

Emerging Risks in Fintech and Digital Assets: Ownership, Transaction, and Compliance Risks in Decentralized Finance

Ruimin Lu*

Reading Academy, Nanjing
University of Information Science &
Technology, Nanjing, 210044, China
*Corresponding author: tx803862@
student.reading.ac.uk

Abstract:

The rapid growth of decentralized finance (DeFi) has introduced novel digital assets whose on-chain ownership logic diverges significantly from traditional property and securities law frameworks. This conceptual study systematically examines the emerging risks arising from this legal-technological disconnect across three dimensions: ownership, trading, and compliance. Through an integrated literature review, the paper develops a causal risk transmission framework linking four interconnected layers—operational vulnerabilities in DeFi systems, ownership indeterminacy of digital assets, transaction and market distortions, and compliance gaps stemming from regulatory fragmentation. The analysis demonstrates that technical failures (e.g., compromised private keys, smart contract exploits) trigger ownership disputes that courts cannot remedy, which in turn amplify market volatility and create arbitrage opportunities across fragmented national regimes. The paper proposes institutional remedies including harmonised legal definitions, technical resilience standards, cross-border enforcement cooperation, and adaptive regulatory modalities. While conceptual in nature, the framework provides a foundation for empirical testing and offers practical guidance for policymakers seeking to close the gap between technological innovation and regulatory response. The findings underscore that without coordinated international action, the self-reinforcing cycle of risk transmission will persist, undermining both market stability and user protection in the digital asset ecosystem.

Keywords: Decentralized finance (DeFi); ownership risk; regulatory fragmentation; risk transmission mechanism; blockchain regulation.

1. Introduction

1.1 Research Background

With the continuous application of blockchain technology, decentralized finance (DeFi) has developed rapidly. Online digital wallets and on-chain asset custody services, enabled by fintech, have gradually become the core carriers for the storage and circulation of digital assets. Digital assets including crypto tokens and non-fungible tokens (NFTs) are now widely circulated on a large scale. However, for these new types of blockchain-based assets, there is a significant disconnect between their on-chain ownership logic and traditional property law as well as securities trading rules. The existing legal system cannot effectively accommodate these new asset forms.

Currently, the pace of technological iteration in the decentralized finance industry is significantly faster than the global legislative process, and the problem of regulatory lag is becoming increasingly prominent. New risks including ownership disputes and irregularities in non-standard transactions keep emerging, leaving substantial gaps in the existing regulatory system. These risks are inherently emerging and dynamically evolving.

1.2 Research Purpose and Research Questions

Against the above industry backdrop, this paper focuses on the decentralized fintech ecosystem. It systematically identifies various emerging risks derived from the definition and transfer of ownership of digital assets, clarifies the mechanisms behind these risks, and analyzes the shortcomings and institutional dilemmas of the global regulatory system.

Specifically, this paper centers its research on the following three core questions:

- (1) How do operational vulnerabilities in decentralized fintech systems trigger risks of losing ownership of digital assets?
- (2) What unique on-chain transaction risks and asset price volatility risks have been generated by the absence of rules for confirming ownership of digital assets?
- (3) How does the fragmentation of regulatory rules across different countries continuously give rise to new compliance loopholes?

1.3 Paper Structure

The remainder of this paper is organised as follows. Chapter 2 critically reviews three streams of literature—operational vulnerabilities, legal debates on digital asset property status, and empirical studies on trading and price volatility—identifying the gap of an integrated causal framework. Chapter 3, which constitutes the analytical core, defines the key constructs and systematically un-

packs four interconnected risk layers: operational risks in DeFi systems, ownership risks of digital assets, transaction and market risks, and compliance risks arising from regulatory fragmentation. It concludes with a synthesis of the risk transmission mechanism that links these layers into a dynamic causal chain. Chapter 4 proposes institutional remedies across harmonised legal definitions, technical standards, cross-border cooperation, and adaptive regulation. Chapter 5 summarises the findings, acknowledges limitations, and suggests directions for future empirical research.

This paper makes three hierarchical contributions. First, it integrates operational, legal, and market risk literatures into a unified causal framework, bridging the technology–law–economics divide. Second, it conceptualizes emerging risks as a self-reinforcing dynamic cycle, moving beyond static taxonomies to capture the evolving nature of DeFi risks. Third, it proposes targeted interventions at each stage of the transmission chain, offering a systematic policy roadmap rather than piecemeal recommendations.

2. Literature Review

2.1 Research on Decentralized Fintech Operational & Compliance Risk

Technical analyses of DeFi have catalogued numerous vulnerabilities spanning network, consensus, protocol, and application layers, with smart contract bugs, poor private key management, and oracle manipulation identified as the most frequent attack vectors [1, 2]. Decentralised wallets are particularly exposed, as private key storage interface flaws and inadequate multi-signature execution often result in irreversible asset losses. Decentralised exchanges (DEXs) are additionally prone to flash-loan attacks and liquidity pool drains due to their automated market-making logic lacking circuit breakers [3]. These technical flaws, however, are rarely extended to legal consequences.

Policy perspectives diverge across international bodies. The European Central Bank (ECB) points to operational resilience in wallet infrastructure and custody services, warning that interface vulnerabilities and key-storage defects create systemic entry points for asset misappropriation [4]. The Basel Committee on Banking Supervision (BCBS) addresses capital adequacy implications of crypto-asset exposures, yet leaves cross-border enforcement mechanisms largely unspecified [5]. The International Monetary Fund (IMF) adds concerns about "crypto-isation" in emerging economies, where wallet-based remittances bypass traditional oversight [6]. Despite these complementary warnings, none systematically trace how a specific operational failure—e.g., a compromised wallet private key—can cascade into ownership disputes or trad-

ing irregularities. As the ECB concedes, the transmission channels from DeFi operational vulnerabilities to legal and market instability remain underexplored [4]. Thus, risk taxonomies are mature, but their causal linkage to ownership and compliance outcomes is largely absent.

2.2 Research on Digital Assets Ownership Definition

The legal status of digital assets remains fragmented across jurisdictions. The UK Law Commission proposed a "third category" of property, culminating in the Property (Digital Assets etc.) Act 2025, which explicitly states crypto-tokens and NFTs as personal property [7, 8]. In contrast, civil-law systems show divergence: Germany treats crypto-assets as "other assets" but struggles with NFT acquisition requirements; China's Civil Code Article 127 offers only principled protection, leaving ownership conceptually uncertain; Poland has no dedicated legislation, creating legal vacuums [9-11].

Critically, most existing scholarship focuses on the threshold question—"Are digital assets property?"—while neglecting downstream risks. For instance, the decoupling of NFT on-chain ownership from copyright has generated frequent infringement disputes, yet few studies examine how this ambiguity affects trading behaviour or secondary-market pricing; Xie proposes a "four-rights separation" model but lacks empirical testing [12]. As Blandin et al. note, without definable property rights, crypto-assets cannot function credibly because users cannot enforce rights after theft—yet this observation is rarely translated into market-friction hypotheses [13]. Hence, a clear gap persists between legal ontology and its transactional consequences.

2.3 Research on Emerging Trading & Price Risks of Crypto Assets

DEX trading risks have been empirically illustrated by major exploits—e.g., the \$42 million GMX V1 attack (July 2025) and the \$128 million Balancer loss (November 2025)—but rigorous academic dissection remains scarce. Among scholarly works, Qin et al. provide a formal framework for flash-loan attack patterns, and OECD shows that absent circuit breakers allow cascading liquidations [14, 15]. However, these studies treat DEX operations as self-contained technical systems; they do not consider whether ambiguous ownership titles (e.g., disputed NFT provenance) exacerbate panic selling or hinder post-exploit recovery.

Price volatility is well documented but conceptually isolated. Crypto assets lack central stabilisers, and even stablecoins have exhibited high swings [16]. The IMF warns that markets may amplify flash crashes via instant settlement and chain reactions, but its analysis is mac-

ro-prudential and does not probe the micro-mechanism: when an ownership dispute arises—e.g., a court injunction or a security designation—market participants react with asymmetric information, triggering herding [6]. Empirical volatility studies typically attribute shocks to regulatory announcements or hack news, not to ownership-clarity events [17]. Thus, the causal pathway from ownership uncertainty to price turbulence remains uncharted.

2.4 Literature Gap

The three strands—operational vulnerabilities (as analysed by ECB and BCBS), legal ambiguity, and trading/price dynamics (as highlighted by IMF)—evolve in separate silos. No existing framework systematically integrates them into a causal chain that begins with technical operational flaws, leads to ownership indeterminacy, then produces transactional friction and price distortion, and ultimately creates compliance loopholes. Moreover, most contributions adopt a static risk taxonomy, while "emerging risks" are defined by constant mutation and regulatory lag [18]. To address these gaps, this paper proposes an integrated, dynamic framework that traces the full pathway from operational genesis through legal mediation to market outcomes and regulatory responses, bridging the technology-law-economics divide that currently fragments both research and policy design.

3. Emerging Risks and Transmission Mechanisms in Decentralised Finance

The literature reviewed in Chapter 2 reveals a clear gap: existing studies treat operational, legal, and market risks as separate domains. No integrated framework connects them into a coherent causal sequence. This chapter fills that gap. It unpacks four interconnected risk layers and then integrates them into a transmission mechanism that explains how technical failures evolve into legal disputes, market distortions, and regulatory gaps.

3.1 Operational Risks in DeFi Systems

Decentralised finance replaces traditional intermediaries with smart contracts and private-key control. Users hold assets directly, settle trades instantly, and rely on no central counterparty. This architecture offers autonomy, but it also removes the buffers that typically absorb operational failures.

The consequences are evident in the data. Wallet infrastructure is a persistent weak point. Private-key storage interfaces contain flaws that attackers routinely exploit. Multi-signature arrangements, intended to distribute control, are often poorly implemented. Phishing attacks continue to deceive users at scale [1, 2]. Decentralised exchanges present their own set of problems. Automated

market-making protocols, designed for efficiency, lack circuit breakers. Flash-loan attacks exploit this absence. Liquidity pools have been drained repeatedly [3]. Oracle manipulation adds another layer of risk: when price feeds are distorted, liquidations follow that would not otherwise occur. Custodial services, though technically less decentralised, are not immune—hacking and insider threats persist across the board.

What makes these failures consequential is not their technical character but their finality. A compromised private key transfers assets permanently. An exploited contract drains funds irreversibly. Courts cannot reverse these transactions. The European Central Bank acknowledges that the transmission from such vulnerabilities to legal and market instability has not been adequately studied [4]. Yet that transmission is precisely where the real risk lies. Operational failures are not endpoints; they are entry points to a longer chain of consequences.

3.2 Ownership Risks of Digital Assets

Once assets are lost or stolen, the question of ownership arises. The answer, under current legal frameworks, is far from clear. Digital assets do not fit neatly into traditional property categories. They have no physical form. No central registry records title. Possession—in the sense of controlling a private key—does not equate to legal ownership in any jurisdiction's courts.

Three specific uncertainties follow from this mismatch. First, when a private key is lost or stolen, no legal mechanism restores the owner's control. Courts cannot order a transaction to be reversed. The blockchain is immutable by design [8]. Second, NFT ownership and copyright are legally distinct, though purchasers often assume otherwise. Buying an NFT does not transfer the underlying intellectual property rights. Disputes have multiplied as a result, and each dispute undermines the perceived value of the asset in question [12]. Third, anonymous address records complicate enforcement. Creditors cannot easily identify debtors. Fraudsters cannot be easily traced.

Property rights economics offers a useful lens here [19]. Clear, enforceable rights are prerequisites for efficient exchange. Where rights are unclear, exchange breaks down. The "private-key-as-ownership" model, combined with the absence of judicial remedies, creates inherent indeterminacy. Cross-jurisdictional divergence makes matters worse. The United Kingdom has enacted legislation recognising crypto-tokens and NFTs as personal property. China's Civil Code offers only general protection. Poland has no relevant legislation at all [10, 11]. The result is a vacuum: rights are asserted by technology, not by law.

3.3 Transaction and Market Risks

Transaction and market risks arise from the environment

in which digital assets are traded. DEXs lack centralised surveillance. Trade-reversal is impossible. Front-running, sandwich attacks, and wash trading are routine features, not exceptions. Major exploits illustrate the scale of the problem—the \$42 million GMX V1 attack and the \$128 million Balancer loss are well-documented cases [14]. Fraudulent "air tokens" and pump-and-dump schemes proliferate because token issuance requires minimal effort and no regulatory approval. Over-the-counter markets, operating through unregulated intermediaries, carry settlement risks and counterparty fraud that are difficult to detect.

Ownership uncertainty amplifies these risks directly. When an asset's legal status is contested—through a copyright claim, a court injunction, or a regulatory classification—information asymmetry widens. Informed participants exit positions quickly. Uninformed participants react with herding behaviour. The result is flash crashes [17, 20]. Simulation studies suggest that a sudden ownership challenge can reduce NFT prices by 15 to 20 per cent within hours [21]. OECD shows that circuit breakers, where absent, permit cascading liquidations [15]. When ownership ambiguity is added to the equation, the effect becomes multiplicative rather than additive [22]. Ownership indeterminacy thus distorts price discovery, widens bid-ask spreads, and makes digital asset markets more volatile than their traditional counterparts.

3.4 Compliance Risks and Regulatory Gaps

Compliance risks emerge from the fragmentation of national regulatory frameworks, which creates pervasive regulatory arbitrage opportunities. The United States adopts an enforcement-based approach, with overlapping jurisdictions between the SEC (treating many tokens as securities) and the CFTC (treating them as commodities), generating significant legal uncertainty. The European Union has introduced MiCA, offering a comprehensive rulebook covering issuance, trading, and custody—yet it explicitly excludes NFTs and protocols, leaving sizeable grey areas. China adopts the strictest stance, prohibiting cryptocurrency trading and initial coin offerings, while its Civil Code offers only vague protection for digital property [10].

This divergence enables regulatory arbitrage: projects incorporate in jurisdictions, serve global users, and exploit loopholes where rules are absent or unenforced. The FATF's Travel Rule is implemented in only about 30% of countries, leaving vast unmonitored corridors [23]. More fundamentally, no mutual recognition mechanism exists for cross-border ownership judgments—a court order in Germany has no effect on a protocol operating in the Cayman Islands. Regulatory lag theory explains why this persists: regulation is inherently reactive, and its revision cycles trail innovation [24]. In DeFi, the absence of re-

porting further prolongs the information-gathering process for regulators. This fragmentation not only permits non-compliance; it also offers a fertile ground for it, as actors shift operations toward the weakest regulatory link, perpetuating and mutating risks.

3.5 Risk Transmission Mechanism

The four layers examined above are not separate problems. They form a causal sequence. Operational failures—compromised keys, exploited contracts—are the starting point. These failures create ownership uncertainty, because legal systems cannot restore control or reverse transactions. Ownership uncertainty, in turn, distorts trading behaviour: assets with contested status become harder to price and harder to trade. Market participants react under asymmetric information, producing sudden sell-offs and cascading liquidations. As these disruptions cross borders, they expose the lack of regulatory coordination and mutual enforcement mechanisms. Compliance gaps become visible—and exploitable. The exploitation of these gaps fosters new operational vulnerabilities, as protocols are updated hastily or forked without adequate security review.

The cycle is self-reinforcing. Each layer feeds back into the others. Regulatory lag ensures that new mutations outpace legal responses. This is what makes risks "emerging" in the truest sense: they are not static categories but dynamic processes that evolve with technology and regulation. The framework presented here directly answers the three research questions posed in Chapter 1. Operational flaws trigger ownership loss. Ownership ambiguity generates transaction and price risks. Regulatory fragmentation creates evolving compliance loopholes.

4. Policy Implications and Institutional Remedies

The risk transmission mechanism set out in Chapter 3 points to a clear conclusion: emerging risks in finance are not inevitable outcomes of technological change. They are exacerbated by legal fragmentation, sluggish regulatory responses, and a lack of international coordination. Intervening at multiple points along the causal chain is necessary if these risks are to be contained. Four areas offer the most promise: legal classifications, tightening technical standards, improving cross-border judicial cooperation, and adopting more flexible regulatory methods. Each has its own difficulties, and none is a cure-all, but together they point toward a more coherent institutional response.

4.1 Towards a Common Legal Language for Digital Assets

Countries classify digital assets differently, and this di-

versity creates real problems. The United Kingdom has passed a law treating crypto tokens and NFTs as personal property. Germany calls them "other assets" but has not resolved issues specific to NFTs. China's Civil Code gives only general protection, leaving ownership rights unclear. Poland has no relevant law at all.

Since digital assets move across borders without restriction, this mix of rules causes confusion. Market participants cannot be sure which law applies. Courts in one country cannot make their decisions effective in another. The same asset may count as property in one place and have no legal status elsewhere. This uncertainty is not just an inconvenience; it holds back the whole market.

International bodies could help reduce this confusion. UNIDROIT and the Hague Conference have worked on model laws for cross-border business before [25]. A model law for digital assets would not force all countries to adopt the same rules. It could set out basic principles for how rights are created, transferred, and lost, while letting each country adapt them locally [8]. It could also explain how on-chain transfers relate to off-chain intellectual property, which has caused many disputes over NFTs. Such a model would give countries a common reference point and reduce uncertainty without requiring identical laws across the board, which is unrealistic given the differences in legal systems around the world. The process would be slow, but even a non-binding model can shape national laws and court decisions over time.

4.2 Raising the Bar for Technical Resilience

Operational failures start the entire risk chain, so cutting down how often they happen and how bad they are should be a top priority. The question is how to do this without driving up costs so much that innovation moves elsewhere.

One option is to set minimum security rules for wallet providers, DEX operators, and smart contract auditors. These rules could cover joint signatures for large transfers, regular outside audits, and automatic trading halts when markets turn unstable [26]. Some platforms already follow these practices, but they are not universal. When security standards vary widely, attackers go after the weakest targets.

A voluntary certification program could work alongside these rules. Platforms that meet recognized standards could get limited legal protection if a breach occurs. The logic is straightforward: certification lowers legal exposure, so platforms have a clear reason to participate. International groups like ISO or BIS could help develop the technical criteria. But certification cannot fix legal uncertainty. A clean audit does not prove who owns an asset. It only makes theft less likely in the first place. Even the best security cannot prevent ownership fights after a breach has happened. So technical safeguards are essen-

tial, but they are not enough on their own. They work best when paired with legal and regulatory improvements.

4.3 Making Cross-Border Enforcement Work

The enforcement gap is the hardest problem to fix, because it involves national sovereignty. A court ruling in Germany does not affect a protocol based in the Cayman Islands. But the assets move freely across borders. This mismatch between where disputes arise and where they can be resolved is a fundamental weakness of the current system.

Bilateral or multilateral agreements could help. A treaty that allows countries to recognise and enforce each other's digital asset judgments would let court orders from one country be carried out through intermediaries or protocol-level tools in another. This idea is not new. Similar arrangements already exist for commercial arbitration and cross-border insolvency. The difficulty is negotiating terms that enough countries will sign on to. Different legal systems have different priorities, and reaching agreement on digital assets would take time and diplomatic effort [27].

The FATF could also do more. At present, its Travel Rule deals only with anti-money laundering and is enforced in less than a third of countries [23]. Expanding it to cover civil matters like ownership verification and fraud prevention would close some of the gaps that projects now use to avoid oversight. But treaties and rule changes move slowly. In the meantime, looser arrangements like information-sharing networks, joint supervisory groups, and bilateral understandings can help build trust. Jurisdictional diversity is not going away. The aim is to stop it from becoming a permanent weak point that market players can repeatedly exploit [24].

4.4 Rethinking Regulatory Timing and Modality

Regulation is slow because legislation takes time. The standard process, which involves spotting a problem, talking to stakeholders, writing a bill, and getting it passed, often runs for years. By the time a new law takes effect, the technology it was meant to govern has already changed. This lag is built into the system [24].

One way around this is to split primary rules from technical adjustments. Primary laws would set out the main principles, such as who is liable for poor security, what standards custodians must meet, and what rights asset holders have. Technical details like capital levels, disclosure requirements, and trading halts would be left to agencies that can act more quickly. Regulatory sandboxes, which several countries already use, offer a way to test this idea [28]. They let new protocols run under temporary rules while regulators collect information that can later

guide permanent frameworks.

Some have suggested dynamic rule-making, where thresholds update automatically based on data from the blockchain. This raises fair questions about transparency and control. Who picks the metrics? How are the systems checked? Could they be gamed? These concerns need answers before any such system is put in place. But they should not stop the conversation. A consultative process that includes regulators, industry participants, and technical experts could put proper safeguards in place. Human oversight would still be central. The aim is not to replace judgement with automation, but to give regulators better information more quickly so they can act before problems grow out of hand.

4.5 How the Proposals Fit Together

Each of these proposals reinforces the others. Legal definitions reduce the ambiguity that fuels market volatility. Technical standards lower the incidence of operational failures. Cross-border cooperation closes the enforcement gaps that enable arbitrage. Adaptive regulation shortens the response time that allows new risks to crystallise. Together, they form a comprehensive strategy to interrupt the risk transmission chain at each of its nodes. The real challenge is political, not technical: persuading national authorities to trade some autonomy for greater collective resilience.

5. Conclusion

This study examined emerging risks in decentralized finance across three interrelated dimensions—ownership, trading, and compliance—and was driven by three core research questions: how operational flaws trigger ownership loss; how ownership ambiguity generates transaction and price risks; and how regulatory fragmentation produces evolving compliance gaps. The analysis yields three main findings. First, operational failures such as hacks, smart contract exploits, and compromised private keys are not isolated technical incidents; because blockchain transactions are irreversible and conventional legal remedies cannot restore control, these failures initiate a causal chain that extends well beyond the immediate loss. Second, ownership indeterminacy is not merely a theoretical legal puzzle; it directly distorts market behaviour by creating information asymmetries that provoke herding and sharp price swings. Simulation evidence suggests that ownership disputes can exert significant downward pressure on asset prices, though the precise magnitude requires further confirmation. Third, the lack of harmonised rules across jurisdictions does more than generate confusion—it actively encourages regulatory arbitrage, and the resulting compliance gaps allow risks to propagate across borders without effective oversight.

Beyond these individual findings, the paper demonstrates that the four risk layers examined—operational, ownership, market, and compliance—are not separate categories but form a dynamic and self-reinforcing chain: failure generates dispute, dispute produces market disruption, disruption exposes regulatory gaps, and gaps in turn invite new operational vulnerabilities. This ongoing, mutating cycle is what distinguishes emerging risks from more traditional, stable forms of financial risk. The integrated framework developed here fills a clear gap in the literature, as prior work treated technical, legal, and economic risks in isolation, whereas this study shows they are connected through identifiable causal pathways. This integrated perspective offers a stronger basis for both academic analysis and policy design.

The policy implications of this framework point toward a coherent institutional response. The four proposals advanced in this paper—harmonised legal definitions, technical resilience standards, cross-border enforcement cooperation, and adaptive regulatory modalities—are not independent fixes but complementary interventions that can interrupt the transmission chain at each of its nodes. Legal harmonisation reduces the ownership ambiguity that fuels volatility; technical standards lower the incidence of operational failures; cross-border cooperation closes enforcement gaps that enable arbitrage; and adaptive regulation shortens the response time that allows new risks to crystallise. If pursued in parallel, these measures could align regulatory capacity with the pace of technological innovation. However, the real challenge is not technical but political: persuading national authorities to trade some degree of regulatory autonomy for greater collective resilience. The feasibility of specific proposals—such as a model law, a mutual recognition treaty, or a certification system—will vary across legal systems and require context-specific adaptation. Bilateral and multilateral discussions, information-sharing networks, and joint supervisory initiatives can build trust incrementally, even as longer-term legal instruments are negotiated. Decentralised finance offers genuine benefits in terms of access, efficiency, and financial inclusion, but these benefits will not materialise if the legal environment remains fragmented and regulatory responses continue to lag behind technological change. The task is pressing, but it also presents an opportunity to build governance systems that are both responsive and durable—systems that can keep pace with the innovation they are meant to oversee.

Nevertheless, this study has several limitations. It is conceptual rather than empirical; it draws on published sources—including reports of major exploits, comparative legal analyses, and simulation studies—but does not include original statistical testing. The causal claims, while logically derived and supported by existing evidence, await empirical validation through event studies

or regression analysis that can measure the magnitude of each step in the transmission chain. As such, the findings should be treated as propositions for further testing rather than as proven facts. The framework also assumes that market participants respond rationally to new information about ownership status. In cryptocurrency markets, this assumption is open to question: sentiment, speculation, and crowd behaviour often drive prices as much as, or more than, careful analysis of fundamentals. Incorporating behavioural factors—such as cognitive biases and social contagion—would strengthen the model and better account for the actual dynamics observed in practice. Furthermore, the policy recommendations remain general in nature. This study does not examine in detail how each proposal would be implemented in specific national contexts, what legal or institutional adjustments would be required, or what political obstacles might arise. Practical feasibility, sequencing, and cost-benefit trade-offs have not been assessed. These limitations do not undermine the utility of the framework, but they delimit its current scope and point directly to the work that remains. Several avenues for future research are particularly promising. Empirical studies could employ event-study methodologies to measure price reactions to ownership-related events—court decisions, copyright claims, regulatory classifications—and thereby test the proposed link between ownership clarity and market stability. Comparative legal research could examine how different jurisdictions resolve digital asset disputes, identifying which procedural features yield faster, cheaper, and more predictable outcomes, and thus inform the design of mutual recognition arrangements. Agent-based simulations or system dynamics models could explore how varying speeds of regulatory updating affect overall systemic risk, helping to identify optimal intervention points and intensities. Behavioural studies could investigate how traders actually process ownership information—whether they overreact, underreact, or follow simple heuristics—and thereby provide a more realistic micro-foundation for the transmission mechanism. Each of these directions would advance both theoretical understanding and practical governance of digital assets.

References

- [1] Caldarelli Giulio, Ellul Joshua. The blockchain oracle problem in decentralized finance—a multivocal approach. *Applied Sciences*, 2021, 11(16): 7572.
- [2] Zhou Liyi, Xiong Xihan, et al. SoK: Decentralized finance (DeFi) attacks. 2023 IEEE Symposium on Security and Privacy (SP), IEEE, 2023: 2444-2461.
- [3] Xu Jiahua, Paruch Krzysztof, et al. Sok: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. *ACM Computing Surveys*, 2023, 55(11): 1-50.

- [4] European Central Bank. ECB Annual Report 2024. Frankfurt: European Central Bank, 2024. [EB/OL]. <https://www.ecb.europa.eu/pub/annual/html/index.en.html>.
- [5] Basel Committee on Banking Supervision. Prudential treatment of cryptoasset exposures. Basel: Bank for International Settlements, 2022. [EB/OL]. <https://www.bis.org/bcbs/publ/d545.pdf>.
- [6] Böhme Rainer, Christin Nicolas, et al. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 2015, 29(2): 213-238.
- [7] Great Britain. Law Commission. Digital assets: final report. London: Law Commission, 2023. [EB/OL]. <https://lawcom.gov.uk/project/digital-assets/>.
- [8] Low Kelvin FK, Hara Megumi. Cryptoassets and property. *Research Handbook on European Property Law*, Edward Elgar Publishing, 2024: 146-156.
- [9] Blocher Walter, Braegelmann Tom H, et al. *Rechtshandbuch smart contracts*. CH Beck, 2019.
- [10] Wang Liming. How to confirm data rights? *Chinese Journal of Law*, 2023, 45(4): 56-73.
- [11] Cryptocurrency regulation landscape in Poland: 2024 update [EB/OL]. (2023-12-09) [2026-07-18]. <https://cryptocurrency.law/cryptocurrency-regulation-landscape-in-poland-2024-update/>.
- [12] Xie Xiao. Beyond the Distinction between Real Right and Creditor's Right: On the Right to Network Virtual Property as a Dominant Right over Property. *Law and Social Development*, 2023(4): 44-62.
- [13] Blandin Apolline, Cloots Ann-Sophie, et al. Global cryptoasset regulatory landscape study. Cambridge: Cambridge Centre for Alternative Finance, 2019. [EB/OL]. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/>.
- [14] Qin Kaihua, Zhou Liyi, et al. Attacking the DeFi ecosystem with flash loans for fun and profit. *Financial Cryptography and Data Security*, Springer, 2021, 12674: 3-32.
- [15] OECD. DeFi liquidations: volatility and liquidity. *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 48, OECD Publishing, 2023. [EB/OL]. https://www.oecd.org/en/publications/defi-liquidations_0524faaf-en.html.
- [16] Gorton Gary B, Klee Elizabeth C, et al. Leverage and stablecoin pegs. *Journal of Financial and Quantitative Analysis*, 2025, 61(1): 99-136.
- [17] Feinstein Brian D, Werbach Kevin. The impact of cryptocurrency regulation on trading markets. *Journal of Financial Regulation*, 2021, 7(1): 48-99.
- [18] Cambridge Centre for Risk Studies. What do we mean when we talk about 'emerging risks'? [EB/OL]. (2019-04-26) [2026-07-18]. <https://risk-studies-viewpoint.blog.jbs.cam.ac.uk/2019/04/26/what-do-we-mean-when-we-talk-about-emerging-risks/>.
- [19] Coase Ronald Harry. The problem of social cost. *The journal of Law and Economics*, 2013, 56(4): 837-877.
- [20] Gibson James. Risk aversion and rights accretion in intellectual property law. *Yale Law Journal*, 2006, 116: 882.
- [21] Cheon Gyeombi, Choi Yunmin, et al. When scarcity backfires: Cyber scam impact on NFT market prices. *Finance Research Letters*, 2025, 86: 108824.
- [22] Chen Yan, Bellavitis Cristiano. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 2020, 13: e00151.
- [23] Financial Action Task Force. Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers. FATF, 2025. [EB/OL]. <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>.
- [24] Kane Edward J. Changing incentives facing financial-services regulators. *Journal of Financial Services Research*, 1989, 2(3): 265-274.
- [25] Smith Edwin E, Weise Steven O. *Unidroit Principles on Digital Assets and Private Law—A Comparison to the Uniform Commercial Code, with an Emphasis on Control, Transfer, Custody, Innocent Acquirers, and Secured Transactions*. UNIDROIT Principles on Digital Assets and Private Law: Context, Content, Perspectives, Springer, 2026: 17-44.
- [26] Bourveau Thomas, Brendel Janja, et al. Decentralized Finance (DeFi) assurance: early evidence. *Review of Accounting Studies*, 2024, 29(3): 2209-2253.
- [27] Financial Stability Board. Thematic review on FSB global regulatory framework for crypto-asset activities. Basel: FSB, 2025. [EB/OL]. <https://www.fsb.org/2025/10/thematic-review-on-fsb-global-regulatory-framework-for-crypto-asset-activities/>.
- [28] Buckley Ross P, Arner Douglas, et al. Building FinTech ecosystems: regulatory sandboxes, innovation hubs and beyond. *Wash. UJL & Pol'y*, 2020, 61: 55.