Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Illicit Use, Legitimacy, and Adoption of Cryptocurrencies: An Integrative Risk–Legitimacy Framework

Mohammed Junaid Rizvi[1], Dr. Asad Ahmad[2]

[1]Research Scholar, Department Of Management, School of Management & Business Studies, Jamia hamdarad University, New Delhi
[2]Assistant professor, Department Of Management, School of Management & Business Studies, Jamia hamdarad University, New Delhi

Abstract

Cryptocurrencies have evolved from niche technological innovations into globally traded financial instruments, prompting growing interest from consumers, firms, and governments. Alongside this expansion, persistent concerns regarding illicit, unethical, and high-risk uses—such as money laundering, ransomware, market manipulation, and regulatory arbitrage—have shaped public discourse and policy responses. While empirical evidence suggests that such activities constitute a minority share of overall cryptocurrency usage, their visibility and symbolic impact have exerted a disproportionate influence on trust, regulation, and adoption outcomes.

This study examines how illicit and high-risk cryptocurrency use affects adoption through legitimacy mechanisms rather than direct economic prevalence. Drawing on interdisciplinary literature from finance, economics, information systems, and regulatory studies, the paper synthesizes empirical findings on misuse prevalence, analyzes cross-country regulatory responses, and evaluates stakeholder-specific adoption dynamics. Building on this synthesis, the study develops an integrative **Risk–Legitimacy–Adoption framework** that explains how misuse-related risks are mediated by regulatory responses and legitimacy perceptions to shape adoption across retail, institutional, and governmental contexts.

The findings demonstrate that effective, proportionate regulation can mitigate legitimacy erosion and support sustainable adoption, whereas inconsistent or overly restrictive approaches may exacerbate distrust and institutional hesitation. By reframing the relationship between cryptocurrency misuse and adoption, this study contributes to theory on financial innovation adoption, informs evidence-based regulatory design, and provides a foundation for future empirical research on digital financial governance.

1: INTRODUCTION AND RESEARCH MOTIVATION

1.1 Background and Context

Over the past decade, cryptocurrencies have transitioned from a fringe technological experiment to a globally traded financial phenomenon with growing relevance for consumers, firms, and governments. Initially conceptualized as decentralized digital currencies operating outside traditional financial intermediaries, cryptocurrencies now underpin a rapidly expanding ecosystem of exchanges, payment services, decentralized finance (DeFi) platforms, and tokenized assets. Their adoption has been driven by promises of efficiency, financial inclusion, censorship resistance, and innovation in value transfer mechanisms (Böhme et al., 2015).

At the same time, the expansion of cryptocurrency markets has been accompanied by persistent concerns regarding their misuse for illicit, unethical, and regulatory-evasive activities. High-profile incidents involving ransomware payments, darknet marketplaces, fraud, tax evasion, and market manipulation have positioned cryptocurrencies at the center of debates surrounding financial crime, regulatory oversight, and systemic risk. This dual character—simultaneously enabling innovation and facilitating misuse—has created a legitimacy paradox that continues to shape public discourse and policy responses worldwide.

Importantly, while cryptocurrencies are often portrayed in popular narratives as predominantly associated with illegal activities, empirical research presents a more nuanced picture. Studies suggest that illicit usage represents a minority share of overall cryptocurrency transactions, yet the *visibility and impact* of such activities exert a disproportionate influence on trust, regulation, and institutional adoption (Foley et al., 2019). This asymmetry between actual prevalence and perceived risk underscores the need for a rigorous academic examination of what may be described as the "dark side" of cryptocurrency ecosystems.

1.2 The Problem of the "Dark Side" in Cryptocurrency Adoption

The concept of a technological "dark side" is not new in management and information systems literature. Technologies that promise efficiency and empowerment frequently generate unintended consequences, externalities, and misuse that challenge their long-term legitimacy. In the context of cryptocurrencies, these darker dimensions manifest through multiple channels: facilitation of illicit finance, exploitation of regulatory gaps, manipulation of largely unregulated markets, and environmental and social externalities arising from energy-intensive consensus mechanisms.

These issues are not merely ethical or legal concerns; they carry material implications for adoption trajectories. Institutional investors, multinational corporations, and governments increasingly assess cryptocurrencies through the lenses of compliance, reputational risk, and governance compatibility. Regulatory bodies, in turn, face the challenge of mitigating misuse without stifling innovation or undermining the potential benefits of decentralized financial systems.

Despite a growing body of literature addressing specific aspects of cryptocurrency misuse—such as money laundering, ransomware, or market manipulation—existing research remains fragmented. Many studies focus narrowly on isolated phenomena, while others adopt a legal or technical perspective that does not adequately connect misuse to broader adoption outcomes. Consequently, there is limited

integrative understanding of how the darker uses of cryptocurrencies interact with regulatory responses and shape their acceptance within mainstream financial systems.

1.3 Research Gap and Motivation

Three critical gaps in the extant literature motivate this study.

First, prior research has largely examined illicit cryptocurrency use in isolation, without systematically situating it within the broader adoption and legitimacy discourse. While empirical evidence on criminal activity exists (e.g., Foley et al., 2019), its implications for investor confidence, corporate participation, and policy design are often assumed rather than explicitly theorized.

Second, regulatory analyses frequently emphasize compliance mechanisms and enforcement outcomes but pay insufficient attention to how regulatory actions themselves influence adoption incentives across different stakeholder groups. The interplay between misuse, regulation, and adoption remains underexplored in an integrated framework.

Third, there is a paucity of conceptual models that synthesize technological, institutional, and socio-economic dimensions of cryptocurrency misuse. Without such integrative perspectives, both academic research and policy debates risk remaining reactive and fragmented.

Addressing these gaps is increasingly urgent as cryptocurrencies move beyond early adopters toward wider retail and institutional integration, particularly in emerging economies where regulatory capacities and financial infrastructures vary significantly.

1.4 Research Objectives

In response to the identified gaps, this paper seeks to achieve the following objectives:

1. To systematically conceptualize the primary forms of illicit, unethical, and regulatory-evasive cryptocurrency use identified in prior academic literature.
2. To examine empirical evidence on the scale and characteristics of these activities and distinguish perception-driven narratives from data-driven realities.
3. To analyze how the darker dimensions of cryptocurrency usage influence regulatory responses and adoption decisions across institutional, corporate, and individual actors.
4. To develop an integrative conceptual framework linking misuse-related risks, legitimacy perceptions, regulatory interventions, and adoption outcomes.

1.5 Contributions of the Study

This study makes four explicit contributions to the literature.

First, it advances a structured and theory-informed categorization of the “dark side” of cryptocurrencies, moving beyond anecdotal or sensational accounts toward analytically grounded classifications.

Second, it synthesizes empirical findings from economics, finance, and information systems research to clarify the actual prevalence and impact of illicit cryptocurrency use, thereby addressing persistent misconceptions in both academic and public discourse.

Third, the study bridges the gap between misuse-focused research and adoption studies by explicitly theorizing how illicit and gray-area uses affect trust, legitimacy, and regulatory acceptance.

Fourth, it proposes an original conceptual framework that integrates risk, legitimacy, and adoption dynamics, offering a foundation for future empirical research and informing policy and managerial decision-making.

2: CONCEPTUALIZING THE "DARK SIDE" OF CRYPTOCURRENCY

2.1 Understanding the "Dark Side" of Digital Financial Technologies

In management and information systems research, the "dark side" of technology refers to unintended, adverse, or exploitative outcomes that emerge alongside technological innovation. Such outcomes may arise due to design features, governance gaps, behavioral incentives, or institutional misalignment. Cryptocurrencies, as decentralized digital financial instruments, exhibit several structural characteristics—pseudonymity, borderless transferability, programmability, and limited centralized oversight—that simultaneously enable innovation and create opportunities for misuse.

Importantly, the dark side of cryptocurrencies should not be equated with illegality alone. Rather, it encompasses a spectrum of activities ranging from explicitly criminal conduct to ethically ambiguous and legally gray practices that challenge existing regulatory frameworks. This broader conceptualization allows for a more balanced and analytically rigorous assessment of risks associated with cryptocurrency adoption.

2.2 A Typology of Cryptocurrency Misuse

Drawing on interdisciplinary literature from economics, finance, criminology, and information systems, this study conceptualizes the dark side of cryptocurrency usage across six primary categories. These categories are analytically distinct yet often interrelated in practice.

2.2.1 Illicit Financial Transactions and Money Laundering

One of the earliest and most widely studied concerns surrounding cryptocurrencies is their use in facilitating illicit financial flows. Due to their pseudonymous nature and the absence of traditional financial intermediaries, cryptocurrencies have been used to obscure transaction trails, thereby complicating anti-money laundering (AML) and counter-terrorist financing (CTF) efforts.

Empirical evidence suggests that cryptocurrencies have been employed in laundering proceeds from drug trafficking, cybercrime, fraud, and other criminal activities. However, contrary to popular narratives, large-scale empirical analyses indicate that illicit transactions constitute a minority share of total cryptocurrency activity (Foley et al., 2019). Nevertheless, the *impact* of such activities on regulatory perception and enforcement priorities remains substantial.

2.2.2 Darknet Marketplaces and Illegal Trade

Cryptocurrencies have played a central role in enabling transactions on darknet marketplaces, where goods and services prohibited under conventional legal systems—such as narcotics, counterfeit

documents, and illegal digital services—are exchanged. Bitcoin initially served as the dominant medium of exchange on these platforms, although privacy-enhancing cryptocurrencies have gained prominence over time.

Research examining the shutdown of major darknet markets demonstrates that enforcement actions often displace, rather than eliminate, illicit trade, with actors migrating to alternative platforms or currencies (Van Wegberg et al., 2018). This persistence highlights the adaptability of illicit actors within decentralized ecosystems.

2.2.3 Ransomware, Cybercrime, and Extortion

The rise of ransomware attacks represents one of the most visible intersections between cryptocurrencies and cybercrime. Cryptocurrencies enable attackers to demand payments that are difficult to trace, irreversible once executed, and transferable across jurisdictions without reliance on formal banking systems.

Studies indicate a strong association between the growth of ransomware incidents and cryptocurrency market expansion, particularly during periods of high price volatility and increased public awareness (Conti et al., 2018). This association has contributed significantly to negative perceptions of cryptocurrencies among policymakers and corporate stakeholders, even when such activities account for a small proportion of overall usage.

2.2.4 Tax Evasion and Regulatory Arbitrage

Beyond overt criminal activity, cryptocurrencies have been used to engage in tax evasion, capital flight, and regulatory arbitrage. Individuals and firms may exploit inconsistencies in national tax regimes, reporting standards, and enforcement capacities to conceal income or assets held in digital form.

While not inherently illegal in all jurisdictions, such practices undermine fiscal transparency and erode trust between regulators and market participants. Recent studies emphasize that regulatory ambiguity—rather than technological design alone—plays a critical role in enabling these behaviors (Marian, 2013).

2.2.5 Market Manipulation and Financial Misconduct

Cryptocurrency markets are particularly susceptible to manipulation due to limited oversight, fragmented exchanges, and varying liquidity conditions. Common forms of misconduct include pump-and-dump schemes, wash trading, spoofing, and insider manipulation, often coordinated through online forums and social media platforms.

Empirical analyses provide evidence of systematic price manipulation in early and contemporary cryptocurrency markets, raising concerns regarding investor protection and market integrity (Gandal et al., 2018). These issues present significant barriers to institutional adoption, where compliance with market conduct norms is mandatory.

2.2.6 Environmental and Social Externalities

Although not illegal per se, the environmental impact of energy-intensive cryptocurrency mining—particularly under proof-of-work consensus mechanisms—has emerged as a critical dimension of the technology's dark side. Excessive energy consumption, carbon emissions, and local environmental

degradation have attracted scrutiny from regulators, environmental groups, and socially responsible investors.

Recent literature positions environmental externalities as a form of systemic risk that may influence long-term adoption and legitimacy, particularly as sustainability considerations become integral to financial decision-making (Truby, 2018).

2.3 Distinguishing Misuse from Technology

A critical analytical distinction must be made between *technology-enabled misuse* and *technology-inherent risk*. Cryptocurrencies do not intrinsically generate criminal behavior; rather, they lower transaction costs and increase efficiency for both legitimate and illegitimate users. This distinction is essential to avoid technological determinism and to inform proportionate regulatory responses.

Overemphasis on the dark side risks obscuring legitimate use cases such as remittances, financial inclusion, and decentralized innovation. Conversely, neglecting misuse undermines trust and exposes systems to exploitation. An effective conceptualization must therefore account for both dimensions simultaneously.

2.4 Implications for Adoption and Governance

The typology presented above underscores that the dark side of cryptocurrency is multidimensional and dynamic. Different forms of misuse exert varying levels of influence on adoption decisions across stakeholder groups. For example, retail users may be more sensitive to fraud and market manipulation, whereas institutional actors prioritize compliance, reputational risk, and environmental impact.

Understanding these differentiated effects is essential for developing governance mechanisms that balance innovation with risk mitigation. This insight provides the foundation for examining how regulatory responses and legitimacy perceptions interact with adoption pathways—a task undertaken in the subsequent sections of this study.

3: CRYPTOCURRENCY ADOPTION PATHWAYS AND STAKEHOLDER PERSPECTIVES

3.1 Conceptualizing Cryptocurrency Adoption

Cryptocurrency adoption refers to the extent to which individuals, organizations, and governments integrate cryptocurrencies into financial decision-making, transactional practices, and institutional frameworks. Unlike traditional financial innovations, cryptocurrency adoption unfolds in a decentralized and uneven manner, shaped by technological readiness, regulatory clarity, trust, and perceived legitimacy. Adoption is therefore not a singular process but a multi-path phenomenon influenced by heterogeneous stakeholder incentives and risk perceptions.

Existing adoption models—such as the Technology Acceptance Model (TAM), diffusion of innovations theory, and institutional theory—provide useful but incomplete explanations when applied to cryptocurrencies. While these frameworks emphasize perceived usefulness, ease of use, and social influence, they often understate the role of *risk, legality, and governance* in financial technology

adoption. In cryptocurrency contexts, concerns related to misuse, compliance, and reputational exposure play a decisive role, particularly beyond early adopters.

3.2 Retail Adoption: Individual Users and Households

Retail adoption constitutes the most visible and widely studied form of cryptocurrency engagement. Individuals adopt cryptocurrencies for diverse reasons, including speculative investment, hedging against inflation, cross-border remittances, ideological preferences for decentralization, and access to financial services outside conventional banking systems.

Empirical studies indicate that retail adoption is strongly influenced by perceived financial returns, technological familiarity, and social signaling effects, particularly during bull market cycles (Li & Wang, 2017). However, exposure to fraud, exchange failures, and market manipulation disproportionately affects retail participants, amplifying perceived risk and volatility. Incidents such as large-scale exchange hacks or fraudulent token offerings contribute to episodic declines in trust, even among technologically literate users.

Notably, while retail users may tolerate higher financial risk, they remain sensitive to issues such as consumer protection and transactional security. The association of cryptocurrencies with ransomware, scams, and darknet activities—discussed in PART 2—has been shown to dampen sustained adoption beyond speculative use, particularly in jurisdictions with strong consumer protection norms.

3.3 Institutional Adoption: Firms, Financial Institutions, and Investors

Institutional adoption represents a critical inflection point in the mainstreaming of cryptocurrencies. Corporations, financial institutions, and asset managers evaluate cryptocurrencies through a fundamentally different lens than retail users, prioritizing regulatory compliance, governance standards, and reputational risk.

Research suggests that institutional adoption is contingent upon legal clarity, market integrity, and custodial infrastructure rather than purely technological considerations (Howell et al., 2020). Concerns related to money laundering, market manipulation, and regulatory enforcement significantly constrain participation by banks, pension funds, and publicly listed firms. Even when economic incentives exist, institutional actors often adopt a cautious or indirect approach, such as gaining exposure through regulated derivatives or blockchain-based services rather than direct cryptocurrency holdings.

Environmental and social externalities further influence institutional adoption, particularly in jurisdictions where environmental, social, and governance (ESG) criteria are embedded in investment mandates. Energy-intensive mining practices have prompted several institutions to delay or limit cryptocurrency engagement, illustrating how non-financial risks shape adoption trajectories.

3.4 Governmental and Regulatory Adoption Perspectives

Governments occupy a dual role in the cryptocurrency ecosystem—as regulators and, increasingly, as adopters of blockchain-based technologies. While most governments remain cautious or skeptical of decentralized cryptocurrencies as legal tender, many actively explore central bank digital currencies (CBDCs) as state-controlled alternatives.

From a regulatory standpoint, concerns regarding illicit finance, tax evasion, and capital control circumvention dominate policy discourse. Empirical evidence indicates that jurisdictions with higher perceived exposure to cryptocurrency misuse tend to adopt more restrictive regulatory frameworks, whereas innovation-oriented economies pursue risk-based regulatory approaches (Auer & Claessens, 2018).

At the same time, outright prohibition has proven difficult to enforce effectively, often resulting in informal or offshore activity rather than elimination of use. Consequently, regulatory adoption increasingly emphasizes surveillance, reporting requirements, and international coordination, reflecting an attempt to balance risk mitigation with technological adaptation.

3.5 Adoption in Emerging versus Developed Economies

Adoption dynamics vary significantly between emerging and developed economies. In emerging markets, cryptocurrencies are frequently adopted as substitutes for unstable domestic currencies, capital controls, or inefficient banking systems. In such contexts, perceived benefits related to financial access and value preservation may outweigh concerns about misuse.

Conversely, in developed economies with robust financial infrastructures, adoption is more sensitive to legal uncertainty, consumer protection standards, and systemic risk considerations. Regulatory scrutiny tends to be higher, and tolerance for gray-area usage is lower, resulting in slower but more institutionally embedded adoption pathways.

These contrasting dynamics suggest that the dark-side risks identified in PART 2 do not exert uniform effects across contexts. Instead, their influence is mediated by institutional capacity, regulatory trust, and economic conditions.

3.6 Linking Misuse Risks to Adoption Outcomes

Synthesizing the above perspectives, it becomes evident that cryptocurrency adoption is not determined solely by technological merit or economic incentives. Instead, adoption outcomes emerge from the interaction between perceived benefits and misuse-related risks. Illicit usage, market misconduct, and environmental externalities affect stakeholders differently, shaping adoption intensity, form, and sustainability.

Retail users may continue speculative engagement despite known risks, whereas institutional and governmental actors exhibit significantly lower tolerance for uncertainty and reputational exposure. This divergence underscores the importance of legitimacy as an intermediary construct linking misuse and adoption—a relationship explored more explicitly in subsequent sections.

4: EMPIRICAL EVIDENCE ON ILLICIT CRYPTOCURRENCY USE—PREVALENCE, TRENDS, AND MISCONCEPTIONS

4.1 The Empirical Debate on Illicit Cryptocurrency Activity

The association between cryptocurrencies and illicit activity has been a defining feature of public and policy discourse since the emergence of Bitcoin. Early narratives frequently portrayed cryptocurrencies

as predominantly criminal instruments, driven by their use in darknet markets and cybercrime. However, as cryptocurrency ecosystems have expanded and diversified, empirical research has increasingly challenged such generalized claims.

Academic inquiry into illicit cryptocurrency use has progressed from anecdotal case studies to large-scale transaction-level analyses leveraging blockchain data. These studies provide a more nuanced understanding of the scale, evolution, and concentration of illegal activity within cryptocurrency networks. Crucially, empirical evidence consistently indicates that while illicit use is non-trivial and persistent, it constitutes a minority share of total cryptocurrency activity.

4.2 Measuring Illicit Activity in Cryptocurrency Markets

Empirically measuring illicit cryptocurrency use presents methodological challenges due to pseudonymity, cross-border transactions, and evolving criminal tactics. Researchers typically rely on blockchain forensics, clustering techniques, law enforcement seizure data, and identification of addresses linked to known illegal services.

One of the most influential empirical studies in this domain estimates that approximately 46% of Bitcoin transactions in its early years were associated with illegal activity, corresponding to about 25% of users (Foley et al., 2019). However, the same study demonstrates a *declining trend* in illicit use over time as legitimate adoption increased and regulatory scrutiny intensified. Subsequent analyses corroborate this downward trajectory, emphasizing that growth in lawful transactions has outpaced illicit activity.

More recent studies highlight the concentration of illicit activity within specific subsets of users and services, rather than widespread participation across the network. This concentration effect implies that a relatively small number of actors account for a disproportionate share of criminal cryptocurrency usage, a finding with significant implications for targeted regulatory intervention.

4.3 Illicit Use Relative to Total Cryptocurrency Adoption

A critical empirical insight emerging from the literature is the distinction between *absolute growth* and *relative prevalence*. While the absolute value of illicit cryptocurrency transactions has increased in some periods—particularly during ransomware surges—their proportion relative to total transaction volume has generally declined.

Comparative analyses indicate that as cryptocurrency markets matured, increased exchange regulation, know-your-customer (KYC) requirements, and transaction monitoring reduced the relative attractiveness of cryptocurrencies for certain forms of financial crime (Fanusie& Robinson, 2018). At the same time, traditional financial systems continue to account for the majority of global money laundering activity, a fact often overlooked in public discourse.

This evidence challenges the narrative that cryptocurrencies are uniquely or predominantly criminal tools. Instead, they appear to function as *complementary* instruments within broader illicit financial ecosystems rather than as primary enablers.

4.4 Ransomware and Cybercrime: A Disproportionate Visibility Effect

Among illicit uses, ransomware occupies a distinctive empirical position due to its high visibility and social impact. Studies document a strong correlation between cryptocurrency adoption and the operational viability of ransomware campaigns, as cryptocurrencies facilitate cross-border extortion payments without reliance on formal banking channels (Conti et al., 2018).

However, despite its prominence, ransomware-related transactions represent a small fraction of total cryptocurrency activity. The outsized attention given to ransomware reflects its societal harm and media salience rather than its quantitative dominance. This visibility effect has nonetheless played a significant role in shaping regulatory responses and public perceptions, illustrating how *salient misuse* can outweigh statistical prevalence in adoption dynamics.

4.5 Darknet Markets and Structural Persistence

Empirical research on darknet markets provides further insight into the adaptability of illicit cryptocurrency use. Studies examining the closure of major darknet platforms reveal that enforcement actions often lead to displacement rather than eradication, with users migrating to alternative markets or currencies (Van Wegberg et al., 2018).

Notably, this persistence does not imply expansion. Instead, darknet activity has exhibited cyclical patterns characterized by disruption, reconfiguration, and consolidation. Over time, increased law enforcement capabilities and blockchain analytics have raised operational risks for illicit actors, contributing to a gradual professionalization and concentration of darknet-related cryptocurrency use.

4.6 Market Manipulation: Evidence from Cryptocurrency Exchanges

Market manipulation constitutes another empirically validated dark-side phenomenon. Academic studies provide evidence of price manipulation through coordinated trading, wash trading, and spoofing, particularly in early and thinly regulated cryptocurrency markets (Gandal et al., 2018).

Such misconduct disproportionately affects retail investors and undermines market integrity, reinforcing perceptions of cryptocurrencies as speculative and unstable. Importantly, empirical evidence suggests that manipulation decreases as markets mature, liquidity improves, and regulatory oversight increases—paralleling historical patterns observed in traditional financial markets.

4.7 Common Misconceptions and Empirical Clarifications

The empirical literature helps dispel several persistent misconceptions:

1. **Cryptocurrencies are mostly used for illegal activities**
   Empirical evidence consistently refutes this claim, demonstrating that illicit use represents a minority share of activity and has declined proportionally over time.

2. **Cryptocurrencies uniquely enable financial crime**
   Research indicates that traditional financial systems remain the primary conduits for global illicit finance, with cryptocurrencies serving as supplementary tools rather than dominant mechanisms.

3. **Illicit use is evenly distributed across users**
   Illicit activity is highly concentrated among specific actors and services, suggesting the effectiveness of targeted interventions over blanket restrictions.

These clarifications are essential for informed regulatory design and balanced adoption assessment.

4.8 Implications for Adoption and Policy Discourse

The empirical evidence reviewed in this section underscores a central paradox: illicit cryptocurrency use is statistically limited yet symbolically powerful. Its influence on adoption far exceeds its quantitative footprint, shaping trust, regulatory urgency, and institutional hesitancy.

Understanding this discrepancy between prevalence and perception is critical for explaining why adoption trajectories remain uneven despite growing empirical evidence of legitimacy. This insight sets the stage for analyzing regulatory responses and their feedback effects on adoption, which is the focus of the next section.

5: REGULATORY RESPONSES TO CRYPTOCURRENCY MISUSE—CROSS-COUNTRY AND INSTITUTIONAL PERSPECTIVES

5.1 Rationale for Regulating Cryptocurrencies

Regulatory intervention in cryptocurrency markets is primarily motivated by concerns related to financial integrity, consumer protection, and systemic stability. Unlike traditional financial instruments, cryptocurrencies operate across borders with limited reliance on centralized intermediaries, challenging the jurisdictional reach of national regulators. The empirical evidence reviewed in PART 4 indicates that while illicit activity constitutes a minority share of overall cryptocurrency use, its concentration, visibility, and societal impact have elevated regulatory urgency.

From a policy perspective, cryptocurrencies represent a regulatory paradox: excessive restriction risks driving activity underground or offshore, while insufficient oversight may facilitate financial crime and erode trust. Consequently, regulatory responses have evolved toward risk-based frameworks that seek to mitigate misuse while preserving legitimate innovation.

5.2 International Standards and Coordinated Regulatory Efforts

At the global level, regulatory coordination has been shaped primarily by international standard-setting bodies rather than unilateral national action. The Financial Action Task Force (FATF) has played a central role in defining expectations for cryptocurrency regulation by extending anti-money laundering (AML) and counter-terrorist financing (CTF) standards to virtual asset service providers (VASPs).

The introduction of the FATF “Travel Rule,” which requires VASPs to collect and transmit originator and beneficiary information for cryptocurrency transactions, represents a significant shift toward parity with traditional financial systems (FATF, 2019). Empirical and policy analyses suggest that the Travel Rule has increased compliance costs and operational complexity for exchanges, while also enhancing transaction traceability and law enforcement cooperation.

Importantly, international coordination has reduced regulatory arbitrage opportunities, though uneven implementation across jurisdictions continues to create compliance asymmetries. These dynamics directly influence institutional adoption, as firms operating across borders prefer jurisdictions aligned with global standards to minimize legal uncertainty.

5.3 Divergent National Regulatory Approaches

5.3.1 Restrictive and Prohibitive Regimes

Some jurisdictions have adopted restrictive or prohibitive approaches toward cryptocurrencies, motivated by concerns over capital controls, monetary sovereignty, and financial stability. Such regimes typically restrict trading, mining, or exchange operations while stopping short of banning ownership outright.

Empirical evidence suggests that outright bans rarely eliminate cryptocurrency use; instead, they often shift activity to informal or offshore channels, reducing regulatory visibility and enforcement effectiveness. These outcomes highlight the limitations of prohibition-based strategies, particularly in digitally connected economies.

5.3.2 Risk-Based and Adaptive Regulatory Frameworks

In contrast, several advanced economies have pursued risk-based regulatory frameworks that integrate cryptocurrencies into existing financial oversight structures. These approaches emphasize licensing of exchanges, AML/KYC compliance, market surveillance, and consumer protection, while allowing regulated participation by institutional actors.

The European Union's Markets in Crypto-Assets (MiCA) framework exemplifies this approach by establishing a harmonized regulatory regime for crypto-asset issuance and service provision. Early policy evaluations suggest that regulatory clarity under MiCA has reduced uncertainty for firms and encouraged legitimate market participation, albeit with increased compliance obligations.

5.3.3 Regulatory Sandboxes and Innovation-Friendly Models

Some jurisdictions have adopted regulatory sandboxes to balance innovation with oversight. These controlled environments allow firms to test cryptocurrency-related products under regulatory supervision, enabling policymakers to learn about emerging risks while supporting responsible innovation.

Evidence from fintech sandbox programs indicates that such approaches can accelerate institutional learning and reduce adversarial relationships between regulators and innovators. However, their effectiveness depends on transparency, enforcement credibility, and integration into broader regulatory frameworks.

5.4 Regulation, Misuse Mitigation, and Adoption Outcomes

Regulatory responses directly influence cryptocurrency adoption through multiple channels. Clear and proportionate regulation enhances legitimacy, reduces uncertainty, and facilitates institutional participation. Conversely, inconsistent or ambiguous regulation increases perceived risk and discourages long-term investment.

Empirical studies suggest that regulatory announcements related to AML enforcement and exchange licensing have measurable effects on market behavior, including price volatility, trading volume shifts, and exchange migration (Auer & Claessens, 2018). These responses underscore the sensitivity of cryptocurrency markets to regulatory signals.

Notably, regulation aimed at mitigating misuse does not uniformly suppress adoption. Instead, it often reallocates participation toward compliant platforms and jurisdictions, contributing to market maturation. This pattern mirrors historical regulatory trajectories observed in traditional financial markets.

5.5 The Role of Central Bank Digital Currencies (CBDCs)

An emerging regulatory response to cryptocurrency misuse is the exploration of central bank digital currencies (CBDCs). CBDCs are frequently framed as state-controlled alternatives that retain the efficiency benefits of digital currencies while ensuring regulatory oversight, traceability, and monetary control.

While CBDCs do not directly replace decentralized cryptocurrencies, their development reflects governmental attempts to address the demand drivers underlying cryptocurrency adoption—such as payment efficiency and digital inclusion—without tolerating the misuse risks associated with decentralized systems. This parallel development has implications for the competitive and regulatory landscape of digital finance.

5.6 Regulatory Trade-Offs and Unintended Consequences

Despite their objectives, regulatory interventions may generate unintended consequences. Excessive compliance burdens can disadvantage smaller firms, leading to market concentration and reduced competition. Similarly, overemphasis on surveillance may raise privacy concerns, potentially alienating users who value decentralization for legitimate reasons.

The literature emphasizes that effective regulation requires adaptive governance capable of responding to technological evolution and behavioral adaptation by illicit actors. Static regulatory models risk becoming obsolete in rapidly changing cryptocurrency ecosystems.

5.7 Synthesis and Implications for Adoption

The analysis presented in this section demonstrates that regulatory responses to cryptocurrency misuse are neither uniform nor static. Instead, they reflect evolving assessments of risk, legitimacy, and economic opportunity. Regulation serves as a critical intermediary between misuse and adoption, shaping how different stakeholders perceive and engage with cryptocurrencies.

These insights provide the foundation for developing an integrative conceptual framework linking misuse-related risks, regulatory legitimacy, and adoption outcomes—a task undertaken in the next section.

6: IMPACT OF ILLICIT AND HIGH-RISK CRYPTOCURRENCY USE ON LEGITIMACY AND ADOPTION

6.1 Legitimacy as a Central Mechanism in Cryptocurrency Adoption

Legitimacy plays a pivotal role in the adoption of financial innovations, particularly those that challenge established institutional arrangements. In institutional theory, legitimacy refers to the generalized perception that an entity's actions are desirable, proper, or appropriate within socially constructed systems of norms, values, and regulations. For cryptocurrencies, legitimacy is not inherent; it is socially and institutionally negotiated over time.

Illicit and high-risk uses of cryptocurrencies undermine legitimacy by associating the technology with criminality, instability, and governance failure. Even when empirical evidence demonstrates that misuse represents a minority of total activity, its symbolic and reputational effects exert a powerful influence on adoption decisions. This legitimacy deficit helps explain why adoption remains uneven across stakeholder groups despite technological maturity and market growth.

6.2 Trust, Risk Perception, and User Adoption

Trust is a foundational determinant of financial behavior. In cryptocurrency ecosystems, trust operates at multiple levels: trust in the technology, trust in intermediaries such as exchanges and custodians, and trust in the surrounding regulatory environment. Illicit usage erodes trust by amplifying perceptions of risk, particularly among non-expert users.

Retail adoption is especially sensitive to fraud, hacking incidents, and market manipulation. Empirical studies show that exposure to security breaches and scams significantly reduces continued usage intentions, even among users with prior positive experiences (Krombholz et al., 2017). The association of cryptocurrencies with ransomware and darknet markets further reinforces perceived moral and legal risk, discouraging adoption beyond speculative engagement.

Importantly, trust erosion does not occur linearly. High-profile incidents generate episodic legitimacy shocks that disproportionately affect adoption sentiment, often independent of underlying usage trends. This volatility in trust contributes to cyclical adoption patterns observed in cryptocurrency markets.

6.3 Institutional Adoption and Reputational Risk

Institutional actors—including banks, asset managers, and publicly listed firms—exhibit substantially lower tolerance for legitimacy risk than retail users. For these actors, engagement with cryptocurrencies entails not only financial exposure but also reputational and compliance risk.

Illicit and gray-area cryptocurrency use raises concerns related to anti-money laundering obligations, fiduciary duty, and brand integrity. Empirical research suggests that institutions are more likely to adopt cryptocurrencies indirectly—through regulated financial instruments or blockchain-based services—when legitimacy remains contested (Howell et al., 2020). Direct holdings or transactional use typically follow only after regulatory clarity and enforcement credibility improve.

Environmental externalities further compound legitimacy challenges for institutional adoption, particularly in jurisdictions where ESG considerations are embedded in investment mandates.

Associations between cryptocurrency mining and carbon emissions have prompted several institutions to delay or restrict engagement, illustrating how non-criminal risks also shape legitimacy perceptions.

6.4 Regulatory Legitimacy and Adoption Feedback Loops

Regulatory responses to illicit cryptocurrency use play a dual role in shaping legitimacy. On one hand, effective regulation enhances trust by signaling oversight, accountability, and enforceability. On the other hand, overly restrictive or inconsistent regulation may reinforce perceptions of illegitimacy by framing cryptocurrencies as inherently problematic.

This dynamic generates feedback loops between regulation and adoption. Regulatory crackdowns prompted by misuse can temporarily suppress adoption or redirect activity to compliant platforms. Over time, however, clear and proportionate regulation tends to legitimize participation by institutional actors and risk-averse users.

Empirical evidence indicates that markets respond positively to regulatory clarity, even when compliance costs increase, suggesting that legitimacy gains may outweigh short-term frictions (Auer & Claessens, 2018). These findings underscore the importance of regulatory design in mediating the relationship between misuse and adoption.

6.5 Differential Impact Across Stakeholder Groups

The impact of illicit cryptocurrency use on adoption is not uniform across stakeholders. Retail users, institutional investors, regulators, and technology developers perceive and respond to risk differently based on incentives, constraints, and normative expectations.

Retail users may prioritize accessibility and potential returns over compliance concerns, particularly in emerging economies with limited financial inclusion. In contrast, institutional actors and regulators emphasize legality, traceability, and systemic stability. This divergence results in fragmented adoption pathways, where cryptocurrencies may achieve widespread retail usage while remaining institutionally marginalized.

Understanding these differentiated impacts is essential for explaining why adoption progresses unevenly despite shared technological infrastructure. It also highlights the limitations of one-size-fits-all regulatory approaches.

6.6 Long-Term Adoption and the Normalization Challenge

For cryptocurrencies to achieve sustained mainstream adoption, they must transition from novelty and speculation toward normalization within financial systems. Illicit and high-risk uses delay this transition by reinforcing narratives of instability and deviance.

Normalization requires not the elimination of misuse—which is unrealistic—but its containment to levels comparable with traditional financial systems. Historical parallels with early electronic banking and online payment systems suggest that legitimacy emerges gradually through a combination of regulation, institutional participation, and cultural acceptance.

In this context, the persistence of illicit cryptocurrency use represents a governance challenge rather than an existential flaw. Adoption outcomes depend on whether stakeholders perceive misuse as manageable and exceptional, rather than systemic and defining.

6.7 Toward an Integrative Perspective

The analysis presented in this section demonstrates that illicit and high-risk cryptocurrency use affects adoption primarily through its impact on legitimacy, trust, and risk perception. These effects are mediated by regulation, institutional norms, and stakeholder-specific incentives.

This insight motivates the need for an integrative conceptual framework that explicitly links misuse-related risks, regulatory legitimacy, and adoption dynamics. Such a framework can reconcile empirical evidence with observed adoption patterns and guide both future research and policy design. The development of this framework constitutes the focus of the next section.

7: AN INTEGRATIVE RISK–LEGITIMACY–ADOPTION FRAMEWORK FOR CRYPTOCURRENCIES

7.1 Rationale for a Conceptual Framework

Despite a growing body of empirical research on cryptocurrency misuse, regulation, and adoption, existing studies remain largely fragmented. Prior work often examines isolated dimensions—such as illicit activity, regulatory design, or user behavior—without integrating these elements into a coherent explanatory structure. This fragmentation limits the ability of researchers and policymakers to understand how misuse-related risks translate into adoption outcomes across stakeholder groups.

To address this limitation, this study proposes an integrative **Risk–Legitimacy–Adoption (RLA) Framework**. The framework synthesizes insights from institutional theory, risk perception literature, and financial innovation adoption research to explain how illicit and high-risk cryptocurrency uses influence adoption trajectories through legitimacy mechanisms.

7.2 Core Constructs of the Framework

The proposed framework consists of four interrelated constructs: **misuse-related risks**, **regulatory response**, **perceived legitimacy**, and **adoption outcomes**. Each construct is analytically distinct yet dynamically linked.

7.2.1 Misuse-Related Risks

Misuse-related risks encompass illicit, unethical, and high-risk activities associated with cryptocurrencies, including money laundering, ransomware, market manipulation, regulatory arbitrage, and environmental externalities. As established in PARTS 2 and 4, these risks are empirically concentrated rather than pervasive but exert disproportionate influence on perception and policy.

Within the framework, misuse-related risks are treated as *exogenous stimuli* that trigger regulatory attention and shape stakeholder perceptions. Importantly, these risks are not static; they evolve in response to technological change, enforcement capacity, and market maturation.

7.2.2 Regulatory Response

Regulatory response represents the set of formal rules, enforcement mechanisms, and supervisory practices developed to address misuse-related risks. This includes AML/CTF regulation, exchange licensing, market surveillance, and international coordination.

In the RLA framework, regulation functions as both a *mediator* and a *signal*. It mediates the translation of misuse into legitimacy outcomes by constraining harmful behavior, while simultaneously signaling institutional acceptance or rejection of cryptocurrency systems. Regulatory clarity and proportionality are therefore central to legitimacy formation.

7.2.3 Perceived Legitimacy

Perceived legitimacy constitutes the core mediating construct of the framework. It reflects the extent to which cryptocurrencies are viewed as acceptable, trustworthy, and appropriate within prevailing legal, moral, and social norms.

Legitimacy is shaped jointly by observed misuse, regulatory responses, and broader societal narratives. Crucially, legitimacy is not binary but exists along a continuum, varying across stakeholder groups and jurisdictions. The framework emphasizes that adoption decisions are driven less by objective risk levels than by legitimacy perceptions constructed through institutional and cultural processes.

7.2.4 Adoption Outcomes

Adoption outcomes refer to the extent, form, and sustainability of cryptocurrency use by different stakeholders, including retail users, institutional investors, firms, and governments. Adoption is conceptualized as multidimensional, encompassing speculative participation, transactional use, infrastructural integration, and policy endorsement.

Within the framework, adoption outcomes are endogenous, shaped by legitimacy perceptions and moderated by stakeholder-specific incentives and constraints.

7.3 Dynamic Relationships Within the Framework

The RLA framework proposes three central relational pathways.

First, **misuse-related risks negatively affect perceived legitimacy**, particularly when such risks are highly visible or socially salient. Even limited empirical prevalence can generate legitimacy deficits if misuse is framed as systemic rather than exceptional.

Second, **regulatory responses moderate the relationship between misuse and legitimacy**. Effective, proportionate regulation mitigates legitimacy erosion by signaling governance capacity and institutional control. Conversely, inconsistent or excessively restrictive regulation may exacerbate legitimacy challenges by reinforcing narratives of deviance or instability.

Third, **perceived legitimacy directly influences adoption outcomes**, with differential effects across stakeholder groups. Retail users may tolerate lower legitimacy thresholds, whereas institutional and governmental actors typically require high levels of legal and normative acceptance prior to adoption.

These pathways form a feedback loop: adoption outcomes influence regulatory evolution and technological design, which in turn reshape misuse risks over time.

7.4 Stakeholder Differentiation and Contextual Moderators

A key contribution of the framework lies in its explicit recognition of stakeholder heterogeneity. The impact of misuse-related risks on legitimacy and adoption is moderated by factors such as:

- **Institutional capacity** (e.g., regulatory enforcement strength)
- **Economic context** (emerging versus developed economies)
- **Normative expectations** (e.g., ESG priorities, privacy norms)
- **Technological literacy**

By incorporating these moderators, the framework explains why cryptocurrencies may achieve widespread retail adoption while remaining institutionally constrained, or why regulatory tolerance varies across jurisdictions.

7.5 Theoretical Contributions

The proposed RLA framework contributes to theory in three ways.

First, it advances cryptocurrency research beyond descriptive accounts by offering a structured explanation of adoption outcomes grounded in legitimacy theory.

Second, it integrates risk and regulation into adoption analysis, addressing limitations of traditional technology acceptance models when applied to financial innovations.

Third, it provides a dynamic perspective that accounts for feedback effects between misuse, regulation, and adoption, enabling longitudinal and comparative research designs.

7.6 Implications for Empirical Research

The framework offers a foundation for future empirical studies by identifying testable relationships among misuse-related risks, regulatory responses, legitimacy perceptions, and adoption behaviors. Researchers may operationalize these constructs using transaction data, regulatory indices, survey measures of trust, and adoption metrics across contexts.

Such empirical extensions would strengthen causal inference and support evidence-based policy design.

7.7 Synthesis

The Risk–Legitimacy–Adoption framework developed in this section synthesizes the central arguments of the paper into a coherent explanatory model. It demonstrates that the dark or high-risk dimensions of cryptocurrency ecosystems influence adoption not directly, but through legitimacy mechanisms shaped by regulation and institutional context.

This framework provides the conceptual bridge between empirical evidence and practical implications, which are explored in the following section.

8: MANAGERIAL, POLICY, AND RESEARCH IMPLICATIONS

8.1 Implications for Policymakers and Regulators

The findings of this study suggest that regulatory effectiveness in cryptocurrency markets depends less on the severity of intervention and more on its *legitimacy-enhancing capacity*. Policymakers should recognize that illicit and high-risk cryptocurrency use affects adoption primarily through perception-driven legitimacy mechanisms rather than direct economic harm alone.

First, regulators should prioritize **risk-based and proportionate frameworks** that distinguish between concentrated misuse and widespread legitimate activity. Empirical evidence demonstrates that illicit activity is highly clustered among specific actors and services. Blanket restrictions or prohibitions risk undermining regulatory credibility while pushing activity into opaque channels, thereby reducing enforcement effectiveness.

Second, **regulatory clarity** is critical for institutional adoption. Clear definitions of crypto-assets, licensing regimes for service providers, and consistent enforcement signals reduce uncertainty and support compliance-driven participation. Jurisdictions aligned with international standards—particularly AML/CTF frameworks—are more likely to attract legitimate market actors and discourage regulatory arbitrage.

Third, regulators must account for **symbolic legitimacy effects** when designing policy responses. Highly visible enforcement actions and public communication strategies shape narratives around cryptocurrencies, influencing trust beyond the immediate regulatory target. Transparent, evidence-based communication can mitigate the perception gap between actual and perceived misuse prevalence.

Finally, the parallel development of **central bank digital currencies (CBDCs)** should be understood as complementary rather than substitutive. CBDCs may address efficiency and inclusion objectives without eliminating demand for decentralized cryptocurrencies. Policymakers should therefore avoid framing CBDCs solely as corrective responses to cryptocurrency misuse.

8.2 Implications for Firms and Financial Institutions

For firms operating in or adjacent to cryptocurrency ecosystems, legitimacy management emerges as a strategic priority. The Risk–Legitimacy–Adoption framework highlights that engagement decisions are shaped not only by technological feasibility and financial returns but also by reputational exposure and regulatory signaling.

First, firms should adopt **compliance-by-design strategies**, integrating AML, transaction monitoring, and governance mechanisms into product and service development. Proactive compliance reduces regulatory friction and signals legitimacy to institutional partners and customers.

Second, financial institutions seeking cryptocurrency exposure may benefit from **graduated adoption pathways**, such as indirect investment vehicles, custody services, or blockchain infrastructure participation. These approaches allow institutions to capture innovation benefits while limiting direct exposure to misuse-related risks.

Third, environmental and social considerations require strategic attention. Firms increasingly face scrutiny from investors and stakeholders regarding ESG alignment. Engagement with energy-efficient consensus mechanisms or sustainability initiatives can mitigate legitimacy challenges associated with environmental externalities.

8.3 Implications for Investors and Market Participants

For investors, particularly institutional and risk-averse participants, the study underscores the importance of distinguishing **systemic risk from concentrated misuse**. Illicit cryptocurrency activity, while persistent, does not uniformly undermine market viability. However, legitimacy shocks triggered by high-profile incidents can generate volatility and adoption setbacks.

Investors should therefore incorporate **regulatory and legitimacy indicators**—such as jurisdictional compliance standards, exchange governance quality, and enforcement trends—into risk assessment frameworks. Such indicators may be as influential as traditional financial metrics in determining long-term adoption prospects.

8.4 Implications for Technology Developers and Innovators

Technology developers play a critical role in shaping the misuse–legitimacy–adoption nexus. Design choices related to transparency, traceability, and governance influence both misuse potential and regulatory acceptance.

Developers should engage constructively with regulators and standard-setting bodies to ensure that innovation aligns with evolving compliance expectations. Privacy-enhancing technologies, for example, must be balanced against traceability requirements to avoid exacerbating legitimacy concerns.

8.5 Implications for Academic Research

This study offers several implications for future research. First, scholars should move beyond binary classifications of cryptocurrency use as legal or illegal and adopt **continuum-based analyses** that reflect empirical realities. Such approaches can better capture the complexity of misuse and legitimacy dynamics.

Second, empirical research should increasingly adopt **longitudinal and comparative designs** to examine how legitimacy evolves over time in response to regulation, market maturation, and technological change. Cross-country studies are particularly valuable given the heterogeneity of regulatory regimes and adoption contexts.

Third, future studies may operationalize the Risk–Legitimacy–Adoption framework using mixed methods, combining blockchain analytics, regulatory data, and perception-based surveys. This integrative approach can strengthen causal inference and inform evidence-based policymaking.

8.6 Synthesis

The implications outlined above reinforce the central argument of this paper: illicit and high-risk cryptocurrency use influences adoption indirectly through legitimacy mechanisms shaped by regulation, institutional norms, and stakeholder perceptions. Effective governance and strategic engagement require recognizing this mediated relationship rather than focusing solely on misuse suppression.

By translating conceptual insights into actionable guidance, this section demonstrates the practical relevance of the proposed framework and prepares the ground for concluding reflections.

9: CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

9.1 Summary of Key Findings

This study set out to examine the darker dimensions of cryptocurrency ecosystems and their implications for adoption in mainstream financial and institutional contexts. Contrary to dominant public narratives, the evidence reviewed throughout the paper demonstrates that illicit and high-risk cryptocurrency use, while persistent and socially consequential, represents a minority share of overall activity. However, its symbolic salience and reputational impact exert disproportionate influence on regulatory responses, legitimacy perceptions, and adoption outcomes.

By synthesizing empirical evidence, regulatory analysis, and adoption theory, the study shows that the relationship between cryptocurrency misuse and adoption is not direct. Instead, it is mediated by legitimacy—constructed through institutional norms, regulatory signaling, and stakeholder perceptions of risk and trust. This mediated relationship helps explain why cryptocurrencies may experience widespread retail engagement while remaining institutionally constrained, or why adoption trajectories diverge sharply across jurisdictions.

9.2 Theoretical Contributions

This paper makes several theoretical contributions to the literature on financial innovation and digital technologies.

First, it advances the conceptual understanding of cryptocurrency misuse by moving beyond sensationalist or binary framings toward a structured, evidence-based typology that distinguishes illicit, unethical, and high-risk activities.

Second, it integrates legitimacy theory into cryptocurrency adoption research, addressing a key limitation of technology-centric adoption models that underplay governance and institutional acceptance in financial contexts.

Third, the proposed **Risk–Legitimacy–Adoption framework** offers an original, integrative perspective that connects misuse-related risks, regulatory responses, and adoption outcomes within a dynamic system. This framework provides a foundation for cumulative theory building and comparative empirical analysis.

9.3 Policy and Practical Significance

From a policy perspective, the findings underscore that effective cryptocurrency governance is not achieved through prohibition or excessive restriction, but through proportionate, credible, and transparent regulation. Regulatory strategies that enhance legitimacy—by reducing uncertainty and signaling institutional control—are more likely to support sustainable adoption while mitigating misuse.

For firms, investors, and technology developers, the study highlights legitimacy management as a strategic concern. Adoption decisions depend not only on economic incentives or technical performance but also on reputational exposure, compliance expectations, and alignment with evolving regulatory norms.

9.4 Limitations of the Study

As with any conceptual and integrative research, this study has limitations that warrant acknowledgment.

First, the analysis relies on secondary empirical studies and policy documents rather than original transaction-level data. While this approach enables broad synthesis, future research could strengthen causal inference through primary data analysis.

Second, regulatory developments in cryptocurrency markets are rapidly evolving. Although the study captures prevailing frameworks and trends, ongoing policy changes may alter specific regulatory dynamics over time.

Third, the study focuses primarily on decentralized cryptocurrencies and does not empirically examine central bank digital currencies in depth. While CBDCs are discussed conceptually, their adoption dynamics merit separate and dedicated investigation.

These limitations do not undermine the study's contributions but rather delineate its scope and inform future research directions.

9.5 Directions for Future Research

Building on the findings of this study, several avenues for future research emerge.

First, empirical testing of the Risk–Legitimacy–Adoption framework using longitudinal data would enhance understanding of how legitimacy evolves in response to regulatory change and market maturation.

Second, comparative cross-country studies examining how institutional capacity, legal traditions, and economic conditions moderate misuse–adoption relationships would provide valuable policy insights.

Third, future research could explore the interaction between decentralized cryptocurrencies and CBDCs, particularly in terms of competition, complementarity, and legitimacy spillovers.

Finally, interdisciplinary approaches combining blockchain analytics, behavioral research, and institutional analysis hold promise for advancing evidence-based cryptocurrency governance.

9.6 Concluding Remarks

Cryptocurrencies embody a fundamental tension between innovation and risk. Their darker dimensions—illicit use, regulatory evasion, and externalities—are neither defining nor negligible. Instead, they represent governance challenges that shape legitimacy and adoption in complex and context-dependent ways.

By reframing the discourse around misuse, legitimacy, and adoption, this study contributes to a more balanced and analytically rigorous understanding of cryptocurrencies' role in contemporary financial systems. As digital finance continues to evolve, such integrative perspectives will be essential for guiding research, policy, and practice toward sustainable and inclusive outcomes.

References

1. Auer, R., & Claessens, S. (2018). Regulating cryptocurrencies: Assessing market reactions. *BIS Quarterly Review*, September, 1–16.
2. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213
3. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060
4. Fanusie, Y. J., & Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. *Journal of Financial Crime, 25*(1), 60–80. https://doi.org/10.1108/JFC-01-2017-0004
5. Financial Action Task Force. (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. FATF.
6. Foley, S., Karlsen, J. R., &Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Economic Studies, 86*(5), 1798–1853. https://doi.org/10.1093/restud/rdy057
7. Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics, 95*, 86–96. https://doi.org/10.1016/j.jmoneco.2018.01.004
8. Howell, S. T., Niessner, M., & Yermack, D. (2020). Initial coin offerings: Financing growth with cryptocurrency token sales. *The Review of Financial Studies, 33*(9), 3925–3974. https://doi.org/10.1093/rfs/hhz131
9. Krombholz, K., Judmayer, A., Gusenbauer, M., &Weippl, E. (2017). The other side of the coin: User experiences with bitcoin security and privacy. In *Financial Cryptography and Data Security* (pp. 555–580). Springer. https://doi.org/10.1007/978-3-662-53357-4_31
10. Li, X., & Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems, 95*, 49–60. https://doi.org/10.1016/j.dss.2016.12.001
11. Marian, O. Y. (2013). Are cryptocurrencies super tax havens? *Michigan Law Review First Impressions, 112*, 38–48. https://doi.org/10.2139/ssrn.2305863
12. Truby, J. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. *Energy Research & Social Science, 44*, 399–410. https://doi.org/10.1016/j.erss.2018.06.009
13. Van Wegberg, R., Oerlemans, J. J., & Van Deventer, O. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime, 25*(2), 419–435. https://doi.org/10.1108/JFC-11-2016-0067

14. Vives, X. (2019). Digital disruption in banking. *Annual Review of Financial Economics, 11*, 243–272. https://doi.org/10.1146/annurev-financial-110118-123745
15. Zetzsche, D. A., Buckley, R. P., Arner, D. W., &Föhr, L. (2020). The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators. *Harvard International Law Journal, 60*(2), 267–324.