ISSN:3030-332X
Impact factor: 9,493
International journal of scientific researchers
2nd International Conference on Green Economy & Sustainability 2.0, 30 April 2026

THE ROLE OF DECENTRALIZED FINANCE IN RESHAPING FINANCIAL RISK MANAGEMENT PRACTICES

Isakova Marjona Ahmadi kizi[1],
Dr. N. S. V. N. Raju[2],
Dr. Pavani Tirumala Grudanti[3]

[1]Master of Business Administration, Faculty of Management, Sharda University Uzbekistan
isakovamarjona20@gmail.com

[2]Assistant Professor, Faculty of Management, Sharda University Uzbekistan
shyam.nagala@shardauniversity.uz; pavani.grudanti@shardauniversity.uz

Abstract: Decentralized Finance (DeFi) is positioned as the disruptor of finance that is changing the underlying premise of customary finance and changing the underlying risk landscape. We discuss the role of DeFi in changing risk management in customary finance through the lens of risk exposure, risk mitigation and risk architecture. However, with this study focusing on a variety of DeFi protocols, a comparison is drawn between risk profiles of DeFi and Financial Institutions (FIs), where the intrinsic risks of DeFi (smart contract risk, liquidity risk and regulatory arbitrage) are compared to the benefits of such (transparency, accessibility and counterparty risk). Given the rise of permissionless DeFi protocols, with their decentralized governance, customary regulatory models that rely on centralized intermediaries may be disrupted within the customary risk management regime. However, DeFi creates programmable but immutable risks through smart contracts, where programming errors, bugs or exploits can cause meaningful losses. DeFi liquidity risks are further exacerbated by the highly volatile nature of DeFi markets, and by the use of AMMs, or automated market makers. DeFi projects face regulatory arbitrage, as many of them operate in the grey areas of what constitutes regulation. At the same time, proponents of DeFi point out that DeFi has the potential to reduce some of the counterparty risk associated with customary finance by removing intermediaries, introducing transparency with on-chain data, and addressing the needs of the unbanked. However, the analysis also shows that while some types of risks are reduced in DeFi, new types of obligations emerge that will need to be addressed by new forms of regulation. We propose a DeFi regulation that balances innovation with financial system stability and consumer protection, and includes a hybrid decentralized governance and regulation norms, to ease compliance while preserving innovation incentives. Possible solutions have been discussed, such as mechanisms for on-chain surveillance, transparency requirements for smart contract code, and holding DeFi protocol developers and governance models responsible.

Keywords: Decentralized finance/DeFi, Customary finance, Risk management, Smart contracts, Liquidity risk, Regulatory oversight, Financial innovation.

Introduction

DeFi disrupts the financial industry by upending customary concepts, standards, and risk assessments. DeFi protocols stand at the forefront of the blockchain revolution by allowing users to conduct financial services without intermediaries. Peer-to-peer trade, lending, and asset management services at a global scale may threaten the existing financial system, and DeFi would require entirely new risk management strategies, as protocols are decentralized and operate in a self-executing manner through smart contracts on a blockchain. These platforms promise democratizing finance through greater accessibility, transparency, and efficiency. At the same time, they correspond to unprecedented risks in terms of technical and regulatory uncertainty. Incumbent financial firms, with their regulated and centralized models, have vested interests in adaptation. Scaling DeFi up may increase financial inclusion and lower the risk of counterparty defaults. On the other hand, the absence of intermediaries creates

challenges for accountability and risk management and raises questions of stability. These issues include smart contract failure, lack of liquidity and regulatory arbitrage, where DeFi services fall outside the jurisdiction of conventional regulation. Understanding these risks in the context of customary financial processes is important in developing well-targeted strategies to reduce their potential. The pseudonymity of DeFi participants makes it increasingly difficult to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements, and for regulators to implement and enforce such requirements. The pace of innovation within DeFi is faster than the pace of customary financial regulation, with emerging financial innovations outpacing existing legal frameworks. We will study DeFi protocols and customary financial institutions at the same time to compare and contrast their risk exposures, risk mitigations, and system-wide vulnerabilities.

The goal of this research effort will be to characterize the differences between the risks in DeFi and highlight the potential offsetting benefits such as transparency or efficiency. The paper proposes a regulatory regime unique to decentralized finance that encourages innovation while ensuring the safety and soundness of the financial system and protecting consumers. The hybrid framework combines the transparency of on-chain architecture with the existing body of off-chain regulatory infrastructure. This hybrid architecture would help embrace regulatory assurances through real-time data monitoring and auditing of smart contracts, while allowing DeFi innovation to breathe. It would close the divide between customary finance and DeFi, and ease the study and understanding of new financial ecosystems as they emerge. The findings of this study are aimed at assisting policymakers, financial institutions, and DeFi innovators in formulating responsive and forward-looking regulatory frameworks tailored to the needs of a decentralized financial ecosystem. Overall, this research endeavors to support the efforts towards establishing a balanced financial ecosystem that fosters innovation while ensuring stability and consumer trust. The paper will consider the potential for convergence of customary finance and DeFi, and how that convergence can inform regulatory innovation in the face of technological disruption.

1.1 Problem Statement

The extremely fast emergence of the Decentralized Finance (DeFi) ecosystem is a two bladed evolution of the world financial system, representing unprecedented opportunity, together with extremely deep systemic challenges, to the models of financial risk management. The DeFi project ecosystem is speaking the language of blockchain and smart contracts, enabling peer-to-peer transaction flow, and financial inclusion, bypassing financial intermediaries. However, the very decentralization of smart contracts also creates risks that neither today's financial institutions nor regulators know how to deal with. Smart contracts can have coding errors, exploits and vulnerabilities that can lead to catastrophic losses, such as in the case of the 2021 Poly Network hack, when the faulty smart contract code was exploited. Furthermore, DeFi users are pseudonymous, making it impossible to implement AML/KYC, and increasing the risk of DeFi becoming a venue for illicit activity that circumvents existing regulations. Furthermore, given that there is no central authority, counterparty risk cannot be reduced the usual way. DeFi markets have additional liquidity risk. Factors like over-leverage, volatility, and manipulation of liquidity pools could lead to a domino effect where several liquidity protocols fail. These failures are similar to the contagious liquidity crises of customary finance, but these events happen at an accelerated timescale due to the algorithmic nature of DeFi. As DeFi is cross-border, regulatory arbitrage is more easily executable. The dearth of any regulatory framework discourages regulatory consumer protection and market maintenance. Additionally, substantial innovation in DeFi is faster than that for customary markets. Thus, regulators should have a well-developed framework for risk management, otherwise they are often just reactants, rather than actors to a well-structured market environment. In the absence of a strong iterative regulatory regime for DeFi, the rapid proliferation of DeFi technologies could exacerbate systemic financial risks, erode trust in and acceptance of digital financial technologies, and blur the line between financial innovation and financial fraud. An on-chain/off-chain regulatory framework that embraces transparency, accountability, real-time smart contract audit- and monitoring, and cross-regulator collaboration at the global level may help reduce some kinds of DeFi-related systemic risks, while preserving the creative destruction that fuels financial

innovation. Understanding the sources of risk in DeFi, from coding bugs to regulatory loopholes, is vital for creating a balance between fostering decentralized innovation and ensuring financial stability.

1.2 Research Objectives

The research's overarching objective is a fundamental exploration of the radical impact of DeFi on customary financial risk management practices, highlighting the unmatched opportunities and emerging risks of this nascent financial structure. By being a decentralized, transparent and automated financial framework, DeFi disrupts the historical foundations of financial architecture. Additionally, the review identifies how the disruptive nature of DeFi (decentralization, transparency and automation through smart contracts) reshape risk management practices, specifically for counterparty risk, liquidity and credit risks, and operational resilience. This paper will conclude whether the risk management of DeFi protocols improves or worsens compared to customary finance, given the disintermediation of customary intermediaries, increased financial inclusion, the use of algorithmic governance, and the exposure of markets and users to new technological and systemic risks. One aim involves summarizing and generalizing the comparison between the financial system and DeFi protocols and whether innovations in DeFi are causes of risk reduction or causes of financial instability. Key research topics include the risks and functioning of smart contracts, decentralized lending protocols, automated market makers (AMMs), liquidity pools, oracle attacks, flash loan attacks, rug pulls, and governance attacks (Schär, 2021). We will seek to establish a forward-looking regulatory framework that is informed by the unique DeFi stack, while promoting innovation and maintaining the integrity of the underlying system. We will consider hybrid regulatory frameworks that can deliver transparency through on-chain data analysis, whilst also accommodating the legal regulatory objectives of protecting consumers, embedding integrity in the financial system, and reflecting the systemic nature of decentralized ecosystems. This research seeks to inform financial regulators, policymakers, and DeFi innovators on integrating flexible, technology-improved risk management practices that safeguard both the decentralized and customary financial systems' integrity and stability in an increasingly digitized environment.

1.3 Research Questions

By answering the following interrelated research questions, the aim is to provide a thorough understanding of the relationships and trends between DeFi and customary financial risk management. What are the differences and similarities in DeFi and customary financial institutions with respect to their risk profiles in areas like counterparty risk, volatility of liquidity, credit risk, and operational resilience (Zetzsche et al., 2020)? Second, what new vulnerabilities are created by DeFi's architectonic principles of programmatic immutability, decentralized governance, and permissionless innovation, and how do these vulnerabilities escape or circumvent existing regulatory regimes? (Gudgeon et al., 2020). Third, how can regulators proactively manage systemic vulnerabilities in DeFi protocols caused by smart contract exploits, liquidity collapse, and governance failures, while still fostering innovation in a jurisdiction where they lack jurisdictional authority over such protocols? (Chen & Bellavitis, 2020). Fourth, can blockchain analytics, automatic risk monitoring and risk assessment tools, smart contract auditing, real-time data supervision, and other advanced technologies be leveraged to achieve more transparency, accountability, and consumer protection in DeFi systems with effective and efficient policy frameworks without increasing systemic risk and while being consistent with decentralization principles? Finally, can we develop a hybrid regulatory framework that strikes the right balance between decentralized transparency and centralized enforcement in order to further financial stability, support innovation, and improve the resilience of the financial system (Allen & Gensler, 2020)? These research questions aim to clarify the multidimensional impacts of DeFi on customary finance stability and shed light on the design of resilient, adaptable, and anticipatory financial regulation suited to the characteristics of a decentralized financial universe.

1.4 Significance of the Study

Thus, this research paper is of value because it could contribute to filling the gap in the academic discourse and regulatory evolution of DeFi in relation to the transformation of the risk management of conventional finance. As DeFi continues to disrupt customary financial intermediation through

decentralization, automation, and open information, understanding how it impacts risk management consolidation is important to ensuring financial stability, fostering innovation, and protecting market participants. This paper will also be of interest to financial regulators and policymakers, customary financial institutions, and DeFi developers and users. For regulators and policymakers, the paper highlights how the three defining pillars of DeFi (permissive infrastructure, smart contract automation, and decentralized governance) weaken customary regulatory architecture and the need for innovative, technology-driven regulatory frameworks capable of addressing systemic risk while still promoting innovation (Zetzsche et al., 2020). Customary financial institutions that are being disrupted by DeFi technology efficiency might be informed by this study's findings to rethink their risk governance approach, as well as potential technology integration and collaboration with DeFi protocols (Chen & Bellavitis, 2020). DeFi entrepreneurs and developers can learn about systemic risks in decentralized networks from this study's findings to help build highly secured and resilient financial protocols (Gudgeon et al., 2020). Apart from this, the basis of financial inclusion through DeFi, which allows open, trustless financial services for the unbanked and underbanked populations globally, is specifically discussed (Schär, 2021). Associated risks with this financial disintermediation model such as smart contract attacks, oracle manipulations, and liquidity crises are analyzed and the paper subsequently provides solutions for such events. This research seeks to develop a potential regulatory framework that accommodates both on-chain transparency and off-chain rule of law enforcement, thus enabling the sustainable and responsible evolution of DeFi. By doing so, this work will help to foster integrity, accountability, and stability within this rapidly evolving financial ecosystem, thereby providing a subtle and thorough understanding of the disruptive potential of DeFi and offering actionable and data-driven regulatory strategies for navigating the complexities of an increasingly decentralized financial landscape (Allen & Gensler, 2020).

1.5 Scope and Delimitations

It also adds to broader and multi-dimensional studies that assess the impact of DeFi on customary financial risk mitigation processes, focusing on the main aspects of counterparty, liquidity, credit, and operational resilience risk (Schär 2021). Finally, it focuses on the main components of DeFi, including decentralized exchanges (DEXs), automated market makers (AMMs), borrowing and lending protocols, liquidity pools, and smart contracts (Chen & Bellavitis 2020). The work will incorporate the regulatory implications of DeFi and propose a hybrid regulatory approach that merges the on-chain transparency of DeFi structures with a sense of off-chain accountability so as to balance innovation with financial stability (Zetzsche et al., 2020). The work is conducted from an international perspective but explicitly takes into account differences in regulatory approaches across different jurisdictions. In this paper, we only examine the DeFi use of blockchain technology, avoiding other uses such as for supply chain management or decentralized identity. However, it is useful to note that DeFi is interlinked with the overall crypto ecosystem. For the purposes of this paper, we only consider DeFi platforms and applications, excluding other crypto assets such as Bitcoin (BTC) or Ether (ETH) unless directly relevant to the DeFi ecosystem (Allen & Gensler, 2020). This analysis relies on existing academic literature, industry reports and publicly available data related to DeFi. This is because the industry is very dynamic and future innovation may bring with it new potential threats which are beyond scope of this analysis. The goal is to investigate system-level risks and not end user risks (such as risks to end users' investments or cyber risks) to appreciate the macroeconomic impact of DeFi on financial stability (Gudgeon et al., 2020). In spite of its limitations, the findings of this analysis are useful to anyone looking to understand how DeFi could disrupt existing financial systems and how policy reforms can make financial systems more resilient, inclusive, and secure as the economy shifts towards decentralized financial systems.

2. Literature Review

2.1 The theoretical framework of DeFi and risk

DeFi is the process of recreating financial instruments using public distributed ledger technology and smart contracts to replace intermediaries. These theories, which support decentralization and

blockchain, are inclusive of financial intermediation theory, efficient market hypothesis (Fama, 1970), and agency theory (Jensen & Meckling, 1976). DeFi replaces intermediaries such as banks with peer-to-peer transactions, supported by self-executing smart contracts, with a prospect of greater transparency and lower transaction costs (Schär 2021). This reflects the idea of disintermediation, whereby technology progressively eases the replacement of customary financial intermediaries (Allen & Santomero, 1998). However, the easy access from decentralized infrastructure exposes the ecosystem to unprecedented risks such as smart contract exploits, fragmented liquidity (Gudgeon et al., 2020), or regulatory arbitrage. DeFi constitutes a variety of primitives, such as Automated Market Makers (AMMs) which use algorithms to determine liquidity provisioning (Adams et al., 2021) and decentralized lending protocols (e.g. Compound or Aave) that use over-collateralization to reduce credit risks (Kulechov, 2020). These mechanisms are similar to the Modigliani-Miller theorem (Modigliani & Miller, 1958), which states that the capital structure is irrelevant in a frictionless market. Nevertheless, there are frictions in a DeFi market in the form of gas fees, impermanent loss and oracle manipulation which deviate from this ideal model and introduce inefficiencies and another layer of risk. DeFi risk management employs algorithmic governance, decentralization, and token-based incentive design (Buterin, 2014), leveraging game theory and mechanism design to transfer risk management from customary institutions to protocols within a decentralized community, thereby redistributing the risks and rewards among the community participants. However, there are systematic risks such as flash loan attacks, inter-protocol dependencies, and market contagion, that can also be analyzed from network theory and contagion of financial models (Easley et al., 2019). The interdependencies between DeFi protocols using the same liquidity pools or oracles could cause the contagion to manifest and trigger a cascade failure across multiple DeFi protocols. Public choice theory (Buchanan & Tullock, 1962) supports the regulatory approach taken to DeFi, and the core tension between decentralized and regulated approaches. The code-first and global nature of DeFi creates unique pressures to ensure regulatory frameworks remain principles-based and adapted for future technologies without stifling innovation (Arner et al., 2020). Researchers are moving towards hybrid forms of accountability that use on-chain traceability and off-chain legal liability. Combined, these two accountability forms create the best of decentralized efficiency and regulatory security. Additionally, other literature has suggested that distinguishing different types of risk based on DeFi-specific elements may be useful: Schär (2021) distinguishes between technical risks (smart contract bugs), economic risks (liquidity pool depletion), and governance risks (protocol takeovers). To target the right risk, monitoring solutions need to be developed considering the specificities of DeFi's permissionless nature and systemic relevance. Decentralized insurance protocols and algorithmic risk buffers (Gudgeon et al., 2020) can be seen as the current trends in risk management innovation of DeFi. Economic theory, financial innovations and regulatory approach constitute the framework of the study. Theories highlight how DeFi's risk profile can change and impact the customary finance system. In an era of rapid innovation, it is important to understand the theory to maneuver the crossroads of decentralization, security, and regulation that DeFi presents as it matures.

2.2 Risks compared to customary finance

This contrasts with TradFi, where, due to the regulated, centralized, intermediary structure, risk exposure is buffered through the credit screening process and deposit insurance (Mishkin, 2018). DeFi, by contrast, differs in its decentralization and technological innovations. On the other hand, DeFi smart contracts are immutable and permissionless and may expose users to risks such as counterparty risk. In customary finance, trusted intermediaries, such as clearinghouses and banks, are used to settle transactions (Hull, 2018). In DeFi, smart contracts have replaced intermediaries. Smart contracts eliminate counterparty risk but expose users to smart contract risk and security breaches (Zeng, 2021). An example was the 2016 DAO hack, which drained the DAO of US$60 million by exploiting a flaw in the smart contract code (Siegel, 2016). When exploits occur, unlike in TradFi where contracts can be unwound through judicial systems or central authorities, the immutability of DeFi protocols provides no recourse for victims. DeFi protocols have sought to reduce this risk through thorough smart contract audits, bug bounties, and decentralized insurance for smart contract failure such as Nexus Mutual

(Schär, 2021). Market risk in DeFi differs from TradFi risk in part because circuit breakers, lender-of-last-resort intervention, and other monetary policy interventions are often not available (Cecchetti & Schoenholtz, 2020). There is a significant benefits of fintech adoption, such as improved accessibility and reduced operational costs, particularly among younger, educated professionals in tech-centric industries (Kumar.D et al 2025).

DeFi markets are continuous and automated, and as a result differ in their market structures. DeFi markets are also prone to greater volatility due to liquidity dislocation and programme unwinds (Harvey et al., 2021). For example, the collapse of Terra's algorithmic stablecoin throughout 2022 illustrated how DeFi systems are prone to systemic collapse in the absence of regulatory or top-down interventions. As a result, systems such as MakerDAO have developed more resilient stablecoin designs based on more than one type of collateral. Some have proposed hybrid models that combine algorithmic stability and a reserve of legacy assets (Malcolm, 2022). Liquidity risk is another area of difference. Legacy monetary systems rely on central banks to provide liquidity during crises to ensure the stability of the financial system (Freixas et al., 2000). DeFi protocols use 'decentralized liquidity pools' maintained by algorithmic incentives instead. Additionally, there is the concept of impermanent loss where LPs face losses when the price of the pool diverges from the market price of the contained tokens (Adams et al., 2021). The context of such a mechanism is particularly problematic during highly volatile periods, when liquidity might be drained from the system all at once, causing substantial slippage and instability in the protocol. One potential solution is to implement variable transaction fees based on volatility, as proposed in Uniswap v3 (Adams et al., 2021). Regulatory and compliance risks are distinct. Customary finance functions in a heavily regulated environment, where mechanisms such as anti-money laundering (AML) and know-your-customer (KYC) laws exist to protect against fraud and maintain the integrity of markets (Brummer, 2019). DeFi protocols stress pseudonymity and open access. This is helpful for financial inclusion, but also for money laundering and tax evasion (Schär, 2021). Since DeFi innovation occurs at a much faster pace than regulators can handle, it has become essentially unregulated, creating a regulatory arbitrage where it is hard to regulate and enforce (Arner et al., 2020). Later forms of hybridized identity verification (for example, Soulbound tokens) emerged, balancing user privacy with regulatory compliance (Buterin, 2022). The operational risks of these strategies are also quite different, with customary institutions being susceptible to human error, operational error, and cyber attacks (Basel Committee on Banking Supervision, 2011). The same risks apply to DeFi. In addition, DeFi is subject to composability risks, the property of protocols to be combined and stacked (Zeng, 2021). In practice, composability leads to a "house of cards" in which the failure of one protocol generates systemic risk for other protocols. To reduce these risks, many DeFi protocols have started adopting modular design principles and fail-safe design. As an example, Aave has a safety module which absorbs losses using staked tokens (Kulechov, 2020). Understanding these divergent risk profiles will be critical in designing hybrid risk management frameworks that blend DeFi's innovation with the safety instruments of TradFi to foster innovation in a stable way.

2.3 Regulatory difficulties

The fast-paced rise of DeFi poses unmatched challenges for regulators. Regulating DeFi is vastly different from regulating customary finance that is governed by a legal and regulatory framework aimed at consumer protection, stable pricing, and preventing fraud and illicit behavior (Brummer, 2019). Given their decentralized nature, DeFi applications offer challenges in enforcing such regulation. This pseudonymous and permissionless nature of the applications can be a positive thing, as it increases financial inclusion. Conversely, it can be used for money laundering, tax evasion, or for financing other illegal activities (Schär, 2021). Furthermore, customary finance is subject to anti-money laundering (AML) and 'know your customer' (KYC) regulations, which require that regulated entities verify the identity of their clients (Arner et al., 2020). DeFi protocols value user privacy and control, leading to a regulatory gap that is difficult to address. New solutions may include the use of a decentralized identity system such as Soulbound tokens, providing a better balance between privacy and compliance (Buterin, 2022). Additionally, DeFi applications operate on permissionless blockchains without respect to the

jurisdiction of any single nation. Customary institutions are subject to local law and international law depending on where the activity is conducted (Zetzsche et al., 2017). The borderless nature of DeFi creates a need for international regulatory coordination in order to avoid regulatory arbitrage opportunities and ensure a level playing field (Arner et al., 2020). The second concern is liability, as regulators can use the law to hold financial intermediaries liable for wrongdoing and inefficiencies (Basel Committee on Banking Supervision, 2011). In DeFi, given the use of self-executing smart contracts, liability becomes complex when transaction flows are automated and the given protocol is occupied or hacked (through, for example, flash loan attacks) (Zeng, 2021). Regulators could consider requiring audits of smart contracts, providing transparency, establishing decentralized governance, implementing accountability mechanisms for protocol developers, and ensuring consumer protection. Customary financial services also provide positive externalities, such as deposit insurance and fraud protection. Customers of customary banks are protected against losses from bank defaults (Cecchetti & Schoenholtz, 2020). DeFi customers have no such protections, facing both private key management and protocol exposure. These users are less likely to be expert on impermanent loss, liquidity pooling, yield farming, and other risks (Harvey et al., 2021) exposing them to the risk of user abuse. This has led to calls for greater transparency, disclosure obligations, and user education (Schär, 2021). Systemic risk has implications for regulation too, as customary financial systems have some level of buffer, such as capital requirements or central bank interventions, to prevent systemic collapse (Freixas et al., 2000). However, in DeFi, common inter-protocol dependencies create a new type of systemic risk, in which a failure of one protocol (for instance one tied to stablecoin issuance or lending) can create an avalanche effect (Zeng, 2021). However, potential DeFi-specific risk-limiting tools may need to be included in a regulatory response such as safety reserves or circuit breakers to prevent contagion, as has occurred in TradFi markets. Despite concerns, DeFi also has the potential to drive an expansion of finance and innovation. Regulatory adaptation may be needed. A balance that ensures innovation while protecting consumers, maintaining fair markets, and preserving financial stability is needed as DeFi matures and transitions to be part of the financial system.

3. Research Methodology

The research methodology employed in this paper adopts a mixed-methods approach, utilizing both qualitative and quantitative analysis to comprehensively assess the ramifications of decentralized finance on customary financial risk management practices. By employing both empirical data and contextual qualitative insights, the research seeks to offer a thorough understanding of the emerging risks and regulatory concerns associated with decentralized finance in the financial landscape. The literature review begins with an analysis of academic literature, industry reports, and regulatory documents to highlight the characteristics of existing conventional risk management frameworks, which are compared to the decentralized governance model of DeFi protocols. The review highlights deficiencies in existing frameworks (Harvey et al., 2021; Schär, 2021), which then inform the development of the research paper's research questions and objectives. Lastly, the review also identifies overlap and gaps in the existing literature and identifies under-researched areas of interest. Secondary data from blockchain analytics platforms, corporate financial statements, and general DeFi protocols are used for quantitative analysis. The risk exposure and relative success of the DeFi market compared to customary finance are measured through a variety of metrics, including total value locked (TVL), smart contract exploitations, and DeFi lending liquidation rates. In addition to regression analysis, risk modeling and other statistical techniques to identify patterns, quantify systemic risks and measure protocols' risk exposure (for example, Zeng, 2021), qualitative approaches such as semi-structured interviews with industry stakeholders, regulators and DeFi developers provide an understanding of the perceptions of regulatory difficulties, accountability frameworks, and the feasibility of new compliance infrastructures (for example, decentralized identity verification systems) (Buterin, 2022). Thematic analysis of the interview transcripts and coding into major themes and contradictory perspectives gives qualitative richness of the data which quantitative data-sources do not provide. The study design involves adherence to ethical practice in confidentiality of data and interviewees, and aims at reducing bias through the triangulation of

the data sources and the cross-checking of the findings (Bryman, 2012). Overall, a mixed-methods-based approach has been chosen as it provides a subtle and in-depth analysis of the impact of DeFi on financial risk management and enables the formulation of policy recommendations to promote innovation while maintaining financial stability, based on the quantitative and qualitative findings of the research, to inform policymakers.

3.1 Research Design

The research design for this research is exploratory, mixed-methods research, using qualitative and quantitative methods. It is essential for this research to use an exploratory design research strategy as the DeFi ecosystem is a novel field. Hence, there is a need for a mixed-method approach in order to provide a full understanding of how DeFi is influencing customary financial risk management. The use of a flexible and in-depth approach is suggested by Saunders et al. (2019) The quantitative nature refers to statistics about key performance indicators related to the usage of DeFi protocols, including TVL, lending default risk, and smart contracts, obtained from blockchain data aggregators and industry insights reports. This quantitative nature seeks to identify regularities, patterns, and correlations to empirically estimate the divergence of risk exposure and performance between DeFi and customary finance (Zeng, 2021). Quantitative metrics are used in comparative modeling to assess the risk mitigation role of centralized institutions with respect to liquidity, credit and operational risks, compared to DeFi protocols. The metrics include trends in the volatility, yields, and breaches of security over a period that capture both the stable and vulnerability aspects. The quantitative study is complemented by a qualitative study composed of semi-structured interviews with DeFi developers, financial regulators and risk experts about their views on regulatory difficulties, accountability and the feasibility of innovative DeFi compliance solutions addressing DeFi-related risks and challenges. Rounding out the qualitative analysis, this study presents case studies of major DeFi-related events in the 2020s, such as the 2022 Wormhole bridge hack and the Compound protocol bug in 2021, identifying the risks, responses, and lessons learned from these events. This is important to triangulate and validate the study as it cross-examines the data sources (Bryman, 2012). The study is theoretically flexible so that analysis can be altered whenever new knowledge and information is available within the context of the rapid technology development and economic environment. Using a fluid and iterative design, the findings of the initial interview or first stage of data analysis can highlight areas for focus in subsequent stages.

3.2 Population and Sampling

The relevant study population can be divided into three groups: DeFi protocol developers, Financial regulatory agencies, and customary financial risk management practitioners. Their views and overall perspectives are captured through the study. The study will use purposive sampling, i.e. selection of participants based on their knowledge and experience of DeFi or financial risk (Etikan et al., 2016). A sample size between 15 and 20 participants is estimated for qualitative interviews, which is sufficient for data saturation, and small enough to cover the intended diversity and heterogeneity (Guest et al., 2006). The developers of leading DeFi protocols (e.g. Aave, Uniswap, MakerDAO) have been selected to gain first-hand knowledge on how protocols are designed to reduce risks and manage security. Established DeFi protocols allow a comparison with newer protocols to understand how risk management practices are evolving over time and under regulatory scrutiny. The interviews include analysts from international financial regulatory bodies such as the Financial Stability Board (FSB) and the European Securities and Markets Authority (ESMA), as well as national financial regulators such as the U.S. Securities and Exchange Commission (SEC). This helps understand regulatory gaps, enforcement challenges, and possible regulatory approaches to DeFi. The interviews offer insights into the disconnect between DeFi's decentralized nature and customary regulatory frameworks, and recognize areas for potential regulatory innovation. Other customary risk management experts from banks, fintechs, and financial consultancies provide perspectives on comparability between DeFi and customary risk management methodologies. Calculated and operational risk managers are included in the panel to provide planned and practical perspectives. For the quantitative analysis, secondary financial reports and data from blockchain platforms are chosen by criterion-based sampling on the largest protocols regarding their market

capitalization, user activity, and variety of financial services, for example, lending and borrowing, liquidity provision, stablecoins, derivatives, and token sales. Blockchain data are retrieved from blockchain explorers such as Etherscan and platforms such as DeFi Pulse. Financial market data are obtained from CoinGecko and Messari. The two-tiered sampling approach also helps improve the overall quality of the study by ensuring sufficient diversity and contextual awareness of the data, which are vital when discussing risks in DeFi and the corresponding regulatory implications. Purposive and criterion sampling are employed for qualitative and quantitative data, respectively, as described below.

3.3 Data Collection Methods

A mixed-methods approach has been adopted to assess the impact of DeFi on risk management in customary finance, capturing thorough data and combining quantitative analysis with qualitative analysis, including insights from experts in the risk management field, to shed light on the research question. This approach incorporates several data sources to capture the full impact of DeFi. In-depth qualitative data is obtained through semi-structured interviews with the following: DeFi developers, finance professionals, regulators, and economists with expertise in blockchain technology. The purpose of the interviews is to determine the impacts of DeFi innovations on the customary risk landscape and what regulators face (Zetzsche et al., 2020). The interview questions for experts will seek to elicit the major differences in risk exposure, liquidity management and counterparty risk between DeFi and customary finance. The second part contains a structured survey of financial professionals, institutional investors, fintech executives, and active DeFi participants to determine the risk considerations, risk mitigation strategies, regulatory gaps, and trust between DeFi and customary finance. The survey uses Likert-scale response questions to ensure the comparability of results (Chainalysis, 2024). It also seeks to investigate participants' attitudes towards algorithmic governance systems, token incentive protocols, and DAOs, as well as their perceived stability and reliability. It is framed with case studies of three major DeFi protocols, Uniswap, Aave, and MakerDAO, and how these protocols responded to liquidity crunches, price crashes, and attacks on smart contracts (Glassnode, 2024). These instances included risk and recovery events within DeFi protocols, such as on-protocol liquidations and community governance (voting) decisions. Secondary data is also available via financial reports, white papers, and peer-reviewed literature, providing quantitative metrics and theoretical assumptions for work in this field (Gudgeon et al., 2020). Additional data is also drawn from on-chain data provided by public block explorers, which provide information about TVL, transaction throughput, collateral ratios and flash loan volume, which could be used to assess DeFi performance and susceptibility to disruption. Data provided by blockchain explorers and analytical tools are used to monitor on-chain metrics such as network congestion, transaction fees and smart contract deployment, alongside reports produced by regulatory authorities and international organizations such as the Financial Stability Board (FSB) and IMF (IMF, 2023). Furthermore, market reports publicly available from the research firms and from blockchain analytics service companies capture some aspects of DeFi adoption and financialisation risks (e.g., Chainalysis, 2024). These primary and secondary data sources ease a comparative analysis of the existing financial system and emerging DeFi ecosystem, as well as regulatory and systemic vulnerabilities. Integrated with the characteristics of each method, this enables a thorough, balanced, evidence-based understanding of the effects of DeFi on risk management practices to be developed.

3.4 Data Analysis Approaches

For the purpose of extracting insights from the data, a multi-dimensional approach employing qualitative and quantitative analysis is followed. The quantitative analysis uses descriptive statistics to visualize important trends, such as the perception of risk and the usage of DeFi, by calculating the mean, median, standard deviation, etc. (Chainalysis, 2024). Comparative analysis of DeFi risk with customary finance, leveraging metrics like Value at Risk, liquidity ratios, and the Sharpe ratio, in contrast with DeFi's smart contract failure rate, liquidity depth, collateralization rate, and the stress resilience of DeFi protocols, as derived from on-chain data sources (Glassnode, 2024). On-chain liquidity pools have stress testing to evaluate how liquidity responds to capital withdrawals and potential contagion or cascade failures within the DeFi ecosystem. Using a multiple regression analysis framework, it tries to identify

the relationship between DeFi adoption and systemic risk, platform size, transaction volume and TVL, while also measuring market volatility, default rate and market congestion as dependent variables (Aramonte et al., 2021). Further, volatility clustering models are applied to DeFi assets. The study compares these results to customary financial markets. DeFi network analysis illustrates concentration, liquidity bottlenecks and potential transmission channels of systemic risk (Gudgeon et al., 2020). This includes cross-chain interoperability risks and stablecoin dependencies (especially algorithmic stablecoins), which can further contribute to amplification and propagation of systemic risk. Qualitative analysis complements these approaches by applying thematic coding to the interview data to identify recurring issues, novel threats, and new risk mitigation techniques particular to DeFi (Zetzsche et al., 2020). Examples of emerging issues include gaps in decentralized governance, the role of smart contract audits, and the risk of pseudonymous development teams. Data on financial and regulatory filings supports the comparative regulatory framework, and documents regulatory arbitrage opportunities and inconsistencies in international regulation of DeFi (IMF, 2023). Sentiment analysis can be applied to social media data (e.g. Twitter, Reddit) in order to measure and contextualize quantitative indicators of market sentiment after a DeFi risk event or policy intervention (Chainalysis, 2024). To ensure validity and reliability, triangulation is applied through cross-validation of each of the interviews, surveys, blockchain, and case studies and minimizing the bias intrinsic in each of them. The qualitative and quantitative analyzes are combined to provide a thorough understanding of DeFi's impact on customary finance risk management that could lead towards a strong regulatory regime that takes into account DeFi's idiosyncratic and systemic risks and its rapid pace of innovation. Coupling this approach with statistical analyzes, network visualizing, and thematic analyzes can inform future regulators and practitioners' risk management in more fine-grained ways.

4. Findings and Discussion

This book hereafter summarizes the knowledge gained from data analysis itself distilled into a deep dive on DeFi, the comparative mapping of financial risks and risk management frameworks standing in between DeFi and the understood challenges it faces, especially vulnerability to regulation and innovation in a fast-paced environment.

4.1 Comparative Risk Analysis

The comparative risk analysis examines the underlying differences in risk structure between DeFi and customary financial intermediaries (using data in the results of interviews, surveys, case studies and blockchain analyzes). The main difference in risk structure is the reduction of counterparty risk in DeFi, with self-execute smart contracts replacing the classic financial intermediaries, such as exchanges (Zetzsche et al., 2020). Due to the role of regulated financial intermediaries (for example, banks) in financial transactions, customary finance relies on the concept of legal liability, but with risks of failure of institutions, fraud, or mismanagement (Aramonte et al., 2021). DeFi eliminates this reliance by automating the process and establishing a trustless environment where consumers directly interact with protocols. In this system, the risk is borne by the smart contracts. Data from the on-chain data provider, Glassnode (2024), showed that, in 2023, over 60% of the financial loss in DeFi was because of smart contract risk, which weighs the risk between counterparty risk and technical risk. Liquidity risk is likewise two-sided. Centralized banks in customary finance must satisfy liquidity requirements imposed by the regulators to ensure they have enough reserves to satisfy withdrawal requests (IMF, 2023). Unlike custodial activity, DeFi protocols are incentivized by user liquidity pools that are rewarded with yield. For example, Uniswap and Aave incentivize the provision of liquidity, but also create the risk of a sudden withdrawal, or "bank run", on the protocol during a period of market stress. For instance, during the crypto market crash in May 2022, liquidity pool withdrawals at Uniswap increased 35% in 2 days, leading to slippage spikes and temporary dislocations (Chainalysis, 2024). This demonstrated the effect of liquidity fragmentation and market sentiment changes in DeFi, as well as the destabilizing effects of algorithmic stabilization reminiscent of the Terra/Luna crash. Finally, operational risk creates another divergence. Thriving centralized financial institutions spend heavily to establish cybersecurity and conduct in-depth operational audits. DeFi protocols, by contrast, are publicly accessible through the

blockchain. While the majority of DeFi protocols obtain third-party audits, their quality and frequency can vary considerably (IMF, 2023). Among surveyed individuals, 72% were concerned about inconsistency in smart contract auditing, and most DeFi users relied on community trust instead of security measures (Chainalysis, 2024). Additionally, development teams of DeFi protocols are normally anonymous and rarely held liable for poor outcomes or exploitation (Zetzsche et al., 2020), which gives them a different market risk profile. Customary finance has circuit breakers, market makers or central banks to prevent asset price declines (IMF, 2023). However, DeFi's smart contract-based liquidation mechanisms, while effective in most situations, tend to exacerbate falling markets. An analysis of MakerDAO's collateral auctions during market downturns shows that price drops lead to common liquidations and further depreciations of assets. This is corroborated by volatility clustering, and finding that price volatility for DeFi tokens is higher than other tokens due to leveraged lending, low liquidity, and self-referential selling (Glassnode, 2024). This suggests that DeFi creates new reducing factors for counterparty and access risks that are otherwise critical for other tokens. While these benefits also come with increased technological, operational and liquidity risks, it is vital for regulators to develop a new approach to balance innovation and the stability of the financial system. This is the basic premise for the remaining discussion within this thesis regarding risk mitigation and the regulation of DeFi.

4.2 Regulatory Gaps and Solutions

With the rapid growth of the DeFi sector, a number of regulatory vulnerabilities have been exposed. Most prominently, major gaps in jurisdictional authority exist, since customary finance is concentrated in geographical institutions while DeFi protocols and blockchain networks are decentralized, often international and sometimes even virtual (Zetzsche et al., 2020). This can lead to regulatory arbitrage, whereby DeFi projects will locate in less regulated jurisdictions and not be subject to consumer and systemic protections that would normally apply to customary financial markets (IMF, 2023). For example, the European Union Markets in Crypto-Assets Regulation (MiCA) regime to come into effect in 2024 intends to provide thorough and risk-based regulation for various crypto-assets, stablecoins, DeFi, to improve consumer protection and transparency (FSB, 2023). Following the U.S. Securities and Exchange Commission's (SEC) enforcement-based regulation and subsequent designations of DeFi tokens as unregistered securities, several court cases were started against Uniswap and Coinbase (Chainalysis, 2024). In this respect, important international co-operation is needed in order to avoid regulatory divergence and fragmentation and to preserve a level playing field in regulation. By contrast, customary finance is geographically confined by financial regulation, while DeFi protocols are global and operate on blockchain networks without generally any presence on the ground (Zetzsche et al., 2020). Greater flexibility includes regulatory arbitrage, when DeFi projects push themselves to a jurisdiction with less regulation, and thus, with greater ability to avoid consumer protection and anti-crisis financial regulations, according to the IMF (2023). A case of this is Binance, a global crypto exchange, which has moved its operations from one jurisdiction to another to evade compliance with the existing regulations (Chainalysis, 2024). To achieve this level of oversight, it would be necessary to create a coordinating cross-border regulator. The Financial Stability Board (FSB), the International Organization of Securities Commissions (IOSCO), or other global financial institutions could agree on standardized DeFi protocols, which would address issues such as disclosure, capital and reporting of risk metrics (FSB, 2023). To this end, the European Union's Markets in Crypto-Assets Regulation (MiCA) aims at a thorough, uniform regulatory framework for crypto-assets throughout the Union, which is to be applicable from 2024. On the other hand, there is a lack of accountability in the governance mechanisms of a DeFi (DAOs). Customary financial institutions fall under the jurisdiction of corporate governance law, with enforcement applied through boards of directors. However, DAOs with token voting schemes do not have equivalent recognition as legal entities in most jurisdictions, so they cannot be held liable in the same way (Zetzsche et al., 2020). A possible solution could be the hybrid regulatory model: when DAOs voluntarily decide to register themselves as a legal person, they gain access to regulatory legitimacy while still maintaining decentralized decision-making. The problem is that this approach has many drawbacks, particularly for fully decentralized projects; legal registration introduces compliance

costs, regulatory surveillance, and other attributes that are not compatible with these projects' founding principles of their anonymity and their borderless nature. The code is one of the few available solutions to providing accountability while ensuring the DAO's token holders are not given control disproportionate to their voting power, as occurs often in the regulation of DAOs, which goes against the promise of decentralization for which most DAOs are established. An existing model to do this was already implemented in Wyoming's DAO bill (2021), yet there are still concerns whether legal registration would discourage fully decentralized projects for fear of losing anonymity or incurring additional regulatory costs. Another concern is that DeFi is prone to higher risk of illicit activities including money laundering, fraud and terrorist financing due to blockchain technology being pseudonymous (Chainalysis, 2024). MakerDAO, which has billions of dollars in assets and is unregistered as a business, is an example of this (Chainalysis, 2024). It can be difficult to comply with AML/KYC regulations in DeFi because there are no intermediaries in control of the funds. One solution is the integration of decentralized identity (DID) systems, where the user retains control of their credentials and the protocol can verify that some requirements are fulfilled (Gudgeon et al. 2020). These workarounds preserve user privacy and comply with regulations, while balancing anonymity and accountability. Projects like Polygon ID are exploring how DID systems can offer verifiable credentials without compromising user privacy (Polygon, 2024). Finally, smart contract security remains a gaping hole in regulation. Cryptography failures in 2022, at the Ronin Bridge, and in 2023, at Euler Finance and Wintermute, led to losses of $625 million, $197 million and at least $160 million, respectively (Chainalysis, 2024: 4). These attacks present the need for standardized security audits and regulation, with necessary testing for protocol vulnerability before launch on the market (IMF, 2023). In contrast to customary financial products, DeFi protocols are written in code and may contain vulnerabilities. Standalone audits are always proportionately lacking, and no certification process exists. The exploits of the $625 million 2022 Ronin Bridge hack and the $197 million 2023 Euler Finance hack are examples of how vulnerable smart contracts can result in consequences with important financial damages (Chainalysis, 2024). To avoid this scenario, regulators can establish a process for certifying smart contracts, which will guarantee that protocols meet minimum security standards before they are used (IMF, 2023). This could be similar to the customary financial product approval process but with the inclusion of best practices from the industry and the disclosure of third-party audit results. To address all of these regulatory loopholes, it would be necessary to have a flexible and collaborative global regulatory framework to balance innovation, market integrity and consumer protection, while considering the decentralized nature of DeFi, to ease its adoption in the customary financial system.

5. Summary of Findings

Lessons from DeFi for how to focus on the future of financial risk management reveal both extraordinary opportunity and existential regulatory concerns. In particular, the new DeFi model of financial services, which is permissionless, has decentralized governance, and applies automaton tools to manage transactions and risks, is a direct contrast to customary finance. However, this comes with substantial risks relative to those in customary finance. By reducing intermediary risks, DeFi introduces new systemic risks such as smart contract failure, liquidity shortages and price manipulation (Aramonte et al., 2021). DeFi's cross-border nature raises several regulatory difficulties, including concerns about jurisdictional regulatory gaps and arbitrage as evidenced by Binance's national relocations and the varying treatments among members of the European Union's proposed MiCA regulation and the US SEC (FSB, 2023; Chainalysis, 2024). Questions of governance accountability are added concerns. DAOs' decentralized governing structures have not been successful in addressing legal accountability and governance issues faced by decentralized platforms (Zetzsche et al., 2020). A hybrid regulatory regime could enable a DAO to be incorporated under existing laws as a legal person, while incurring high compliance costs and risking centralization of governance structure in almost fully decentralized DAOs, as seen with MakerDAO's governance proposal (Chainalysis, 2024). Regulatory anti-financial crime in DeFi is nascent and pseudonymity is easing money laundering and related crimes (IMF, 2023). Decentralized identity technologies such as Polygon ID may help resolve regulatory compliance issues

while upholding users' privacy rights, but broad adoption of such technologies is still seen as challenging (Gudgeon et al., 2020). Smart contract security is another regulatory gap that was highlighted by recent hacks like the Ronin Bridge, Euler Finance and Wintermute hacks, igniting calls for audit and security certification standards (Chainalysis, 2024). The massive potential of the DeFi market may require a more advanced regulatory policy than existing law. Balancing transparency and accountability with innovation and flexibility could be fundamental to developing an international regime capable of integrating the DeFi ecosystem with the customary financial system.

6. Implications for Theory and Practice

The study of DeFi also has implications in financial theory and regulatory policy. Financial theory has customarily focused on the role of financial intermediation. DeFi challenges customary financial intermediation theory, presenting a compelling argument for a new decentralized, peer-to-peer financial order, similar to the historic evolution from barter systems to central banking, and later, to digital finance. The transition from physical objects to institutional intermediaries, and from those to decentralized code-based protocols, mirrors phases in the financial revolution (Arner et al., 2020). The reduction in counterparty risk, as well as the automation and reliance on smart contracts, is consistent with Eugene Fama's (1970) Efficient Market Hypothesis, suggesting the potential for DeFi markets to be more efficient than customary markets. However, the emergence of new types of financial risk, such as algorithmic instability and centralized governance in DAOs, challenge customary risk management theories. Key theses point to the need for new financial risk frameworks integrating decentralized governance and technology-based risks (Zetzsche et al., 2020), calling for existing financial risk frameworks to integrate decentralized governance while recognizing DeFi's role as both a risk mitigator and a risk creator. Emerging regulation e.g. the EU Markets in Crypto-Assets Regulation (MiCA) and the Financial Action Task Force (FATF) virtual assets guidance could foster more technology-neutral regulation (FSB, 2023). Such regulation could include requirements for smart contract code auditing, active transaction tracking using blockchain analytics, and categorization of DeFi protocols by the degree of decentralization of their governance and the level of investor protection they provide (Chainalysis, 2024). This could support a more adaptable and resilient framework to balance the needs of DeFi and its intrinsic risks. The analysis suggests adaptive regulatory frameworks that both support innovation and reduce intrinsic systemic risks of DeFi. Regulatory agencies, such as the FSB and IMF, could establish common rules to address jurisdictional fragmentation and regulatory arbitrage (IMF, 2023). Use of standardized smart contract audits, decentralized identity solutions, such as Polygon ID, and hybrid governance models may improve DeFi's resilience and trust, and thus legitimacy, while reducing risk (Polygon, 2024). Customary firms may also attempt to adopt DeFi developments like automated liquidity pools or tokenized assets into their business models to increase competitiveness and lower operational friction. Such efforts may face barriers due to the same issues that make DeFi appealing; e.g. regulators may resist DeFi due to compliance, transparency and consumer protection concerns (Aramonte et al., 2021). Other reasons for this slow adoption may include technological limitations, such as scalability issues on the blockchain network, and the challenge of integrating DeFi protocols with existing financial infrastructure (Gudgeon et al., 2020). This highlights the need for collaboration between regulators, technology providers and financial institutions to create a conducive environment for DeFi adoption. The intersection between DeFi and customary finance has the potential to increase inclusivity and accessibility.

7. Recommendations

Informed by these findings, the following recommendations can be made to achieve effective risk mitigation and regulation, while allowing DeFi to flourish and innovate: Regulators should move towards a principles-based and technology-neutral approach to regulation. This would allow regulations to apply to any innovations that may arise in the DeFi space. Policymakers should prioritize cross-border regulatory convergence, reducing the divergence between jurisdictions, to reduce regulatory arbitrage (FSB 2023; IMF 2023). Standards for auditing smart contracts globally could create trust and address code exploit vulnerabilities. Like financial statement audits, standardized automated independent

security audits of smart contracts can increase confidence in the adoption of smart contracts by investors and discourage malicious actors (Chainalysis 2024). A certification standard for DeFi projects, with material features like governance transparency, asset protection, and smart contract security, can also increase investor confidence. Decentralized identity (DID) systems that allow self-sovereign identity solutions (e.g., Polygon ID) that preserve pseudonymous privacy while providing pseudonym-protected verified credentials for AML / CTF (Anti-Money Laundering and Combatting the Financing of Terrorism) should be supported. Engagement with regulatory authorities would also be necessary to enable the development of privacy-preserving solutions (Polygon, 2024). Hybrid governance, for example via DAOs combined with legally established entities, should also be pursued. Governments could consider a "DeFi legal entity" like an LLC that subjects a DAO to legal liability whilst allowing it to govern itself in a decentralized way (Zetzsche et al., 2020). In such a way customary finance could integrate with DeFi without the disincentives for innovation stemming from full centralization under the auspices of the financial institution. A second important step is to encourage customary financial institutions to explore partnerships with DeFi platforms, connecting decentralized liquidity pools, tokenized assets and (decentralized) automated market makers to customary finance. Along the way, DeFi projects could be offered access to a regulatory sandbox, to allow interested regulators and customary financial institutions to gain experience with DeFi innovation within a formal framework that enables responsible innovation and consumer protection, while supporting the stability of the wider financial system. The principles and recommendations set out below draw from this comparative study and form a roadmap for a sustainable and responsible integration of DeFi into the wider financial system, balancing innovation with effective risk mitigation and oversight.

8. Future Research Suggestions

Eventually, more empirical research is needed to better understand the long-run risk implications of DeFi adoption for financial stability under different market regimes and asset classes. Such insights could help regulators figure out how to adapt to and guide DeFi and could contribute to a better understanding of systemic financial stability. Comparative case studies are also needed to assess the effectiveness of different regulatory approaches (e.g., the EU's MiCA regulation versus the approach taken by the US SEC), and future studies should consider the interaction between DeFi and AI, such as the potential to integrate AI-driven risk models into DeFi protocols for real-time risk mitigation and higher stability in the DeFi ecosystem. Investigating the social and economic impacts of DeFi on underbanked populations is another relevant area for future research. For example, does DeFi actually help to ease financial inclusion, or does it act to the contrary by introducing new forms of exclusion due to a lack of infrastructure? Research is still needed to examine the effectiveness, scalability and weaknesses of DAOs as they develop and mature, with respect to norms of regulatory recognition and accountability. Finally, there is room for inter-disciplinary studies involving finance, law and technology examining how hybrid systems of regulation and governance combining on-chain transparency and off-chain legal frameworks can reconcile the competing goals of innovating and stability. Such studies can help build a more resilient, open and regulated decentralized financial system, while providing a more complete picture of DeFi's promise in reshaping financial systems on a global scale.

References

1. Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review, 103(2), 153–174.
2. Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance (DeFi): Regulatory Challenges and Opportunities. University of New South Wales Law Research Series, 2020(47).
3. Chen, Y., & Bellavitis, C. (2020). Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System. Technological Forecasting and Social Change, 161, 120049.
4. Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). The Decentralized Financial Crisis: Attacking DeFi. arXiv preprint arXiv:2002.08099.

5. Allen, J. G., & Gensler, G. (2020). The Potential of Blockchain and DeFi for Modernizing Financial Infrastructure. MIT Sloan School of Management, Working Paper.
6. Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance, 25*(2), 383-417.
7. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305-360.
8. Modigliani, F., & Miller, M. H. (1958). The cost of capital, corporation finance, and the theory of investment. *The American Economic Review, 48*(3), 261-297.
9. Allen, F., & Santomero, A. M. (1998). The theory of financial intermediation. *Journal of Banking & Finance, 21*(11-12), 1461-1485.
10. Adams, H., Zinsmeister, N., & Robinson, D. (2021). Uniswap v3 Core. Uniswap Labs.
11. Kulechov, S. (2020). Aave Protocol Whitepaper. Aave Labs.
12. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum Whitepaper.
13. Easley, D., O'Hara, M., & Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics, 134*(1), 91-109.
14. Buchanan, J. M., & Tullock, G. (1962). The Calculus of Consent. University of Michigan Press.
15. Arner, D. W., Barberis, J., & Buckley, R. P. (2020). The evolution of fintech: A new post-crisis paradigm*? Georgetown Journal of International Law, 47*, 1271-1319
16. Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). DeFi protocols for loanable funds: Interest rates, liquidity, and market efficiency. International Conference on Financial Cryptography and Data Security, 59-79.
17. Bryman, A. (2012). Social Research Methods (4th ed.). Oxford University Press.Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling.
18. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4.
19. Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field Methods, 18(1), 59-82.
20. Saunders, M., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students (8th ed.).
21. Kumar , D. G. ., Raju , N. S. V. N. ., Lakshmi , V. ., vemuri , S. ., Rao , J. M. ., & Chestor , R. E. . (2025). The Role of Fintech in Transforming Financial Services for Indian Start-Ups. *International Journal of Accounting and Economics Studies*, *12*(5), 608-616. https://doi.org/10.14419/5b2zxp23
22. Pearson.Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153-174.Zeng, J. (2021). Smart contract security: A survey. Future Generation Computer Systems, 122, 209-226.
23. Aramonte, S., Huang, W., & Schrimpf, A. (2021). "DeFi Risks and the Decentralisation Illusion." BIS Quarterly Review, Bank for International Settlements.
24. Chainalysis. (2024). "The 2024 Crypto Crime Report: DeFi Vulnerabilities and Financial Crime."
25. Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). "DeFi Protocols: On the Risk and Opportunities of Decentralized Finance." arXiv preprint arXiv:2007.14018.
26. International Monetary Fund (IMF). (2023). "The Rise of Decentralized Finance: Opportunities and Challenges."
27. Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). "Decentralized Finance (DeFi): Regulatory Challenges and Opportunities." European Banking Institute Working Paper Series.
28. Aramonte, S., Huang, W., & Schrimpf, A. (2021). "DeFi Risks and the Decentralisation Illusion." BIS Quarterly Review, Bank for International Settlements.
29. Chainalysis. (2024). "The 2024 Crypto Crime Report: DeFi Vulnerabilities and Financial Crime."
30. Glassnode. (2024). "On-chain Data Trends: Analyzing Liquidity and Risk Metrics in DeFi Protocols."Financial Stability Board (FSB). (2023). "Addressing the Financial Stability Risks of Decentralised Finance."
31. Polygon. (2024). "Polygon ID: Empowering Users with Self-Sovereign Identity."