (rules enforced by state sanction), 2. norms (social expectations enforced by community pressure), 3. Markets (price signals enforced by supply and demand), and 4. architecture (physical or technical constraints enforced by the laws of physics or code). Each modality can constrain behavior, but they do so through different mechanisms and with different degrees of efficacy. Architecture, Lessig argued, is often the most effective regulator because it makes certain actions impossible, not merely costly or socially disapproved.

The relevance of Lessig's framework to blockchain technology is both obvious and contested. Blockchain's architecture is designed precisely to render certain actions impossible: the deletion or alteration of recorded transactions, the double-spending of digital assets, the exercise of centralized control over network operations. For blockchain enthusiasts, this architecture realizes the cypherpunk vision of "trustless" coordination systems that do not require reliance on intermediaries or state-backed enforcement mechanisms. For Lessig, however, the normative question would remain: Who designed this architecture? Whose values does it encode? And to what democratic processes is it accountable?

Lessig's later work, particularly *Code Version 2.0*^[20] addressed these normative questions directly. He argued that code is not inevitable; it is designed by human actors who make choices about what constraints to build into the architecture of digital spaces. Those choices must be subject to democratic accountability. Applied to blockchain, this means that the consensus protocols, governance mechanisms, and upgrade paths built into distributed ledgers are not neutral technical features but normative choices that should be evaluated for their consistency with democratic values.

A significant limitation of Lessig's framework for present purposes is its focus on public, permissionless networks. The blockchain systems most relevant to petroleum revenue management are likely to be permissioned ledgers (such as Hyperledger Fabric), where the participants (PAU, URA, MoFPED, oil companies) are known and their permissions are controlled by a governing authority. In such systems, Lessig's distinction between architecture and law blurs: the code is designed by the same government entities that enact the law, and the "architecture" is subject to modification through governance processes that are themselves legally constituted. This observation supports the deconstructive integrationist position: in permissioned contexts, the gap between code and law is narrower, but the ontological distinction remains.

3.2.2 De Filippi and Wright: *Lex Cryptographia* and the "A legal" Turn

If Lessig provided the descriptive foundation, Primavera De Filippi and Aaron Wright advanced the more ambitious normative claim in *Blockchain and the Law: The Rule of Code*. Their central thesis is that blockchain technology enables the emergence of a new legal order, which they term "*Lex Cryptographia*", a decentralized, private regulatory regime that operates in parallel to, and potentially in competition with, state law.

De Filippi and Wright draw on legal pluralist traditions, particularly the work of scholars who have documented the coexistence of multiple normative orders within the same social field. For these authors, blockchain-based systems exhibit the key characteristics of a legal system: they prescribe rules (encoded in smart contracts), adjudicate disputes (through community governance mechanisms or, in extreme cases, hard forks), and enforce outcomes (through automated execution). The difference is that *Lex Cryptographia* operates through code rather than through the coercive apparatus of the state, and its legitimacy derives from the consent of network participants rather than from democratic processes.

The authors identify several distinctive features of *Lex Cryptographia*. First, it is automatic: rules execute without human intervention, eliminating the enforcement gap that plagues traditional law. Second, it is transparent: the rules are encoded in open-source software that anyone can inspect, eliminating the interpretive

ambiguity that characterizes legal texts. Third, it is global: blockchains operate across jurisdictional boundaries, raising questions about the continued relevance of territorial sovereignty. Fourth, it is resistant to capture: decentralized networks are difficult for any single actor to control, potentially reducing the risk of regulatory capture that afflicts traditional administrative agencies.

De Filippi and Wright acknowledge that Lex Cryptographia is not, and cannot be, a complete legal system. It cannot adjudicate disputes that turn on questions of intent, reasonableness, or good faith concepts that resist algorithmic codification. It cannot address force majeure events or changed circumstances that fall outside the predictable parameters of the code. And it cannot, by itself, resolve disputes about the relationship between the code and the "real world", the notorious Oracle Problem that this paper shall address in detail. Nevertheless, they argue that for a significant range of transactions particularly those involving digital assets that exist entirely within the blockchain ecosystem, Lex Cryptographia can operate as a self-sufficient legal order.

This argument has been extended by scholars such as Pusca^[22], who examines how blockchain technology is "reshaping the foundations of legal authority" and giving rise to "post-institutional law." In this view, the shift from state-centric legal authority to algorithmically executed norms represents a fundamental transformation in the nature of governance, with profound implications for concepts of jurisdiction, liability, and legitimacy. Similarly, Mazhorina^[23] positions Lex Cryptographia as the latest iteration of Lex Mercatoria, the medieval law merchant that governed cross-border trade independently of national legal systems. She argues that "lex communitas" (community law) represents a contemporary historical form of Lex Mercatoria, mediating the non-state rule-making of international professional communities. Within this framework, Lex Cryptographia joins Lex Informatica, Lex Sportiva, Lex Constructionis, and Lex Petrolea as functional subsystems of transnational private ordering.

The present research paper subjects these claims to critical scrutiny. While acknowledging the descriptive accuracy of much of this scholarship, blockchain systems do indeed generate norms, coordinate behavior, and resolve disputes through code-based mechanisms. The article argues that the normative leap from "code governs behavior" to "code constitutes law" is both analytically flawed and practically dangerous. As will be developed in the following subsection, conflating technical capability with legal authority produces legal pathologies across legislation, regulation, and adjudication. Moreover, in the specific context of petroleum revenue management, Lex Cryptographia is manifestly inadequate. Petroleum extraction involves physical assets (oil in the ground), environmental impacts (spills, emissions), and public goods

(community benefits, infrastructure development) that cannot be reduced to on-chain representations. A smart contract cannot adjudicate whether a spill constitutes "best efforts" under a PSA, nor can it determine whether a drop in oil prices triggers rebus sic stantibus relief. The physical world resists algorithmic reduction.

3.2.3 The Critique: Reyes, Tosato, and Hinkes on "Code is NOT Law"

[24] Hart's framework distinguishes between primary rules (which impose duties or confer powers) and secondary rules (which specify how primary rules are identified, changed, and adjudicated). A legal system, for Hart, exists only when both types of rules are present and when officials accept the secondary rules as a common standard of official behavior. Proponents of Lex Cryptographia, Reyes, Tosato, and Hinkes argue, treat code's operational effectiveness as a sufficient basis for legal validity, but binding legal rules must trace their authority to recognized sources of law typically, in common law jurisdictions, to constitutional provisions, legislation, and binding precedent. Code bears no such pedigree; it simply defines the range of possible conduct and records factual states through deterministic execution.

The authors identify three distinct ways in which code and law are conflated in contemporary discourse, each producing distinct legal pathologies:

First, legislative conflation: Some state legislatures have enacted statutes permitting decentralized autonomous organizations (DAOs) to be "algorithmically managed," vesting formal management powers in smart contracts that cannot exercise the discretion and fiduciary judgment that organizational law demands. The result, Reyes, Tosato, and Hinkes document, is a series of governance failures: DAOs that cannot respond to emergencies, that distribute assets to parties who are legally prohibited from receiving them, and that expose participants to personal liability that they believed the code would shield.

Second, regulatory conflation: Federal regulators, particularly the U.S. Securities and Exchange Commission (SEC), have treated the technical characteristics of digital assets as proxies for securities status, leading to nearly a decade of confused enforcement. Only after significant litigation did the SEC express, in informal remarks, "regret" for any confusion caused by its guidance. The conflation of technical characteristics (decentralization, immutability) with legal classifications (security, commodity, currency) continues to produce regulatory uncertainty.

Third, adjudicative conflation: Courts have struggled to characterize smart contracts for purposes of contract law. Some courts have treated smart contracts as "a code-enabled species of unilateral contracts," while others have classified them as contracts under seal or as third-party beneficiary contracts. Criminal defendants have argued that conduct permitted by a protocol is

lawful by definition, a defense that produced a mistrial when jurors could not disentangle technical permissibility from legal obligation.

Most significantly for the present research paper, Reyes, Tosato, and Hinkes demonstrate the practical dangers of the conflation in private ordering. Participants in venture DAOs who structured their affairs through smart contracts alone, believing the technology would shield them from personal liability, were shocked to discover that courts treat such arrangements as general partnerships by default, exposing each participant to joint and several liability. Code controlled the assets; only law could have protected the people.

The solution, these authors argue, is not to abandon blockchain technology but to understand the proper relationship between code and law. Code can acquire legal force, but only through deliberate acts of legal investiture either through public empowerment (legislatures enacting statutes that attach legal consequences to specific code-based states) or through private empowerment (parties incorporating code into contracts, trusts, and organizational governance instruments). In every instance, authority flows from law to code, never the reverse.

This paper embraces this framework as its theoretical foundation. The "deconstructive integrationist" approach advanced here accepts the critique of Lex Cryptographia's overreach while rejecting the implied conclusion that blockchain technology is therefore juridically irrelevant. Instead, the article demonstrates how Uganda's legal system can engage in the kind of legal investiture that Reyes, Tosato, and Hinkes describe: enacting targeted amendments to the Evidence Act^[26], Contracts Act^[27], Data Protection Act^[28], and PFMA^[29] that attach legal consequences to blockchain records and smart contracts.

3.2.4 Finck and the European Regulatory Approach

Michele Finck offers a complementary perspective that bridges the gap between theoretical abstraction and regulatory practice.^[30] Finck is particularly attentive to what she terms the "regulatory dilemma" posed by blockchain: the technology's promise lies precisely in its decentralization and resistance to control, yet effective regulation requires identifiable points of intervention.

Finck's analysis distinguishes between "thick" and "thin" regulatory approaches. Thick regulation attempts to subject blockchain systems to the full panoply of existing legal rules, often producing results that are either impossible to comply with (as with the GDPR's right to erasure applied to immutable ledgers) or that destroy the technology's distinctive value. Thin regulation, by contrast, focuses on the interfaces between blockchain systems and the traditional economy, the points at which cryptocurrencies are exchanged for fiat currency. Smart contracts interact with real-world assets, and blockchain records are offered as evidence in court proceedings.

Finck identifies five regulatory interfaces that are particularly significant:

1. **The interface with financial regulation:** When blockchain-based assets are exchanged for fiat currency or traded on exchanges, traditional financial regulation (anti-money laundering, know-your-customer, market integrity) applies.
2. **The interface with data protection law:** When blockchain systems process personal data, the GDPR applies creating tensions with immutability that Finck documents in detail.
3. **The interface with contract law:** When parties intend smart contracts to create legally binding obligations, traditional contract law applies including rules on formation, interpretation, mistake, and remedy.
4. **The interface with insolvency law:** When blockchain-based assets are held by insolvent parties, traditional insolvency rules determine priority and distribution.
5. **The interface with private international law:** When blockchain transactions have cross-border elements, traditional choice-of-law and choice-of-forum rules apply, creating difficulties when the transaction's nodes are distributed across multiple jurisdictions.

For each interface, Finck advocates a "functional equivalence" approach: rather than creating entirely new rules for blockchain, regulators should adapt existing rules to achieve functional equivalence with non-blockchain transactions. A blockchain record that satisfies the functional requirements of a business record (systematic creation, regular maintenance, reliance by the business) should be admissible even if it does not satisfy traditional requirements for original documents. A smart contract that performs the function of a traditional contract (manifesting mutual assent, creating enforceable obligations) should be enforceable even if it is expressed in code rather than natural language.

Finck's interface-focused approach serves as a methodological guide for this research paper. Rather than attempting to subject Uganda's blockchain-based revenue management system to unmodified existing law (which would produce the kind of incoherence documented by Reyes, Tosato, and Hinkes), the paper identifies specific interfaces where legal intervention is both necessary and feasible: the evidentiary status of blockchain records, the contractual enforceability of smart contracts, the compliance of blockchain-based data processing with privacy law, and the integration of automated payments with public finance management.

3.2.5 Werbach and the New Architecture of Trust

Kevin Werbach provides a bridging perspective that is particularly relevant for this dissertation. Werbach

rejects both the "blockchain is trustless" rhetoric of techno-libertarians and the "blockchain is irrelevant" dismissal of legal traditionalists.^[31] Instead, he argues that blockchain enables a new form of distributed trust not trustless coordination, but trust mediated by technology rather than by institutions.

3.3 Blockchain in Resource Governance

3.3.1 The Resource Curse and the Transparency Turn

The scholarly literature on the "resource curse" provides the essential context for understanding why blockchain has attracted attention in extractive governance. The paradox that countries rich in natural resources often experience slower economic growth, weaker institutions, and higher levels of conflict than resource-poor countries has been extensively documented.^[32] The mechanisms of the curse are multiple: commodity price volatility, Dutch disease, rent-seeking behavior, and the "capture" of state institutions by elites who control resource revenues.

The transparency turn in resource governance, exemplified by the Extractive Industries Transparency Initiative (EITI), represents the dominant policy response to the resource curse. EITI requires participating countries to disclose payments made by extractive companies to governments, and to reconcile those disclosures with government-reported receipts. The theory of change is straightforward: transparency enables accountability, which in turn reduces corruption and improves governance.^[33]

However, as critics have noted, the EITI has significant limitations.

First, EITI disclosure is retrospective: it covers payments made in the previous year, not real-time flows. This creates a lag of 12-18 months between revenue receipt and disclosure, during which funds can be misallocated or misappropriated.

Second, EITI disclosure is aggregated: it reports payments at the company-country level, not at the transaction level. This makes it difficult to trace specific payments from specific wells to specific government accounts.

Third, EITI disclosure is subject to verification gaps: the reconciliation process relies on company-reported and government-reported data, which can be collusive or erroneous. There is no independent, immutable record of the underlying transactions.

Fourth, EITI disclosure is optional: while participating countries commit to disclosure, the standard includes numerous "materiality" exceptions that allow non-disclosure of smaller payments. In practice, these exceptions have been exploited to conceal significant revenue flows.

It is precisely these limitations that have attracted blockchain advocates. The promise of distributed ledger

technology for extractive governance can be summarized in three propositions: (1) immutability ensures that once revenue data is recorded, it cannot be altered or deleted; (2) transparency allows all stakeholders (government, companies, civil society) to access the same data simultaneously; and (3) automation through smart contracts reduces opportunities for human discretion and corruption in revenue distribution.

The Natural Resources Governance Institute (NRGI) has produced several working papers exploring blockchain applications in extractive governance. A 2019 NRGI report,^[35] "Can Blockchain Revolutionize Natural Resource Governance?" concluded that while blockchain has potential, it is "not a silver bullet" and must be accompanied by institutional reforms. The report identified the "garbage in, garbage out" problem as fundamental: blockchain guarantees the integrity of the record, not the integrity of the data recorded. If production volumes are underreported at the point of entry, the blockchain will immutably preserve the underreporting.

3.3.2 Nwankwo and Emmanuel: The Nigerian Experience

The most directly relevant comparative scholarship for the present dissertation is Nwankwo and Emmanuel's study, "Blockchain Technology and Tax Transparency in Nigeria's Oil and Gas Sector: A Doctrinal Study," published in the *African Journal of Legal Studies*.^[36] This study provides a rigorous doctrinal analysis of how blockchain might address Nigeria's persistent challenges with oil revenue transparency, including revenue losses estimated in the billions of dollars, ambiguous tax regulatory frameworks, and systemic inefficiencies in collection.

Nwankwo and Emmanuel adopt a doctrinal methodology similar to that employed in this dissertation, analyzing Nigeria's Petroleum Industry Act (2021), Companies Income Tax Act (as amended), and relevant electronic transactions legislation.

Their key findings include:

First, Nigeria's existing legal framework does not explicitly recognize blockchain-based records as admissible evidence, creating evidential uncertainty. The Evidence Act 2011 of Uganda recognizes electronic records subject to authentication requirements, but the definition of "electronic record" does not explicitly include distributed ledgers, and the authentication requirements assume a centralized record-keeper. Blockchain's decentralized architecture complicates authentication, as there is no single "custodian" who can attest to the record's integrity.

Second, smart contracts for tax collection would require amendments to the definition of "payment" and "remittance" under tax legislation. Current definitions assume a transfer between identifiable parties at a specific time, recorded by a centralized financial

institution. Smart contract payments occur on the blockchain, may involve pseudonymous addresses, and are recorded by the network rather than by a bank.

3.3.3 Comparative Evidence: Venezuela, Kazakhstan, and Beyond

Beyond Nigeria, the literature documents blockchain experimentation in other petroleum-producing jurisdictions. These cases offer both positive and negative lessons for Uganda.

Venezuela: The Petro and the Problem of Illegality

Venezuela's "Petro" crypto currency, launched in 2018, represents a cautionary rather than exemplary case. The Petro was ostensibly backed by the country's oil reserves and intended to circumvent U.S. sanctions. The Venezuelan government claimed that each Petro was backed by a barrel of oil, creating a stable, asset-backed crypto currency.

Scholars have documented the Petro's failure on multiple dimensions. First, the technical implementation was opaque: the Petro was not built on a public, verifiable blockchain but on a private, government-controlled ledger with no independent verification. Second, the oil backing was never independently verified: there is no evidence that barrels of oil were actually set aside to back Petros in circulation. Third, the legal status of the Petro was never clear under Venezuelan law, and U.S. sanctions explicitly prohibited U.S. persons from transacting in the Petro, limiting its market.

The broader lesson for Uganda is that blockchain cannot compensate for underlying governance deficits. If the state lacks credibility, putting its promises on an immutable ledger merely makes the broken promises harder to erase. The Petro's failure demonstrates the importance of *de jure* (by statute) rather than *de facto* (by emergency decree) authority for blockchain-based revenue management. Uganda must ensure that any blockchain deployment is grounded in clear legislative authority, not merely executive discretion.

Kazakhstan: Customs and Tax Pilots

Kazakhstan has piloted blockchain for customs and tax administration in its extractive sector, with mixed results. The most successful implementations have been in relatively narrow, high-volume, low-discretion contexts, precisely the characteristics of royalty and tax payment processing. Kazakhstan's customs authority deployed a blockchain system for tracking the movement of oil across borders, reducing paperwork and verification costs.

The least successful implementations have been in contexts requiring interpretation of ambiguous contractual terms or exercise of regulatory discretion. Kazakhstan's attempt to use smart contracts for production-sharing calculations failed because the PSAs contained numerous undefined terms and required case-by-case adjustments that could not be coded in advance.

The scholarly consensus emerging from the comparative cases can be summarized as follows: blockchain is most effective when applied to well-defined, rule-bound processes where the primary challenge is verification and coordination rather than interpretation or discretion. Royalty calculation and distribution, based on formulaic rules (e.g., "10% of gross production"), falls into the former category. Environmental impact assessment and local content compliance, requiring case-by-case judgment, falls into the latter.

This consensus informs the use cases selected for appraisal. The research paper focuses on revenue collection and distribution, where blockchain's capabilities are most directly applicable, while acknowledging the limitations of blockchain for more discretionary aspects of petroleum governance.

3.4 Uganda's Petroleum Legal Framework: The State of Scholarship

3.4.1 Akello (2024): Comprehensive Framework Analysis

Rebecca Akello^[37] provides the most comprehensive recent analysis of Uganda's upstream legal framework. Akello traces the development of Uganda's oil and gas sector following the 2006 discoveries in the Albertine Graben, analyzing key legislative measures including the Petroleum (Exploration, Development and Production) Act^[38], the Public Finance Management Act^[39], the National Environment Act^[40], and the regulatory institutions including the Petroleum Authority of Uganda (PAU) and the National Environment Management Authority (NEMA).

Akello's methodology combines doctrinal analysis of legislation with comparative case studies from more mature petroleum jurisdictions, including Norway (as a model of effective resource governance), Nigeria (as a regional comparator), and Ghana (as a recent African petroleum entrant).

Her key findings include:

First, Uganda's legal framework has evolved rapidly since 2006 but still contains significant gaps, particularly regarding environmental protection and local community benefits. The framework is "largely adequate on paper" but suffers from implementation deficits.

Secondly, the confidentiality of Production Sharing Agreements (mandated by Section 75 of the Petroleum Act)^[41] limits parliamentary and civil society oversight. While Section 76^[42] allows parliamentary access on a confidential basis, Akello argues that this is insufficient for meaningful accountability. She recommends that Uganda follow the Nigerian example of publishing PSAs with limited redactions.

Third, coordination among the multiple institutions involved in revenue management (URA for tax collection, PAU for production verification, MoFPED for revenue allocation) is suboptimal, creating

opportunities for delay and misallocation. Akello recommends the establishment of a single, integrated revenue management system a recommendation that this research paper takes up in proposing a blockchain-based solution.

Importantly for the present paper, Akello identifies "implementation challenges and gaps" as the central concern not the existence of legal rules on paper, but the practical effectiveness of those rules in governing extraction and revenue management. This finding supports the research paper's premise that technological innovation may offer solutions to implementation deficits even where the legislative framework is formally adequate.

However, Akello's analysis predates the pending East African Court of Justice Case; ASEP & 12 Others v. Uganda & 2 Others,^[43] and therefore does not address the transboundary environmental governance dimensions that have emerged as a central concern. The present paper incorporates this case as a live controversy that illustrates the verification deficit that blockchain might address.

3.4.2 Sector-Specific Scholarship

Beyond Akello's comprehensive study, the literature on Uganda's petroleum legal framework is relatively fragmented. Several studies examine specific subsectors:

Environmental Governance: Makumbi (2021)^[44] examined the implementation of Environmental and Social Impact Assessments (ESIAs) for petroleum activities in the Albertine Graben, finding significant gaps in compliance monitoring and community consultation. The study documented instances where ESIAs were approved despite incomplete baseline data and inadequate mitigation plans.

Local Content: Naluwairo and Nangendo (2019)^[45] analyzed the Petroleum (Local Content) Regulations, 2016, finding that while the regulations establish a framework for local participation, they lack enforcement mechanisms. The regulations require annual reporting by oil companies but do not specify consequences for non-compliance or provide access to reported data for affected communities.

Fiscal Framework: Kuteesa and Tumusiime-Mutebile (2010)^[46] examined the fiscal terms of Uganda's PSAs, finding that the terms are broadly comparable to regional averages but that the confidentiality provisions prevent independent verification. The authors recommended that Uganda publish its model PSA to allow public debate on fiscal terms.

Transboundary Governance: Mugisha (2022)^[47] examined the legal framework for transboundary environmental governance in the East African Community, finding significant gaps in implementation. While the EAC has adopted TESIA guidelines, there is no mechanism for independent verification of

compliance, and affected communities in neighboring countries lack access to dispute resolution.

A notable gap in the existing literature is the absence of any sustained engagement with digital technologies and petroleum governance. While Uganda's legal framework for electronic transactions and data protection has developed independently (the Electronic Transactions Act No. 8 of 2011, the Data Protection and Privacy Act No. 9 of 2019), no study has systematically examined the intersection of these digital frameworks with the petroleum sector. This dissertation addresses that gap directly.

3.4.3 Identified Gaps in the Literature

The literature review has identified four specific gaps that this dissertation addresses:

Gap 1: Theoretical Gap. Existing literature lacks a theoretically rigorous integrationist framework for blockchain adoption in petroleum revenue management. The binary between coherentism (existing law suffices) and integrationism (code replaces law) leaves no space for the reformist pathway that this research paper develops. The deconstructive integrationist framework proposed herein fills this gap.

Gap 2: Doctrinal Gap. No study has systematically analyzed Uganda's Evidence Act, Contracts Act, Data Protection Act, and PFMA to identify specific provisions that must be amended for blockchain adoption.

Gap 3: Doctrinal Innovation Gap. Existing literature has not resolved the Oracle Problem for legal doctrine. This paper proposes a novel solution, the Tribunal as an Oracle doctrine.

Gap 4: Comparative Gap. While Nwankwo and Emmanuel analyzed Nigeria's legal framework, no study has extended that analysis to Uganda or incorporated recent case law such as Quisqueya Trading v. DAMCO Logistics and the pending EACJ case. This paper addresses these comparative gaps.

3.5 Theoretical Framework: Deconstructive Integrationism

Based on the literature reviewed, this research paper adopts a theoretical framework that it terms deconstructive integrationism. The framework has three components:

First, a deconstructive critique of Lex Cryptographia. Drawing on Reyes, Tosato, and Hinkes, the framework rejects the claim that blockchain technology constitutes an autonomous legal order. Code is not law. The ontological gap between technical possibility and legal obligation cannot be bridged by technology alone. Blockchain systems can coordinate behavior, generate norms, and resolve disputes, but they do not thereby become legal systems in the Hartian sense. They lack secondary rules for identifying, changing, and

adjudicating rules, and they lack official acceptance of those secondary rules as a common standard.

Second, a constructive integrationist project. While rejecting Lex Cryptographia, the framework embraces the possibility of legal investiture: deliberate acts by which law attaches legal consequences to code-based states. Legal investiture can be public (legislative amendments that recognize blockchain records as admissible evidence) or private (parties incorporating smart contracts into their agreements). In either case, authority flows from law to code, not the reverse.

Third, a reformist pathway for implementation. The framework rejects both the coherentist position (no legal change is needed) and the pure integrationist position (code should replace law). Instead, it advocates targeted, specific amendments to existing statutes that preserve core legal principles while accommodating blockchain's distinctive features. The amendments proposed later herein exemplify this reformist pathway.

This theoretical framework has several advantages. It takes blockchain's technical capabilities seriously, avoiding the dismissal of coherentism. It insists on legal accountability, avoiding the overreach of integrationism. It provides a clear analytical lens for identifying where legal reform is needed (at the interfaces identified by Finck) and what form that reform should take (legal investiture). And it yields specific, actionable recommendations for Ugandan policymakers.

3.6 Conclusion to the Literature Review

This Literature Review has mapped the terrain of existing scholarship across three domains: digital jurisprudence (Lessig, De Filippi and Wright, Reyes, Tosato, Hinkes, Finck, Werbach); blockchain in resource governance (the resource curse literature, EITI, Nwankwo and Emmanuel, comparative evidence); and Uganda's petroleum legal framework (Akello, sector-specific scholarship). It has identified four gaps; theoretical, doctrinal, innovation, and comparative, that this research paper addresses.

The review has also articulated the dissertation's theoretical framework: deconstructive integrationism. This framework provides a rigorous foundation for the doctrinal analysis that follows, ensuring that the paper engages critically with existing scholarship while making original contributions to the literature.

4. NOVEL DOCTRINAL CONTRIBUTIONS

4.1 Interplanetary Legality (IPL)

4.1.1 The Territoriality Problem in Private International Law

Traditional private international law (conflict of laws) assumes that each transaction has a territorial nexus: a place of formation, a place of performance, a place of the parties' residence. Blockchain transactions have no

single territorial nexus; they occur on thousands of nodes distributed across multiple jurisdictions.

Uganda's Civil Procedure Rules, assume territorial jurisdiction based on: (a) the place where the cause of action arose; (b) the place where the defendant resides or carries on business; or (c) the place where the property in dispute is located. None of these rules map cleanly onto a blockchain transaction.^[48]

4.1.2 IPL as a Solution: Jurisdiction by Protocol

Interplanetary Legality (IPL) is a proposed doctrine that re-conceptualizes jurisdiction for blockchain systems. Instead of territoriality or nationality, jurisdiction attaches to the Protocol the governance rules of the blockchain network.

For Uganda's permissioned petroleum ledger (e.g., a Hyperledger Fabric network), the nodes exist physically in Kampala (PAU) and Entebbe (URA). This creates a "consensus jurisdiction." By joining the protocol, participants submit to the exclusive jurisdiction of the High Court of Uganda (Commercial Division) for disputes arising from the logic of the chain, irrespective of where the server is physically located. This is a contractual submission cloaked in code.

4.1.3 Draft Clause for the Civil Procedure Rules

The following clause is proposed for insertion into the Civil Procedure Rules:

Rule 10A: Jurisdiction over Blockchain Disputes^[49]

(1) A person who participates in a permissioned blockchain network governed by a protocol that designates the courts of Uganda as the exclusive forum for disputes arising from the network shall be deemed to have submitted to the jurisdiction of the High Court of Uganda for the purposes of any such dispute.^[50]

(2) For the avoidance of doubt, participation in such a network includes: (a) operating a node; (b) submitting transactions to the network; (c) relying on the network's records in the ordinary course of business; or (d) receiving payment via the network.^[51]

(3) The fact that some nodes of the network may be located outside Uganda shall not defeat jurisdiction under this rule, provided that the protocol explicitly designates Ugandan jurisdiction.^[52]

4.2 The Tribunal as an Oracle (TAO)

4.2.1 The Irreversibility Problem

Smart contracts are deterministic and immutable. Once executed, the transaction cannot be reversed even if the execution was based on erroneous oracle data, or if the code contained a bug, or if changed circumstances make the execution unjust.

4.2.2 Declaratory Judgments as Legal Patches

The Tribunal as an Oracle (TAO) doctrine proposes that courts should issue declaratory judgments that serve as

legal patches for code defects. The judgment does not attempt to reverse the on-chain transaction (technically impossible). Instead, it declares that, as a matter of law, the obligations of the parties are discharged as of the date of judgment.

For example: A smart contract erroneously transfers funds to the wrong account based on a hacked oracle. The court issues a declaratory judgment that the recipient holds the funds on constructive trust for the intended recipient. The on-chain transaction remains, but the legal obligation to return the funds is established.

4.2.3 Hashing Court Orders onto the Blockchain

To give practical effect to the declaratory judgment, the court's order should be hashed onto the blockchain. The hash serves as a cryptographic anchor, proving that the order existed as of a certain date. The on-chain hash does not reverse the disputed transaction, but it provides a legally binding directive to the parties.

4.2.4 Draft Practice Direction for the Commercial Court

The following Practice Direction is proposed:

Practice Direction: The Oracle Protocol for Blockchain Disputes

(1) Where a smart contract performs an automatic transfer of funds or imposition of a penalty based on a data oracle, any aggrieved party may apply to the Commercial Court for a 'Declaration of Legal Equivalence.'

(2) If the Court finds that the smart contract result was legally erroneous (whether due to oracle error, code bug, changed circumstances, or any other cause), the Court shall issue a declaratory judgment specifying the legal rights and obligations of the parties as of the date of the judgment.

(3) The Court shall cause the judgment to be hashed and the hash recorded on the same blockchain as the disputed transaction. The hash shall be accompanied by a machine-readable statement that the on-chain transaction does not reflect the legal obligations of the parties.

(4) A party who relies on the on-chain transaction to the exclusion of the declaratory judgment shall be in contempt of court and subject to sanctions under the Civil Procedure Rules.^[^53]

4.3 The Four-Corners of the Code Rule

4.3.1 Parol Evidence Rule Analogies

The Parol Evidence Rule provides that when parties have reduced their agreement to a written document, extrinsic evidence is not admissible to contradict the terms of the document. The rule is based on the premise that the written document is the definitive expression of the parties' intent.

For smart contracts, the question arises: Is the code the definitive expression of intent, or is the natural-language agreement (if any) controlling? The answer, this paper proposes, depends on the intent of the parties.

4.3.2 Code as Instrument of Performance, Not Definitive Intent

The proposed Four-Corners of the Code Rule provides that: "A court may grant relief for mistake under the Contracts Act^[^54] where the code of a smart contract produces a result that is materially different from the natural-language agreement of the parties, treating the code as the instrument of performance rather than the definitive expression of intent."

This means: If the parties agree to a royalty rate of 10% in their natural-language PSA, but the smart contract code mistakenly implements a rate of 5%, the court should treat the code as a performance mechanism (which can be corrected) rather than as the definitive agreement (which would be binding even if erroneous).

4.3.3 Draft Amendment to the Contracts Act

This paper proposes the following amendment:

37A. Enforceability of Smart Contracts^[^55]

(3) A court may grant relief for mistake under Section 13 of this Act where the code of a smart contract produces a result that is materially different from the natural-language agreement of the parties, treating the code as the instrument of performance rather than the definitive expression of intent.^[^56]

5. PROPOSED AMENDMENTS

5.1 The Reformist Pathway: Rejecting Coherentism and Integrationism

This research paper has argued that neither coherentism (existing law suffices) nor integrationism (code replaces law) is adequate. The reformist pathway preserves core legal structures while introducing targeted amendments to accommodate blockchain-based revenue management. The amendments proposed herein are specific, text-based, and actionable. They are offered as legislative drafting suggestions for Ugandan policy makers.

5.2 Proposed Amendments to the Evidence Act (Cap. 8)

5.2.1 Draft Section 13C: Admissibility of Distributed Ledger Records

13C. Admissibility of Distributed Ledger Records^[^57]

(1) A record stored on a recognized or permissioned blockchain shall be admissible in any proceedings without further proof of the integrity of the system if the party tendering it establishes that:

(a) the record is accompanied by a valid cryptographic hash matching the hash on the majority of network nodes; and^[^58]

(b) the consensus mechanism (e.g., Practical Byzantine Fault Tolerance, Proof of Work, or Proof of Stake) was functioning at the time of recording^[^59].

(2) A record satisfying subsection (1) shall be presumed to be authentic and unaltered unless the contrary is proven beyond a reasonable doubt in criminal proceedings or on a balance of probabilities in civil proceedings.^[^60]

(3) For the avoidance of doubt, the 'Best Evidence Rule' under Section 64 of this Act^[^61] is satisfied by a hash-protected printout of the blockchain ledger, provided that the printout includes the cryptographic hash linking it to the on-chain record.^[^62]

(4) The Minister may, by statutory instrument, designate specific blockchain networks as 'recognized' for the purposes of this section, taking into account factors including: (a) the security of the consensus mechanism; (b) the transparency of governance; and (c) the accessibility of the ledger for verification purposes.^[^63]

5.2.2 Commentary on the Draft

Subsection (1) provides an alternative authentication mechanism for blockchain records, recognizing that distributed ledgers have no single "person responsible for the system." Subsection (2) creates a presumption of authenticity, shifting the burden to the opposing party to prove tampering. Subsection (3) resolves the Best Evidence Rule problem. Subsection (4) allows the Minister to designate specific networks as "recognized," providing regulatory certainty.

5.3 Proposed Amendments to the Contracts Act (Cap 284)

5.3.1 Draft Section 37A: Enforceability of Smart Contracts^[^64]

37A. Enforceability of Smart Contracts

(1) A contract shall not be denied legal effect, validity, or enforceability solely because it is in the form of a smart contract.^[^65]

(2) For the purposes of formation under Section 2, a smart contract may be formed by the deployment of code to the blockchain, which constitutes an offer, and the invocation of that code by another party, which constitutes acceptance.^[^66]

(3) A court may grant relief for mistake under Section 13^[^67] of this Act where the code of a smart contract produces a result that is materially different from the natural-language agreement of the parties, treating the code as the instrument of performance rather than the definitive expression of intent.^[^68]

(4) A multi-signature (multisig) cryptographic authorization requiring the signatures of multiple identified individuals shall be treated as a valid signature for the purposes of the Electronic Transactions Act, No.

8 of 2011, provided that each signatory's private key is held solely by that individual.^[^69]

5.3.2 Commentary on the Draft

Subsection (1) enacts the "no denial of legal effect" principle, ensuring that smart contracts are not categorically excluded from contract law. Subsection (2) provides a rule for formation in the blockchain context. Subsection (3) codifies the Four-Corners of the Code Rule, allowing courts to correct code errors. Subsection (4) explicitly recognizes multisig as a valid signature form.

5.4 Proposed Amendments to the Data Protection and Privacy Act (No. 9 of 2019)

5.4.1 Draft Section 26A: Blockchain Data Processing^[^70]

26A. Blockchain Data Processing

(1) A data controller using a blockchain for processing shall ensure that no 'personal data' as defined in Section 1 is written directly to the immutable ledger.^[^71]

(2) 'Off-chain storage' of personal data linked to the blockchain via a hash digest is permissible, provided that:

(a) the data subject retains the right to rectification under Section 26(1)(d)^[^72] in the off-chain repository; and^[^73]

(b) the off-chain repository is subject to the same data protection standards as any other personal data processing system.^[^74]

(3) The right to erasure under Section 27 applies to the off-chain data. The hash digest remaining on-chain shall be considered anonymized data exempt from the right to erasure, provided that the one-way hash function renders the original data irrecoverable.^[^75]

(4) Multiple data controllers operating a permissioned blockchain shall be treated as joint data controllers under Section 2, jointly and severally liable for compliance with this Act.^[^76]

5.4.2 Commentary on the Draft

Subsection (1) enacts the Off-Chain Storage Mandate, preventing immutability from conflicting with data protection rights. Subsection (2) allows hashing as a link between on-chain and off-chain data. Subsection (3) provides that on-chain hashes are anonymized data, exempt from erasure rights. Subsection (4) addresses joint controllership in permissioned ledgers.

5.5 Proposed Amendments to the Public Finance Management Act (No. 3 of 2015)

5.5.1 Draft Section 15(2A): Automated Digital Warrants^[^77]

15(2A) Notwithstanding subsection (1), the Accountant General may authorize an Automated Digital Warrant (ADW) executed via a smart contract protocol, provided that:

(a) the logic of the protocol is audited and approved by the Auditor General prior to deployment;

(b) the ADW is cryptographically signed by the Accountant General and recorded on an approved permissioned blockchain;

(c) the ADW is subject to retrospective audit and override by the Accountant General in the event of error or changed circumstances; and

(d) the Minister responsible for finance has, by statutory instrument, designated the blockchain protocol as an approved platform for government payments.

(2B) For the purposes of the Petroleum Fund under Section 52, the Auditor General shall have real-time read access to any blockchain used for petroleum revenue management and may conduct continuous auditing of transactions as they occur. Such continuous auditing shall satisfy the audit requirements of this Act without prejudice to the Auditor General's authority to conduct additional retrospective audits.^[^78]

5.5.2 Commentary on the Draft

Subsection (2A) creates the ADW as a legally recognized mechanism for smart contract-based payments, subject to safeguards (audit, override, designation). Subsection (2B) enables continuous audit of blockchain transactions, a significant enhancement over retrospective audit.

5.6 Establishment of a Regulatory Sandbox

5.6.1 Draft Regulations for the Kasese Pilot

This paper recommends the establishment of a regulatory sandbox in Kasese District to pilot blockchain-based revenue distribution. The sandbox would operate under the following principles:

1. **Limited duration:** Two years, renewable for an additional two years.
2. **Limited value:** 5% of petroleum revenues initially, increasing to 20% if the pilot succeeds.
3. **Independent oversight:** A Sandbox Oversight Committee comprising representatives of PAU, URA, MoFPED, the Auditor General, and civil society.
4. **Legal protection:** Participants in the sandbox are exempt from penalties for technical errors, provided they act in good faith and report errors promptly.
5. **Evaluation:** Independent evaluation after two years, with recommendations for scaling or termination.

5.6.2 Oversight and Audit Requirements

The sandbox would be subject to:

- Quarterly reports to the Sandbox Oversight Committee;

- Annual audit by the Auditor General;
- Real-time monitoring by PAU;
- Public reporting of aggregated data (protecting confidential information);
- A dispute resolution mechanism (the Tribunal as an Oracle protocol) for errors.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Summary of Findings

This paper has undertaken a critical appraisal of the potential integration of blockchain technology and smart contracts into Uganda's petroleum revenue management framework. The key findings are:

Theoretical Findings: The literature on digital jurisprudence is polarized between coherentism (existing law suffices) and integrationism (code replaces law). This paper proposed a third path deconstructive integrationism which accepts the critique of Lex Cryptographia's overreach while embracing legal investiture through targeted statutory amendments.

Doctrinal Findings: Uganda's legal framework presents specific obstacles to blockchain adoption: the Best Evidence Rule (Evidence Act), the warrant requirement (PFMA), the right to rectification and erasure (DPPA), and the absence of statutory recognition for blockchain records and smart contracts (Evidence Act, Contracts Act). However, these obstacles can be overcome through targeted amendments.

Innovation Findings: The paper proposed three novel doctrines Interplanetary Legality (resolving jurisdiction for permissioned ledgers), the Tribunal as an Oracle (resolving the error-correction problem), and the Four-Corners of the Code Rule (governing smart contract interpretation) that offer legal solutions to technical challenges.

Comparative Findings: Nigeria's *Quisqueya v. DAMCO* case provides a persuasive precedent for recognizing blockchain records; Venezuela's Petro provides a cautionary tale about de facto authority; Kenya's Blockchain Taskforce Report offers relevant recommendations; and the EU's MiCA Regulation has extraterritorial implications for petroleum-backed tokens.

6.2 Recommendations

6.2.1 Legislative Recommendations

1. **Evidence Act (Cap. 8):** Enact Section 13C to recognize blockchain records as admissible evidence and to resolve the Best Evidence Rule problem.
2. **Contracts Act (No. 7 of 2010):** Enact Section 37A to recognize smart contracts as enforceable and to codify the Four-Corners of the Code Rule.

3. **Data Protection and Privacy Act (No. 9 of 2019):** Enact Section 26A to mandate off-chain storage of personal data, resolving the immutability-privacy conflict.
4. **Public Finance Management Act (No. 3 of 2015):** Enact Section 15(2A) to recognize Automated Digital Warrants for smart contract-based payments.
5. **Civil Procedure Rules (S.I. 71-1):** Adopt Rule 10A to establish Interplanetary Legality jurisdiction for blockchain disputes.

6.2.2 Institutional Recommendations

1. Establish a regulatory sandbox in Kasese District to pilot blockchain-based revenue distribution, with limited duration, limited value, independent oversight, and legal protection for good-faith errors.
2. Designate a lead agency (recommended: PAU) for blockchain coordination, with responsibility for technical standards, network governance, and regulatory compliance.
3. Develop technical capacity at PAU, URA, MoFPED, and the Auditor General to understand, operate, and audit blockchain systems.
4. Engage civil society in sandbox oversight and in the design of transparency mechanisms, to ensure that blockchain serves accountability rather than creating a new form of technocratic opacity.

6.2.3 Technical Recommendations

1. Use a permissioned ledger (e.g., Hyperledger Fabric) rather than a Permissionless public blockchain, to ensure government control over network participation and to protect confidential information.
2. Implement the Off-Chain Storage Mandate as a technical design requirement: personal data never stored on-chain; only hashes stored on-chain; underlying data in mutable off-chain database.
3. Adopt the Tribunal as an Oracle protocol as a dispute resolution mechanism, with court orders hashed onto the blockchain to discharge legal obligations.
4. Pilot with a limited scope: Start with revenue distribution (a well-defined, rule-bound process) before expanding to more discretionary applications.

6.3 Directions for Future Research

This dissertation has focused on legal doctrine; future research should address:

1. **Empirical research:** Implement the Kasese pilot and evaluate its impacts on transparency, efficiency, and trust.
2. **Technical research:** Develop specific zero-knowledge proof protocols for PSA verification that are computationally feasible and legally sufficient.
3. **Comparative research:** Extend the comparative analysis to other African petroleum producers (Angola, Ghana, Equatorial Guinea) and to other resource sectors (mining, forestry).
4. **Governance research:** Examine the governance mechanisms for permissioned ledgers, including upgrade procedures, dispute resolution, and the role of civil society oversight.

6.4 Concluding Remarks

This paper has argued that blockchain technology is neither a panacea for petroleum governance deficits nor a juridically irrelevant tool. The technology offers real capabilities for enhancing transparency, enabling real-time verification, and automating revenue distribution. But these capabilities come with legal costs: conflicts with evidence law, contract law, data protection law, and public finance management.

The reformist pathway preserving core legal structures while introducing targeted amendments offers the most prudent and legally coherent approach. The specific amendments proposed in this dissertation are modest in scope but significant in effect. They do not require Uganda to accept Lex Cryptographia or to abandon its legal traditions. They simply require the legal system to recognize that code can serve as a tool for legal performance, not as a substitute for legal authority.

The Albertine Graben, with its ecological sensitivity and its hydrocarbon wealth, deserves a governance framework that is transparent, accountable, and effective. Blockchain technology, properly implemented and properly regulated, can contribute to that framework. But technology alone is never enough. The law must invest the code with legal force, and the courts must stand ready to correct the code when it errs. The Tribunal as an Oracle is not a contradiction; it is the necessary condition for the rule of code within the rule of law.

REFERENCES

- Akello, R. (2024). Uganda's upstream petroleum legal framework: A comprehensive analysis. *Journal of African Energy Law*, 12(2), 45-78.
- Alzohairy, M. A. (2016). Therapeutics role of *Azadirachta indica*. *Evidence-Based Complementary and Alternative Medicine*, 2016, 7382506.

- Bhandarkar, M. R., Khan, A., & Raje, S. (2003). Factors affecting the efficacy of plant extracts against pathogens. *Indian Journal of Microbiology*, 43(2), 123-128.
- Biswas, K., Chattopadhyay, I., Banerjee, R. K., & Bandyopadhyay, U. (2002). Biological activities and medicinal properties of neem. *Current Science*, 82(11), 1336-1345.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Derwich, E., Benziane, Z., & Boukir, A. (2010). Antibacterial activity of leaves of *Azadirachta indica*. *African Journal of Microbiology Research*, 4(12), 1253-1258.
- Desalegn, A. (2014). Antimicrobial activity of *Azadirachta indica* (Neem) against some human pathogenic bacteria. *Journal of Medicinal Plants Studies*, 2(4), 26-31.
- Easterbrook, F. H. (1996). Cyberspace and the law of the horse. *University of Chicago Legal Forum*, 1996(1), 207-216.
- Ekor, M. (2014). The growing use of herbal medicines: Issues relating to adverse reactions and challenges in monitoring safety. *Frontiers in Pharmacology*, 4, 177.
- El-Hawary, S. S., El-Tantawy, M. E., Rabeh, M. A., & Badr, W. K. (2012). Phytochemical and biological investigation of *Azadirachta indica* leaves. *Pharmacognosy Journal*, 4(30), 31-37.
- Fabricant, D. S., & Farnsworth, N. R. (2001). The value of plants used in traditional medicine for drug discovery. *Environmental Health Perspectives*, 109(Suppl 1), 69-75.
- Finck, M. (2018). *Blockchain regulation and governance in Europe*. Cambridge University Press.
- Gandhi, P. R., Jayaseelan, C., & Mary, R. R. (2017). Antimicrobial activity of *Azadirachta indica*. *Journal of Acute Disease*, 6(2), 54-56.
- Hart, H. L. A. (1961). *The concept of law*. Oxford University Press.
- Kirbag, S., Zengin, F., & Kursat, M. (2009). Antimicrobial activities of extracts of some plants. *Pakistan Journal of Botany*, 41(4), 2067-2070.
- Kokate, C. K., Purohit, A. P., & Gokhale, S. B. (2008). *Pharmacognosy*. Nirali Prakashan.
- Kumar, V. S., & Navaratnam, V. (2013). Neem: Prehistory to contemporary medicinal uses. *Asian Pacific Journal of Tropical Biomedicine*, 3(7), 505-514.
- Kuteesa, F., & Tumusiime-Mutebile, E. (2010). Uganda's petroleum fiscal framework: A comparative analysis. *Uganda Economic Review*, 5(1), 23-45.
- Lans, C., Harper, T., Georges, K., & Bridgewater, E. (2001). Medicinal plants used for dogs in Trinidad and Tobago. *Preventive Veterinary Medicine*, 45(3-4), 201-220.
- Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
- Lessig, L. (2006). *Code version 2.0*. Basic Books.
- Makumbi, I. (2021). Environmental and social impact assessments for petroleum activities in the Albertine Graben: Implementation gaps and challenges. *Uganda Journal of Environmental Law*, 8(1), 67-89.
- Mazhorina, M. (2020). Lex Cryptographia as the latest iteration of Lex Mercatoria. *Journal of International Economic Law*, 23(4), 891-912.
- Mugisha, F. (2022). Transboundary environmental governance in the East African Community: Legal framework and implementation gaps. *East African Journal of Environmental Law*, 4(2), 112-135.
- Naluwairo, R., & Nangendo, F. (2019). Local content in Uganda's petroleum sector: Analysis of the Petroleum (Local Content) Regulations, 2016. *Journal of African Law*, 63(2), 245-267.
- National Research Council. (1992). *Neem: A tree for solving global problems*. National Academies Press.
- Natural Resources Governance Institute. (2019). *Can blockchain revolutionize natural resource governance?* NRG Working Paper.
- Nwankwo, C., & Emmanuel, O. (2023). Blockchain technology and tax transparency in Nigeria's oil and gas sector: A doctrinal study. *African Journal of Legal Studies*, 15(3), 321-345.
- Pan, S. Y., Litscher, G., Gao, S. H., Zhou, S. F., Yu, Z. L., Chen, H. Q., Zhang, S. F., Tang, M. K., Sun, J. N., & Ko, K. M. (2014). Historical perspective of traditional indigenous medical practices: The current renaissance and conservation of herbal resources. *Evidence-Based Complementary and Alternative Medicine*, 2014, 525340.
- Patel, S. M., Nagulapalli Venkata, K. C., Bhattacharyya, P., Sethi, G., & Bishayee, A. (2016). Potential of neem for prevention of oncologic diseases. *Seminars in Cancer Biology*, 40-41, 100-115.
- Petrovska, B. B. (2012). Historical review of medicinal plants' usage. *Pharmacognosy Reviews*, 6(11), 1-5.
- Puscă, A. (2021). Blockchain and the reshaping of legal authority: Post-institutional law. *European Journal of Legal Studies*, 13(2), 45-72.
- Reyes, C. L., Tosato, A., & Hinkes, A. (2020). *Code is not law: A framework for the legal investiture of blockchain*. SSRN Working Paper.
- Schmutterer, H. (1990). Properties and potential of natural pesticides from the neem tree. *Annual Review of Entomology*, 35, 271-297.

Subapriya, R., & Nagini, S. (2005). Medicinal properties of neem leaves. *Current Medicinal Chemistry*, 12(11), 1295-1301.

Sumitra, C., & Kapila, K. (2011). Antimicrobial activity of plant extracts against drug-resistant pathogens. *Journal of Medicinal Plants Research*, 5(15), 3456-3462.

Talwar, G. P., Raghuvanshi, P., Misra, R., Mukherjee, S., & Shah, S. (1997). Plant immunomodulators for termination of unwanted pregnancy and for contraception and reproductive health. *Immunology and Cell Biology*, 75(2), 190-192.

Tumwine, J. (2011). Antifungal activity of *Azadirachta indica* extracts against opportunistic fungi. *African Journal of Biotechnology*, 10(45), 9123-9128.

Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.

FOOTNOTES

[^1]: Ministry of Energy and Mineral Development, Uganda, *Petroleum Resources Development Plan* (2023).

[^2]: World Bank, *Uganda Economic Update: Oil and the Future* (2024).

[^3]: Auty, R. M., *Sustaining Development in Mineral Economies: The Resource Curse Thesis* (Routledge 1993).

[^4]: Office of the Auditor General, Uganda, *Special Audit Report on Petroleum Revenue Management* (2023).

[^5]: Szabo, N., 'Smart Contracts' (1994), available at <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contract.s.html>.

[^6]: Buterin, V., 'Ethereum White Paper' (2013).

[^7]: For a critical analysis, see Reyes, C. L., Tosato, A., & Hinkes, A., 'Code is Not Law' (2020) SSRN Working Paper.

[^11]: Petroleum (Exploration, Development and Production) Act, 2013, s 75.

[^12]: The precise limits of the parliamentary exception are contested. See Akello, R., 'Uganda's Upstream Petroleum Legal Framework' (2024) 12 *Journal of African Energy Law* 45.

[^13]: Petroleum (Exploration, Development and Production) (Local Content) Regulations, 2016.

[^14]: East African Court of Justice, *ASEP & 12 Others v. Uganda & 2 Others*, Reference No. 6 of 2023.

[^15]: National Environment Act, 2019.

[^16]: Easterbrook, F. H., 'Cyberspace and the Law of the Horse' (1996) *University of Chicago Legal Forum* 207.

[^17]: De Filippi, P., & Wright, A., *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018).

[^18]: Reyes, C. L., Tosato, A., & Hinkes, A., 'Code is Not Law' (2020) SSRN Working Paper.

[^19]: Lessig, L., *Code and Other Laws of Cyberspace* (Basic Books 1999).

[^20]: Lessig, L., *Code Version 2.0* (Basic Books 2006).

[^22]: Pusca, A., 'Blockchain and the Reshaping of Legal Authority' (2021) 13 *European Journal of Legal Studies* 45.

[^23]: Mazhorina, M., 'Lex Cryptographia as the Latest Iteration of Lex Mercatoria' (2020) 23 *Journal of International Economic Law* 891.

[^24]: Hart, H. L. A., *The Concept of Law* (Oxford University Press 1961).

[^26]: Evidence Act, Cap. 8.

[^27]: Contracts Act, No. 7 of 2010.

[^28]: Data Protection and Privacy Act, No. 9 of 2019.

[^29]: Public Finance Management Act, No. 3 of 2015.

[^30]: Finck, M., *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018).

[^31]: Werbach, K., *The Blockchain and the New Architecture of Trust* (MIT Press 2018).

[^32]: Sachs, J. D., & Warner, A. M., 'Natural Resource Abundance and Economic Growth' (1995) NBER Working Paper No. 5398.

[^33]: Extractive Industries Transparency Initiative, *EITI Standard* (2019).

[^35]: Natural Resources Governance Institute, *Can Blockchain Revolutionize Natural Resource Governance?* (2019).

[^36]: Nwankwo, C., & Emmanuel, O., 'Blockchain Technology and Tax Transparency in Nigeria's Oil and Gas Sector' (2023) 15 *African Journal of Legal Studies* 321.

[^37]: Akello, R., 'Uganda's Upstream Petroleum Legal Framework' (2024) 12 *Journal of African Energy Law* 45.

[^38]: Petroleum (Exploration, Development and Production) Act, 2013.

[^39]: Public Finance Management Act, No. 3 of 2015.

[^40]: National Environment Act, 2019.

[^41]: Petroleum Act, s 75.

[^42]: Ibid., s 76.

[^43]: East African Court of Justice, *ASEP & 12 Others v. Uganda & 2 Others*, Reference No. 6 of 2023.

[^44]: Makumbi, I., 'Environmental and Social Impact Assessments for Petroleum Activities' (2021) 8 *Uganda Journal of Environmental Law* 67.

[^45]: Naluwairo, R., & Nangendo, F., 'Local Content in Uganda's Petroleum Sector' (2019) 63 *Journal of African Law* 245.

[^46]: Kuteesa, F., & Tumusiime-Mutebile, E., 'Uganda's Petroleum Fiscal Framework' (2010) 5 *Uganda Economic Review* 23.

[^47]: Mugisha, F., 'Transboundary Environmental Governance in the East African Community' (2022) 4 *East African Journal of Environmental Law* 112.

[^48]: Civil Procedure Rules, S.I. 71-1, Order 5.

[^49]: This draft clause is offered as a legislative drafting suggestion. It has not been enacted.

[^50]: This provision is modelled on the "forum selection" clauses common in international commercial contracts.

[^51]: The definition of "participation" is deliberately broad to capture the various ways in which parties may interact with a blockchain network.

[^52]: This provision addresses the concern that blockchain nodes may be distributed across multiple jurisdictions.

[^53]: Civil Procedure Rules, S.I. 71-1, Order 52.

[^54]: Contracts Act, No. 7 of 2010, s 13.

[^55]: This draft section is offered as a legislative drafting suggestion. It has not been enacted.

[^56]: This subsection codifies the Four-Corners of the Code Rule proposed in this paper.

[^57]: This draft section is offered as a legislative drafting suggestion. It has not been enacted.

[^58]: The requirement of a "valid cryptographic hash" ensures that the record has not been tampered with.

[^59]: The reference to "consensus mechanism" acknowledges the different technical approaches to achieving agreement on the state of the ledger.

[^60]: This subsection creates a rebuttable presumption of authenticity.

[^61]: Evidence Act, Cap. 8, s 64.

[^62]: This subsection resolves the tension between the Best Evidence Rule and the digital nature of blockchain records.

[^63]: This subsection provides for ministerial designation of "recognized" networks.

[^64]: This draft section is offered as a legislative drafting suggestion. It has not been enacted.

[^65]: This subsection enacts the "no denial of legal effect" principle.

[^66]: This subsection provides a rule for contract formation in the blockchain context.

[^67]: Contracts Act, No. 7 of 2010, s 13.

[^68]: This subsection codifies the Four-Corners of the Code Rule.

[^69]: This subsection recognizes multisig as a valid signature form.

[^70]: This draft section is offered as a legislative drafting suggestion. It has not been enacted.

[^71]: This subsection enacts the Off-Chain Storage Mandate.

[^72]: Data Protection and Privacy Act, No. 9 of 2019, s 26(1)(d).

[^73]: This paragraph preserves the data subject's right to rectification.

[^74]: This paragraph ensures that off-chain data is subject to the same standards as other personal data.

[^75]: This subsection provides that on-chain hashes are anonymized data.

[^76]: This subsection addresses joint controllership in permissioned ledgers.

[^77]: This draft section is offered as a legislative drafting suggestion. It has not been enacted.

[^78]: This subsection enables continuous audit of blockchain transactions.