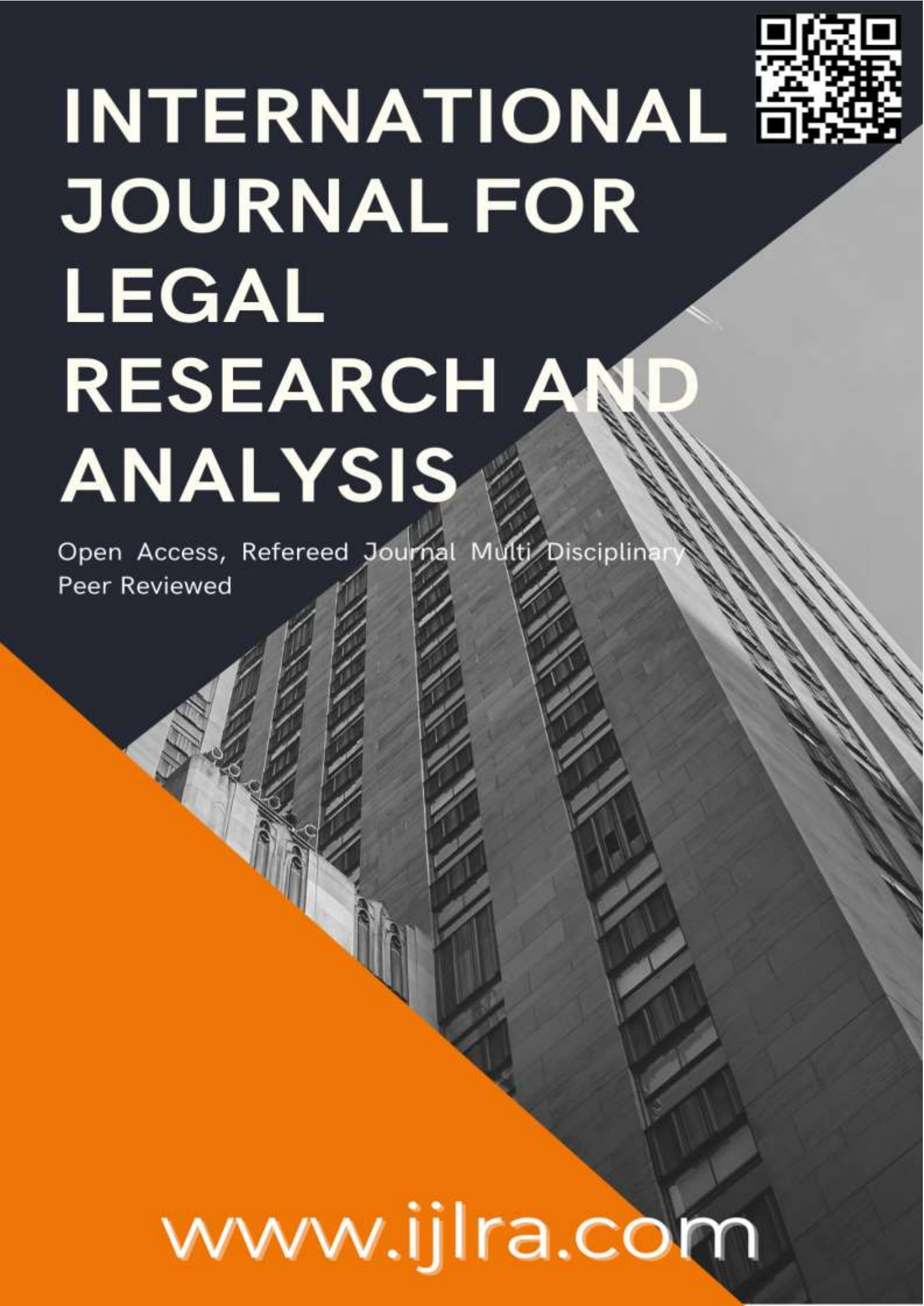
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

BLOCKCHAIN AND CROSS-BORDER INVESTMENT LAW: JURISDICTIONAL CHALLENGES

AUTHORED BY - AKIL K

I. TABLE OF CONTENTS

 ISSN: 2582-6433

II. LIST OF STATUTES

1. International Instruments

1. UNCITRAL Model Law on Electronic Commerce (1996)
2. ICSID Convention (1965)
3. General Agreement on Trade in Services (GATS)
4. New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958)
5. Hague Convention on Choice of Court Agreements (2005)
6. Financial Action Task Force (FATF) Recommendation 15
7. OECD Guidelines on Data Governance and DFFT
8. GDPR – General Data Protection Regulation (EU) 2016/679

2. Domestic Legislation (Selected Jurisdictions)

- **India**
    1. Information Technology Act, 2000
    2. Digital Personal Data Protection Act, 2023
    3. Reserve Bank of India Circular on Data Localization, 2018
- **European Union**
    1. Markets in Crypto-Assets Regulation (MiCA), 2023
- **China**
    1. Cybersecurity Law, 2017
    2. Data Security Law, 2021
- **Russia**
    1. Federal Law on Personal Data
- **USA**
    1. Securities Act of 1933
    2. Securities Exchange Act of 1934
    3. California Consumer Privacy Act (CCPA)

 ISSN: 2582-6433

IV. TABLE OF CASES

CASE NAME	CITATION
SEC v. W. J. Howey Co.	328 U.S. 293 (1946)
Quoine Pte Ltd v. B2C2 Ltd	[2020] SGCA(I) 02
SEC v. Telegram Group Inc.	No. 19-cv-9439 (PKC), SDNY
SEC v. Ripple Labs Inc.	Case No. 1:20-cv-10832 (AT) (S.D.N.Y. 2023)
India v. Vodafone Group	(2012) 6 SCC 613 *(re BIT scope and taxation)*
VanEck Vectors Bitcoin ETN Case (EU BaFin)	[2021] BaFin Decision

 ISSN: 2582-6433

IV. LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
AML	Anti-Money Laundering
BIT	Bilateral Investment Treaty
DAO	Decentralised Autonomous Organisation
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation
ICSID	International Centre for Settlement of Investment Disputes
ICO	Initial Coin Offering
KYC	Know Your Customer
MiCA	Markets in Crypto-Assets Regulation
OECD	Organisation for Economic Co-operation and Development
SCC	Standard Contractual Clauses
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
VASP	Virtual Asset Service Provider
WTO	World Trade Organization

 ISSN: 2582-6433

Chapter 1: Introduction

Blockchain technology has swiftly emerged as a transformative force in the global economy, reshaping how value is exchanged and investments are made across borders. Originating with the advent of Bitcoin in 2008 and expanding through thousands of cryptocurrencies and distributed applications since, blockchain's rise marks a disruptive shift in cross-border investment. Today, digital assets and blockchain-based financial instruments enable individuals and enterprises to transact globally without traditional intermediaries. Investors from different continents can contribute capital to a project via token sales or decentralised finance platforms instantaneously, often outside the purview of any single national regulator. In numeric terms, by 2021 the total market capitalisation of crypto-assets surpassed two trillion US dollars, illustrating the scale of capital pouring into this new asset class worldwide. Likewise, initial coin offerings and other token-based fundraising methods have raised tens of billions of dollars from participants across the globe in a few short years. This unprecedented connectivity and disintermediation hold great promise for efficiency and inclusion in international investment, opening avenues for funding and innovation that were previously unimaginable.

However, these developments also unsettle the legal frameworks built around territorial jurisdiction and state oversight. The borderless nature of blockchain operations means that capital can flow in ways that elude the traditional gatekeepers and checkpoints of the financial system. A technology startup in Singapore, for instance, might attract investments from Europe, Asia, and North America via a blockchain token sale without ever establishing a legal presence in those jurisdictions. Such scenarios exemplify both the opportunity and the regulatory conundrum: while cross-border investment becomes more accessible, the clear allocation of legal responsibility and oversight becomes far more complex. It is against this backdrop of immense opportunity and profound legal uncertainty that the present research is situated, examining how blockchain's global reach challenges the fundamentals of cross-border investment law.

Research Problem

The borderless nature of blockchain transactions introduces fundamental jurisdictional challenges in cross-border investment law. Modern legal systems—both domestic and international—have long anchored jurisdiction, regulatory authority, and the enforcement of

 ISSN: 2582-6433

laws to geography and identifiable parties. Investment law, whether in national legislation or in international treaties, presumes clearly defined participants (investors and host states) and a discernible location for assets or transactions. Blockchain undermines these assumptions. Transactions occur on a decentralised ledger spread across nodes worldwide rather than in any single location, and parties often remain pseudonymous or represented only by digital addresses. As a result, when disputes arise or when regulators seek to apply investor protection laws, it is often unclear which jurisdiction's laws should apply or which forum has authority. The research problem, therefore, is the uncertainty and conflict that stem from applying traditional jurisdictional principles to blockchain-based investments. How can legal accountability, investor rights, and regulatory oversight be maintained when an investment transcends national boundaries in both structure and operation? For example, if a government unilaterally bans cryptocurrency trading or expropriates digital assets held in a nationwide crackdown, foreign investors affected might struggle to invoke protections under investment treaties or local law because it is debatable whether their blockchain-held assets count as investments "in" that jurisdiction. Such dilemmas highlight the core question this study confronts: how existing notions of jurisdiction can be reconciled with, or reimagined for, an environment where the conventional anchors of location and identity are in flux. Without clarity on this issue, both investors and states face significant risks—investors may lack recourse under law for cross-border grievances, and regulators may find their authority and tools increasingly ineffective in a digitized global marketplace.

Objectives of the Study

In light of the above problem, this dissertation sets out several interrelated objectives. Foremost, it aims to elucidate the nature of the jurisdictional challenges posed by blockchain in the context of cross-border investment. This involves dissecting how features such as decentralisation, immutability, and pseudonymity complicate the application of traditional legal concepts like territorial jurisdiction, applicable law, and enforcement mechanisms. A further objective is to evaluate the adequacy of existing legal frameworks—ranging from international investment agreements and arbitration mechanisms to national regulatory regimes—in addressing these challenges. By examining current laws and dispute resolution practices, the study seeks to identify gaps, inconsistencies, or uncertainties that blockchain-based investments expose. Additionally, the research undertakes a comparative analysis of different jurisdictions and regulatory approaches. By reviewing how various countries and international bodies have responded (or struggled to respond) to cryptocurrency markets, token

 ISSN: 2582-6433

offerings, and blockchain enterprises, the study aims to glean insights into best practices or emerging standards. Ultimately, the dissertation's objective is not only to analyse and critique the current state of affairs but also to lay the groundwork for conceptual solutions. It strives to contribute to the broader discourse on harmonising technology and law by suggesting principles or approaches that could better align blockchain's borderless operations with the jurisdiction-bound nature of investment law.

Scope and Limitations

This research is focused on the intersection of blockchain technology and cross-border investment law, with particular emphasis on jurisdictional questions. It will cover a range of issues that arise when investments utilise blockchain platforms or digital assets across multiple jurisdictions. Key topics include legal identification of assets and parties on decentralised networks, conflicts of law in blockchain transactions, and the challenges of enforcing rights or regulations transnationally. The study gives considerable attention to international investment law instruments (such as bilateral investment treaties and arbitration conventions) and domestic financial regulation, insofar as they pertain to foreign or cross-border investments in blockchain ventures.

However, certain delimitations are necessary. The analysis is primarily legal and conceptual; it does not delve into the detailed technical design of cryptographic algorithms or the engineering aspects of blockchain beyond what is relevant for lawyers and policymakers. Likewise, while issues of fraud, money laundering, and cybersecurity are discussed as they impact cross-border investment, the dissertation does not purport to be a comprehensive study of criminal law or data protection in the blockchain context. Rather, those topics are addressed only to the extent that they create or highlight jurisdictional problems for investment and regulatory oversight. Geographically, the comparative element means that only select jurisdictions and regulatory frameworks can be examined in depth – these are chosen for their relevance and influence. For example, the approaches of the United States, the European Union, and key Asian jurisdictions (among others) are considered, alongside international standards and model laws where applicable. The study is also limited by the current state of development: given that blockchain regulation is rapidly evolving, some legal questions remain open or speculative. The dissertation therefore acknowledges that its conclusions are drawn from the law as of 2025 and the still-emerging body of case law and regulatory guidance on blockchain investments. These inherent limitations notwithstanding, the scope is sufficiently

 ISSN: 2582-6433

broad to capture the major themes of jurisdictional challenge, while remaining focused on the core issue of aligning blockchain innovation with existing legal paradigms.

Significance of the Research

The significance of this study lies in its contribution to both legal scholarship and practical policymaking at a time when technology and law are intersecting in unprecedented ways. From a legal perspective, the research addresses a gap in the literature concerning how international investment law – traditionally concerned with physical foreign investments like factories or shareholdings – can adapt to intangible, decentralised assets that do not fit neatly within territorial boundaries. By systematically examining jurisdictional challenges, the study enhances the understanding of how foundational legal principles may need reinterpretation or reform in the digital age. This is not merely a theoretical exercise; it carries tangible importance for investor protection and the rule of law. Investors engaging in cross-border blockchain ventures, be they individuals participating in global token sales or institutions trading cryptocurrency across jurisdictions, currently face significant uncertainty about their legal rights and remedies. Similarly, regulators and courts worldwide are under pressure to respond to cross-border crypto-financial activities that could affect market stability, financial integrity, and consumer confidence. In this context, the research is timely and relevant: it can inform policymakers about the shortcomings of the status quo and the potential paths for legal development.

Technologically, the study is significant in that it promotes a dialogue between the innovative ethos of the blockchain community and the normative frameworks of law and governance. By highlighting jurisdictional issues, the dissertation implicitly argues for more robust interfaces between technologists and lawmakers – whether through clearer regulations, international cooperation, or new technical solutions that respect legal requirements. On a regulatory level, the findings of this research could be valuable for the development of more harmonised approaches to blockchain across different countries. As nations and international bodies consider guidelines or treaties for digital assets, they can benefit from understanding the jurisdictional pitfalls and possibilities uncovered in this study. In sum, the significance of the research is multifaceted: legally, it pushes the evolution of investment law; practically, it aims to protect participants in the global digital economy; and strategically, it contributes to shaping a regulatory environment that can foster innovation while upholding legal order.

 ISSN: 2582-6433

Methodology

The dissertation adopts a doctrinal and analytical methodology, complemented by comparative and interdisciplinary perspectives. At its core, the research is doctrinal: it involves a close examination of legal texts, including statutes, regulations, international treaties, case law, and arbitration awards that are pertinent to blockchain and cross-border investments. This black-letter law approach is used to ascertain what the law currently says about jurisdiction, investment, and digital technology. Given that blockchain-related jurisprudence is nascent, the study also analyses analogous legal principles from fields like internet law and private international law to draw parallels and highlight where existing doctrines may or may not extend to blockchain scenarios. In conducting this analysis, the methodology remains analytical in the sense that it critically evaluates the effectiveness and coherence of legal rules when faced with the unique attributes of blockchain. The research does not merely describe laws; it interrogates them, identifying tensions between traditional legal concepts and the realities of decentralized networks.

A comparative analysis is employed to broaden the understanding of how different legal systems are grappling with the issues. This involves reviewing the approaches of several jurisdictions—such as comparing the regulatory stances of developed financial centers versus emerging economies, or civil law versus common law approaches to defining digital assets. For example, one part of the study might contrast how the European Union, the United States, and jurisdictions like Singapore or Switzerland define and regulate crypto-assets as investments, and how these definitions impact jurisdictional claims. Additionally, international instruments and soft law guidelines are reviewed, including any relevant work by bodies like UNCITRAL, the G20 (particularly the Financial Action Task Force's guidance on virtual assets), or the OECD, to gauge efforts at creating cross-border consensus. Throughout, the methodology is underpinned by extensive literature review, engaging with academic commentary from legal scholars, economists, and technologists. This interdisciplinary touch ensures that the analysis accounts for the technical underpinnings of blockchain (to the extent necessary) and the economic realities of cross-border investment flows. Importantly, while the methodology is comprehensive in gathering legal sources and perspectives, it does not include empirical fieldwork or statistical analysis; the research is qualitative, grounded in reasoning from legal principles and documented cases or examples. Such a methodology is well-suited for a field where clarity and theory-building are needed, given the relative scarcity of decided cases or codified rules on point.

 ISSN: 2582-6433

Structure of the Dissertation

This introductory chapter (Chapter 1) has set out the context, problem statement, objectives, scope, significance, and methodology of the research. The remainder of the dissertation is organized as follows. Chapter 2 provides a conceptual foundation by examining the core features of blockchain technology and how they disrupt conventional notions of jurisdiction and regulatory oversight. It explains the decentralised nature of distributed ledgers, the role of consensus mechanisms, and the absence of a central controlling entity, highlighting why these attributes create uncertainty in determining which laws apply to cross-border transactions. Chapter 3 turns to one of blockchain's most prominent innovations—smart contracts—and discusses their impact on legal enforceability in investment arrangements. It explores scenarios where investment agreements are executed in code and the difficulties courts or arbitral tribunals face in interpreting and intervening in such self-executing agreements that span multiple jurisdictions. In Chapter 4, the discussion moves to conflicts of law and the collapse of traditional jurisdictional tests in blockchain-based investment disputes. This chapter analyses how principles like territoriality and party domicile falter when investments are conducted through decentralized platforms, and it assesses the resulting challenges for both national courts and international arbitration bodies in asserting authority or agreeing on applicable law.

Chapter 5 addresses the tension between blockchain's borderless operation and state sovereignty through the lens of data. It focuses on data localization laws and the concept of data sovereignty, examining how requirements to keep financial or personal data within national borders clash with the distributed architecture of blockchain systems. This chapter uses examples from jurisdictions enforcing strict data localization to illustrate the frictions between domestic regulatory imperatives and technologies that are inherently transnational. Chapter 6 then evaluates investor and consumer protection concerns in blockchain investments, identifying regulatory gaps. It looks at the prevalence of fraud (such as scams in initial coin offerings) and market volatility, evaluating why existing securities and financial regulations have struggled to cope with these phenomena across jurisdictions. The chapter also discusses how the lack of harmonised classification of digital tokens (whether as securities, commodities, or utilities) leaves loopholes that bad actors exploit and leaves investors without uniform safeguards globally.

Moving to dispute resolution, Chapter 7 explores how conflicts arising from blockchain

 ISSN: 2582-6433

investments can be resolved, comparing traditional mechanisms with emerging alternatives. It reviews the suitability of international arbitration and litigation for blockchain disputes and then examines novel decentralised dispute resolution platforms that have appeared within blockchain ecosystems. This analysis highlights whether such "on-chain" dispute resolution methods could supplement or challenge traditional legal forums, especially for cross-border issues. Chapter 8 considers the fiscal dimension by discussing how different national tax regimes classify and tax cryptocurrency holdings and blockchain-based assets. Given that tax law is often a direct expression of national jurisdiction, this chapter illustrates the complexities investors face in remaining compliant when engaging in cross-border blockchain transactions, and how mismatches between tax systems can lead to both opportunities and enforcement difficulties. Chapter 9 looks at proactive measures to mitigate jurisdictional uncertainty. It examines the role of technological and regulatory tools—such as blockchain geofencing to limit access based on user location, and regulatory sandboxes that allow innovators to operate under supervision—in bridging the gap between a decentralised investment environment and the jurisdictional mandates of states. These measures are assessed for their effectiveness and for the trade-offs they entail for the openness of blockchain networks. Finally, Chapter 10 concludes the dissertation by synthesizing the insights from all previous chapters. It revisits the research questions to articulate the findings on how blockchain challenges jurisdiction in cross-border investment law and summarizes the recommendations or principles for addressing these challenges. In doing so, the concluding chapter reflects on the broader trajectory of blockchain regulation and suggests areas for future research, underscoring the need for ongoing adaptation as technology and law continue to evolve in tandem.

Chapter 2: Cross-Border Jurisdictional Complexity

 ISSN: 2582-6433

Blockchain technology introduces a profound structural shift in the way legal systems and regulatory frameworks engage with cross-border transactions. Its defining characteristics—decentralisation, immutability, pseudonymity, and transnational operation—challenge the very foundations of jurisdiction, regulatory enforcement, and legal accountability. In the context of cross-border investment, blockchain operates beyond the confines of traditional financial architectures, rendering territorial notions of law and governance increasingly obsolete.

The Nature of Decentralised Ledgers

Unlike traditional financial systems that rely on centralised intermediaries such as banks, clearinghouses, or regulatory authorities, blockchain is built upon decentralised ledger technology (DLT). Each transaction is validated through consensus mechanisms and stored across a distributed network of nodes, often spanning multiple jurisdictions simultaneously. There is no single point of control, no fixed location, and frequently no identifiable legal entity operating the infrastructure.

The removal of intermediaries has two significant legal implications. First, it blurs the line between private actors and infrastructure providers, as any user participating in the network may contribute to data validation and governance. Second, it detaches digital financial systems from state-backed enforcement mechanisms. This decentralised structure means that disputes, regulatory enforcement, and jurisdictional control cannot be mapped onto a single geographic or sovereign framework. Consequently, the traditional nexus between physical presence and legal oversight becomes difficult to establish.

A pivotal feature of blockchain systems is the use of smart contracts—self-executing pieces of code that automatically perform contractual terms when predefined conditions are met. These contracts are embedded directly into the blockchain and operate without the need for judicial oversight or traditional enforcement mechanisms.

From a legal standpoint, smart contracts challenge the conventional understanding of offer, acceptance, and intention to create legal relations. They operate deterministically, leaving little room for judicial discretion or equitable intervention. Furthermore, their immutable nature can lead to outcomes that, while technically valid, may violate legal norms such as unconscionability, good faith, or capacity[1].

[1] *Georgios Dimitropoulos*, 'The Law of Blockchain' (2020) 95 *Washington Law Review* 1117 https://digitalcommons.law.uw.edu/wlr/vol95/iss3/3 accessed 20 March 2025.

 ISSN: 2582-6433

Smart contracts complicate jurisdictional determinations because their execution is not tied to a physical location or to parties who are necessarily domiciled in a recognizable jurisdiction. The code may have been written in one country, executed on a node located in another, and may affect parties situated in several others. This raises profound questions about which legal system governs the contract, where a breach occurs, and how remedies may be pursued.

Decentralised Autonomous Organizations (DAOs)

DAOs are organizational structures encoded entirely through smart contracts and governed by token-holders rather than directors or managers. They do not possess a centralized management hierarchy or a registered seat of incorporation. This allows them to raise funds, manage investments, and execute collective decisions without establishing a legal entity under any specific national law.

DAOs are often governed by voting mechanisms, with token holders determining operational decisions. However, this structure introduces regulatory uncertainty. Since DAOs lack incorporation, they do not enjoy legal personhood in most jurisdictions, and questions arise as to who may be held liable in the event of fraud, misrepresentation, or breach of contract. Investors may face significant challenges in seeking redress against DAOs due to the absence of a legal representative, registered office, or clear national affiliation[2].

This lack of legal identity renders enforcement of rights and obligations extremely difficult. Moreover, since DAOs can interact directly with smart contracts and control significant financial assets without regulatory licensing, they may operate beyond the reach of traditional investor protection mechanisms. This is particularly problematic in cross-border contexts where parties may reside in jurisdictions with differing regulatory standards.

Transnational Operation and Legal Dislocation

One of the most disruptive features of blockchain is its inherent disregard for national borders. The operation of decentralised networks is indifferent to geographic location. Transactions may be initiated in one jurisdiction, validated in others, and stored across dozens more. This lack of territorial anchoring undermines the efficacy of laws that rely on physical presence or incorporation to establish jurisdiction.

[2] **De Filippi P and Wright A,** *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) https://ebookcentral.proquest.com/lib/uconn/detail.action?docID=5340266 accessed 20 March 2025.

 ISSN: 2582-6433

In a traditional legal framework, jurisdiction is typically asserted based on criteria such as domicile, place of business, or the location where the harmful act occurred. Blockchain transactions do not fit neatly into any of these categories. They occur "on-chain", often via pseudonymous addresses, and involve smart contracts that may execute without any human intervention at all.

This makes it extremely difficult to determine the appropriate forum for legal disputes, let alone identify the governing law. For instance, if a smart contract fails or a DAO engages in deceptive practices, the question of which court holds jurisdiction or which national laws apply becomes virtually unresolvable under traditional doctrines.

Legal and Regulatory Implications

The borderless nature of blockchain raises significant implications for both regulators and private legal actors. Jurisdictional uncertainty undermines regulatory oversight, exposes investors to risks, and creates opportunities for bad actors to engage in regulatory arbitrage. Moreover, national laws that attempt to exert control over blockchain-based activity may prove ineffective if enforcement depends on establishing links with an identifiable party or location.

In response, some jurisdictions have proposed frameworks to domesticate blockchain activity by requiring registration, licensure, or legal identification of DAO structures. Others have introduced statutes that attempt to bridge the legal gap between code-based systems and human-readable contracts. Still, these approaches are limited in scope and largely untested in cross-border contexts[3].

In the absence of international consensus or harmonisation, conflicting national rules may lead to fragmented regulation and inconsistent enforcement. For blockchain-based investments, this legal uncertainty threatens both market stability and investor confidence.

Jurisdictional Challenges in Blockchain Transactions

Blockchain transactions, by design, operate beyond the constraints of national borders, creating serious complications for traditional legal systems premised on territoriality and identifiable parties. Determining the applicable law, competent forum, and regulatory authority becomes a complex exercise when the parties are pseudonymous, the transaction is automated through

[3] *Nova University Lisbon*, 'The Role of International Arbitration in Smart Contract Disputes' (2023) https://run.unl.pt/bitstream/10362/159462/1/BorbaOliveira_2023.pdf accessed 22 March 2025.

 ISSN: 2582-6433

smart contracts, and the infrastructure is globally distributed. This section examines the key jurisdictional dilemmas associated with blockchain activity, especially within cross-border investment contexts.

The Problem of Legal Attribution

A central issue in cross-border blockchain transactions is identifying the applicable legal framework governing the rights and obligations of the parties involved. In conventional legal settings, jurisdiction is established through physical connections—such as the place of incorporation, location of the parties, or situs of the transaction. Blockchain transactions defy these markers. The absence of fixed geographic reference points complicates the application of traditional private international law doctrines such as lex loci contractus (law of the place of contract formation) and lex loci solutionis (law of the place of performance).

When a smart contract is deployed on a global blockchain network, its creation and execution occur simultaneously across multiple jurisdictions. As such, no single national legal system can be definitively tied to the transaction. Moreover, parties often transact using pseudonymous blockchain addresses, making it difficult to establish identity, residence, or intent—factors that are typically foundational for contractual enforcement.

Regulatory Asymmetries and Conflicts

Blockchain networks and crypto-asset markets are regulated differently across jurisdictions, creating a fragmented legal landscape. Some countries have embraced digital assets with comprehensive regulatory frameworks, while others have imposed strict prohibitions or remained silent on the matter. These discrepancies foster regulatory arbitrage, where actors exploit cross-border gaps by relocating their operations to jurisdictions with lax oversight.

For instance, a blockchain-based investment fund may operate from a jurisdiction with minimal regulation while attracting investors globally, including from countries with stricter requirements for securities offerings or investor protection. In such cases, determining which country's law governs the relationship becomes highly contested. Without harmonised standards or a universally accepted classification of crypto-assets, it is difficult to define the legal nature of such investments or to adjudicate disputes arising from them.

Regulatory inconsistencies also extend to areas such as anti-money laundering (AML), data protection, consumer rights, and taxation. A smart contract executed on a blockchain may

 ISSN: 2582-6433

trigger different legal obligations depending on the jurisdictions involved—many of which may not even be aware that a relevant transaction has occurred within their borders.

Challenges in Identifying Legal Jurisdiction

In private international law, jurisdiction is typically asserted based on a demonstrable connection between the legal issue and the forum state. However, blockchain transactions often lack such connections. Since the ledger is distributed and participants may interact from any location, courts face difficulty establishing a basis for adjudicating disputes.

Moreover, standard conflict-of-law rules assume the ability to identify and locate the parties, determine the nature of the contract, and interpret the governing law. With blockchain transactions, these assumptions break down. The anonymity of users, the automation of contractual execution, and the absence of negotiated terms all obscure the legal foundations upon which jurisdiction is usually built.

Even when parties specify a governing law and jurisdiction clause within a smart contract, enforcing such provisions is not always straightforward. The question arises whether an automated interaction with a smart contract constitutes consent to those terms, especially when they are embedded in code rather than explicitly communicated to users in a legal document. This raises issues of transparency, informed consent, and contractual validity—particularly in cross-border settings where different legal systems may interpret these elements differently.

Enforcement Barriers and Legal Fragmentation

Once a dispute arises, enforcing legal rights across borders remains a formidable obstacle. Even if a court asserts jurisdiction and renders a decision, enforcement may be practically impossible if the assets are held in decentralised wallets or controlled by smart contracts with no off-chain linkage. Unlike bank accounts or corporate assets, blockchain-based holdings are not always subject to seizure or judicial control[4].

Furthermore, differences in national enforcement mechanisms may hinder cooperation. A judgment rendered in one country may not be recognized in another, especially if the latter deems the legal process or contractual form incompatible with its own standards. This is particularly relevant when the contract involves decentralised systems that lack a clear legal

[4] *ElgarOnline*, 'Digital Assets and Smart Contracts: Legal Perspectives' in *Handbook of Digital Law* (2024) https://www.elgaronline.com/edcollchap/book/9781035331802/chapter3.xml accessed 21 March 2025.

 ISSN: 2582-6433

status, such as Decentralised Autonomous Organizations (DAOs) or DeFi protocols.

These enforcement challenges contribute to legal fragmentation. Parties engaging in cross-border blockchain transactions face high degrees of legal uncertainty, which in turn deters institutional investment and undermines consumer protection. The absence of a predictable, enforceable legal regime risks fostering a regulatory void that incentivises opportunism and erodes trust in decentralised systems.

To address these challenges, legal systems must adapt by developing rules that better reflect the realities of blockchain-based transactions. Some jurisdictions have taken initial steps by introducing legislation that defines the legal status of digital assets and clarifies applicable law in certain contexts. However, a piecemeal national approach is unlikely to resolve the broader problem of jurisdictional incoherence.

Instead, there is growing recognition of the need for harmonised international principles, particularly through model laws or multilateral instruments. Proposed solutions include defining the "location" of a digital asset by reference to the network protocol, designating a default governing law for smart contracts, or applying jurisdictional rules based on user identity verification protocols. These initiatives seek to reorient conflict-of-law rules to account for the distributed, digital nature of blockchain systems.

The Role of Public and Private International Law

The borderless and decentralised nature of blockchain technology has compelled a reassessment of the traditional functions and scope of both public and private international law. While public international law typically governs state-to-state relations and investment protections through treaties and conventions, private international law deals with conflict-of-law rules applicable to private parties operating across borders. As blockchain-enabled activities increasingly involve cross-border financial flows, decentralised business arrangements, and autonomous entities like DAOs, both frameworks are being challenged and tested in unprecedented ways.

Public International Law

Public international law, particularly in the context of bilateral investment treaties (BITs) and multilateral agreements, has long provided the legal basis for cross-border investor protection. Central to these instruments are principles of non-discrimination, fair and equitable treatment,

 ISSN: 2582-6433

and guarantees against unlawful expropriation. However, their application to blockchain-based investments remain unclear, primarily due to definitional gaps and jurisdictional ambiguities.

One of the most contentious issues is whether blockchain-based assets—such as cryptocurrencies, tokenised shares, or digital real estate—constitute "investments" within the meaning of BITs and the ICSID Convention. These agreements were drafted in an era of physical capital and traditional corporate structures. Blockchain disrupts this by enabling investments to be made through digital wallets, smart contracts, and decentralised autonomous entities, often without any physical presence or incorporation in the host state.

The problem is exacerbated when DAOs or other decentralised collectives operate without incorporation or recognition under any state law. If such an entity were to invest in a host country and later face regulatory intervention or asset freezing, it would be unclear whether the protections of a treaty could be invoked, who the investor is, and whether a claim can even be brought under investor-state dispute settlement mechanisms.

Public international law traditionally relies on state consent for arbitration under mechanisms like ICSID or UNCITRAL. In blockchain transactions, identifying the contracting parties, much less establishing a clear expression of state consent to arbitrate disputes involving pseudonymous or unincorporated actors, poses serious legal obstacles. These uncertainties indicate a pressing need to update treaty definitions and mechanisms to reflect the growing role of digital assets in international investment.

Private International Law

Private international law provides the tools for resolving disputes between private parties across jurisdictions. It includes principles governing choice of law, jurisdiction, and the recognition and enforcement of foreign judgments or arbitral awards. These principles are traditionally based on physical location, legal personality, and intention as reflected in written contracts. Blockchain transactions, which are often autonomous, borderless, and pseudonymous, disrupt each of these foundational assumptions.

A key question in blockchain-related disputes is determining which law governs the legal relationships formed via smart contracts. Conventional principles like lex loci contractus or lex loci solutionis require identifying a place of contract formation or performance—criteria that are largely inapplicable in decentralised environments. Similarly, the doctrine of lex situs

 ISSN: 2582-6433

(location of an asset) becomes incoherent when dealing with assets that exist solely on distributed ledgers and have no geographical location.

The legal fragmentation is further illustrated by the varying national approaches to classifying and regulating digital assets. Some jurisdictions have adopted legislation recognizing crypto-assets as property or securities, while others remain silent or explicitly prohibit them. As a result, the same transaction may be treated as legal, illegal, or unregulated depending on the forum, leading to unpredictability and potential injustice[5].

In response, some international organizations and legal scholars have proposed harmonising private international law rules for digital assets. Proposals include default rules based on the location of the relevant blockchain node, the law chosen in the underlying protocol, or even the habitual residence of the parties interacting with the smart contract. While these suggestions are still developing, they reflect the recognition that new forms of digital legal interaction require new conflict-of-laws principles.

Intersection Between Public and Private Law

The intersection of public and private international law is particularly important in the context of blockchain-based investment disputes. For instance, a dispute between an investor and a host state involving a blockchain-based asset may involve both treaty-based claims (under public international law) and contract-based claims (under private international law). Yet the fragmented nature of applicable legal regimes may prevent coherent resolution, especially where there is no agreed-upon forum or applicable law.

One area of convergence is arbitration. Both public and private international law rely heavily on arbitration as a dispute resolution mechanism. Yet, blockchain introduces procedural complexities—particularly when disputes arise from smart contracts that lack formal arbitration clauses or are governed by non-negotiable code. Courts and arbitral tribunals must grapple with how to interpret intent, consent, and fairness when these are not expressed in human-readable language[6].

Another area of overlap is enforcement. Even if a tribunal renders an award under a BIT or

[5] *University of Hong Kong – Law Faculty*, 'Comparing Private International Law Approaches to Blockchain Regulation' (2024) https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/blawintnl24&section=16 accessed 23 March 2025.

[6] *Brill Open Access*, 'Blockchain and Private International Law' (2023) https://library.oapen.org/bitstream/handle/20.500.12657/87971/1/9789004514850.pdf accessed 21 March 2025.

 ISSN: 2582-6433

commercial arbitration, enforcement in blockchain cases may be complicated by asset anonymity, jurisdictional gaps, or lack of recognition of the legal status of the parties involved. Without enforceable cross-border standards for blockchain-related rights, both public and private mechanisms may fall short.

Efforts are underway to bridge these gaps. Some international law bodies are exploring the development of model laws or soft law instruments addressing the unique features of blockchain and digital assets. These efforts aim to standardise the classification of digital assets, clarify jurisdictional rules, and offer guidance on choice-of-law principles. Others suggest that a new convention—similar to the New York Convention on arbitration or the Hague Convention on Choice of Court Agreements—may be needed specifically for blockchain-based interactions.

The evolving nature of blockchain demands flexible legal tools that can operate effectively in decentralised environments. Harmonising public and private international law principles, especially through model clauses, jurisdictional presumptions, and consensus on asset classification, will be critical in ensuring legal certainty and enforceability in blockchain transactions.

Chapter 3: Smart Contracts and Legal Enforceability

Smart contracts are self-executing computer programs embedded on blockchain networks, designed to automate, enforce, and verify the performance of contractual terms without the need for intermediaries. First conceptualized by Nick Szabo in 1996, these digital protocols execute contractual obligations through “if-this-then-that” logic and can significantly reduce transactional costs and time delays.

The Italian legal system was among the first to codify smart contracts, defining them in 2019 as "computer programs that operate on distributed registers-based technologies and whose execution automatically binds two or more parties according to effects predefined by said parties". These contracts differ from traditional ones in that they rely on software code to

 ISSN: 2582-6433

define, execute, and enforce agreements autonomously.

Evolution of Smart Contracts and the Rise of Blockchain Integration

While early digital contracts could be considered rudimentary precursors to smart contracts, it was the introduction of blockchain technology that provided the necessary infrastructure for secure, immutable, and decentralized contract execution. Initially, smart contracts remained a theoretical concept due to the lack of a trustworthy computational substrate. Blockchain, especially with the advent of Ethereum in 2015, provided that substrate by offering decentralized consensus, transparency, and tamper-proof data storage.

Ethereum introduced Solidity, a dedicated programming language for writing smart contracts, enabling a programmable layer on top of blockchain infrastructure. Other platforms followed suit, such as Vyper, Rust for Solana, and Chaincode for Hyperledger, each contributing to the versatility of smart contract architecture[7].

Smart contracts evolved from simple transactional automations (e.g., automated payments) to complex decentralized applications (dApps) supporting functions like decentralized finance (DeFi), governance voting, supply chain tracking, and cross-border investment processing.

Technical Architecture and Functionality

A smart contract is executed on a distributed ledger (i.e., blockchain) and performs the following core functions:

1. **Self-Execution:** The contract is deployed on a blockchain and automatically executes outcomes based on predefined triggers without human intervention.

2. **Distributed Ledger:** All transactions and conditions are stored immutably across nodes, ensuring transparency and resistance to tampering.

3. **Digital Identity:** Smart contracts often integrate with digital ID systems to verify the parties involved.

4. **Event-Driven Programming:** Contracts respond to blockchain events or off-chain data feeds (via oracles) to initiate or halt execution.

[7] Nakul Garg and Rahul Rao, *A Case for Integrating Blockchain-based Smart Contracts in Cross-Border Investments* (Crowd Investments Ltd 2023) https://ssrn.com/abstract=4561807 accessed 16 March 2025.

 ISSN: 2582-6433

5. **Consensus Mechanism:** Smart contracts function within blockchain protocols like Proof of Work (PoW) or Proof of Stake (PoS), ensuring trustless validation.

These features enable seamless, secure, and deterministic execution of complex transactions in real-time, often across borders.

Smart Contracts vs Traditional Investment Contracts

A core distinction between smart contracts and traditional investment contracts lies in their form, execution mechanism, and legal framework.

Feature	**Traditional Investment Contract**	**Smart Contract**
Form	Natural language, often paper-based or electronic PDF documents	Code-based protocols deployed on blockchain
Execution	Requires manual or institutional enforcement (e.g., courts, regulators)	Automated and self-enforcing through pre-defined conditions
Enforcement Mechanism	Subject to national laws, litigation, or arbitration	Executed through blockchain protocol logic; legal enforceability still evolving
Intermediaries	Lawyers, banks, custodians, notaries	Typically no intermediaries; replaces trust with cryptographic guarantees
Dispute Resolution	Litigation, arbitration, mediation	Still uncertain; smart contract-based dispute mechanisms emerging
Complexity Accommodation	Handles nuance, ambiguity, and subjective clauses (e.g., best efforts)	Limited to binary logic; challenges in interpreting abstract terms

In cross-border investment contexts, the automation provided by smart contracts can be

 ISSN: 2582-6433

especially beneficial. They reduce transaction costs, improve transparency, and limit the need for third-party validation or enforcement. According to Garg and Rao, smart contracts eliminate time-consuming bureaucratic barriers in transnational private equity investment and startup financing.

However, their rigidity presents a challenge for complex investments where flexibility, interpretation, and negotiation are key. As observed, smart contracts work well for clearly defined, discrete transactions but fall short when parties must rely on equitable doctrines or negotiate in good faith during performance[8].

Use in Cross-Border Transactions

Cross-border investment contracts frequently face issues like legal ambiguity, high transactional costs, and regulatory inconsistency. Smart contracts offer compelling solutions by automating verification, execution, and fund disbursement in line with agreed-upon triggers. For example, escrow functions, dividend distributions, and milestone-based payments in venture financing can be coded and executed through smart contracts.

Furthermore, the integration of smart contracts with oracles allows them to reference real-world events—such as project completion, receipt confirmations, or market price movements—enhancing their relevance in cross-border contexts.

Yet, enforcement issues remain. Disputes over coding errors or unexpected outcomes can't always be resolved within the blockchain ecosystem, necessitating hybrid contracts that combine legal language with coded components.

Hybrid and Smart Legal Contracts

Legal scholars increasingly emphasize the utility of "smart legal contracts" – contracts that embed smart contract elements but retain a traditional legal framework to address potential disputes[9]. These hybrid contracts allow for a more flexible integration into existing legal systems and are better suited for use in cross-border investments where enforceability is a critical concern.

[8] Scott A McKinney, Rachel Landy and Rachel Wilka, 'Smart Contracts, Blockchain, and the Next Frontier of Transactional Law' (2018) 13(3) *Washington J L Tech & Arts* 313 https://digitalcommons.law.uw.edu/wjlta/vol13/iss3/5 accessed 17 March 2025.
[9] Raghav Pathak, *Interoperability, Legal Interpretation and Application of Smart Contracts, DLT & Blockchain in India* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=496494* accessed 17 March 2025

 ISSN: 2582-6433

For instance, investment agreements could include a smart contract layer that automates payments, while reserving dispute resolution, governing law, and interpretation clauses to traditional documents. This model helps preserve the advantages of automation while retaining the adaptability of human legal interpretation.

Legal Challenges in Smart Contract Enforcement

Are Smart Contracts Legally Binding? Enforceability in International Arbitration and Litigation

Smart contracts have redefined how parties transact, particularly in cross-border investment scenarios. These self-executing agreements eliminate traditional intermediaries and rely on pre-set code to execute performance. However, the legal enforceability of smart contracts remains ambiguous, especially when disputes arise. This chapter addresses whether smart contracts can be legally binding, the extent of their enforceability in courts and international arbitration, and the challenges presented by jurisdictional fragmentation, code-based ambiguity, and public policy exceptions.

Are Smart Contracts Legally Binding?

To determine whether smart contracts are legally enforceable, traditional contract elements—offer, acceptance, intention to create legal relations, and consideration—must be analyzed in the context of automated code-based systems[10].

Most jurisdictions have indicated that smart contracts can satisfy these requirements. English law, for instance, has affirmed that smart contracts, even those expressed wholly in code, can be legally binding if they fulfill standard contractual requirements. Similarly, the Iraqi and UAE civil codes recognize contracts formed via electronic means, validating smart contracts when the essential elements of consent, legality, and offer/acceptance are present.

However, problems arise when these contracts are entirely in code, making it difficult for non-programmers to comprehend their content. This creates issues around *consensus ad idem* (meeting of minds). As noted in the literature, consent in smart contracts is presumed when a party interacts with the contract's logic—such as triggering payment via an interface—but

[10] **Vikas Kathuria and Basheerhussain Miniya**, 'From smart legal contracts to contracts on blockchain: An empirical investigation' (2024) *Computer Law & Security Review* 55, 106035 https://doi-org.egateway.chennai.vit.ac.in/10.1016/j.clsr.2024.106035 accessed 17 March 2025.

 ISSN: 2582-6433

courts may question whether such actions equate to informed, voluntary consent.

Smart contracts are also immutable, which raises questions about how traditional contract doctrines like mistake, misrepresentation, or duress apply. Once executed, reversal is technically impossible without additional code-based contingencies or off-chain adjudication—a sharp departure from conventional contract law that permits rescission or renegotiation.

Jurisdictional and Legal Framework Challenges

Smart contracts complicate the application of private international law. When parties are pseudonymous and transactions occur across distributed ledgers rather than nation-states, determining applicable law and competent jurisdiction becomes highly problematic.

There is no consensus on whether lex loci contractus (the place where the contract was formed), lex loci solutionis (place of performance), or the location of a server validating the contract should determine jurisdiction. As smart contracts are often cross-jurisdictional, this ambiguity undermines predictability and investor confidence.

In Quoine v. B2C2, the Singapore Court of Appeal enforced a smart contract formed by algorithmic agents, affirming its binding nature. Yet, this ruling remains jurisdiction-specific and cannot be generalized globally. Several nations such as India, UAE, and some U.S. states like Arizona and Nevada have enacted legal provisions to recognize smart contracts, but these frameworks remain fragmented and primarily domestic.

Litigation: Procedural and Substantive Barriers

When smart contracts give rise to disputes, litigation faces unique challenges:

1. **Proof and Interpretation**: If the contract is entirely in code, courts must interpret machine logic—a task for which most judges are not equipped. Scholars propose using a “reasonable programmer” standard to interpret coded terms, but this approach remains underdeveloped in case law.

2. **Public Policy Exceptions**: Even where a smart contract is validly executed, enforcement may be denied on public policy grounds. For example, if the contract automates an anti-competitive agreement, states may invalidate awards based on public interest considerations.

 ISSN: 2582-6433

3. **Irreversibility and Restitution**: Courts traditionally offer restitution in cases of unjust enrichment or mistake. Smart contracts challenge this principle due to their irrevocability. For example, if a software bug leads to premature disbursement, rectification becomes technically difficult unless specific reversal mechanisms are pre-programmed.

International Arbitration: A More Flexible Alternative

Arbitration presents a more suitable mechanism for resolving smart contract disputes, especially in the context of cross-border investment[11]:

- **Flexibility**: Arbitration allows parties to choose procedural rules, arbitrators with technical expertise, and tailored timelines.
- **Anonymity**: Parties to smart contracts often operate under pseudonyms; arbitration protects their identity better than court proceedings.
- **Recognition of Awards**: Arbitral awards are enforceable in over 170 countries under the New York Convention, making them more globally viable than court judgments.

That said, arbitration involving smart contracts still faces barriers:

- **Form Requirements**: The New York Convention requires arbitration agreements to be in writing. Code-only smart contracts may not meet this requirement unless accompanied by a Ricardian or hybrid contract that includes a textual counterpart.
- **Jurisdictional Uncertainty**: The arbitral seat determines the procedural law and extent of judicial oversight. Choosing a seat favorable to digital assets is critical but remains underappreciated by contracting parties.
- **Interim Measures**: Smart contracts cannot be paused easily. Even if a tribunal orders interim relief, the automated code may execute obligations before relief is granted.

Hybrid and Blockchain-Based Arbitration Models

In response to these challenges, hybrid models are emerging. Some platforms like Mattereum

[11] MADSJS Niriella, 'Role of Smart Contract in Arbitration: A Critical Analysis' (2024) 1(2) *International Journal of Juridical Studies and Research Sciences* https://doi.org/10.5281/zenodo.14243009 accessed 19 March 2025.

 ISSN: 2582-6433

and Kleros propose blockchain arbitration, where arbitral rulings serve as oracles that smart contracts consult before proceeding. These rulings are then enforced "on-chain" using programmable logic.

However, these decentralized arbitration systems are still in their infancy and face questions about legitimacy, due process, and recognition under existing international frameworks. They are currently more suitable for low-value, low-complexity disputes.

Recommendations and Future Directions

To improve the enforceability of smart contracts, especially in international investment scenarios, several recommendations merit serious consideration. First, contracting parties should adopt Ricardian contracts—hybrid agreements that integrate machine-readable code with human-readable legal text. These ensure that smart contracts meet both technical execution requirements and formal legal standards, including writing and consent. Second, contracts should explicitly specify the governing law, dispute resolution mechanism, and jurisdiction. These clauses are critical in reducing uncertainty and enabling enforcement, particularly in a cross-border context where conflicting legal regimes may apply[12].

Third, international organizations such as UNCITRAL and ICSID should take the lead in developing model laws, guidelines, or treaties that specifically address smart contract disputes. Such frameworks could provide uniformity and predictability, filling the current vacuum of transnational legal governance in this area. Fourth, judicial and arbitral training programs should incorporate technical modules on blockchain and smart contracts. Additionally, legal systems could formally recognize the role of expert witnesses or technical consultants to assist in interpreting code and understanding decentralized networks. Finally, states should support regulatory sandboxes and pilot programs to experiment with blockchain dispute resolution mechanisms. These environments can help build precedents, test governance models, and cultivate public trust in the system. By combining technological innovation with legal safeguards, smart contracts can evolve from a disruptive innovation to a stable and enforceable instrument in international investment law.

[12] Ahmed Abdulkhudhur Jasim, Ghassan Adhab Atiyah and Ahmed Ismael Ibrahim, 'Enforcement of Smart Contracts in Cross-Jurisdictional Transactions' (2024) *International Journal of Law and Management* https://www.researchgate.net/publication/387176520_Enforcement_of_smart_contracts_in_cross-jurisdictional_transactions accessed 18 March 2025.

 ISSN: 2582-6433

Chapter 4: Conflict of Jurisdictions in Investment Disputes

The Collapse of Traditional Jurisdiction in Decentralised Investments

The emergence of blockchain technology has fundamentally challenged traditional legal principles related to jurisdiction, particularly in the context of cross-border investments. Traditionally, legal systems have relied on clear indicators such as the physical location of parties, incorporation status, and the situs of assets to determine applicable jurisdiction. Blockchain-based investment, however, is characterised by decentralisation, pseudonymity, and the absence of a central authority. These features blur territorial boundaries and introduce unprecedented uncertainty in determining the competent forum for dispute resolution.

Blockchain transactions operate across distributed networks without geographic anchorage. Smart contracts are executed automatically by code, and parties often interact via cryptographic keys rather than legal names or corporate entities. As a result, the location of transaction execution, a foundational element in asserting jurisdiction under private international law, becomes practically irrelevant or untraceable. This undermines core doctrines like lex loci contractus and lex loci solutionis. Without clarity on where the contract was formed or where its obligations are performed, applying traditional rules of jurisdiction becomes infeasible.

Additionally, the identity of investors and platforms involved in blockchain-based investments is often concealed or unverifiable due to the use of pseudonyms and anonymizing technologies. In such cases, the basic prerequisite of identifying a legal person or entity subject to a court's

 ISSN: 2582-6433

or arbitral tribunal's jurisdiction cannot be fulfilled. This frustrates not only national courts but also international arbitration forums that require minimum standards of party identification and consent[13].

At the same time, state sovereignty remains the central organizing principle of traditional legal systems. State courts derive their authority from the ability to regulate conduct within their territory, but blockchain-based activity, by design, circumvents state control. Transactions are recorded on distributed ledgers, maintained by globally dispersed nodes, and validated by consensus protocols rather than legal authorities. Consequently, states struggle to enforce their jurisdictional claims over blockchain investments, leading to fragmented and overlapping assertions of legal authority. Some states respond with aggressive regulation or outright bans, while others adopt liberal or sandbox regimes to attract innovation—intensifying global jurisdictional inconsistency.

State Sovereignty and the Rise of Regulatory Arbitrage

This lack of harmonisation creates fertile ground for jurisdictional arbitrage, where entities strategically locate operations or route transactions through jurisdictions with favourable regulatory environments. This enables actors to exploit gaps between legal systems and escape liability in less permissive jurisdictions. In cross-border investment disputes, such arbitrage introduces complexity, as multiple states may claim competence, or none may assert clear authority. This generates legal uncertainty and increases the risk for investors, particularly when protections under bilateral investment treaties or customary international law cannot be effectively invoked due to the absence of a recognized investor or identifiable host state conduct.

Furthermore, when blockchain investment disputes arise, litigating such disputes through national courts becomes highly problematic. Courts often lack the technical expertise to interpret code-based transactions or to reverse outcomes triggered by smart contracts. More critically, national enforcement mechanisms are ineffective against decentralized protocols that operate without a central point of control. Even if a judgment is obtained, enforcing it may be impossible if the assets in question are digital and controlled by immutable code.

[13] **Kremer, Maria and Orsini, Giacomo**, 'Investor–State Dispute Settlement in the Era of Crypto Assets: Sovereign Regulatory Space versus Blockchain Borderlessness' (2024) *ICSID Review - Foreign Investment Law Journal* (Advance article) https://academic.oup.com/icsidreview/advance-article-abstract/doi/10.1093/icsidreview/siae040/8043136 accessed 18 March 2025

 ISSN: 2582-6433

In this environment, traditional concepts of jurisdiction are not just inadequate—they may be irrelevant. The territorial logic of international law, built on the assumption of sovereign boundaries and physical presence, cannot accommodate the stateless nature of blockchain ecosystems[14]. The application of legal personality, corporate domicile, and habitual residence does not translate meaningfully to DAOs or peer-to-peer protocols. This disconnect between legal form and technological function generates a fundamental gap in cross-border investment regulation.

Additionally, certain blockchain-related investment activities—such as Initial Coin Offerings, tokenized equity sales, and decentralised lending platforms—may not meet the criteria for "investment" under many bilateral investment treaties or the ICSID Convention. The lack of formal incorporation, physical assets, or substantive business activity can make it difficult for claimants to establish that their digital activities fall within the ambit of protected investments. This denies them access to dispute resolution mechanisms designed to shield foreign investments from arbitrary state actions or unfair treatment[15].

Compounding the problem, states may also find it challenging to assert jurisdiction over DAO-operated investment vehicles or anonymous smart contract developers when damage arises. Unlike conventional enterprises, blockchain-based actors often operate outside formal legal structures, making it difficult for states to identify responsible entities or impose liability. As a result, legal gaps persist on both ends: investors may lack remedies, and states may lack the power to regulate.

Private International Law in Conflict with Blockchain Logic

Private international law has traditionally provided the tools to resolve jurisdictional questions in cross-border disputes. These tools depend heavily on clear notions of party identity, territorial connection, and mutually recognized legal norms. In blockchain-based investment arrangements, however, such clarity is often absent. Smart contracts—self-executing pieces of code—operate independently of legal jurisdictions, and the parties interacting with them may not even know each other's national identities or legal status. This complicates the application

[14]**Chiu, Iris HY**, 'Jurisdictional Arbitrage: Combatting an Inevitable By-product of Cryptoasset Regulation' (2022) *Journal of Financial Regulation and Compliance* https://www.emerald.com/insight/content/doi/10.1108/jfrc-02-2022-0013/full/pdf accessed 17 March 2025.
[15]**Shehata, Ibrahim**, 'Smart Contracts & International Arbitration' (2018) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290026 accessed 17 March 2025.

 ISSN: 2582-6433

of conventional rules that determine which law governs the contract and which court or tribunal has the authority to resolve disputes.

When parties do not specify governing law or forum selection in their agreements, courts must apply default rules of private international law. These typically hinge on factors such as the place where the contract was formed or where it was to be performed. In blockchain-based contracts, the "place" of performance may be distributed across multiple jurisdictions or not exist in any legal sense. Transactions may execute automatically across nodes located worldwide, without any single point of origin or control. Consequently, identifying the applicable law becomes speculative and inconsistent, undermining the predictability and reliability that investors depend upon.

Jurisdictional problems are compounded when blockchain-based transactions involve smart contracts with no express legal language. While some platforms allow for hybrid documentation—such as Ricardian contracts, which combine code and legal text—many do not. As a result, courts may be unable to determine whether a binding agreement exists at all, or what its terms are. In the absence of conventional offer, acceptance, and consideration expressed in natural language, establishing the existence of a contract becomes a legal challenge. Even if such a contract is recognized, the court must still determine which legal system governs its interpretation and enforcement.

The lack of uniform standards for recognising smart contracts and associated investments leads to forum shopping, where parties seek to exploit legal systems that are more favourable or permissive. In certain jurisdictions, digital assets and smart contracts are formally recognised, whereas in others they are not enforceable or are even banned. This fragmentation leads to inconsistent outcomes and may discourage legitimate investment, particularly in high-risk or developing markets[16]. Parallel proceedings may also arise, where multiple jurisdictions assert authority over the same dispute. This undermines the finality and efficiency of dispute resolution, creating increased costs and uncertainty.

Complicating matters further is the technological opacity of smart contracts and blockchain platforms. Unlike traditional legal agreements, smart contracts are not written in natural language but in code, which is not readily accessible to judges, arbitrators, or legal

[16] **Walters, Robert**, 'Smart Contracts and International Commercial Arbitration' in *Handbook on Transnational Commercial Law* (Routledge 2025) https://www.taylorfrancis.com/chapters/edit/10.4324/9781003394822-25/smart-contracts-international-commercial-arbitration-robert-walters accessed 18 March 2025

 ISSN: 2582-6433

practitioners. Without specialized technical expertise or access to blockchain records, adjudicators may be unable to determine how a contract functions, what obligations were triggered, or whether a breach occurred. This undermines the ability of legal systems to fairly resolve disputes, especially in cross-border cases where language, legal culture, and access to evidence already present significant challenges.

Arbitration as a Flexible but Limited Alternative

In addition to court litigation, arbitration is often employed in cross-border commercial and investment disputes. Arbitration offers flexibility in procedure, neutrality of forum, and international enforceability through the New York Convention. These advantages make arbitration a preferred method for resolving blockchain-related disputes. However, arbitration too faces limitations when applied to decentralized technologies. Most arbitration laws require that the parties have entered into a written agreement to arbitrate. In smart contract transactions, especially those executed automatically on blockchain networks, it is not always clear that such an agreement exists in a form that meets this requirement.

In many cases, parties do not consciously opt into arbitration, and the inclusion of a dispute resolution clause within a coded contract may be insufficient to prove mutual consent. Moreover, where such clauses do exist, they may not identify a seat of arbitration, the applicable institutional rules, or a governing law. This vagueness can render the clause unenforceable or lead to procedural complications that delay or derail the arbitration process. Additionally, the pseudonymity of blockchain users poses significant challenges in forming arbitration tribunals or serving notices

The Need for Legal-Tech Harmonisation in Jurisdictional Governance

As arbitration adapts to the demands of blockchain-related disputes, new models are emerging that attempt to align with decentralised legal infrastructure. Blockchain-based arbitration platforms aim to automate the dispute resolution process by integrating adjudication mechanisms into smart contracts themselves. These platforms, often operating on the same networks as the transactions they govern, use programmed logic, token-weighted voting, or decentralised juror pools to resolve disputes. This approach seeks to eliminate reliance on centralised legal systems altogether and create self-contained dispute ecosystems. While innovative, these mechanisms raise questions regarding due process, impartiality, and

 ISSN: 2582-6433

enforceability, particularly under existing legal frameworks[17].

Traditional arbitration is based on legal principles that guarantee fairness, the opportunity to be heard, and impartial adjudication. In blockchain-based arbitration, these principles are often replaced by automated processes with limited transparency or review. While these models may be effective in resolving low-value, high-volume disputes—such as minor consumer claims or transactional disagreements—they remain unsuitable for complex, high-stakes investment disputes involving significant legal and factual analysis. Additionally, awards issued by decentralised arbitral platforms may not be recognised under international conventions due to their informal nature or lack of procedural compliance with institutional standards.

Enforceability is a central issue in blockchain-related jurisdictional conflicts. Even where a tribunal or court asserts jurisdiction and renders a decision, enforcing that decision can be highly problematic. Digital assets may be held in self-custodied wallets, inaccessible to any central authority. If a judgment awards damages or requires the return of assets, there may be no mechanism to compel compliance unless enforcement measures have been pre-coded into the contract itself. This technological limitation weakens the deterrent value of legal rulings and undermines the legitimacy of judicial or arbitral processes.

Some blockchain developers have attempted to address enforcement concerns through the use of "programmable compliance." Smart contracts may include embedded legal logic that enforces jurisdictional restrictions or dispute resolution outcomes automatically. For example, a contract could be coded to release funds only upon confirmation of a dispute resolution decision submitted by a recognised oracle or arbitrator. These designs aim to reconcile code-based execution with legal authority, enabling enforceability by design. However, the adoption of such structures remains limited, and their validity under national and international legal frameworks is still evolving.

The broader issue is the absence of harmonised rules for jurisdiction and enforcement in blockchain-based investment. Jurisdictions around the world are responding inconsistently to blockchain innovation. Some adopt crypto-friendly regulatory environments to attract digital businesses and investment, while others enforce strict bans or vague restrictions. This

[17] **Chaisse, Julien and Kirkwood, Jamieson**, 'Smart Courts, Smart Contracts and the Future of Online Dispute Resolution' (2022) *Stanford Journal of Blockchain Law & Policy* https://www.researchgate.net/publication/357794881_Smart_Courts_Smart_Contracts_and_the_Future_of_Online_Dispute_Resolution accessed 17 March 2025

 ISSN: 2582-6433

fragmented landscape creates uncertainty and encourages strategic structuring of business operations to minimise regulatory exposure. Without international consensus, both states and investors face heightened risk in navigating blockchain investment disputes.

Efforts to harmonise legal responses to blockchain remain nascent but necessary. Model law initiatives can help provide baseline standards for recognising smart contracts, defining digital assets, and determining applicable law and forum in disputes. These standards can guide national legislation, international treaty reform, and institutional rulemaking by arbitral bodies. Principles of mutual recognition, cross-border enforceability, and technological neutrality must be central to any harmonisation effort. Moreover, states must coordinate to ensure that blockchain regulation respects the rule of law while preserving innovation.

Technology can also play a complementary role. Through geofencing, smart contracts can limit interactions to parties in pre-approved jurisdictions, mitigating exposure to conflicting legal systems[18]. Integration of identity verification protocols, compliance oracles, and standardised dispute clauses can enhance legal predictability. Parties can pre-define governing law and dispute resolution forums, supported by hybrid contract structures that combine code with legal text. These practical tools offer a bridge between the decentralised nature of blockchain and the centralised requirements of legal adjudication.

Finally, reconciling public and private international law is essential for resolving jurisdictional tensions in blockchain investment. While public international law focuses on state responsibility, investor protection, and treaty obligations, private international law addresses contractual relationships and forum selection. In blockchain contexts, these spheres frequently overlap. An investor harmed by a decentralised protocol may seek remedy against a state for regulatory failure, while also pursuing private claims against developers or platform operators. Harmonising standards between these domains can reduce legal uncertainty and clarify avenues for redress.

[18] **Vadi, Valentina**, 'Investments in the Digital Era: Blockchain, Crypto-Assets and International Investment Law' (2023) 24 *Business Law International* 135 https://heinonline.org/HOL/Page?handle=hein.journals/blawintnl24&id=135 accessed 19 March 2025

 ISSN: 2582-6433

Chapter 5: Data Localization and Blockchain

Data sovereignty has become a significant legal and economic issue as the world increasingly relies on digital technologies. Data sovereignty refers to the concept that data generated within a country's borders is subject to its laws and regulations. To enforce this principle, governments implement data localization laws, requiring data to be stored, processed, and managed within national boundaries. These laws are often justified as necessary measures to enhance national security, protect citizens' privacy, and promote economic development. However, data localization requirements also create significant challenges, particularly for blockchain technology, which operates on a decentralized and borderless framework. This essay provides an overview of data sovereignty laws in various regions and examines the inherent conflicts between blockchain technology and data localization requirements.

Understanding Data Sovereignty and Localization

Data sovereignty laws are designed to ensure that governments maintain control over data generated within their jurisdiction. Countries use data localization as a tool to achieve this control by mandating that data be stored and processed within their borders[19]. Localization laws can vary in their application, with some imposing full data localization and others allowing cross-border transfers under strict regulatory oversight[20]. These laws are typically justified on the grounds of national security, data privacy, and economic protectionism. However, while data localization laws aim to safeguard citizens' information, they often create

[19] OECD, *Data Free Flow with Trust* (2020) https://www.oecd.org/sti/ieconomy/data-localisation.htm accessed 2 April 2025.
[20] Matthias Bauer and others, *'The Costs of Data Localisation: Friendly Fire on Economic Recovery'* (ECIPE Occasional Paper No. 3/2014) https://ecipe.org/publications/the-costs-of-data-localisation/ accessed 8 March 2025.

 ISSN: 2582-6433

barriers to the seamless flow of data across borders, hindering global business operations and technological innovation.

Data Sovereignty Laws in Key Regions

In the European Union (EU), the General Data Protection Regulation (GDPR) is a landmark regulation that governs data protection and privacy. While the GDPR does not explicitly mandate data localization, it imposes stringent conditions on cross-border data transfers. Data can only be transferred to countries that provide an equivalent level of protection, requiring companies to adopt mechanisms such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). The right to be forgotten, a key provision under the GDPR, also presents challenges for blockchain systems, which rely on immutable ledgers that cannot be altered or deleted.[21]

China has one of the strictest data localization regimes, primarily under its Cybersecurity Law (2017) and Data Security Law (2021). Companies operating in China are required to store critical data within the country and obtain government approval before transferring it abroad. The laws apply particularly to sectors handling personal, financial, and national security-related data. While these regulations enhance China's control over its data ecosystem, they significantly restrict cross-border blockchain operations, forcing companies to create localized blockchain networks that comply with domestic laws.[22]

India has similarly introduced stringent data localization measures. The Digital Personal Data Protection Act (DPDP) mandates the localization of sensitive personal data, especially in sectors such as finance. Additionally, the Reserve Bank of India (RBI) requires financial institutions to store payment data exclusively within India. Although some cross-border data transfers are permitted under specific conditions, companies must ensure that a copy of the data remains stored within the country. These restrictions pose challenges for blockchain companies operating across multiple jurisdictions, as blockchain's decentralized nature makes it difficult to comply with localized data storage requirements.

In Russia, the Federal Law on Personal Data enforces strict data localization mandates. Organizations collecting personal data from Russian citizens must store and process this data

[21] Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet' (2015) 23(2) *International Journal of Law and Information Technology* 129 http://heinonline-org.egateway.chennai.vit.ac.in/HOL/P?h=hein.journals/ijlit18&i=180 accessed 2 April 2025.
[22] Ibid.

 ISSN: 2582-6433

on servers within the country[23]. Non-compliance can result in hefty fines and service suspensions. Russia's strict regulations are a reflection of its broader push for data sovereignty, aiming to reduce reliance on foreign technology companies and ensure state control over sensitive information. This rigid enforcement complicates the implementation of blockchain-based financial services and decentralized platforms within Russia.

The United States, on the other hand, does not have a comprehensive federal data localization law. Instead, the country relies on sector-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA). While the US has traditionally promoted the free flow of data across borders, growing concerns over national security and foreign data access have led to discussions on implementing stricter data sovereignty measures[24]. This fragmented regulatory landscape creates uncertainty for blockchain companies seeking to operate across state and national boundaries.

In Brazil, the General Data Protection Law (LGPD) closely mirrors the GDPR, establishing data protection and privacy regulations. Although the LGPD does not enforce strict data localization, it requires companies to ensure that data transferred abroad receives an adequate level of protection[25]. Similarly, countries in Southeast Asia, including Vietnam and Indonesia, have introduced data localization laws to enhance cybersecurity and protect personal information. Vietnam's Cybersecurity Law mandates the storage of certain data locally, while Indonesia's data protection regulations enforce localization in sectors like financial services.

Motive Behind Data Sovereignty Laws

Governments often justify data sovereignty laws as necessary for ensuring national security. By localizing data, they seek to protect sensitive information from foreign surveillance and cyberattacks. Data localization also enables governments to monitor and regulate digital activities within their borders, enhancing law enforcement capabilities. In regions like China and Russia, where state control over information is prioritized, data localization serves as a tool for political and economic control.

[23] Acronis, *Data Sovereignty Around the World: Data Protection and Residency Laws by Country* (White Paper, 2023) https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cloud-Data-Sovereignty-Around-the-World-EN-US.pdf accessed 9 March 2025.
[24] Ibid.
[25] Ibid.

 ISSN: 2582-6433

Data privacy and consumer protection are also major drivers behind data localization laws. Regulations like the GDPR and LGPD aim to ensure that individuals have greater control over their personal data. By requiring companies to store data within domestic jurisdictions, governments can enforce strict privacy laws and hold businesses accountable for data breaches and misuse[26]. Additionally, data localization laws are often framed as measures to promote economic growth. By compelling companies to establish local data centres and infrastructure, governments create jobs, stimulate investment, and reduce reliance on foreign cloud providers.[27]

However, the effectiveness of data localization in achieving these objectives remains a subject of debate. Critics argue that concentrating data within a single jurisdiction increases the risk of cyberattacks and data breaches. Furthermore, data localization can lead to economic inefficiencies by limiting access to global data markets and increasing operational costs for businesses.

The WTO, OECD, and UNCTAD in the Digital Age

The digital economy's reliance on the seamless flow of data across borders has prompted a growing debate on the adequacy of existing international frameworks. Institutions such as the World Trade Organization (WTO), the Organisation for Economic Co-operation and Development (OECD), and the United Nations Conference on Trade and Development (UNCTAD) have all taken distinct but interconnected steps to address the legal, economic, and jurisdictional implications of cross-border data flows.

The WTO, despite its roots in pre-digital trade governance, has increasingly recognized the centrality of digital trade and data flows. As noted by Meltzer (2019), cross-border data flows underlie virtually all modern trade, from e-commerce to digitally-enabled services. The WTO's 1998 Work Programme on E-commerce, while limited in scope, initiated foundational discussions[28]. However, it wasn't until the Joint Statement Initiative (JSI) on E-commerce (2019) that a formal attempt to modernize rules for digital trade began. Countries engaging in the JSI have advocated for binding rules that ensure free data flows while accommodating exceptions for privacy and national security.

[26] Supra note 2.
[27] Roberto Saia and others, *'A Blockchain-Based Distributed Paradigm to Secure Localization Services'* (2021) 21 *Sensors* 6814 https://doi.org/10.3390/s21206814 accessed 10 March 2025.
[28] Joshua P Meltzer, *'A WTO Reform Agenda: Data Flows and International Regulatory Cooperation'* (Brookings Institution, 2019) https://ssrn.com/abstract=3595188 accessed 8 March 2025.

 ISSN: 2582-6433

Despite these efforts, a lack of consensus persists. According to Mitchell and Mishra (2019), WTO law in its current form is not fully equipped to govern digital trade. While some provisions of the General Agreement on Trade in Services (GATS) apply—particularly those related to market access and non-discrimination—they are outdated for the complex architecture of digital services. The authors advocate for new horizontal disciplines to govern cross-border data flows, including obligations that allow such flows while permitting domestic regulation on legitimate policy grounds such as cybersecurity and data privacy.[29]

The OECD has played a pivotal role in shaping norms for cross-border data governance, often serving as a laboratory for policy coordination. The OECD's Privacy Guidelines and its ongoing efforts to establish frameworks for "Data Free Flow with Trust" (DFFT) underscore its commitment to balancing free flow with privacy and security[30]. The OECD principles advocate that data should move freely as long as adequate protections are in place in recipient jurisdictions. The OECD's 2021 reports emphasize that mutual recognition and interoperability of legal standards are essential for sustainable data governance in trade, particularly for technologies like blockchain, where the location of data is often ambiguous.

The UNCTAD, in contrast, represents the interests of developing countries and focuses on equitable digital development. In its Digital Economy Report 2021, UNCTAD stresses that unregulated cross-border data flows can entrench global asymmetries in digital power. Countries with dominant digital platforms and cloud infrastructure can extract disproportionate value from developing economies, exacerbating digital dependency. UNCTAD supports a more cautious approach, advocating for the right of nations to regulate data flows based on development priorities and sovereign interests. In this way, UNCTAD acknowledges the benefits of data localization as a tool for digital industrialization, while also warning against overly protectionist policies that hinder trade.

These three institutions—WTO, OECD, and UNCTAD—represent different visions of data governance. The WTO seeks legal certainty and trade openness; the OECD fosters interoperability and soft-law norms; while UNCTAD prioritizes equity, development, and

[29] Andrew D Mitchell and Neha Mishra, *'Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute'* (2019) 22(3) *Journal of International Economic Law* https://ssrn.com/abstract=3390038 accessed 8 March 2025.
[30] F Casalini and JL González, *Trade and Cross-Border Data Flows* (OECD Publishing, 2019) https://read.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en.html accessed 9 March 2025.

 ISSN: 2582-6433

national autonomy[31]. However, all agree that new frameworks are necessary to manage the tensions between the borderless nature of digital trade and the territorial sovereignty of national data laws.

Data Localization in Investment Disputes

The intersection between data localization laws and blockchain architecture has emerged as one of the most complex and contentious areas in the governance of digital investment. As blockchain technology matures and sees adoption across various sectors, its decentralized structure increasingly clashes with national legal regimes that prioritize data sovereignty. Blockchain's core design—distributed ledgers that are immutable and globally dispersed—makes compliance with jurisdiction-specific data storage and processing rules extremely difficult. This conflict has begun to surface in the form of investment disputes, litigation, and regulatory pushback, especially where blockchain-based firms or platforms operate across borders.

Data localization mandates require that certain types of data, often personal or financial, be stored within the national territory where they are generated. While such measures are often justified on grounds of national security, privacy protection, and economic policy, their application in blockchain contexts becomes problematic. In the case of blockchain networks, data is shared across a distributed set of nodes, often hosted in multiple jurisdictions, making compliance with data localization nearly impossible without fundamentally restructuring the system. This regulatory friction poses major concerns for both investors and developers, raising legal and operational risks that can deter foreign direct investment in blockchain ventures.

In practice, this tension has already materialized in multiple regulatory contexts. In India, a circular issued by the Reserve Bank mandated that all payment-related data be stored exclusively on local servers. This effectively created a barrier for blockchain-based financial platforms operating cross-border payment systems. These platforms often rely on global networks to process transactions, and the localization rule introduced significant friction, requiring them to either isolate operations or exit the market[32]. Although no formal investment arbitration was triggered, the regulatory imposition prompted domestic litigation and industry

[31] Yik-Chan Chin and Jingwu Zhao, *'Governing Cross-Border Data Flows: International Trade Agreements and Their Limits'* (2022) 11 *Laws* 63 https://doi.org/10.3390/laws11040063 accessed 9 March 2025.
[32] Reserve Bank of India, *'Storage of Payment System Data'* Notification RBI/2017-18/153 (6 April 2018) https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244 accessed 12 March 2025.

 ISSN: 2582-6433

lobbying, highlighting the incompatibility between national data laws and decentralized finance.

China presents another prominent case, where its cybersecurity framework demands strict compliance with domestic data storage requirements. Blockchain companies operating in China must not only store data locally but also grant authorities access when requested. As a result, several blockchain startups and crypto exchanges chose to relocate their operations outside of China. The requirement to localize data within national borders is inherently at odds with the borderless architecture of blockchain[33]. Attempts to create permissioned blockchains for localized use have emerged as a partial solution, but these platforms compromise key features such as openness and decentralization.

In the European Union, the General Data Protection Regulation creates another layer of complexity. One of the regulation's hallmark provisions—the right to erasure—clashes with blockchain's immutable nature. Since data recorded on a blockchain cannot be modified or deleted, businesses using blockchain solutions face significant hurdles in ensuring compliance. This has led some firms to adopt hybrid models, storing personal data off-chain and linking it to on-chain hashed references. While this approach offers partial compliance, it also adds operational complexity and undermines blockchain's seamless design.

The legal issues arising from these conflicts extend into the realm of international trade and investment law. Under the WTO framework, data localization mandates may be challenged if they are found to be unnecessarily restrictive and not justifiable under exceptions such as public morals, privacy, or national security. However, these exceptions must be interpreted narrowly and applied proportionally, meaning that broad or vague localization laws may not withstand scrutiny[34]. The lack of jurisprudence in this area leaves uncertainty about how such conflicts would be resolved, especially in the context of rapidly evolving technologies like blockchain.

Investment treaties and arbitration mechanisms are likely to play an increasing role in these disputes. Investors can argue that localization measures constitute indirect expropriation or a denial of fair and equitable treatment, particularly when such laws are applied retroactively or

[33] S Cao and others, *Enabling Cross-Border Trade in the Face of Regulatory Barriers to Data Flow: The Case of the Blockchain-Based Service Network (BSN)* (2022) https://eprints.qut.edu.au/229873/1/Enabling_cross_border_trade_in_the_face_of_regulatory_barriers_to_data_flow_the_case_of_the_BSN.pdf accessed 9 March 2025.
[34] Supra note 11.

 ISSN: 2582-6433

without sufficient transparency[35]. If a blockchain firm has made infrastructure investments in a country that later imposes strict localization rules, it could claim that its legitimate expectations were violated. The argument becomes stronger when there is evidence of discriminatory treatment or where regulatory changes appear to target foreign digital service providers disproportionately.

Although there have been no landmark arbitration cases specifically focused on blockchain and data localization, existing disputes in adjacent sectors provide precedents. Internet service providers, digital payment platforms, and cloud storage companies have all faced regulatory challenges related to localization, some of which have escalated to formal dispute resolution under bilateral investment treaties. These cases establish that localization rules can have tangible investment implications and may be subject to legal challenge if they lack necessity, proportionality, or non-discriminatory application.

Multilateral institutions such as the WTO have been slow to develop comprehensive frameworks for resolving these issues. The existing mechanisms do not adequately address the unique features of decentralized systems. The risk is that in the absence of binding global norms, countries will continue to adopt unilateral or regional data policies that further fragment the legal landscape. This increases the compliance burden for blockchain developers and investors, potentially stifling innovation and diminishing the technology's promise for global financial and commercial integration.

Ultimately, the ongoing evolution of national data regimes and the rigidity of blockchain protocols suggest that conflict is likely to persist unless innovative regulatory frameworks are developed. Legal adaptation—whether through regulatory sandboxes, multilateral agreements, or context-sensitive arbitration—will be necessary to reconcile data localization laws with the realities of decentralized technology. Blockchain, as a driver of cross-border investment and trade, cannot thrive in a regulatory vacuum, nor can it flourish under fragmented and conflicting national data laws. A more harmonized international approach is imperative to ensure legal certainty, investor protection, and technological advancement.

[35] Emmanuelle Ganne, *'Can Blockchain Revolutionize International Trade?'* (2018) WTO Staff Working Paper ERSD-2018-07 https://www.wto.org/english/res_e/reser_e/ersd201807_e.htm accessed 10 March 2025.

 ISSN: 2582-6433

Chapter 6: Consumer Protection and Regulatory Gaps

Investor Protection in Blockchain Investments

The rise of blockchain technology has profoundly altered the global investment landscape, creating new opportunities and unprecedented risks for investors. While the decentralization and automation of blockchain systems offer the promise of transparency and efficiency, they also expose investors—particularly retail participants—to significant vulnerabilities. Fraudulent schemes, manipulative trading practices, market volatility, and weak regulatory oversight have become recurring issues in blockchain-based investments, revealing a critical need for stronger and more coherent investor protection frameworks.

One of the most significant risks faced by blockchain investors is fraud. Initial Coin Offerings (ICOs), which rapidly gained popularity as an alternative fundraising method, have frequently been used as vehicles for financial deception. The lack of standardized disclosures, the anonymity of project founders, and jurisdictional ambiguities have made it easier for malicious actors to launch fraudulent tokens and exit scams. Ponzi schemes disguised as blockchain investment platforms have also proliferated, often promising unrealistic returns to lure in unsuspecting investors. A notable example includes the OneCoin scheme, which masqueraded as a legitimate cryptocurrency but defrauded investors of billions globally. In the absence of a central regulatory body overseeing these offerings, enforcement has been reactive and inconsistent, leaving victims with limited recourse[36].

The risk of money laundering within blockchain systems compounds investor vulnerability. The pseudonymous nature of blockchain transactions facilitates the movement of illicit funds across borders without detection. Despite regulatory attempts to impose Know Your Customer (KYC) and Anti-Money Laundering (AML) standards on crypto exchanges, the decentralized

[36] Aleksandr P Alekseenko, *'Model Framework for Consumer Protection and Crypto-Exchanges Regulation'* (2023) 16(7) *Journal of Risk and Financial Management* 305 https://www.mdpi.com/1911-8074/16/7/305/pdf accessed 9 March 2025.

 ISSN: 2582-6433

and transnational nature of blockchain platforms often evades traditional enforcement mechanisms. Decentralized finance (DeFi) protocols, which operate without central intermediaries, are particularly challenging to regulate. Their open-source nature and permissionless architecture allow users to bypass KYC requirements entirely, creating ideal conditions for laundering proceeds from criminal activity[37]. This not only exposes retail investors to heightened risk by enabling bad actors to exploit these systems but also undermines the integrity of the broader financial ecosystem.

Another investor risk lies in the technological complexity and opacity of blockchain investment products. Smart contracts, the backbone of many decentralized applications, are often written in complex code that is inaccessible to non-technical investors. This asymmetry of information creates a barrier to informed decision-making and makes it easier for project developers to obscure risks. Additionally, the lack of standardized reporting or regulatory audits for most blockchain-based projects limits investors' ability to verify the legitimacy or solvency of these ventures. Retail investors, in particular, are ill-equipped to evaluate the technical and financial soundness of such offerings, rendering them highly susceptible to manipulation.

While some jurisdictions have attempted to address these challenges through regulatory reform, significant gaps persist in the global legal architecture. Existing regulatory frameworks are often ill-suited to address the hybrid nature of blockchain investments, which straddle the boundaries between securities, commodities, and utility tokens. In the United States, for example, the application of the Howey Test to determine whether a digital asset constitutes a security has generated legal uncertainty. Many blockchain assets remain in a grey zone, unregulated or inconsistently classified, which leaves investors without the protections afforded under securities law. Similarly, the fragmented nature of global regulation has allowed projects to engage in regulatory arbitrage, relocating to jurisdictions with lax oversight to evade scrutiny.

The absence of cross-border cooperation and uniform standards has further complicated enforcement. Investors harmed by blockchain projects operating in foreign jurisdictions often find it difficult to pursue legal remedies, especially when the perpetrators operate anonymously or from countries lacking robust investor protection regimes. In such cases, even when fraud is

[37] Tatjana Jovanić, *'An Overview of Regulatory Strategies on Crypto-Asset Regulation: Challenges for Financial Regulators in the Western Balkans'* (2021) https://www.researchgate.net/publication/348884909 accessed 9 March 2025.

 ISSN: 2582-6433

established, victims may be unable to recover their funds due to jurisdictional hurdles or the absence of regulatory frameworks that recognize their claims.

In response to these risks, scholars and regulatory bodies have proposed a range of measures aimed at enhancing investor protection in blockchain markets. These include mandating disclosures for digital asset offerings, establishing regulatory sandboxes to test blockchain products under supervised conditions, and developing harmonized international AML and KYC standards[38]. Some have also advocated for a tiered regulatory approach, wherein retail investors are afforded greater protections through investment limits and access to verified platforms, while institutional investors engage in blockchain investments under looser constraints.

Existing Consumer Protection Laws and Their Limitations

The global spread of blockchain-based financial technologies has outpaced the development of effective legal safeguards, raising urgent concerns over the sufficiency of existing consumer protection laws[39]. As blockchain increasingly intersects with financial markets and digital commerce—through cryptocurrencies, tokens, Initial Coin Offerings (ICOs), and decentralized finance (DeFi) platforms—regulators face a growing challenge: how to apply traditional legal frameworks, developed for centralized and intermediated financial systems, to decentralized, pseudonymous, and borderless technologies. While various jurisdictions have begun adapting securities, anti-money laundering (AML), and general consumer protection laws to the blockchain ecosystem, these efforts remain fragmented and inconsistently enforced, often leaving consumers without effective remedies[40].

One of the most significant legal strategies for regulating blockchain investments is through the classification of tokens as securities. In the United States, the Securities and Exchange Commission (SEC) applies the Howey Test from *SEC v W. J. Howey Co.*, 328 U.S. 293 (1946), which asks whether there is (1) an investment of money, (2) in a common enterprise, (3) with the expectation of profit, (4) derived from the efforts of others. If a token satisfies these criteria, it is deemed a security and must comply with the Securities Act of 1933 and Securities

[38] Tareq Na'el Al-Tawil, *'Anti-money laundering regulation of cryptocurrency: UAE and global approaches'* (2023) *Journal of Money Laundering Control* https://www.emerald.com/insight/content/doi/10.1108/JMLC-07-2022-0109/full/html accessed 9 March 2025.
[39] Supra note 1.
[40] **Mohammed Ahmad Naheem**, *'Exploring the Links Between AML, Digital Currencies and Blockchain Technology'* (2019) *Journal of Money Laundering Control* www.emeraldinsight.com/1368-5201.htm accessed 9 March 2025.

 ISSN: 2582-6433

Exchange Act of 1934[41]. This imposes disclosure, registration, and investor protection obligations on the issuer. However, the application of the Howey Test to crypto-assets remains controversial, especially in relation to utility tokens and governance tokens in decentralized platforms that do not rely on centralized managerial efforts.

The lack of legal certainty around the definition of digital assets has allowed many blockchain projects to circumvent regulatory oversight by structuring tokens to avoid classification as securities. Jurisdictions that lack formal definitions—such as India and parts of Southeast Asia—face even greater challenges. In these regions, blockchain companies often operate without licensing, without investor disclosures, and without liability for loss or misrepresentation. Consequently, investors in these unregulated or loosely regulated jurisdictions are frequently exposed to fraudulent schemes and unbacked financial products.

Another area of concern relates to anti-money laundering (AML) and counter-terrorism financing (CTF) regulations. Most developed countries have expanded AML statutes to cover Virtual Asset Service Providers (VASPs), including exchanges, wallet providers, and payment processors. The Financial Action Task Force (FATF) published its Recommendation 15, which requires countries to impose Know Your Customer (KYC), suspicious transaction reporting, and record-keeping obligations on VASPs[42].

In the European Union, the landmark Markets in Crypto-Assets Regulation (MiCA)—adopted in 2023—represents one of the most comprehensive attempts to regulate digital assets under a single framework. MiCA establishes rules for crypto-asset issuers and service providers, including licensing requirements, risk disclosures, whitepaper mandates, and provisions addressing market abuse. Crucially, MiCA includes investor protection measures such as mandatory technical audits for token issuers and liability clauses in cases of misleading disclosures[43]. However, MiCA does not apply to non-fungible tokens (NFTs) or decentralized finance (DeFi) protocols that lack centralized intermediaries, leaving a substantial portion of the blockchain ecosystem unregulated. Additionally, until MiCA's provisions are uniformly enforced across member states, divergent national practices may continue to create confusion

[41] SEC, *Framework for "Investment Contract" Analysis of Digital Assets* (2019) https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets accessed 9 March 2025.
[42] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (June 2019) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html accessed 9 March 2025.
[43] **European Parliament and Council**, *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)* [2023] OJ L150/40 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114 accessed 9 March 2025.

 ISSN: 2582-6433

and legal uncertainty for consumers. The European consumer law framework further supplements MiCA through horizontal directives such as the Consumer Rights Directive (2011/83/EU) and the Unfair Commercial Practices Directive (2005/29/EC). These laws require transparency, the right to withdraw from online contracts, and protections against misleading marketing—principles that are directly relevant to blockchain-based platforms offering digital tokens or financial services. Nonetheless, enforcement remains a challenge. Many blockchain service providers operate outside of the EU or present themselves as "decentralized," thereby circumventing jurisdictional reach and accountability mechanisms. Even when domiciled within the EU, some platforms avoid compliance through complex organizational structures or disclaimers asserting non-liability.

General consumer protection laws are primarily designed to prevent misleading advertising, unfair contract terms, and fraudulent commercial practices. In the European Union, laws like the Consumer Rights Directive (Directive 2011/83/EU) and the Unfair Commercial Practices Directive (Directive 2005/29/EC) provide comprehensive protections for consumers purchasing goods or services online, including the right to withdraw from contracts and to receive clear and accurate information. These laws theoretically apply to blockchain platforms offering investment packages or token purchases.

The UAE, in contrast, has proactively addressed these gaps through its Virtual Assets Regulatory Authority (VARA) and the Central Bank's AML Guidelines (2021), which extend AML obligations specifically to virtual asset entities operating in Dubai[44]. These frameworks mandate registration, transparency in ownership, and real-time monitoring of suspicious activities, setting an example for adaptive legislation in the blockchain space[45].

Though, enforcement is hampered by the pseudonymous and cross-border nature of most blockchain projects. Many operate outside the EU or avoid listing their legal entities, making it difficult for regulators to impose penalties or pursue enforcement. Smart contracts—self-executing code operating on blockchains—may fulfill legal functions without offering consumers a meaningful way to dispute outcomes, obtain refunds, or reverse transactions. Even where contract law applies, identifying a liable counterparty is often impossible.

[44] Dubai Virtual Assets Regulatory Authority (VARA), *Virtual Assets Regulatory Framework* (2023) https://www.vara.ae/en/regulations accessed 9 March 2025.
[45] Central Bank of the UAE, *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Virtual Assets* (2021) https://www.centralbank.ae/en/cbuae-aml-guidelines accessed 9 March 2025.

 ISSN: 2582-6433

In the United States, the Federal Trade Commission Act (15 U.S.C. §§ 41–58) prohibits unfair or deceptive acts in commerce and has been invoked against crypto platforms for misrepresentation and failure to secure customer data. However, such interventions are retrospective, occurring after consumer harm has already been done. At the state level, California's Consumer Privacy Act (CCPA) adds further obligations on businesses that collect personal data, which may be relevant to wallet providers or exchanges collecting KYC information. New York's BitLicense regime (NYDFS 2015) imposes consumer protection, AML, and cybersecurity standards on virtual currency businesses. Yet, many platforms sidestep these by either geo-blocking U.S. residents or operating from offshore jurisdictions[46].

The United Kingdom employs the Financial Services and Markets Act 2000 (FSMA) to regulate certain digital assets that qualify as "specified investments." The Financial Conduct Authority (FCA) has issued guidance distinguishing between security tokens, e-money tokens, and unregulated utility tokens[47]. The Consumer Protection from Unfair Trading Regulations 2008 also apply to misleading crypto advertisements and influencer campaigns. Despite this, many crypto-assets do not meet the threshold for regulation and remain outside FCA jurisdiction, particularly decentralized or non-custodial platforms.

In Brazil, the Consumer Protection Code (Código de Defesa do Consumidor) ensures consumer rights against deceptive advertising, contract abuse, and product liability. The General Data Protection Law (Lei Geral de Proteção de Dados – LGPD) also applies to crypto exchanges handling personal information. However, enforcement remains fragmented and many platforms evade scrutiny, particularly in peer-to-peer markets or foreign-hosted apps.

In India, although there is no dedicated crypto law, the Consumer Protection Act 2019 and Information Technology Act 2000 provide some consumer rights. For example, the Consumer Protection Act allows consumers to file complaints against unfair trade practices, while the IT Act criminalizes identity theft and data breaches. Still, enforcement is weak, and Indian users typically invest via platforms that lack a regulatory footprint within the country. This undermines both financial stability and legal recourse.

Even in jurisdictions with robust legal tools, structural challenges persist. Blockchain's

[46] New York Department of Financial Services, *Virtual Currency Business Activity (BitLicense)* https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses accessed 9 March 2025.
[47] Financial Conduct Authority, *Guidance on Cryptoassets* (PS19/22) https://www.fca.org.uk/publication/policy/ps19-22.pdf accessed 9 March 2025.

 ISSN: 2582-6433

decentralized architecture renders traditional enforcement mechanisms ineffective. Pseudonymous actors, smart contracts operating without a corporate entity, and cross-border data flows create barriers to identifying responsible parties. Legal doctrines like contractual privity and tort liability falter when there is no identifiable counterparty. Moreover, many jurisdictions lack extraterritorial enforcement mechanisms, meaning investors often have no recourse if harmed by foreign-based platforms.

 ISSN: 2582-6433

Chapter 7: Dispute Resolution Mechanisms in Blockchain

Traditional vs. Decentralized Dispute Resolution

As blockchain technology reconfigures the global transactional ecosystem, legal frameworks for dispute resolution are being challenged by the rise of decentralised systems. Traditional international commercial arbitration, grounded in instruments such as the UNCITRAL Model Law, the New York Convention (1958), and institutional rules of bodies like the ICC, LCIA, and ICSID, has historically provided robust and enforceable mechanisms for resolving cross-border commercial disputes. However, with the proliferation of blockchain-native interactions—such as smart contracts, decentralised finance (DeFi) platforms, and Decentralised Autonomous Organisations (DAOs)—there is growing traction for Decentralised Dispute Resolution (DDR), including platforms like Kleros and Aragon Court.

International commercial arbitration has long been favoured for its neutrality, party autonomy, and enforceability, especially under the New York Convention, which mandates the recognition and enforcement of arbitral awards in over 170 jurisdictions. The UNCITRAL Model Law on International Commercial Arbitration (1985, amended 2006) provides a harmonised legal foundation adaptable to domestic legal systems. Traditional arbitration relies on legally constituted arbitral tribunals, defined procedural safeguards, and state court oversight at the recognition and enforcement stages.

These mechanisms are well-suited for traditional legal entities with fixed nationality, seat of incorporation, and a clear choice-of-law clause. However, when disputes arise from blockchain interactions—often involving pseudonymous actors, code-executed obligations, and globalised nodes—they strain the assumptions underpinning traditional arbitral practice[48].

Decentralised Dispute Resolution (DDR) mechanisms are emerging in response to the unique decentralisation and automation of blockchain transactions. Notable among them are Kleros which is a blockchain-based dispute resolution layer operating on Ethereum, using randomly selected jurors incentivised by tokens to adjudicate disputes. And Aragon Court which Part of

[48]Michaelson PL and Jeskie SA, 'Arbitrating Disputes Involving Blockchains, Smart Contracts and Smart Legal Contracts' (2020) SSRN https://ssrn.com/abstract=3720876 accessed 20 March 2025.

 ISSN: 2582-6433

the broader Aragon DAO governance platform, allowing DAOs to engage in native dispute resolution without recourse to state-based institutions.

These DDR platforms embed arbitration logic into the transactional framework, enabling automated decision enforcement via smart contracts. The jurors or adjudicators are pseudonymous peers selected through algorithmic means, and decisions are enforced by blockchain logic rather than state courts.

Arguably these systems have the potential to evolve into "smart courts", capable of resolving cross-border disputes efficiently, cheaply, and transparently within the ecosystem where the transaction occurs. The value proposition of DDR lies in its speed, cost-effectiveness, and automation—traits that traditional arbitration, with its formal procedural steps and institutional bureaucracy, often lacks[49].

Key Differences

The fundamental distinction lies in the location of adjudicatory authority. Traditional arbitration is anchored in legal sovereignty and recognized legal instruments, while DDR operates within code-based communities and "lex cryptographica"—rules embedded in software rather than law.

Another divergence is the enforcement mechanism. In traditional systems, enforcement depends on judicial intervention—especially under the New York Convention. DDR, in contrast, uses self-enforcing smart contracts, which execute decisions autonomously, bypassing national legal enforcement channels. Ortolani observes that this model represents a potential paradigm shift—one where state oversight of arbitration may be marginalised altogether[50].

However, this shift is theoretical at best. As of now, national courts retain ultimate authority in cross-border commercial enforcement. While Kleros rulings may work in a decentralised marketplace, they lack legal recognition in courts of law, particularly for disputes exceeding the scope of smart contract execution.

[49] Kirkwood J and Chaisse J, 'Smart Courts, Smart Contracts and the Future of Online Dispute Resolution' (2022) ResearchGate https://www.researchgate.net/publication/357794881_Smart_Courts_Smart_Contracts_and_the_Future_of_Online_Dispute_Resolution accessed 22 March 2025.

[50] De Filippi P and Wright A, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) https://ebookcentral.proquest.com/lib/uconn/detail.action?docID=5340266 accessed 20 March 2025.

 ISSN: 2582-6433

Legal and Ethical Limitations of DDR

Despite the innovation, DDR systems face legitimacy, transparency, and due process concerns. Critics argue that the lack of procedural safeguards, limited appeal rights, and the pseudonymity of jurors undermine the foundational fairness that traditional arbitration espouses.

Moreover, Kleros-style token-weighted systems may suffer from manipulation, collusion, and vote buying, particularly in high-stakes disputes. These systems also lack oversight, accountability, or compliance with recognised principles of natural justice.

Further observed that while DDR may suffice for micro-level technical disputes (e.g., bug bounties, DAO governance infractions), it is ill-equipped for complex, multi-jurisdictional legal conflicts, where interpretation of law and factual nuances are critical.

A promising development is the integration of DDR with traditional arbitration, creating "hybrid arbitration" mechanisms. For instance, Ricardian contracts embed human-readable legal terms alongside machine-executable code. Parties can pre-agree to trigger traditional arbitration in the event of a smart contract malfunction—an approach endorsed by Shehata and others as a legally defensible compromise[51].

Such hybrid models could benefit from the speed and automation of DDR while retaining the legitimacy and enforceability of formal arbitration. Additionally, international arbitration institutions are increasingly considering model clauses compatible with blockchain-based contracts, while UNCITRAL's Working Group III is exploring reforms that may accommodate new forms of technology-assisted arbitration.

Challenges in Enforcing Blockchain Arbitration Decisions

As blockchain-based systems of transaction and governance mature, the possibility of resolving disputes through decentralised arbitration platforms has gained traction. However, while such systems promise cost-efficiency, speed, and automation, they also introduce significant legal and institutional challenges, particularly when it comes to the recognition and enforcement of

[51] Shehata IM, 'Smart Contracts and International Arbitration' (2020) SSRN https://ssrn.com/abstract=3290026 accessed 21 March 2025.

 ISSN: 2582-6433

their decisions within established legal frameworks[52].

The foremost difficulty lies in aligning decentralised arbitration mechanisms with existing international legal instruments. Under conventions such as the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, specific procedural and formal requirements must be met for arbitral decisions to be recognised and enforced by state courts. Decentralised rulings, especially those delivered through automated systems on blockchain platforms, often fall outside these conventional definitions. They may lack identifiable arbitrators, written reasoned awards, or procedural records—features typically required for recognition under public international law[53].

Moreover, the legitimacy of blockchain-based arbitration decisions is frequently questioned due to procedural inconsistencies. Decentralised arbitration systems may operate through pseudonymous juror pools, token-based incentives, or algorithmic selection, raising serious concerns about due process, impartiality, and transparency. Without clear mechanisms for appeal or review, and absent any identifiable governing law or jurisdiction, these processes may be deemed incompatible with the minimum standards of fairness upheld in traditional dispute resolution.

Another major concern is the self-executing nature of blockchain arbitration. Many systems are designed to bypass traditional court enforcement entirely, implementing decisions via smart contracts that automatically execute rulings, such as transferring digital assets or altering permissions on-chain. While this feature enhances efficiency, it deprives parties of the procedural safeguards offered by judicial oversight. If a party contests the decision, there is often no recourse to challenge the outcome within the blockchain environment, nor is there an obvious forum to seek remedies externally, especially when legal jurisdiction is unclear or lacking altogether.

Further complicating matters is the issue of enforceability across borders. National courts are hesitant to enforce decisions that do not comply with local procedural norms or public policy considerations. In many jurisdictions, the anonymity of participants, lack of transparency in adjudication, and absence of a physical or legal seat for the arbitration tribunal may all lead

[52] Awada GM, 'Alternative Dispute Resolution (ADR) for International Commerce Disputes through UNCITRAL' (2023) Russian Journal of Comparative Law https://cyberleninka.ru/article/n/alternative-dispute-resolution-adr-for-international-commerce-disputes-through-uncitral accessed 23 March 2025.
[53] Supra note 3.

 ISSN: 2582-6433

courts to decline enforcement on the basis that such processes violate fundamental principles of natural justice. Additionally, rulings generated by decentralised systems often lack any certified documentation or verification by an authorised arbitral institution, further undermining their legal weight.

Beyond procedural concerns, technological finality also creates enforcement challenges. Decisions once executed on-chain are typically irreversible, due to the immutable nature of blockchain architecture. If a decision is later challenged and deemed invalid or illegal by a court, reversing the transaction may prove technologically infeasible. This irreversible enforcement can lead to outcomes that are legally or ethically problematic, particularly when one party has acted in bad faith or when the automated decision-making process fails to account for nuance or context[54].

Despite these challenges, decentralised arbitration can be appropriate for specific categories of disputes, particularly those involving digital-native parties and low-value, high-frequency transactions. In such contexts, the benefits of speed and automation may outweigh the risks. However, for disputes requiring interpretation of law, consideration of equity, or examination of complex factual circumstances, decentralised platforms often fall short of the rigor and reliability offered by conventional arbitration or litigation.

To bridge this gap, hybrid approaches have been proposed. One model involves embedding traditional arbitration clauses within smart contracts, allowing parties to rely on state-recognised mechanisms in the event that the decentralised process fails or is disputed. These hybrid agreements may also incorporate dual-mode logic—enabling execution on-chain while preserving access to conventional enforcement pathways off-chain. Such approaches strive to maintain the advantages of blockchain-based efficiency while ensuring legal validity and compliance with existing frameworks[55].

Institutional reform may also play a role in resolving these challenges. Ongoing discussions within international legal bodies suggest a willingness to adapt existing treaties and arbitration models to accommodate technological evolution. Proposals include the development of model arbitration clauses for smart contracts, clarification of how digital signatures and automated

[54] Chevalier M, 'From Smart Contract Litigation to Blockchain Arbitration' (2021) *Journal of International Dispute Settlement* (Advance article) https://academic.oup.com/jids/article-abstract/12/4/558/6414874 accessed 21 March 2025.
[55] J Chauhan, 'Technological Innovations and International Law Reform in Blockchain Arbitration' (2024) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4640977 accessed 23 March 2025.

 ISSN: 2582-6433

systems can satisfy procedural requirements, and the inclusion of decentralised adjudication within broader legal definitions of arbitral awards. These reforms aim to foster convergence between traditional and blockchain-native systems, rather than allowing fragmentation and uncertainty to persist.

Finally, judicial education and technological literacy will be essential in building trust and functional interaction between courts and decentralised systems. As courts and arbitral tribunals encounter an increasing volume of disputes arising from smart contracts and digital assets, understanding the operational and legal dynamics of blockchain-based arbitration will be critical to ensuring fair and consistent application of the law.

Reforming International Dispute Resolution for Blockchain

The emergence of blockchain-based technologies and decentralised contractual relationships has exposed critical gaps in the current framework of international dispute resolution. Traditional arbitration structures—rooted in bilateral treaties, multilateral conventions, and institutional rules—were designed for a world where parties have physical presence, defined national identity, and legal incorporation. The growing prevalence of pseudonymous participants, Decentralised Autonomous Organisations (DAOs), and code-based contracts calls for a comprehensive reassessment of these mechanisms. Reform is essential not only to preserve the legitimacy of international arbitration but also to ensure the legal sustainability of cross-border blockchain commerce.

The Incompatibility of Traditional Definitions

One of the central problems lies in the definitional scope of "investment" under most bilateral investment treaties (BITs) and conventions like the ICSID Convention. These definitions were drafted with tangible, traditional economic activities in mind—such as factories, natural resources, and contractual concessions. However, blockchain-based investments, such as token issuance, decentralised finance participation, and non-fungible token (NFT) exchanges, rarely conform to these conventional categories. The question arises whether algorithmic contributions to DAOs or participation in a decentralised liquidity pool constitute protected "investments" under international law.

Reforming these definitions is imperative to ensure that investors engaging in legitimate blockchain activities are not left outside the protective scope of dispute resolution frameworks.

 ISSN: 2582-6433

Doing so may require amending model BITs or issuing interpretative guidance under existing treaties to accommodate digital assets and blockchain-related contributions as recognised forms of investment.

Nationality, Legal Personality, and Jurisdictional Identity

Traditional international arbitration requires clear attribution of legal personality and nationality to both investors and respondent states. This presumption is increasingly challenged by the digital nature of blockchain transactions. Many participants in blockchain-based systems operate under pseudonyms, may lack national affiliation, or are incorporated under decentralised governance models. DAOs, for instance, may have no headquarters, board of directors, or incorporation under the laws of any nation-state.

This poses significant obstacles in establishing jurisdiction, particularly under frameworks like ICSID which hinge upon the investor's nationality and the host state's consent. Without clearly defined legal identity, it becomes difficult to verify the applicability of consent clauses, determine treaty eligibility, or invoke jurisdiction under investor-state dispute settlement (ISDS) mechanisms. Reform efforts must, therefore, address the ambiguity of party identity in blockchain environments and propose workable solutions—such as recognising digital corporate forms, permitting self-certifying identities, or extending legal standing to unincorporated decentralised entities under specified conditions[56].

Institutional Adaptation and Model Law Integration

Efforts by major institutions, particularly UNCITRAL and ICSID, are gradually beginning to respond to technological shifts. UNCITRAL has actively examined digital technologies through its Working Group III on investor-state dispute settlement reform, contemplating whether online dispute resolution systems can be integrated into international commercial and investment arbitration.

One possible pathway lies in the adoption of model arbitration clauses specifically designed for smart contracts and decentralised governance. These clauses could include detailed specifications about jurisdiction, choice of law, arbitration seat, and procedural conduct, ensuring clarity and predictability despite the technical execution of agreements through code.

[56] Ortolani P, 'The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration and Court Litigation at the Crossroads' (2019) *Uniform Law Review*, vol 24(2) https://academic.oup.com/ulr/article-pdf/24/2/430/32905092/unz017.pdf accessed 22 March 2025.

 ISSN: 2582-6433

Furthermore, such clauses could accommodate hybrid models where smart contracts are coupled with human-readable legal agreements, thereby preserving enforceability under existing frameworks while embracing automation[57].

Additionally, UNCITRAL could consider expanding its Model Law on Electronic Commerce and Model Law on International Commercial Arbitration to explicitly address digital asset transactions, decentralised contracting, and blockchain-based procedural mechanisms. These updates would offer legal certainty to courts and tribunals when interpreting agreements and enforcing awards involving blockchain parties.

Hybrid Mechanisms and Ricardian Contracts

One of the more promising approaches involves hybridisation between code and law. Smart contracts can be designed as Ricardian Contracts—agreements that contain both human-readable legal terms and machine-readable code. This structure allows for seamless execution while preserving a legal record that can be interpreted and enforced under traditional legal frameworks. When disputes arise, the Ricardian format ensures that there is a conventional arbitration clause embedded within the smart contract logic.

This model facilitates compatibility with state-based arbitration institutions, allowing traditional arbitrators to adjudicate disputes involving blockchain logic without sacrificing procedural integrity. Furthermore, it preserves access to national courts for enforcement purposes, avoiding the jurisdictional opacity associated with purely decentralised rulings.

Procedural Innovations and Technology-Aware Arbitration

Beyond definitional reform and legal hybridisation, procedural innovation is needed to handle blockchain-related disputes effectively. International arbitration institutions may consider implementing technology-aware panels, composed of arbitrators with expertise in smart contract mechanics, tokenomics, and distributed ledger systems. Such appointments would ensure that arbitrators are equipped to interpret the technical dimensions of disputes and understand the implications of automated performance.

Moreover, procedural reforms could include provisions for on-chain evidence collection, secure digital witness authentication, and blockchain-based case management systems. By

[57] Supra note 3.

 ISSN: 2582-6433

integrating such tools into procedural rules, institutions can modernise the dispute resolution process without undermining legal safeguards.

Chapter 8: Jurisdictional Aspect of Tax and Blockchain

 ISSN: 2582-6433

The classification and taxation of cryptocurrencies and digital assets vary significantly across jurisdictions, creating a fragmented regulatory landscape that complicates global compliance. As blockchain technology reshapes finance and commerce, tax authorities are under pressure to adapt legacy systems that were never designed for decentralized, pseudonymous, or borderless digital value exchange. The disparity in legal definitions and tax treatment across countries not only fosters uncertainty for investors and developers but also opens avenues for regulatory arbitrage and tax avoidance.

United States

In the United States, the Internal Revenue Service (IRS) classifies virtual currencies as property for federal tax purposes. This means that gains or losses from the sale, exchange, or use of cryptocurrencies are treated under capital gains tax rules. If the asset is held for more than a year, long-term capital gains apply; otherwise, short-term gains are taxed as ordinary income rates. Furthermore, the IRS mandates that every crypto-to-crypto transaction be recognized as a taxable event. This includes using cryptocurrency to purchase goods or services, which requires the taxpayer to determine the fair market value of the digital asset at the time of each transaction.

The IRS has also expanded reporting requirements. Under the Infrastructure Investment and Jobs Act of 2021, "brokers"—which include exchanges and wallet providers—must issue Form 1099-DA to users and report transaction data to the IRS. Despite this clarity in classification, critics argue that U.S. tax law remains ill-suited to decentralized finance (DeFi) platforms and emerging token types such as non-fungible tokens (NFTs) and governance tokens.

European Union

The European Union (EU) has taken steps toward harmonizing crypto regulation through initiatives like the Markets in Crypto-Assets Regulation (MiCA) and DAC8 (Directive on Administrative Cooperation). However, when it comes to taxation, EU member states vary significantly in their classification and treatment of digital assets.

At the VAT level, the landmark case of *Skatteverket v David Hedqvist* (C-264/14) established that the exchange of traditional currencies for Bitcoin is exempt from VAT, recognizing Bitcoin as a means of payment. Following this decision, many EU countries began treating

 ISSN: 2582-6433

cryptocurrencies similarly for VAT purposes. Still, differences persist. For instance, Germany classifies cryptocurrencies as private money, and their sale is tax-exempt if held for more than one year. In contrast, France treats crypto-assets as digital assets, subjecting them to a flat 30% capital gains tax rate, while mining and staking income are classified as non-commercial profits[58].

MiCA aims to standardize the regulatory treatment of crypto-assets, especially regarding issuer obligations and consumer protection, but tax policy remains under the purview of individual member states. Meanwhile, DAC8 will require crypto-asset service providers—both centralized and decentralized—to report user transactions for cross-border tax information exchange, mirroring the OECD's Crypto Asset Reporting Framework (CARF)[59].

India

India's approach to classifying and taxing digital assets is among the most rigid globally. The Finance Act 2022 introduced the term "Virtual Digital Assets (VDAs)", broadly defined to include cryptocurrencies, tokens, and NFTs. Under Section 115BBH of the Income Tax Act, any income arising from the transfer of VDAs is taxed at a flat rate of 30%, with no deductions allowed for costs other than acquisition.

Additionally, India imposes a 1% Tax Deducted at Source (TDS) under Section 194S on every transaction involving a VDA, regardless of the size or profit. There is currently no differentiation in classification between utility, payment, or security tokens[60]. The lack of nuanced classification results in over-inclusive tax enforcement, placing a compliance burden on even non-commercial or low-value transactions. This strict approach has drawn criticism for disincentivizing innovation while failing to distinguish between investment and utility use cases.

China

China maintains a prohibition-first model, banning cryptocurrency trading, mining, and

[58] International Cybersecurity Law Review, 'VAT/GST Harmonisation Challenges for Digital Assets such as Bitcoin and NFTs in the EU following Case C-264/14 (Skatteverket v David Hedqvist)' (2024) 5(1) ICLR 459 https://doi.org/10.1365/s43439-024-00124-2 accessed 15 March 2024.
[59] **OECD,** *Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues* (OECD Publishing 2020) https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.htm accessed 14 March 2024.
[60] PwC, *2023 Global Crypto Tax Report* (2023) https://www.pwchk.com/en/financial-services/publications/pwc-launches-global-crypto-tax-report-2024.pdf accessed 14 March 2024.

 ISSN: 2582-6433

exchanges. While digital assets are not legally recognized as a medium of exchange or store of value, individuals continue to access foreign exchanges using virtual private networks (VPNs). In terms of classification, China treats digital tokens as intangible assets when they are considered for tax purposes, though this treatment is largely theoretical given the overarching prohibition[61].

Although there are no detailed crypto tax regulations in place, any capital gains from digital assets—if acknowledged—would fall under individual income tax. The State Taxation Administration has made sporadic statements suggesting such income should be declared, but lack of clarity and enforcement discretion mean that crypto taxation remains largely untested in China.

Brazil

In Brazil, the Federal Revenue Service classifies cryptocurrencies as financial assets. Transactions involving more than BRL 35,000 per month are subject to capital gains tax at rates ranging from 15% to 22.5%, depending on the amount of profit. All taxpayers holding crypto assets above BRL 5,000 must report them annually, while monthly declarations are required for larger transactions.

Brazil does not formally differentiate between different types of tokens (e.g., payment vs. utility), but any appreciation in value is taxable upon realization. Additionally, income derived from mining is taxable as ordinary income, and cryptocurrencies held abroad are subject to foreign asset declaration laws. Although comprehensive in reporting scope, enforcement remains weak, especially for trades occurring on foreign platforms.

Japan

Japan takes a rigorous approach by classifying gains from cryptocurrency activities as "miscellaneous income", subject to income tax rates that can exceed 55%. The National Tax Agency (NTA) requires taxpayers to report gains from trading, mining, and even airdrops. Unlike capital gains, losses from crypto cannot offset other income categories, making Japan's regime relatively harsh.

Cryptocurrency-to-cryptocurrency exchanges are also considered taxable events, requiring

[61] Ibid.

 ISSN: 2582-6433

real-time calculation of market values at the time of each trade. While Japan has issued guidance distinguishing between different types of digital assets, all remain under the miscellaneous income category for tax purposes, making classification less relevant from a taxation standpoint.

Singapore and Hong Kong

Singapore and Hong Kong are considered crypto-friendly jurisdictions. Singapore does not impose capital gains tax, and crypto-assets are generally only taxed if they are part of a business activity. The Inland Revenue Authority of Singapore (IRAS) classifies tokens based on their function—payment tokens, utility tokens, and security tokens. However, only income derived from trading or staking is subject to tax.

Hong Kong also exempts capital gains from tax, provided the investor is not carrying out crypto trading as a business. The Inland Revenue Department uses the "badges of trade" test to assess whether an individual is engaged in a trading activity, which would trigger income tax. Both jurisdictions benefit from regulatory clarity and favourable tax treatment, attracting global crypto firms.

Existing Tax Frameworks and Their Gaps: OECD, FATF, EU, and Blockchain's Role in Tax Administration

As blockchain technologies become more integrated into global finance, tax authorities are under pressure to adapt existing regulatory frameworks to digital assets that transcend borders, anonymize transactions, and resist central oversight. The OECD, FATF, and the European Union have all introduced tax-related frameworks aimed at bringing some coherence to the taxation of digital assets, particularly cryptocurrencies. Despite these efforts, significant gaps remain, especially in dealing with decentralized financial platforms (DeFi), enforcing cross-border compliance, and integrating new tax-reporting tools. Simultaneously, blockchain's own transparency features offer unique potential to enhance global tax administration—providing a paradoxical but promising intersection between technology and governance.

OECD and the Crypto-Asset Reporting Framework (CARF)

The OECD has played a central role in shaping global responses to crypto-taxation through the

 ISSN: 2582-6433

creation of the Crypto-Asset Reporting Framework (CARF)[62]. CARF builds on the Common Reporting Standard (CRS), extending automatic exchange of financial account information to crypto-asset transactions. The goal is to reduce tax evasion by requiring Virtual Asset Service Providers (VASPs) such as crypto exchanges, brokers, and wallet providers to report customer holdings and transaction data to national tax authorities, which in turn share it internationally.

The framework defines a "reporting crypto-asset service provider" as any intermediary that facilitates crypto-to-crypto or crypto-to-fiat trades, transfers, or custody services. However, CARF excludes peer-to-peer transactions conducted through unhosted wallets or decentralized exchanges unless a regulated intermediary is involved. This leaves a large segment of the DeFi ecosystem outside the purview of mandatory reporting, thereby creating a substantial compliance gap.

Another limitation lies in the lack of harmonized token classification. CARF does not mandate a universal taxonomy for tokens, leading to inconsistent tax treatment across jurisdictions. For example, staking rewards might be considered income in one country and capital gains in another. Similarly, NFTs and governance tokens are inconsistently treated, if recognized at all. These variations not only hinder consistent reporting but also encourage regulatory arbitrage.

FATF Standards and Tax Implications

Although the Financial Action Task Force (FATF) is primarily focused on anti-money laundering (AML) and counter-terrorism financing (CTF), its frameworks significantly influence the taxation of crypto-assets. Under FATF's Recommendation 15, countries are required to subject VASPs to the same obligations as traditional financial institutions. This includes Know Your Customer (KYC) requirements, suspicious transaction reporting, and customer due diligence.

These measures help tax authorities indirectly by establishing identity trails and transaction histories that can be matched with tax declarations. FATF's "travel rule" further mandates the sharing of originator and beneficiary information for transactions over a certain threshold. Yet, DeFi protocols and self-hosted wallets often bypass these requirements due to their decentralized, non-custodial nature. This creates significant blind spots for enforcement and

[62] Supra note 2.

 ISSN: 2582-6433

undermines FATF's broader objectives, which align with those of tax authorities[63].

Moreover, FATF's definitions are not legally binding and require implementation through national legislation, which varies in scope and efficiency. This lack of uniformity often results in gaps where certain VASPs may operate without fulfilling reporting obligations, either due to regulatory ambiguity or jurisdictional avoidance.

EU's DAC8 and Regional Harmonization Efforts

The European Union has made progress in tightening crypto tax compliance through the Directive on Administrative Cooperation (DAC8). Building on DAC7, DAC8 explicitly includes crypto-assets in the scope of tax information reporting, obligating all crypto-asset service providers—whether established in the EU or not—to report on transactions involving EU resident taxpayers.

DAC8 is directly aligned with the OECD's CARF, ensuring consistency in reporting templates, data fields, and timelines. However, implementation depends on national tax authorities, and the directive does not automatically harmonize tax classifications or rates across member states. For instance, some EU countries consider crypto gains as personal income, while others treat them as capital gains[64]. This disjointed regulatory architecture hinders seamless enforcement and introduces legal uncertainty for taxpayers operating across borders.

DAC8 continues to rely on the presence of an identifiable service provider. Transactions executed via smart contracts or between unhosted wallets often remain untraceable under this regime. Enforcement challenges are exacerbated by jurisdictional fragmentation, a common weakness in both EU-level and global tax policy[65].

Gaps in Enforcement and Regulatory Arbitrage

Despite efforts by OECD, FATF, and the EU, major enforcement gaps persist. These include:

[63] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html accessed 15 March 2024.
[64] European Commission, *Directive on Administrative Cooperation (DAC8) – Tax Transparency Rules for Crypto-Assets* (2023) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023L2226 accessed 16 March 2024.
[65] European Parliamentary Research Service, *Tax Transparency Rules for Crypto-Asset Transactions (DAC8 Briefing)* (2024) https://www.europarl.europa.eu/doceo/document/TA-9-2022-0335_EN.html accessed 15 March 2024.

 ISSN: 2582-6433

- **Lack of real-time reporting**: Most frameworks are retrospective, relying on annual declarations or audits, which are inadequate for fast-moving crypto markets.
- **Overreliance on intermediaries**: The absence of service providers in decentralized networks limits data availability.
- **Regulatory arbitrage**: Taxpayers and platforms can exploit differing national laws by domiciling in jurisdictions with lenient enforcement or ambiguous regulations.
- **Non-cooperation and capacity gaps**: Many countries, especially in emerging markets, lack the technical or legal infrastructure to enforce cross-border crypto tax compliance effectively.

These issues illustrate the tension between innovation and governance. Without coordinated global action, decentralized technologies will continue to outpace regulatory frameworks, and taxation gaps will widen.

Blockchain as a Tool for Tax Enforcement

Paradoxically, the very technology that complicates taxation also offers new solutions. Blockchain's inherent features—immutability, transparency, and traceability—make it a promising tool for enhancing tax administration.

Governments are increasingly exploring the use of blockchain to automate tax processes. For example, blockchain can be used to establish tamper-proof records of financial transactions, reducing opportunities for manipulation or fraud[66]. Smart contracts can facilitate automatic withholding and remittance of taxes in real-time, based on pre-programmed rules embedded in the code.

Blockchain also enables real-time auditability, which reduces the reliance on costly post-factum audits and increases compliance. Moreover, integrating blockchain with digital identity frameworks could allow tax authorities to trace ownership of wallets, ensuring accountability even in pseudonymous networks.

[66] Rasmi K, 'Blockchain Technology Used in Taxation' (2023) SSRN https://ssrn.com/abstract=4381323 accessed 16 March 2024.

 ISSN: 2582-6433

Chapter 9: The Role of Technology in Jurisdiction and Compliance

How Technology Can Aid Legal Compliance

 ISSN: 2582-6433

The integration of technology into legal compliance frameworks is a promising development in the regulation of blockchain ecosystems. As blockchain continues to disrupt traditional regulatory paradigms, jurisdictions worldwide are experimenting with technical and institutional innovations to ensure compliance with legal mandates. Two significant tools in this context are blockchain geofencing and regulatory sandboxes—each representing a distinct approach to reconciling technological innovation with jurisdictional integrity and governance.

Blockchain Geofencing: Restricting Jurisdictional Access

Blockchain geofencing refers to the use of geographic restrictions embedded into blockchain infrastructure or decentralized applications (dApps) to limit access or transactions to users in specific regions. This method is particularly relevant in the context of decentralized finance (DeFi), token sales (ICOs), and crypto exchanges, where service providers must comply with regional laws like securities regulations, anti-money laundering (AML) provisions, and consumer protection laws.

For example, many platforms deploy IP-address blocking and location-based identification tools to ensure that users from prohibited jurisdictions (such as U.S. residents in unregistered token offerings) are denied access. This method is a technological implementation of regulatory boundaries—enabling decentralized protocols to self-police in alignment with national laws[67]. Smart contracts may also include built-in location-based restrictions that prevent execution if the origin of a transaction lies within a blacklisted region.

The limitation, however, lies in the fact that blockchain networks are inherently borderless and pseudonymous. Users can bypass geofencing measures through VPNs or proxy servers, which undermines the effectiveness of compliance. Furthermore, enforcing geofencing may contradict the foundational ethos of blockchain, which champions decentralization, open access, and censorship resistance. Despite these challenges, the increasing adoption of regulatory requirements—like Know Your Customer (KYC) obligations and identity verification APIs—has strengthened the feasibility of geolocation-aware compliance mechanisms.

Jurisdictions such as the United States and the European Union have begun encouraging or

[67] Andrej Zwitter and Jilles Hazenberg, 'Decentralized Network Governance: Blockchain Technology and the Future of Regulation' (2020) 3 *Frontiers in Blockchain* 12 https://doi.org/10.3389/fbloc.2020.00012 accessed 15 March 2025.

 ISSN: 2582-6433

even mandating geofencing practices for crypto platforms. In some cases, the inability to implement geofencing effectively has led to enforcement actions by securities regulators or the refusal of operational licenses.

Regulatory Sandboxes: Innovation in a Supervised Setting

Regulatory sandboxes are controlled environments where blockchain startups and financial technology (FinTech) innovators can test their products under the supervision of regulatory authorities. These frameworks are especially useful in areas where legal classification is uncertain or where technology operates in regulatory gray zones. They offer temporary authorization to operate while still being monitored for compliance and systemic risks.

The United Kingdom's Financial Conduct Authority (FCA) was among the first to introduce a regulatory sandbox in 2016, allowing fintech startups to test their products without the burden of full regulatory compliance. This model has since been replicated in several jurisdictions including Singapore, the United Arab Emirates, Canada, Australia, and emerging economies in Latin America and Africa. Within the blockchain context, sandboxes provide a secure channel for launching tokenized assets, decentralized platforms, and blockchain-based financial instruments that would otherwise face legal uncertainty.

These environments typically come with defined time limits, entry criteria (such as genuine innovation and consumer benefit), and exit requirements. Companies operating within a sandbox are expected to share performance data, risk evaluations, and compliance metrics with the regulator. This information is used to assess the systemic impact of new technologies and potentially shape future regulations.

One of the key benefits of sandboxes is their facilitation of dialogue between regulators and innovators[68]. Blockchain developers gain clarity on compliance expectations, while authorities better understand the operational realities of emerging technologies. In developing countries, sandboxes have been instrumental in fostering blockchain-based financial inclusion initiatives such as identity verification systems, digital wallets, and remittance platforms.

Regulatory sandboxes are not without challenges. Critics argue that they offer limited scale, favour well-funded firms, and risk regulatory capture. The burden of deciding which

[68] Joshua Durham, 'Regulatory Sandboxes Enable Pragmatic Blockchain Regulation' (2023) 18 Washington Journal of Law, Technology & Arts https://ssrn.com/abstract=4342821 accessed 17 March 2025.

 ISSN: 2582-6433

companies qualify for sandbox participation often falls on under-resourced regulatory bodies. Moreover, sandbox participants may operate with perceived legitimacy, even if their products fail outside the test environment. Therefore, sandboxes must be designed to encourage innovation without relaxing oversight or undermining long-term policy goals.

To address these concerns, some jurisdictions have introduced cross-border or thematic sandboxes focused specifically on blockchain or digital assets. For example, the Global Financial Innovation Network (GFIN) promotes multilateral collaboration between sandbox regulators, allowing blockchain firms to test products simultaneously in several countries with aligned compliance benchmarks. This represents an evolution in sandbox design—from national to supranational governance structures tailored for a borderless digital economy.

Ultimately, both geofencing and regulatory sandboxes demonstrate that technology and law are not mutually exclusive but mutually reinforcing. Blockchain geofencing illustrates how technology can enforce legal mandates in real-time, while sandboxes provide legal flexibility to encourage innovation under controlled conditions. These tools collectively reduce jurisdictional conflicts, encourage good faith innovation, and serve as blueprints for a more responsive, technology-integrated legal infrastructure.

Technological Solutions for Legal Compliance

As blockchain technology becomes increasingly embedded in financial and legal infrastructures, new avenues are emerging for leveraging it to enhance legal compliance. One of the most promising developments is the integration of blockchain-based verification systems, which ensure the authenticity and integrity of digital records, automate enforcement through smart contracts, and eliminate the need for centralized enforcement bodies. These solutions mark a shift toward technology-led legal compliance models, particularly in cross-border investment environments where traditional enforcement mechanisms are often inefficient or inaccessible.

Blockchain-based verification involves the use of distributed ledger technology (DLT) to authenticate transactions and maintain tamper-proof records of legal and financial activities. Each block in the chain is cryptographically linked and validated by a consensus mechanism, ensuring that data entered into the system is immutable and traceable. This feature is particularly valuable in regulatory environments where audit trails are required for compliance, such as Know Your Customer (KYC), Anti-Money Laundering (AML), and securities

 ISSN: 2582-6433

regulations. By logging every transaction or event in real-time, blockchain eliminates the possibility of data manipulation and facilitates instant regulatory reporting and auditing.

One of the most significant innovations in legal compliance has been the emergence of smart contracts—self-executing code stored on a blockchain that automatically enforces the terms of an agreement when predefined conditions are met. Smart contracts are considered both automatable and enforceable. Automatable by computer systems—albeit with some parts requiring human oversight—and enforceable either by legal force or through autonomous digital execution[69]. The key benefit is the removal of reliance on third-party enforcers or adjudicators, which is particularly important in cross-border investments where parties are located in different legal jurisdictions.

These smart contracts are increasingly being used to encode complex rights and obligations in financial agreements, token issuance, and regulatory adherence processes. For example, a token offering can be embedded with regulatory restrictions coded into the contract itself, such as eligibility checks for accredited investors or geographic restrictions using blockchain geofencing technologies. In legal contexts, frameworks such as Ricardian Contracts have been proposed, combining legal prose with code and parameters. These create a hybrid model where the contract is both readable by humans and executable by machines, bridging the gap between legal text and automated compliance mechanisms.

Beyond smart contracts, technological platforms have introduced a range of "RegTech" (Regulatory Technology) and "SupTech" (Supervisory Technology) tools that harness blockchain's transparency and security. RegTech applications allow firms to comply with regulation more efficiently through automation, reducing cost and human error. For instance, these tools can automate the generation and submission of compliance reports, conduct real-time monitoring of transaction anomalies, and facilitate risk assessments[70]. On the regulatory side, SupTech enhances the capacity of supervisory bodies to monitor markets by digitizing data collection, pattern analysis, and early-warning systems. Blockchain-based SupTech platforms can help regulators monitor compliance with investment rules, identify patterns of fraud or market manipulation, and ensure greater accountability without increasing

[69] Vitalik Buterin, *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform* (Ethereum Foundation, 2014) https://static.peng37.com/ethereum_whitepaper_laptop_3.pdf accessed 15 March 2025.
[70] Harry Surden, 'Computable Contracts' (2012) 46 *University of California Davis Law Review* 629 https://ssrn.com/abstract=2216866 accessed 16 March 2025.

 ISSN: 2582-6433

administrative burden.

Blockchain identity management is another area where compliance is seeing technological transformation. Traditional KYC processes are cumbersome and often require redundant document submissions across multiple institutions. With blockchain, digital identities can be securely created, stored, and verified by authorized nodes, reducing duplication and enabling seamless identity sharing across platforms. This is especially beneficial in cross-border investments, where consistent identity verification across jurisdictions remains a challenge. Verified digital identities stored on a blockchain can also be linked to wallet addresses, making it easier for regulators to trace ownership and enforce sanctions or tax compliance.

Legal enforcement has also seen advancements through blockchain timestamping and notarization services. These allow parties to record legal documents on the blockchain, creating immutable proof of existence, ownership, and consent. Courts in countries like China, Italy, and the United States have started accepting blockchain-based evidence, signalling a shift in the legal acceptance of technological verification mechanisms. For instance, smart contracts and blockchain logs have been admitted in evidentiary hearings to resolve disputes, especially in IP rights and financial fraud.

But still, challenges remain. The enforceability of smart contracts is still being tested in courts, especially in scenarios where human intervention is needed to interpret ambiguous terms or enforce remedies[71]. Jurisdictional issues also complicate the legal status of blockchain evidence and smart contracts, as legal systems differ in their recognition of digital instruments. Furthermore, decentralization can sometimes obscure accountability—particularly in public, permissionless blockchains—raising questions about whom to hold responsible when things go wrong.

Future Innovations: AI and Blockchain in Investment – Legal Implications and Opportunities

The convergence of artificial intelligence (AI) and blockchain is rapidly redefining the architecture of investment law and its enforcement, particularly in cross-border contexts. While blockchain has already transformed transactional security and transparency in international

[71] Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2019) https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/6C9F1D9312A51D716C3A32E9E524BD0B accessed 17 March 2025.

 ISSN: 2582-6433

finance, the inclusion of AI offers a robust toolset for refining regulatory compliance, dispute resolution, and predictive analysis in investment governance. These two technologies, in tandem, herald a paradigm shift that demands not only technical innovation but also significant legal recalibration.

AI in Investment Law Enforcement and Monitoring

AI's potential to support investment law enforcement lies in its ability to automate regulatory oversight and enhance the responsiveness of governance frameworks. AI systems can detect patterns of non-compliance, simulate policy outcomes, and even assist regulators in designing risk-based enforcement models. For example, AI-driven tools could analyse thousands of investment contracts or investor-state arbitration filings to identify clauses that frequently result in disputes or investor claims. This could empower regulatory authorities and investment tribunals to pre-emptively flag red-flagged practices and improve policy outcomes[72].

Additionally, AI can significantly optimize stakeholder engagement. Natural language processing (NLP) models can process vast volumes of public comments during bilateral or multilateral treaty renegotiations, summarizing sentiments and clustering similar arguments for legal review. This capability can streamline the consultation process in investment treaty reform, especially where investor protection intersects with public interest. Similarly, predictive analytics can help identify jurisdictions where regulatory gaps are likely to be exploited, enabling proactive rulemaking.

Importantly, AI can help maintain institutional memory in regulatory bodies. By capturing the tacit knowledge of retiring experts and converting it into decision-support systems, AI enables continuity in interpreting complex investment frameworks. As the Deloitte framework notes, these models can even assist in generating first drafts of regulatory decisions, improving both speed and accuracy without removing human discretion.

Blockchain's Role in Investment Transparency and Dispute Resolution

Blockchain technology's application to investment is no longer speculative. Smart contracts and decentralized autonomous organizations (DAOs), as highlighted in the Ethereum Whitepaper, represent programmable legal structures that can self-execute based on preset

[72] Deloitte Center for Government Insights, 'AI Can Turbocharge Government Regulatory Operations' (16 November 2023) https://www2.deloitte.com/content/dam/insights/articles/us176850_cgi-gen-ai-series-chapter4-ai-enabled-regulator/DI_CGI_Gen-AI-series-chapter4-AI-enabled-regulator.pdf accessed 15 March 2025.

 ISSN: 2582-6433

conditions. In a cross-border investment context, such contracts can reduce reliance on local enforcement mechanisms, especially in jurisdictions with weak rule of law. For instance, an investor-state contract embedded on a blockchain could release funds based on fulfillment of environmental or human rights obligations, monitored via IoT sensors and validated by independent AI models.

Also, the immutability and transparency of blockchain make it an ideal tool for dispute prevention. By providing tamper-proof audit trails of all investor-state interactions, blockchain records can serve as critical evidence in arbitration. This reduces reliance on oral testimonies and non-uniform documentation, improving legal certainty. In international investment law, where disputes often revolve around facts and procedural inconsistencies, blockchain-stored records can significantly enhance evidentiary reliability.

Another innovation lies in tokenization of assets and investments. Blockchain-based tokens representing shares, debt, or real estate allow for fractional ownership, expanding access to investment opportunities globally. However, this innovation also poses legal questions regarding jurisdiction, investor classification, and cross-border enforcement. Regulatory bodies will need to revise securities law definitions and jurisdictional rules to accommodate digital tokens, especially those issued across multiple legal systems.

Synergies and Legal Innovations: AI and Blockchain

The real breakthrough emerges when AI and blockchain are integrated. AI can monitor blockchain-based investment transactions for compliance in real-time, flagging anomalies that deviate from legal norms. Conversely, blockchain can ensure the integrity of AI training data and decision outputs by recording them on an immutable ledger. This is especially useful in regulatory sandboxes, where experimental legal frameworks are tested on fintech products.

For example, a cross-border investment platform could use blockchain to manage investor identity, investment flows, and contract execution, while AI assesses risk profiles, recommends dispute resolution pathways, or even drafts arbitration submissions. Such hybrid systems demand new legal standards for liability—who is accountable when an AI-model misclassifies risk or a smart contract fails to execute properly?

Moreover, legal frameworks must evolve to ensure that AI and blockchain adhere to principles of fairness, transparency, and proportionality. The Deloitte report proposes six dimensions of

 ISSN: 2582-6433

trustworthy AI—including fairness, transparency, and privacy—which must guide the deployment of AI in investment enforcement. Without such safeguards, technological enforcement could replicate or exacerbate existing biases in investment adjudication.

Chapter 10: Adaptation of Legal Frameworks and Policy Recommendations

How Existing Legal Instruments Can Be Adapted

The rapid development of blockchain technology has outpaced the evolution of traditional legal instruments, particularly in the realm of cross-border investment. Bilateral Investment Treaties (BITs), WTO regulations, and UNCITRAL guidelines were designed in an era where the physical presence of investors, identifiable entities, and centralized records formed the basis of legal and commercial frameworks. As blockchain introduces decentralization, pseudonymity,

 ISSN: 2582-6433

and immutability, existing legal tools require recalibration rather than wholesale replacement to maintain relevance in this digital investment ecosystem.

Reforming Bilateral Investment Treaties (BITs)

BITs form the backbone of international investment law, offering protections such as fair and equitable treatment, protection against expropriation, and access to investor-state dispute settlement mechanisms. However, they assume the presence of identifiable investors and tangible investments, which contrasts sharply with blockchain-enabled investment forms such as tokenized assets, smart contract-based transactions, and decentralized autonomous organizations (DAOs). To adapt, BITs must broaden their definitions of "investment" to include digital assets and virtual tokens that have economic value and contribute to capital formation[73]. Furthermore, the term "investor" should be modernized to encompass decentralized entities and pseudonymous participants, provided that adequate mechanisms exist to verify beneficial ownership or economic control through technical means such as cryptographic keys or digital ID systems.

Additionally, dispute resolution clauses in BITs often depend on identifying the state of incorporation or the nationality of the investor. Given blockchain's borderless nature, reliance solely on territorial incorporation fails to capture the realities of decentralized investment. BITs could adopt functional criteria such as the location of project impact, the place of blockchain node majority, or the governing law embedded in smart contracts to establish jurisdiction and eligibility for treaty protections.

Adapting WTO Frameworks

The World Trade Organization (WTO) governs a wide array of multilateral trade relationships through agreements that rely on member state obligations and non-discriminatory treatment. Blockchain, especially through smart contracts and decentralized marketplaces, introduces new forms of trade and service delivery that challenge the traditional categorization of goods, services, and modes of supply under WTO rules. The General Agreement on Trade in Services (GATS) must evolve to incorporate digital services executed entirely through code without human intermediaries. For instance, the concept of "mode 1" (cross-border supply) in GATS

[73] Rodrigo Polanco, 'The Impact of Digitalization on International Investment Law: Are Investment Treaties Analogue or Digital?' (2023) 24 German Law Journal 574 https://doi.org/10.1017/glj.2023.30 accessed 23 March 2025.

 ISSN: 2582-6433

could be clarified to include services deployed via decentralized platforms or blockchain protocols, where the supplier may not reside in a defined jurisdiction.

Moreover, blockchain technology could serve as a compliance tool within WTO disciplines. Smart contracts could be used to automate adherence to WTO technical standards or rules of origin, enabling real-time verification and reducing transaction costs. However, for such adaptation to occur, WTO member states must agree on interoperability standards and recognize blockchain-generated records as valid documentation within trade processes[74].

Reinterpreting UNCITRAL Instruments

The United Nations Commission on International Trade Law (UNCITRAL) has pioneered harmonization efforts through model laws and conventions, particularly in areas such as electronic commerce, arbitration, and secured transactions. While UNCITRAL's existing instruments already show a degree of technological neutrality, their application to blockchain systems necessitates interpretive guidance or supplementary protocols.

For example, UNCITRAL's Model Law on Electronic Commerce supports the legal recognition of data messages and electronic signatures. This provides a foundation for recognizing blockchain-based transactions and smart contracts as legally enforceable, especially where public key infrastructure and hash functions satisfy functional equivalence requirements[75]. However, blockchain introduces immutable and self-executing features that exceed the capabilities of traditional electronic records. Legal reforms should clarify how obligations embedded in smart contracts can be enforced or overridden in cases of fraud, duress, or public policy considerations, which are traditionally reserved for human adjudication[76].

Another area of reform involves UNCITRAL's work on investor-state dispute settlement (ISDS). With blockchain reducing the need for centralized arbitration institutions, the emergence of on-chain dispute resolution mechanisms poses questions about procedural

[74] **WTO and Blockchain Trade Facilitation**, *Blockchain and the WTO: Implications for Trade Rules* (2022) https://example.org/wto-blockchain-analysis.pdf accessed 24 March 2025
[75] United Nations Commission on International Trade Law, *Modernizing International Trade Law to Support Innovation and Sustainable Development: Proceedings of the Congress* (Vienna, 4–6 July 2017) https://ssrn.com/abstract=3566691 accessed 22 March 2025
[76] **UNCITRAL, Blockchain and Investment Law**
Koji Takahashi, 'Implications of the Blockchain Technology for the UNCITRAL Works' in *UNCITRAL Congress Volume 4* (2017) https://ssrn.com/abstract=3566691 accessed 23 March 2025

 ISSN: 2582-6433

fairness and enforceability. UNCITRAL could explore hybrid mechanisms where blockchain-based adjudication is recognized under the New York Convention, provided it meets minimum standards of due process and neutrality.

Institutional and Procedural Considerations

In addition to doctrinal reforms, there is a need to recalibrate institutional procedures to accommodate blockchain. Investment treaties and trade agreements must account for the decentralized nature of digital asset issuance, where no single party may have control over the platform. Regulatory sandboxes and experimental pilot regimes can be used to test legal adaptation without the full-scale commitment to rigid rules. Similarly, digital identity systems and legal entity identifier frameworks must be updated to align with the pseudonymous nature of blockchain transactions, balancing privacy with accountability.

Moreover, the principles of technological neutrality and legal certainty must guide these adaptations. Legal frameworks should avoid being overly prescriptive about specific technologies, instead focusing on functional outcomes, such as the ability to verify identity, validate transactions, and resolve disputes[77]. This allows for flexibility as blockchain architectures evolve, including developments like zero-knowledge proofs, layer-2 protocols, and cross-chain interoperability.

Policy Recommendations for Governments and Regulators

As blockchain technology continues to evolve and become embedded in cross-border investment practices, national governments and international regulatory bodies must proactively adopt coherent and forward-looking policy frameworks. A balanced approach is required—one that fosters innovation while addressing regulatory, economic, and jurisdictional concerns. The decentralized nature of blockchain, coupled with its potential to disrupt traditional models of financial intermediation, calls for adaptive regulatory tools, enhanced cooperation between states, and alignment with global legal norms. This section outlines key policy recommendations and best practices that regulators can employ to effectively integrate blockchain into the existing legal and economic architecture.

Embrace Technological Neutrality and Principle-Based Regulation

[77] Usha Rodrigues, *Law and the Blockchain* (Iowa Law Review, 2018) https://ssrn.com/abstract=3191766 accessed 23 March 2025

 ISSN: 2582-6433

Governments should adopt a technology-neutral stance, regulating outcomes rather than the technology itself. Prescriptive or overly specific regulations may become obsolete as blockchain evolves. Instead, regulators should focus on principle-based frameworks that emphasize investor protection, transparency, accountability, and systemic stability. For instance, regulations can require that any investment platform, whether centralized or decentralized, must ensure traceability of transactions, compliance with anti-money laundering standards, and availability of dispute resolution mechanisms—regardless of whether the underlying infrastructure uses blockchain or conventional databases.

Technological neutrality also ensures flexibility for new innovations such as zero-knowledge proofs, sidechains, and cross-chain interoperability, which may not be anticipated under rigid laws. Legal frameworks should be designed with modularity, allowing integration with emerging technologies without significant legislative overhaul.

Strengthen Legal Recognition of Blockchain-Based Transactions

Legal certainty is paramount in attracting investment and fostering trust. Regulators should ensure that blockchain-based transactions, smart contracts, and tokenized assets are recognized under domestic commercial law. This includes amending existing statutes on contracts, property, and securities to accommodate digital equivalents[78]. Where possible, smart contracts should be deemed enforceable provided they satisfy essential legal requirements such as offer, acceptance, consideration, and intention to create legal relations.

Additionally, national legislation should include provisions that facilitate the use of distributed ledger technologies for maintaining corporate records, notarization, and trade documentation. Ensuring the legal validity of cryptographic signatures and time-stamped blockchain entries can significantly streamline commercial processes and lower transaction costs.

Establish Regulatory Sandboxes and Innovation Hubs

To encourage responsible experimentation, governments should establish regulatory sandboxes that allow blockchain startups and investment platforms to operate under relaxed regulatory conditions for a defined period. These sandboxes provide a controlled environment to test new business models without compromising consumer protection or systemic integrity.

[78]*United Nations Conference on Trade and Development, Harnessing Blockchain Technologies for Sustainable Development: Prospects and Challenges (2021)* https://unctad.org/system/files/official-document/ecn162021d3_en.pdf *accessed 23 March 2025.*

 ISSN: 2582-6433

Regulators can use insights from such pilots to refine policy approaches, identify regulatory gaps, and develop risk-based oversight mechanisms.

Alongside sandboxes, innovation hubs should be created within financial regulatory authorities to serve as points of contact for technology firms. These hubs can facilitate dialogue, clarify regulatory expectations, and disseminate best practices in blockchain governance.

Develop Interoperable and Globally Aligned Standards

Given the inherently cross-border nature of blockchain transactions, policy harmonization is essential. Fragmented regulatory responses increase compliance costs and introduce legal uncertainty, deterring international investment. Governments should therefore collaborate through regional and international forums to align legal definitions, licensing requirements, and compliance protocols. Standardization bodies such as the International Organization for Standardization (ISO) and UNCITRAL should be supported in developing shared terminologies and frameworks for blockchain-based investment activities.

Moreover, interoperability of digital identity systems, transaction monitoring tools, and regulatory reporting interfaces must be prioritized. Public-private partnerships can be instrumental in designing technical standards that balance security, privacy, and regulatory needs. For instance, regulators should encourage the development of blockchain protocols that allow selective disclosure of transaction data to authorized authorities, thereby meeting compliance requirements without undermining decentralization[79].

Address Financial Integrity Risks: AML/CFT and Data Governance

Blockchain technologies present challenges and opportunities in anti-money laundering (AML) and combating the financing of terrorism (CFT). On one hand, public blockchains offer traceability through immutable records. On the other, the use of privacy-enhancing technologies and unhosted wallets can hinder transaction monitoring. Governments should implement FATF-compliant regulations for Virtual Asset Service Providers (VASPs), ensuring they conduct customer due diligence, report suspicious activities, and comply with the “travel rule” for fund transfers.

[79] Organisation for Economic Co-operation and Development, *Regulatory Sandboxes in Artificial Intelligence* (2023) https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf accessed 22 March 2025.

 ISSN: 2582-6433

To address privacy and data protection concerns, policy frameworks must clarify the application of existing data protection laws to blockchain environments. Since data stored on-chain is typically immutable, regulators should provide guidance on how to comply with rights such as data erasure and correction. Encouraging the use of off-chain storage for personal data and on-chain pointers or hashes can be one way to reconcile blockchain's technical features with legal obligations.

Promote Public Sector Adoption and Capacity Building

Governments should lead by example in adopting blockchain for public administration, especially in areas such as customs, public procurement, land registries, and digital identity. Such initiatives can improve efficiency, transparency, and accountability while familiarizing government agencies with blockchain systems. In the investment domain, using blockchain for issuing sovereign bonds or maintaining public securities registries can help build trust in digital finance.

Capacity building among regulators, policymakers, and judicial officers is equally important. Training programs, knowledge exchanges, and joint task forces involving technical and legal experts will equip public institutions to better assess and respond to blockchain-related developments.

Ensure Inclusivity and Support for Emerging Economies

Policymakers must ensure that blockchain regulation supports the participation of small and medium-sized enterprises (SMEs), investors from developing countries, and underserved communities. Excessive compliance burdens may exclude legitimate participants from accessing cross-border capital or financial infrastructure. Tiered regulatory models based on risk exposure can allow micro-investment platforms or community-based DAOs to operate with lighter regulatory requirements, subject to certain thresholds.

International development institutions should provide technical assistance and funding to help emerging economies adopt blockchain infrastructure in line with global standards. This would ensure that developing countries are not left behind in the blockchain-driven transformation of international investment.

Towards a Harmonized Blockchain Investment Law

 ISSN: 2582-6433

The emergence of blockchain has precipitated one of the most profound disruptions to legal systems, economic governance, and regulatory models in the context of cross-border investment. It has forced a reconsideration of how law interacts with technology—particularly in domains traditionally defined by physical presence, legal identity, and jurisdictional certainty. Throughout this research, it has become evident that the core challenge of integrating blockchain into cross-border investment law lies not in the absence of legal principles, but in their structural incompatibility with decentralised, pseudonymous, and globally distributed technologies.

The decentralised nature of blockchain—manifested through smart contracts, DAOs, and tokenised assets—dismantles the assumptions that underpin traditional legal frameworks. Jurisdictional doctrines built on territorial anchors fail to address the reality of transactions executed by code across a global network of nodes. Legal identity, once tied to corporate registration and nationality, becomes elusive when participants interact pseudonymously. This transformation necessitates a shift from static legal categorisations to dynamic, functional legal adaptations.

Jurisdictional incoherence remains a central problem. Whether examining the formation and enforcement of smart contracts, the treatment of DAOs, or the application of investment protection under bilateral treaties, the inability to determine which law governs and which court has competence has destabilised legal predictability. Smart contracts, while offering efficiency and automation, challenge traditional doctrines of offer, acceptance, and intention. Dispute resolution mechanisms are strained, especially when national courts are ill-equipped to interpret code or enforce blockchain-native rulings.

Efforts to resolve jurisdictional fragmentation must begin with reconceptualising investment law to accommodate blockchain's non-territorial nature. Legal instruments such as BITs, WTO frameworks, and UNCITRAL guidelines can be incrementally reformed. BITs must redefine investment to include digital and tokenised forms, and WTO agreements must expand the definition of trade in services to incorporate algorithmically executed interactions. UNCITRAL's work on digital commerce offers a valuable template, but it requires expansion to address automated enforcement, blockchain governance, and transnational smart contracts. Importantly, the incorporation of blockchain into these frameworks must be guided by principles of legal certainty, investor protection, and technological neutrality.

 ISSN: 2582-6433

Parallel to jurisdictional reform is the imperative for regulatory modernization. Governments and international bodies must adopt adaptive and principle-based policy frameworks that encourage innovation without compromising financial integrity or investor safety. Regulatory sandboxes and geofencing technologies are examples of tools that balance experimentation with oversight. Blockchain geofencing, although technically limited by pseudonymity, serves as a digital analogue to jurisdictional boundaries and provides a preliminary form of regulatory compliance. Meanwhile, regulatory sandboxes have proven essential in allowing blockchain ventures to develop under guided supervision, particularly in jurisdictions with emerging fintech ecosystems.

Investor protection, often an overlooked casualty in the race to innovate, must be reinforced. As documented in numerous jurisdictions, the lack of coherent classification for digital assets, absence of disclosures, and reliance on pseudonymous actors have exposed retail investors to fraud, scams, and opaque risks. This research has highlighted how projects exploit legal ambiguities to operate in regulatory vacuums. Therefore, international cooperation is vital to establish common definitions, disclosure obligations, and licensing requirements. Policymakers must move toward harmonized standards under frameworks like FATF's Recommendation 15, EU's MiCA, or OECD's CARF—ensuring cross-border regulatory convergence.

Data localization presents another formidable challenge. The demand by states to control data flows and impose localization laws collides with the decentralized architecture of blockchain. The GDPR, China's Cybersecurity Law, and India's DPDP regime reveal the friction between blockchain's distributed ledgers and national data sovereignty. As explored, blockchain systems cannot be easily confined within national borders without undermining their core functionalities. Consequently, any harmonization must be based on mutual recognition mechanisms, such as interoperability standards, instead of hard localization mandates.

Taxation of blockchain assets adds yet another layer of jurisdictional complexity. From the United States' property-based approach to India's flat-rate taxation regime, divergent national practices have created a fragmented landscape that encourages regulatory arbitrage. The classification of assets—as utility tokens, securities, or commodities—remains jurisdiction-specific and inconsistently applied. Initiatives like the OECD's CARF and EU's DAC8 represent crucial steps in global reporting and transparency. However, tax enforcement remains difficult in decentralized finance (DeFi) environments where peer-to-peer transactions occur

 ISSN: 2582-6433

without intermediaries. Here, blockchain's own transparency features—such as immutable audit trails—could be leveraged to aid compliance through RegTech and SupTech tools.

Dispute resolution mechanisms must also evolve. Traditional arbitration remains robust and enforceable through the New York Convention, but it is increasingly misaligned with blockchain-native transactions. Decentralised Dispute Resolution (DDR) platforms such as Kleros and Aragon provide experimental alternatives, yet they face legitimacy and enforceability constraints in formal legal systems. Hybrid models—combining smart contracts with arbitration clauses—offer a middle path, ensuring that technology-enhanced enforcement remains legally grounded. To support this evolution, international arbitration institutions must adapt procedural rules and model clauses for blockchain contexts, and courts must develop technical literacy to interpret code-based agreements.

Technology itself offers solutions to many of the legal challenges posed by blockchain. Tools such as blockchain-based identity verification, timestamping, and smart legal contracts blur the divide between law and code. They enable real-time compliance, automate enforcement, and reduce dependency on human intermediaries. Regulatory agencies can harness SupTech platforms for market surveillance, risk profiling, and fraud detection, especially in cross-border scenarios where traditional reporting fails. The integration of AI into compliance and monitoring further enhances the capacity of legal systems to adapt to dynamic blockchain environments.

Ultimately, the harmonisation of blockchain investment law requires a multipronged approach. First, legal definitions must be modernised to reflect digital realities. Second, jurisdictional principles must be rethought to accommodate non-territoriality. Third, policy frameworks must incentivise innovation while preserving regulatory coherence. And fourth, international coordination must replace fragmented national regimes with interoperable standards for taxation, data governance, and investor protection.

The future of cross-border investment depends not on rejecting blockchain’s decentralised potential, but on designing legal architectures that are resilient, flexible, and adaptive. Law and blockchain are not adversaries; they are co-constructors of a new global order. The responsibility lies with legislators, regulators, technologists, and scholars to bridge this divide, ensuring that blockchain’s promise of trustless innovation is not undermined by legal uncertainty—but enabled by legal clarity.

 ISSN: 2582-6433

LITERATURE REVIEW

I. Blockchain Technology and Legal Adaptation

1. **Georgios Dimitropoulos, 'The Law of Blockchain' (2020)**
    - Findings: Outlines how blockchain challenges conventional legal categories in commercial and public law. Proposes adaptive legal mechanisms to resolve jurisdictional ambiguity.
    - Relevance: Supports the foundational framework for adapting existing legal infrastructure to decentralized environments.
2. **Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (2018)**
    - Findings: Discusses how blockchain rewrites legal relationships using code. Suggests law should evolve in parallel with these techno-legal constructs.
    - Relevance: Helps contextualize smart contracts and DAOs as quasi-legal agents.
3. **Maria Kremer and Giacomo Orsini, 'Investor–State Dispute Settlement in the Era of Crypto Assets' (2024)**

 ISSN: 2582-6433

- Findings: Argues that traditional investment law is insufficient for blockchain disputes due to its borderless nature.
- Relevance: Directly informs jurisdictional issues in cross-border blockchain investments.

II. Smart Contracts and International Arbitration

4. **Nova University Lisbon, 'The Role of International Arbitration in Smart Contract Disputes' (2023)**
   - Findings: Reviews doctrinal gaps in arbitral frameworks when applied to smart contracts.
   - Relevance: Bridges technology with enforcement via international arbitration mechanisms.
5. **Ibrahim Shehata, 'Smart Contracts & International Arbitration' (2018)**
   - Findings: Evaluates enforceability of smart contracts through UNCITRAL and New York Convention standards.
   - Relevance: Forms the doctrinal base for dispute resolution models in blockchain commerce.
6. **Robert Walters, 'Smart Contracts and International Commercial Arbitration' (2025)**
   - Findings: Discusses automation's impact on arbitral procedure and transparency.
   - Relevance: Important for evaluating future institutional reforms.

III. Jurisdiction and Private International Law

7. **University of Hong Kong – Law Faculty, 'Comparing Private International Law Approaches to Blockchain Regulation' (2024)**
   - Findings: Compares EU, US, and Asian approaches on blockchain conflict rules.

 ISSN: 2582-6433

- Relevance: Informs comparative analysis of jurisdiction.

8. **Brill Open Access, 'Blockchain and Private International Law' (2023)**
    - Findings: Proposes model law for dealing with blockchain's jurisdictional opacity.
    - Relevance: Core reference for Chapter 4 of the dissertation.
9. **Iris H.Y. Chiu, 'Jurisdictional Arbitrage' (2022)**
    - Findings: Highlights regulatory shopping by blockchain entities.
    - Relevance: Critical to understanding blockchain's regulatory evasion tactics.

IV. Cross-Border Data and Digital Asset Regulation

10. **OECD, Data Free Flow with Trust (2020)**
    - Findings: Calls for interoperable cross-border frameworks to regulate blockchain data flows.
    - Relevance: Provides support for WTO law reform in Chapter 10.
11. **Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet' (2015)**
    - Findings: Reviews extraterritorial enforcement of data laws.
    - Relevance: Applicable to blockchain's pseudonymous and stateless architecture.
12. **SEC, Framework for "Investment Contract" Analysis of Digital Assets (2019)**
    - Findings: Applies Howey test to crypto assets.
    - Relevance: Forms basis for token classification in investment law.

 ISSN: 2582-6433

BIBLIOGRAPHY

Books

- De Filippi, Primavera and Aaron Wright. *Blockchain and the Law: The Rule of Code*. Harvard University Press, 2018.
- Michèle Finck, *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2019.
- Walters, Robert. *Handbook on Transnational Commercial Law*. Routledge, 2025.

Journal Articles

- Dimitropoulos, Georgios, 'The Law of Blockchain' (2020) 95 *Washington Law Review* 1117.
- Kremer, Maria and Orsini, Giacomo, 'Investor–State Dispute Settlement in the Era of Crypto Assets' (2024) *ICSID Review – Foreign Investment Law Journal*.
- Chiu, Iris HY, 'Jurisdictional Arbitrage' (2022) *Journal of Financial Regulation and Compliance*.
- Vadi, Valentina, 'Investments in the Digital Era' (2023) 24 *Business Law International* 135.
- McKinney, Scott A, Rachel Landy and Rachel Wilka, 'Smart Contracts, Blockchain,

 ISSN: 2582-6433

and Transactional Law' (2018) 13(3) *Washington Journal of Law, Technology & Arts* 313.

- Ahmed Abdulkhudhur Jasim et al., 'Enforcement of Smart Contracts in Cross-Jurisdictional Transactions' (2024) *International Journal of Law and Management*.
- Niriella, MADSJS, 'Role of Smart Contract in Arbitration: A Critical Analysis' (2024) 1(2) *International Journal of Juridical Studies and Research Sciences*.
- Kathuria, Vikas and Basheerhussain Miniya, 'From Smart Legal Contracts to Contracts on Blockchain' (2024) *Computer Law & Security Review* 106035.

Working Papers & Reports

- OECD, *Data Free Flow with Trust* (2020).
- FATF, *Guidance for a Risk-Based Approach to Virtual Assets and VASPs* (2019, 2021).
- Brookings Institution, Joshua Meltzer, *WTO Reform Agenda: Data Flows and Regulatory Cooperation* (2019).
- Deloitte, *AI Can Turbocharge Government Regulatory Operations* (2023).
- United Nations Commission on International Trade Law, *Modernizing International Trade Law* (2017).

Online Resources and White Papers

- Buterin, Vitalik. *Ethereum Whitepaper* (Ethereum Foundation, 2014).
- Acronis, *Data Sovereignty Around the World* (White Paper, 2023).
- Reserve Bank of India, 'Storage of Payment System Data' Notification (2018).
- SEC, *Framework for Investment Contract Analysis of Digital Assets* (2019).
- Organisation for Economic Co-operation and Development, *Regulatory Sandboxes in Artificial Intelligence* (2023).