



## Article

# Risk Management in DeFi: Analyses of the Innovative Tools and Platforms for Tracking DeFi Transactions

Bogdan Adamyk<sup>1,\*</sup>, Vladlena Benson<sup>1</sup>, Oksana Adamyk<sup>2</sup> and Oksana Liashenko<sup>2</sup><sup>1</sup> Aston Business School, Aston University, Birmingham B4 7ET, UK; v.benson@aston.ac.uk<sup>2</sup> Loughborough Business School, Loughborough University, Loughborough LE11 3TU, UK; o.o.adamyk@lboro.ac.uk (O.A.); o.liashenko@lboro.ac.uk (O.L.)

\* Correspondence: b.adamyk@aston.ac.uk

**Abstract:** Decentralized Finance (DeFi) is a recent advancement of the cryptocurrency ecosystem, giving plenty of opportunities for financial inclusion, innovation, and growth domains by providing services such as lending, borrowing, and trading without traditional intermediaries. However, inadequate regulatory oversight and technological vulnerabilities raise pressing concerns around market manipulation, fraud, and regulatory compliance, exposing a clear research gap in effective DeFi risk management. This paper addresses this gap by proposing a utility-based framework to evaluate six leading DeFi tracking platforms—Chainalysis, Elliptic, Nansen, Dune Analytics, DeBank, and Etherscan—focusing on two critical metrics: transaction accuracy and real-time responsiveness. Applying a mixed methods approach that combines a quantitative survey (n = 138) with qualitative interviews (n = 12), we identified critical platform features and found significant differences across these platforms with respect to compliance features, advanced analytics, and user experience. We used a utility-based model that links accuracy and responsiveness metrics, allowing us to adjust differing priorities and risk management needs for users. The results show the need for balanced, user-centric solutions that accommodate regulatory, technological efficiency and affordability requirements. Our study contributes to the growing knowledge base by providing a structured evaluation model and empirical insights, offering clear directions for practitioners, platform developers, and policymakers aiming to strengthen the DeFi ecosystem.

Academic Editor: Xianrong  
(Shawn) Zheng

Received: 19 December 2024

Revised: 8 January 2025

Accepted: 14 January 2025

Published: 16 January 2025

**Keywords:** risk management; decentralized finance; blockchain; cryptocurrency; transaction tracking; AML; AI; ML

**Citation:** Adamyk, B., Benson, V., Adamyk, O., & Liashenko, O. (2025). Risk Management in DeFi: Analyses of the Innovative Tools and Platforms for Tracking DeFi Transactions. *Journal of Risk and Financial Management*, 18(1), 38. <https://doi.org/10.3390/jrfm18010038>

**Copyright:** © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Decentralized Finance (DeFi) has rapidly expanded into one of the fastest-growing cryptocurrency sectors. DeFi platforms enable users to borrow, lend, trade, and stake their digital assets—marking an exciting development in financial services (Auer et al., 2024).

DeFi has a lot of potential benefits, such as greater financial inclusion and operational efficiency (Jensen et al., 2021), but it also carries some risks that should not be disregarded. Smart contract vulnerable areas, price swings, market manipulation, liquidity issues, and management uncertainty are a few of these (Johnson, 2024). Users and investors have already suffered large financial losses due to DeFi risks, ranging from flash loan attacks to smart contract vulnerabilities (Bhambhwani & Huang, 2024), underlining the need for efficient risk management tools and systems that track DeFi transactions and look for possible threats to the ecosystem. Furthermore, the sector's decentralized structure

complicates regulatory oversight, creating challenges for Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance (Xiong et al., 2023).

Investors and traders have taken notice of the spectacular rise in popularity of DeFi platforms over the past few years, resulting in the emergence of numerous DeFi tracking systems and platforms (Wronka, 2023). These instruments simplify portfolio management and transaction tracking within the DeFi environment, assisting users in identifying potential risks and opportunities. This empowers them to make well-informed decisions while navigating the intricacies of the ecosystem.

An in-depth discussion of the methods that guide investors through the complex world of risk management in the decentralized finance market is provided in this paper. Effective risk assessment and management become increasingly important as traders and investors use DeFi platforms that soar. This causes a variety of platforms and tools to emerge that are designed to make it easier to monitor transactions inside this ecosystem.

Understanding the benefits and restrictions that come with the DeFi world is key to solving the problem. With this knowledge in hand, users can choose the tools and platforms that best suit their unique requirements. Investors can develop a detailed understanding of potential risks and possibilities by choosing the appropriate tools for tracking transactions and managing portfolios.

Several studies have researched different aspects of DeFi risk—such as smart contract auditing (He et al., 2023) and liquidity management (Irresberger et al., 2024)—highlighting the nascent but urgent need for practical, transparent risk mitigation approaches. Nevertheless, few studies comprehensively analyzed the platforms for transactional tracking and anomaly detection on DeFi protocols. Against this backdrop, our work makes three key contributions:

1. The utility-based evaluation model is proposed. We suggest a new framework in which accuracy (e.g., minimizing error rates in spotting suspicious activity) and responsiveness (how quickly and effectively alerts are issued in real-time) can be combined. Using these metrics, we can weigh them based on user priorities and use the framework as a comprehensive but flexible way of comparing DeFi tracking platforms.
2. We conducted a comparative analysis of DeFi leading analytic platforms. On the basis of compliance tools, advanced analytics, and user interface, we evaluate six widely used platforms—Chainalysis, Elliptic, Nansen, Dune Analytics, DeBank, and Etherscan. In this way, our study fits into the emerging literature on DeFi security and transaction monitoring and fills gaps in user-centered research (Kshetri, 2021; Wu et al., 2021).
3. We integrated a quantitative survey (138 respondents) with qualitative interviews (12 stakeholders) to capture statistical trends in user preferences and contextual nuances regarding adoption barriers. In addition to technical discussions, this mixed-method approach points out practical risk management strategies and trade-offs faced by users and developers and recommends actions.

Previous research mainly treated DeFi risks (for example, market volatility and compliance issues) as isolated challenges (Mitchell, 2022; Schär, 2021), yet little research integrated these strands into a coherent framework of DeFi platform evaluation. Our approach addresses this shortfall by focusing on multi-dimensional metrics encompassing technological and user-centric considerations, aiming to guide more informed decision-making for DeFi users.

The paper also details the factors to consider while choosing these monitoring tools and platforms. It emphasizes the significance of proactive monitoring and rapid mitigation techniques in efficient DeFi risk management.

The central task of this research is summarized in the following question: How can risks in DeFi transactions be effectively managed, and what role do existing platforms play in mitigating these risks to ensure the stability, security, and adoption of decentralized financial systems?

As DeFi systems are based on decentralized, trustless architecture, use smart contracts, and lack centralized oversight, they have unique challenges compared to traditional financial frameworks (Benson et al., 2023). The risks of these challenges take the form of smart contract vulnerabilities, liquidity crises, compliance challenges, market volatility, and operational inefficiencies. For instance, errors or bugs in smart contract code can cause devastating exploits leading to significant financial losses (Chu et al., 2023). Liquidity withdrawals can be sudden and destabilize entire ecosystems, and blockchain transactions are by nature pseudonymous, making it difficult to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements. Additionally, high token price volatility, along with flash loan attacks, are amplified by financial instability (Xiong et al., 2023). For users, especially those new to DeFi, navigating complex interfaces and understanding technical intricacies makes it easy to end up using these platforms incorrectly, which only exacerbates the risks.

In recent incidents, these vulnerabilities have been made painfully clear. High-profile events such as the \$120 million BadgerDAO hack in 2021 and innumerable flash loan exploits also call out the high risk in the ecosystem of financial losses and the incapacity to pre-emptively manage these risks (Bhambhwani & Huang, 2024). The lack of robust risk management frameworks not only exacerbates financial losses but also damages user trust and degrades participation, making it difficult to attract potential participants and slow down mainstream adoption.

There are several critical factors that are driving the growing need for comprehensive risk management frameworks within DeFi. First of all, ecosystem stability is important. DeFi protocols are very interlinked, and assets are locked across multiple platforms. All of this can cascade through the ecosystem if one protocol fails. Early detection and addressing of such vulnerabilities is crucial to the effectiveness of risk management systems. Second, user funds must be secured. In DeFi, users deposit large amounts of capital into protocols without the legal protections or recourse as in traditional finance. These funds remain exposed to risks from exploits, mismanagement, or technical failures unless robust safeguards are in place. Thirdly, it is important to foster user trust. DeFi is decentralized and pseudonymous, which makes it hard to use for users, especially if fraud or hacking happens. Advanced risk management tools, such as real-time monitoring and transparent reporting, can be integrated with platforms to increase confidence and attract more users.

Although DeFi faces an immediate need for risk management, its practices are still fragmented and inadequate (Uzougbo et al., 2024). As a result, DeFi tracking platforms like Nansen, DeBank, Elliptic, Chainalysis, Etherscan, and Dune Analytics are becoming critical ecosystem components with tools for transaction monitoring, compliance, and advanced analytics. These platforms offer crucial risk management tools but have yet to be systematically tested for their capacity to mitigate the full range of DeFi risks. It is essential to understand their capabilities and limitations so that we can design comprehensive frameworks to ensure the stability, security, and trustworthiness of DeFi systems.

This research seeks to address these challenges through the following objectives:

1. Assess the ability of DeFi-leading tracking platforms to reduce risks of technological, financial, operational, and compliance domains.
2. Identify gaps in existing tools and propose improvements to risk management practices.
3. Develop a theoretical framework for DeFi risk management that combines technological, operational, and regulatory dimensions.

4. To evaluate DeFi platforms based on their ability to mitigate risks through accuracy and responsiveness.

This research aims to enhance academic understanding of DeFi risk management by addressing these objectives and offering actionable insights for platform developers, users, and policymakers. While DeFi applications have rapidly proliferated, there is a lack of comprehensive evaluations of the platforms that identify, detect, and prevent fraudulent or high-risk activities. Existing research focuses on either isolated technical vulnerabilities or covers regulatory issues without putting these in the context of user adoption and platform capabilities through a single framework. Limited guidance is available to both institutional and individual stakeholders, who must make decisions among competing priorities, including compliance, advanced analytics, and cost-effectiveness. In this work, we aim to fill this gap by looking at these multi-dimensional challenges and employing a structured, user-adaptive evaluation framework for DeFi tracking platforms, incorporating both technical performance metrics and user-focused considerations. By empowering stakeholders to balance accuracy and responsiveness, the model developed by the authors supports informed decision-making and fosters greater trust and efficiency in the DeFi ecosystem.

## 2. Overview of Decentralized Finance (DeFi)

DeFi is a rapidly growing ecosystem of financial applications running on blockchain technology, which often seamlessly integrates with multiple networks, including Ethereum, Binance Smart Chain, Solana, and others (Makarov & Schoar, 2022). DeFi differs from traditional financial systems because it is decentralized, trustless, and transparent. Smart contracts are used to automate financial operations, which reduces the need for intermediaries and makes the operation more accessible. The services provided in the DeFi ecosystem include lending, borrowing, trading, staking, and liquidity provision (Harvey & Rabetti, 2024). The DeFi applications are constantly evolving to meet the changing needs of the users, and they provide an environment that is innovative, experimental, and ever-improving.

The DeFi protocols have brought lending and borrowing arrangements that do not require the mediation of traditional brokers and allow people to lend or borrow digital assets. Market demand and supply decide the emergence of interest rates. Aave, Compound, and MakerDAO are the perfect examples of this trend that enables a borrower to take out a loan in cryptocurrency using collateral and, in turn, earn interest on their assets (Cedra, 2024). By departing from conventional credit systems, the users have gained more autonomy and direct involvement in managing their financial assets.

DeFi typically involves trading between decentralized exchanges (DEXs), which allow for direct peer-to-peer cryptocurrency transactions without reliance on centralized intermediaries (Hägele, 2024). Smart contracts used by exchanges such as Uniswap, CurveDAO, and PancakeSwap allow for real-time trades, more control, transparency, and lower costs than traditional centralized exchanges (Ghosh et al., 2023). On these platforms, users can trade digital assets at market-driven prices and keep their funds in their own control throughout the process.

In addition, staking has become a key function of DeFi, where cryptocurrency is being held in a wallet to help network operations and liquidity. In return, users are rewarded with additional digital coins. Staking protocols, including Ethereum 2.0, Binance Smart Chain, and Cardano, show how participants may simultaneously participate in network security and earn some incremental returns for their involvement (Milk Road, 2023). These services complement liquidity provision, which allows users to provide liquidity to decentralized

exchanges. This is evidenced by protocols like Uniswap, Curve, and dYdX and in return, liquidity providers earn a share of the platform's trading fees (BeInCrypto, 2022).

Even with these innovations, DeFi has its challenges. Smart contracts can automate the terms of a transaction, and smart contracts themselves can be vulnerable to attacks or exploited by malicious players. A decentralized model complicates risk management, compliance, and security issues (Schär, 2021; Kirvesoja, 2022), as it can reduce costs and streamline processes without intermediaries. This is especially important as regulatory pressures increase and risk management tools are in the early stages of development.

### 2.1. Practical Complexities in DeFi

DeFi transactions are complex and have no traditional intermediaries, making traditional AML and KYC procedures problematic. Various platforms and tools have emerged to improve transparency, monitoring, and analysis in the DeFi landscape (Weingärtner et al., 2023). The first is the basis of blockchain explorers, which serve as foundational instruments to track and examine on-chain data. These services include Blockchair.com, TokenView, Etherscan, BSCScan, and Solscan, and they provide transaction history, balances of wallets, and network activity (Feng et al., 2023). These platforms help stakeholders identify irregularities and potential unauthorized activities. Despite this, blockchain explorers typically provide raw data with little to no sophisticated analytics or contextual metrics, which users use to manually infer patterns and detect anomalies (Cholevas et al., 2024).

As a solution to these limitations, Dune Analytics, DeBank, Nansen, and other more advanced data analytics providers have emerged. These platforms aim to provide insights specifically tailored to the users, real-time monitoring, and metric-based analysis (Chatziamanetoglou & Rantos, 2024). Sometimes, they use blockchain data and social media inputs to generate dynamic dashboards and visualizations. Users can track total value locked (TVL), trading volumes, fees, liquidity movements, and large transactions across many DeFi protocols (Cedra, 2024). These analytics platforms are crucial for DeFi risk management as they allow the capacity to detect unusual activities, identify evolving market trends, and even oversee liquidity pools in real time.

Beyond analytics, such services as clustering, wallet attribution, and risk scoring functions are offered by transaction monitoring companies Chainalysis and Elliptic (Pocher et al., 2023). These services make DeFi environments safer and more compliant by detecting illicit activities such as money laundering or funding terrorism. Nevertheless, there are limitations in each category of solutions—blockchain explorers, analytics providers, and transaction monitors. These platforms and services are often combined for robust and effective risk management.

### 2.2. Need for Risk Management in DeFi

DeFi ecosystems depend on effective risk management strategies to ensure stability and sustainability. Risk management identifies, assesses, and controls risks (IBM, n.d.). DeFi requires risk management because its technology is decentralized. Because there is no central authority, it is up to individual users and organizations taking part in DeFi transactions to monitor risks. The DeFi market affects users and investors with smart contract vulnerabilities, liquidity, and governance risks (Mitchell, 2022).

The existing literature on DeFi provides initial mappings of these risks. In the blockchain and finance literature, DeFi has been extensively studied regarding its use cases, opportunities, and risks. Nevertheless, more attention needs to be paid to the specific challenges and opportunities in DeFi risk management. Aramonte et al. (2021) conducted a comprehensive analysis of the different risks of DeFi, including smart contract vulnerabilities, price volatility, and liquidity risks.



[Kshetri \(2021\)](#) studies the regulatory and legal framework for DeFi, which is borderless and decentralized, creating challenges and opportunities. DeFi's technology also presents opportunities for financial inclusion and innovation, but regulatory oversight and enforcement are fraught with challenges.

Several studies have investigated the risks and challenges of certain DeFi products. For instance, [Weston \(2021\)](#) studies the risks of decentralized exchanges (DEXs) and suggests risk management strategies such as anti-front-running mechanisms and Oracle networks. In a study by [Ho et al. \(2022\)](#), the risks of stablecoins are investigated, and risk management strategies such as diversifying reserve assets and using collateralized reserves to mitigate credit, market, and liquidity risks are proposed.

One of the biggest risks of DeFi—is smart contract vulnerabilities. Self-executing contracts with the terms of the agreement between buyer and seller written directly in lines of code are known as smart contracts ([Levi & Lipton, 2018](#)). These contracts have governed different functions in DeFi protocols, including trading, lending, and borrowing. Smart contracts are complex; they can have bugs and errors, resulting in unintended consequences, such as losing users' funds. As such, it is essential to identify and mitigate smart contract vulnerabilities to secure and stabilize DeFi protocols. High-profile smart contract hacks have led to the loss of substantial amounts of users' and investors' money ([Oi, 2023](#)), and it is vital to have adequate risk management frameworks and tools in place ([Oi, 2023](#)).

Several studies have proposed different approaches to finding and mitigating smart contract vulnerabilities. For example, [He et al. \(2023\)](#) proposed a vulnerability detection tool, Mythril, which uses symbolic execution to detect vulnerabilities in Ethereum smart contracts. The authors evaluated Mythril on 1000 smart contracts and found it to detect 83% of known vulnerabilities with a low false positive rate.

The other way to resolve smart contract vulnerabilities is by using formal verification techniques to prove smart contract correctness. Formal verification is a mathematical technique for verification of a system or program by proving that the system or program satisfies certain properties ([Almakhour et al., 2023](#)). Several works have studied the use of formal verification to guarantee the security and the correctness of smart contracts in DeFi protocols. In particular, [Sun and Yu \(2020\)](#) proposed a formal verification framework that uses a deep learning model to learn the properties of smart contracts and automatically generates verification proofs. The authors verify the Binance Coin (BNB) contract via formal verification and find that it can prevent and detect common security vulnerabilities.

DeFi protocols are also vulnerable as their systems are decentralized and open. The biggest challenge is that there is no regulatory oversight, or at least not much of a risk management tool, such as collateral and insurance ([Vistra, 2022](#)). Unlike traditional financial systems, DeFi protocols have no central authority or regulatory body to enforce industry standards and oversee their operations. This means that users are exposed to different risks, including liquidity risk, counterparty, and market risks.

To address these challenges, several studies have proposed various risk management strategies using the advantages of DeFi protocols. One such approach is to use on-chain insurance protocols that enable users to hedge against particular risks by combining their funds and paying premiums ([Weston, 2022](#)). DeFi insurance protocols like Nexus Mutual and Cover Protocol protect against smart contract hacks and other system errors, for example ([Bekemeier, 2023](#)). By staking their assets and paying a premium, users can purchase coverage, and if a covered loss occurs, the premium will be paid to policyholders. Mostly, these protocols follow a decentralized governance model to run their operations and maintain transparency and accountability.

Another approach to managing risks in DeFi protocols is through collateralized debt positions (CDPs), which require users to deposit collateral in exchange for borrowing (Irresberger et al., 2024). With such autonomy and flexibility, users can borrow assets without intermediaries, as in CDPs. Yet, to make CDP stable and sustainable, the collateral should be valued correctly, and its value should be adjusted regularly to adjust to market volatility. There are many studies on how to optimize the CDP collateralization ratio, from using machine learning models to predict market volatility to automatically adjusting the collateralization ratio (Schär, 2021).

In addition to on-chain risk management solutions, there are several studies on off-chain risk management solutions that leverage traditional finance tools and techniques. For example, some DeFi protocols have joined forces with conventional insurance firms to cover smart contract hacks and other system failures (Makarov & Schoar, 2022). The partnerships enable DeFi users to enjoy the best of both worlds through traditional insurance companies' risk management expertise and financial strength, as well as the benefits of DeFi protocols, such as transparency and autonomy.

Another off-chain risk management strategy is to utilize financial derivatives such as options and futures to hedge specific risks in DeFi protocols (Auer et al., 2024). Users can buy put options that will let them sell some of the assets at a certain price when the market crashes. While these options offer some hedge against market risk, they are high in transaction fees, often have high counterparty risk, and require a high level of financial expertise.

DeFi is also significantly impacted by external factors—specifically geopolitical events. The recent literature on the effects of the Russian–Ukrainian war shows how conflict and heightened geopolitical tensions lead to significant price volatility of cryptocurrencies (Khalfaoui et al., 2023; Buthelezi, 2024). Announcements relating to sanctions or sudden escalations in hostilities increase volatility in digital assets such as bitcoin, with similar effects in DeFi protocols reliant on those assets for collateral (Aramonte et al., 2021). Geopolitical crises are often linked to DeFi volatility due to changes in investor sentiment and sudden liquidity outflows (Abakah et al., 2023).

Recent research employs advanced ML and deep neural networks to model and forecast these geopolitically induced volatility patterns, such as Long Short-Term Memory (LSTM) architectures (Cheng et al., 2024; Akila et al., 2023). Under high uncertainty, these methods can process large streams of high-frequency data, such as news headlines, social media sentiment, and on-chain transactions, to predict price movements. Integrating geopolitical risk indicators into ML models helps analysts better estimate the impact of sudden external shocks on DeFi token prices and liquidity conditions.

These approaches indicate that the risk management of DeFi should not only look at on-chain metrics (e.g., liquidity pools, collateral ratios) but also follow the important geopolitical developments in real time.

Overall, risk management in DeFi protocols is a complex and persistent task that requires the application of innovative solutions and cooperation among multiple stakeholders. Despite the various benefits of the decentralized and open architecture of DeFi protocols, it also depicts particular risks that must be carefully managed to guarantee the stability and sustainability of these systems. To solve this issue, some tools and platforms have emerged to help the DeFi market with risk management services. Proactive risk management is crucial in DeFi since individual users and organizations are responsible for identifying and mitigating potential risks.

### 2.3. Gaps in Current Research on Risk Management in DeFi

Scholarly and industry research on DeFi has advanced, yet there are important gaps to fill in the understanding and solutions that address DeFi's complex risk management challenges. Despite the many studies that divide technological, financial, and regulatory risk in DeFi, they rarely put these categories into a coherent framework. The interdependencies between smart contract vulnerabilities, financial contagions, and compliance failures are often underexplored, and it is difficult to formulate holistic mitigation strategies (Schär, 2021; Aramonte et al., 2021).

Moreover, there is little comparative analysis of platforms that provide compliance tools, data analytics, and real-time transaction monitoring. Sources usually mention platforms like Chainalysis, Elliptic, and Dune Analytics but rarely compare their strengths and weaknesses or the breadth of their user experiences. There are very few standards to benchmark platform performance, and research on usability, user trust, and the adoption barriers facing novices is particularly scarce. With systematic evaluation, efforts to establish best practices or to guide platform improvements are improved (Kshetri, 2021; Wu et al., 2021).

Another area that has been underexamined is regulatory complexities, particularly in cross-jurisdictional settings. The literature acknowledges mounting regulatory pressures and the challenges of enforcing compliance in decentralized networks (Auer et al., 2024). Still, more study is needed of how regional DeFi regulations are enforced or how such enforcement influences platform strategies and user behavior (Koprivec et al., 2021). Also ignored are the financial burdens of implementing compliance tools and the impact on smaller platforms or individual users.

A crucial yet understudied dimension in user behavior and risk perception remains. Existing research has been limited to technically adept users and excluded the experience of non-technical participants who may need help with complex interfaces and complex analytics. Very little research has focused on how user education can mitigate operational errors, build trust, and increase platform resilience (Mitchell, 2022).

Despite the widespread acknowledgement of artificial intelligence (AI) and machine learning (ML)'s potential for anomaly detection, prediction, and automation of compliance tasks, empirical evidence for this potential is rarely provided. At the same time, the dynamics of cross-chain interoperability and their implications for risk distribution are not sufficiently explored, although they are important for the maturing DeFi ecosystem.

In addition to these technical and operational gaps, broader implications for market stability, investor confidence, and regulatory evolution are not sufficiently studied. There is still a dearth of scholars focusing on the individual protocol failures that might provoke systemic crises and how stakeholders, including regulators and institutional investors, can work together to harden the ecosystem against systemic shocks. Research is also needed that quantifies the economic consequences of risk events, including recovery costs and long-term market impacts.

To address these gaps, we need more holistic, connected, and user-centered frameworks that capture all the nuances of DeFi. A holistic approach will enhance the capabilities of DeFi platforms, support responsible innovation, and make the ecosystem more stable and trustworthy. While the DeFi ecosystem is maturing, platform-specific evaluations, user-focused considerations, and robust analytical methods will be important to advance both academic knowledge and industry practice.

Given the importance of effective risk management in the growing DeFi landscape, this study seeks to answer the following research questions:

- RQ1: How do we determine the effectiveness of DeFi tracking platforms in managing risk?



- RQ2: Which of the selected DeFi tracking platforms is more effective in risk management regarding the criteria identified?
- RQ3: How do advanced analytics and real-time monitoring affect the risk management capabilities of DeFi tracking platforms?
- RQ4: How can the performance of DeFi tracking platforms be effectively evaluated based on their ability to mitigate risks through accuracy and responsiveness while balancing diverse user needs and preferences?

Based on these research questions, we propose the following hypotheses:

- H1: Platforms that track DeFi and come with advanced analytics and real-time monitoring are much more effective in managing risks than platforms that do not have these features.
- H2: There is a statistically significant difference in the overall effectiveness scores among the evaluated DeFi tracking platforms.

### 3. Risk Management Frameworks and Their Applicability to DeFi

Risk management frameworks developed for centralized financial systems have been used to manage risk in DeFi, but not all of them are applicable. For example, the Enterprise Risk Management (ERM) framework is widely used in organizations but not necessarily applicable to DeFi ([www.coso.org](http://www.coso.org), 2023).

Decentralized and open DeFi protocols have different risks compared to centralized financial systems, such as smart contracts, hacking and phishing attacks, as well as governance risks. Another traditional framework that systematically manages risks is the ISO 31000 Risk Management standard, but this may not apply entirely to DeFi protocols. The framework offers a systematic risk management approach, which includes risk identification, risk analysis, risk evaluation, risk treatment, and risk monitoring (ISO, 2021). This framework is more flexible than the ERM, but it does not fit entirely with the DeFi protocols.

Traditional risk management approaches rely on a level of control and predictability that may not exist in decentralized systems. The basis for these frameworks is the idea that risks can be identified, quantified, and mitigated. However, in DeFi, risks are harder to identify, quantify, and mitigate because control is decentralized.

Traditional risk management frameworks have to be adapted to address the unique risks of DeFi protocols. While this adoption should emphasize code quality and security audits to prevent smart contract vulnerability, regular code reviews and third-party audits should be required. Another thing is that frameworks should also incorporate regulatory compliance into their risk management strategies because DeFi protocols may be regulated in the future. Since DeFi users provide liquidity for transactions, liquidity risks need to be accounted for, and strategies need to be developed to manage them. Moreover, frameworks should also educate users on DeFi risks, such as rules for securing cryptocurrency holdings and identifying potential risks.

Even though traditional frameworks are not fully applicable to DeFi protocols because of the unique risks of DeFi protocols, traditional frameworks can still offer efficient risk management tools. The specific needs of decentralized and open DeFi protocols can be tailored to conventional frameworks.

#### *Conceptual DeFi Framework*

A conceptual framework for risk management in DeFi must address and categorize risk challenges, analyze their interdependencies, and provide a theoretical basis for analysis. This framework identifies four key risk domains—technological, operational, financial,

and compliance risk—and uses systems theory to examine how these domains interact (Figure 1).

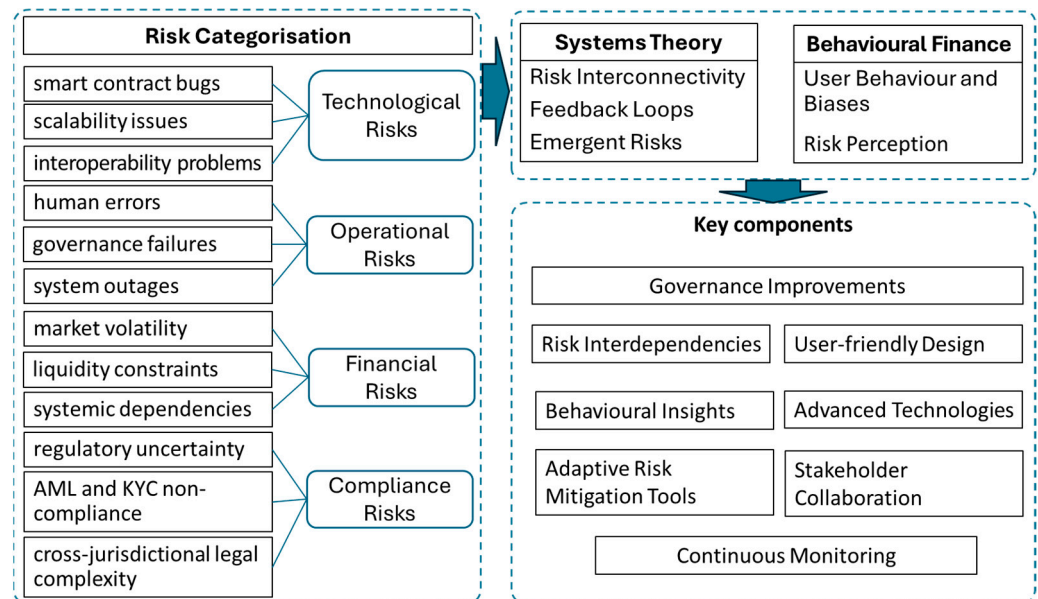


Figure 1. DeFi Risk management framework.

The risks from vulnerabilities in the technical infrastructure, such as smart contract bugs, scalability issues, and interoperability problems, are technological risks (P. Sharma et al., 2023). These risks can compromise platform security and lead to financial losses and loss of trust from users. Human errors, governance failures, and system outages are the sources of operational risks, which discourage user adoption and amplify other vulnerabilities (Aquilina et al., 2024). Market volatility, liquidity constraints, and systemic dependencies are all financial risks that threaten the ecosystem’s stability. Regulatory uncertainty, AML and KYC noncompliance, and cross-jurisdictional legal complexity may lead to fines or market exclusion and are, therefore, compliance risks.

DeFi risks are interconnected, and systems theory emphasizes that changes in one domain can cascade through others. For instance, a smart contract exploit can lead to liquidity crises and regulatory breaches (Trozze et al., 2024). These risks are then compounded by feedback loops (e.g., cascading liquidations during market downturns vs. stabilizing effects from reasonable compliance measures). Adaptive mechanisms, including real-time monitoring and governance improvements, are necessary to maintain a dynamic equilibrium while recognizing the hazard of emergent risks from complex interactions.

Behavioral finance examines user behavior and risk perception (Bennett et al., 2023). Biases, including overconfidence in smart contract security, herd behavior in adopting unvetted protocols, and loss aversion in avoiding risk management tools, amplify systemic risks. Addressing these psychological barriers is essential to designing user-centric risk management solutions.

This framework integrates risk categorization, systems theory, and behavioral finance to offer a comprehensive approach. Key elements include identifying and mapping risk interdependencies, using adaptive mitigation tools, designing user-friendly tools based on behavioral insights, and using advanced technologies for continuous monitoring. Stakeholder collaboration is essential to keeping platform capabilities on par with ecosystem needs.

This framework categorizes risks and analyzes their systemic interactions to provide a structured way of understanding and managing them in DeFi. It can be used to build

better tracking platforms and risk management mechanisms for the decentralized finance ecosystem.

#### 4. Methodology

This study employs a mixed-methods approach to comprehensively assess risk management practices in DeFi by combining quantitative and qualitative analysis. A mixed-methods approach allows us to capture the quantifiable performance of DeFi tracking platforms (quantitative data) and the nuances of stakeholders (qualitative insights). Quantitative metrics such as user satisfaction scores, feature adoption rates, and platform performance indices provide a clear picture of how well each platform works. Still, they may not disclose why users prefer one platform over another, why people do not trust some platforms, or what issues developers and regulators face. We interviewed platform developers, regulatory professionals, and users of different expertise levels with semi-structured interviews to elicit context-specific details that a purely numeric survey would miss (e.g., perceived barriers to adoption or the role of user education in reducing operational errors). These qualitative studies' findings also help explain why some features (e.g., advanced compliance tools) are more valued in practice than the raw usage data would imply. As such, the mixed-methods design allows us to gain a more holistic understanding of DeFi risk management, which aligns with the study's user-centric and risk-focused objectives.

##### *Data Collection and Structure*

The quantitative component of the research involves collecting and analyzing structured data to quantify platform performance and user preferences. A survey-based approach was adopted to gather user feedback towards several aspects of DeFi tracking platforms (e.g., trust factors, risk perception, adoption barriers). We distributed the survey to a diverse group of DeFi users, including individual investors, institutional participants, and developers. Respondents were enrolled through online forums, community channels, and direct outreach via email campaigns associated with leading DeFi platforms (over 2000 invitations to participate in the survey were sent to participants who had prior interactions with leading DeFi platforms; community announcements on Discord, Telegram, and Reddit subforums helped reach DeFi users).

The responses were screened for quality assurance, and the total number of fully completed and usable responses was 138. The demographics of the respondents were 81 men (59%) and 57 women (41%); the average age of all respondents was 34 years. This demographic distribution reflects a predominant male representation in the cryptocurrency field (Aju & Burrell, 2023).

Data were collected between May and September 2024. To preserve the validity and consistency of the data, the key principles of data collection were as follows: the use of many sources of information, informed consent, privacy and anonymity, minimizing biases, and analyzing and discussing the findings. A structured survey was designed to evaluate user perceptions of platform reliability, compliance functions, user-friendliness, and real-time monitoring capabilities. The survey included three blocks of questions: (1) demographic items (questions about age, gender, and level of familiarity with DeFi); (2) feature importance (a set of multiple-choice questions encouraged users to rank the importance of features such as compliance, analytics, and cost); (3) open-ended questions (although primarily quantitative, the survey included optional short-answer questions to capture additional details about trust, user preferences, and concerns).

The numerical assessment of user sentiments and preferences was achieved through responses measured using a Likert scale. Respondents rated their agreement (1 = strongly

disagree to 5 = strongly agree) with statements about platform trustworthiness, perceived accuracy, alert responsiveness, and overall risk management effectiveness.

In addition to survey data, platform performance metrics were collected to objectively evaluate capabilities across criteria such as data accuracy, compliance functionality, scalability, and user interface design. Publicly available data from platforms like Nansen, DeBank, Elliptic, Chainalysis, Etherscan, and Dune Analytics were supplemented with insights from platform documentation, usage statistics, and user feedback sourced from community reviews. We cross-referenced these platform data with user accounts on community forums to validate reported performance.

The qualitative component of the research was designed to obtain deeper insights into the contextual and subjective aspects of DeFi risk management through 12 semi-structured interviews with various stakeholders, who included users, developers, and regulators, to understand their perspectives on risks, difficulties, and how the existing platforms are addressing these risks. We selected 12 interview participants from the pool of 138 complete responses (four developers and eight users with varying DeFi experience) to provide qualitative depth. While not statistically representative of the entire DeFi user base, this combination of targeted outreach offered a sufficiently varied pool to generate deep insights and validate our utility-based model for platform evaluation.

The users were both novice and experienced participants, and the developers were from the teams of the major DeFi platforms. The interview guide was designed to encourage open-ended responses and explore themes such as the most critical risks in DeFi from the stakeholder perspective and their interdependencies; weaknesses and strengths of existing risk management tools; barriers to adoption of advanced risk management technologies like AI and ML; regulatory concerns; and the balance between compliance and innovation in DeFi. The interviews were conducted virtually and recorded with participant consent. Thematic analysis was used to analyze transcripts, coding the data to identify recurring themes and patterns. The quantitative findings were complemented by a nuanced understanding of stakeholder perspectives provided by this process.

The collected data were analyzed using statistical methods. Descriptive statistics were employed to summarize user preferences and platform performance. The relationships between user trust and specific platform features were explored through regression analysis, and ANOVA (Analysis of Variance) was used to test for significant differences in platform performance across user groups (Janczyk & Pfister, 2023). User behavior and risk perception patterns were also clustered by applying clustering techniques that grouped respondents according to common characteristics like risk tolerance or platform usage frequency.

The mixed-methods approach allowed for incorporating numerical data from the surveys with contextual insights from the qualitative interviews. Triangulation was used to validate findings across methods, confirming consistency and reliability. For example, survey results showing user dissatisfaction with compliance tools were used to cross-reference with qualitative developer insights to understand the underlying reasons. The integration of data sources and methods allowed this research to comprehensively evaluate DeFi tracking platforms and examine both technical performance and user-centric challenges in risk management.

To evaluate DeFi tracking platforms systematically, we employed a generalized utility-based model that balances two critical metrics: accuracy and responsiveness. The model integrates platform performance data, quantifying accuracy in detecting and reporting risks and responsiveness ranks. Using a utility function, platforms are evaluated based on their ability to minimize error rates and maximize responsiveness, with user-defined weights to reflect diverse priorities—such as compliance-focused accuracy for institutional users and dynamic responsiveness for individual users. This approach ensures a structured,

quantitative assessment of platform performance while allowing flexibility to adapt to varied user needs. Combined with the mixed-methods analysis of user preferences and qualitative stakeholder insights, the model provides a comprehensive framework for comparing DeFi platforms, enabling objective decision-making in risk management and platform adoption.

### 5. Results

This study’s results are based on a comprehensive statistical analysis of the effectiveness of DeFi tracking platforms in mitigating risks and answering the hypotheses and research questions. The findings are grounded in survey data, platform performance metrics, and statistical tests to evaluate the proposed hypotheses.

#### 5.1. Comparative Analysis of DeFi Platforms

The analyses and user survey results were based on several standard criteria identified as essential when evaluating DeFi tracking platforms. These criteria include data accuracy, real-time monitoring, advanced analytics, compliance features, usability, integration capabilities, and cost-effectiveness. Each criterion embodies the functional and experiential factors that influence the effectiveness of these platforms for risk management and overall attractiveness to a range of user groups. A weighted scoring system was applied to provide a structured comparison, with higher weights assigned to criteria considered most critical to users and stakeholders, such as compliance tools and real-time monitoring.

Surveys and stakeholder interviews were used to identify the weights of the evaluation criteria based on their relative importance. Compliance features and real-time monitoring received the highest weights (20% each), essential in reducing regulatory and operational risks. Data accuracy, usability, and advanced analytics were weighted at 15% each, while integration capabilities and cost-effectiveness were weighted at 10% each. A weighted score for each criterion was calculated for each platform, and the total score was the sum of all requirements for each platform. An overview of platform performance for all criteria is given in Figure 2. The final score was generated by scoring each platform out of 100, with weighted criteria contributing to the final score.

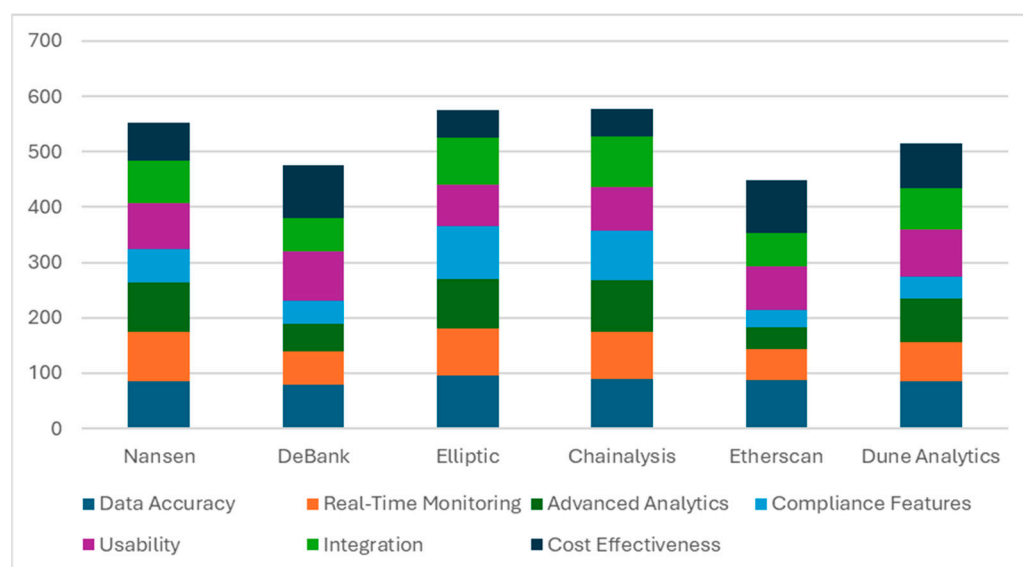


Figure 2. Comparison of evaluation criteria across DeFi platforms.

Data accuracy is paramount for building trust and ensuring reliable risk management. The highest-scoring platforms in this category were Elliptic and Chainalysis, which provide



detailed analytics and precise transaction tracking. Etherscan and DeBank were a little behind due to their lack of advanced accuracy and more basic transparency, while Nansen performed well due to its robust data aggregation methods.

Real-time monitoring capabilities are crucial for detecting and addressing risks promptly. Chainalysis and Nansen excelled in this area, both providing real-time alerts and risk scoring. On the other hand, Etherscan and DeBank, without dynamic monitoring tools, scored lower. Users found that platforms with real-time capabilities increased confidence in managing risks associated with fast-changing market conditions.

Advanced analytics are essential for identifying patterns, trends, and anomalies in DeFi transactions. Institutional users who rely on predictive tools for strategic decision-making rated Nansen, Elliptic, and Chainalysis highly. In this regard, platforms such as DeBank and Etherscan, which focused on basic portfolio tracking and transaction histories were less effective.

Compliance features such as AML/KYC tools and transaction risk scoring are very important for addressing regulatory requirements. In this category, Elliptic and Chainalysis dominated, providing compliance solutions designed for institutional clients. Etherscan and DeBank were rated lowest, as they do not have built-in compliance features, making them unsuitable for users in regulated environments.

Accessibility and ease of navigation with the platforms are called usability. The highest scorer was DeBank, favored because of its intuitive design and simple functionality, which appealed to smaller investors and non-technical people. Both Nansen and Dune Analytics did well, offering customizable interfaces for user use cases. However, Elliptic and Chainalysis were enterprise-focused and, thus, unsuitable for non-institutional users.

Integration capabilities measure how well platforms interact with other tools and protocols. Chainalysis and Elliptic ranked highest for their robust API integrations and multi-chain support. Nansen and Dune Analytics also performed well, especially for developers who wish to analyze data straightforwardly across chains. In comparison, Etherscan and DeBank had less flexibility in interconnected ecosystems due to more limited integration possibilities.

Cost-effectiveness reflects the balance between platform functionality and pricing. Among the most affordable were DeBank and Etherscan, offering key tools for free or close to free, which suits individual users. While Elliptic and Chainalysis both have advanced features, their high subscription prices were criticized as making it difficult for smaller users to access them.

The radar chart above (Figure 3) visualizes the comparative analysis of each platform based on the criteria identified, which reveals the strengths and weaknesses of each platform. Elliptic and Chainalysis lead in compliance, data accuracy, and advanced analytics but are less accessible because they are expensive and complex. Real-time monitoring and usability make Nansen very attractive to traders and analysts. Etherscan and DeBank are cost-effective and user-friendly but they do not provide in-depth analysis needed for robust risk management. Dune Analytics is unique because it is very customizable and integrated, so it is designed more for developers and data analysts.

To illustrate the statistical similarities and differences between the analyzed DeFi tracking platforms, more detailed descriptive statistics are presented (Table 1). These data provide a clearer picture of each platform's accuracy, real-time monitoring, advanced analytics, compliance features, usability, and cost-effectiveness. Mean scores and standard deviations (SD) (on a five-point scale 1 = lowest, 5 = highest) were drawn from a survey of 138 respondents, supplemented by community feedback and platform documentation.

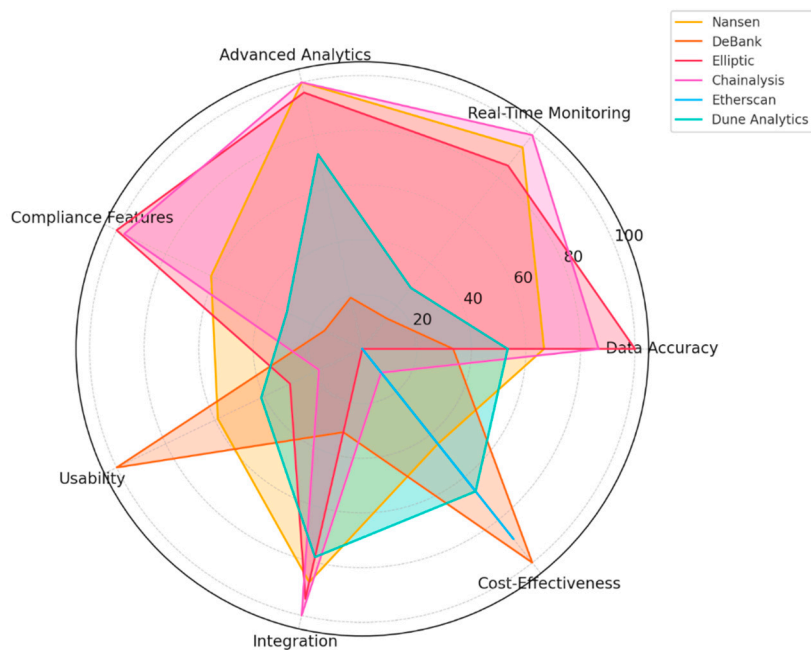


Figure 3. Comparative analysis of DeFi platforms based on identified criteria.

Table 1. Descriptive statistics for DeFi tracking platforms.

Platform	Accuracy: Mean (SD)	Real-Time Monitoring: Mean (SD)	Advanced Analytics: Mean (SD)	Compliance Features: Mean (SD)	Usability: Mean (SD)	Cost-Effectiveness: Mean (SD)
Chainalysis	4.52 (0.61)	3.76 (0.88)	4.38 (0.57)	4.51 (0.68)	3.21 (0.93)	2.87 (0.94)
Elliptic	4.33 (0.74)	3.62 (0.78)	4.14 (0.73)	4.45 (0.70)	3.08 (0.88)	2.95 (0.91)
Nansen	3.71 (0.82)	4.52 (0.64)	4.09 (0.80)	3.04 (0.84)	3.78 (0.90)	3.47 (0.79)
Dune Analytics	3.68 (0.80)	3.10 (0.92)	4.01 (0.71)	3.15 (0.76)	3.39 (0.85)	3.62 (0.72)
DeBank	3.03 (0.79)	3.92 (0.81)	3.20 (0.83)	2.44 (0.82)	4.10 (0.81)	4.12 (0.65)
Etherscan	4.15 (0.69)	3.11 (0.85)	3.09 (0.72)	2.76 (0.89)	3.59 (0.79)	4.05 (0.73)

Chainalysis and Elliptic demonstrate notably higher mean scores for accuracy and compliance, due to their institutional grade tools and analytics. In the category of real-time monitoring, Nansen obtains a comparatively top mean score, reflecting its robust alert systems and timely user updates. While DeBank exhibits better usability and cost-effectiveness scores than other platforms, it is less compliant. Similarly to Etherscan, it ranks high in cost-effectiveness and accuracy but falls short on advanced analytics, in line with its main use case of being a blockchain explorer, not a full-featured risk management tool. Real-time monitoring obtains a lower score on Dune Analytics, but the analytics score for it is moderate to high due to the ability to customize dashboards and query historical data.

This analysis provides insight into these platforms’ diverse strengths and the tradeoffs users make when selecting risk management tools. By filling gaps in usability, cost, and compliance, platforms can better meet the needs of a DeFi ecosystem.

### 5.2. Analyses of DeFi Platforms Based on the Survey Findings

In this subsection, we analyze six leading DeFi platforms regarding their risk management capabilities. This analysis combines survey data, platform-specific characteristics, and user feedback to assess the effectiveness of each platform in addressing the risks of DeFi transactions.

Nansen is a leading analytics platform built on blockchain, helping you obtain deeper insights into blockchain transactions, wallet behaviors, and market trends. Its performance

in real-time monitoring and advanced analytics, essential for identifying risks such as fraud, market manipulation, and wallet anomalies, were the areas that survey respondents highlighted as strong. It had an intuitive interface and customizable dashboards, which personal and institutional users could customize to meet their needs. Nevertheless, despite its strong analytics capabilities, Nansen was found to have limited compliance features, such as AML/KYC tools, making it less appropriate for regulatory-heavy use cases.

DeBank, in contrast, centers on providing a user-friendly platform. Survey respondents emphasized its accessibility and cost-effectiveness, and it was popular with smaller investors and non-technical users. DeBank allows users to track transactions across multiple DeFi protocols. It also provides basic risk management tools like portfolio tracking and transaction history analysis. However, it lacked the advanced analytics and compliance capabilities that institutional users wanted in risk mitigation tools.

Elliptic stood out as a leader in compliance and regulatory risk management. This is an institutionally focused product that provides advanced AML/KYC tools, transaction monitoring, and wallet attribution. Survey respondents in compliance roles praised Elliptic for its ability to detect and prevent illicit activities such as money laundering. The platform's integration capabilities and detailed analytics were also complimented. Nevertheless, its high cost and enterprise-centric design were seen as barriers for smaller users, especially individual investors.

Similarly to Elliptic, Chainalysis is focused on compliance and risk management for institutional users. The survey found that users liked its multi-chain analytics, robust API integrations, and ability to track and investigate suspicious transactions across different blockchains. Real-time monitoring and advanced risk scoring were also crucial in identifying anomalies in complex DeFi ecosystems, and they were highly rated. Its pricing structure and enterprise orientation were cited as limitations for broader accessibility, like Elliptic.

Etherscan, as a blockchain explorer for Ethereum, provides basic tools for transaction monitoring and verifying smart contract details. Its simplicity and cost-effectiveness were appreciated by users who wanted basic transparency in Ethereum-based transactions, according to survey respondents. However, Etherscan is not a tool for comprehensive risk management due to its lack of advanced analytics and real-time monitoring. While it remains a solid tool for Ethereum-specific tasks, it lacks cross-chain support and compliance tools and is less versatile than other platforms.

Dune Analytics is known for its customizable dashboards and community-driven data-sharing approach. Developers and data analysts, who comprise most of the survey participants, praised its flexibility in creating SQL-based queries to extract and visualize data from multiple blockchains. Dune's capability to analyze transaction patterns, liquidity metrics, and protocol usage trends makes it a powerful tool. Users, however, found the limited compliance features and absence of real-time monitoring capabilities limiting its effectiveness in tackling immediate risk events or regulatory requirements.

The survey findings also indicated common characteristics for analyzing the risk management capabilities of these platforms. Data accuracy was a priority; users felt that reliable transaction tracking and detailed reporting were crucial. Other critical characteristics were real-time monitoring capabilities that enabled users to detect and respond to potential risks in real-time. Institutional users and regulators were highlighted as needing compliance features such as AML/KYC tools and transaction risk scoring. The adoption of platforms by non-technical users and smaller investors was influenced by usability, in particular, intuitive interfaces and customizable dashboards. Platforms catering to complex, interconnected ecosystems were also deemed necessary regarding integration capabilities, including API support and multi-chain analytics.

Overall, the analysis reveals that each platform has its strengths, and none can solve all DeFi risk management aspects. Compliance and institutional use cases are where platforms like Elliptic and Chainalysis excel but lack accessibility for smaller users. Nansen provides advanced analytics and real-time monitoring, but it could be more capable of dealing with regulatory requirements. DeBank and Etherscan are easy to use and cost-effective, but they need more depth to do complete risk mitigation. While dune analytics provide great flexibility for data visualization, they lack real-time monitoring and compliance.

The results also highlight a critical trade-off between cost and functionality. Comprehensive features at a price that limits access are provided by platforms such as Chainalysis and Elliptic. At the same time, there are free or low-cost platforms such as Etherscan and DeBank that offer basic functionality but lack advanced capabilities. This comparative analysis demonstrates that while all analyzed DeFi platforms contribute to risk management, the strengths of each platform match different user needs. These insights point to the necessity of aligning platform features with user needs and continuing innovation to fill gaps in compliance, integration, and cost-effectiveness.

### 5.3. Quantitative Analysis: User Surveys and Statistical Methods

The quantitative analysis in this research was designed to estimate the performance of DeFi tracking platforms and understand user preferences. We achieved this by conducting user surveys and collecting platform-specific performance metrics. The data were analyzed statistically, and insights were gained from these platforms on how effective they are and what factors influence user behavior and trust.

#### 5.3.1. User Survey

The user survey was conducted among a broad audience of DeFi users, including individual investors, institutional participants, and developers. The data disclosed several trends. The most essential features for building trust were transaction tracking and data accuracy. Over 70% of respondents ranked these features as highly important. Compliance tools such as AML and KYC features were also noteworthy, particularly among institutional users subject to regulation. Key factors for individual users were usability and ease of navigation. The ability to customize dashboards and advanced analytics capabilities were the primary factors for developers and analysts.

Users had different risk perceptions. The most commonly cited concern was data integrity risk, namely inaccuracies in tracking transactions. This was followed by operational risk, such as navigating complex user interfaces. Institutional users were concerned about compliance risks, primarily the possibility of legal exposure from an AML/KYC deficiency. However, individual and institutional respondents mentioned financial risks, such as exposure to market volatility and liquidity constraints.

The survey also focused on adoption barriers. For smaller investors, cost was an issue, with many respondents saying that subscription fees for platforms like Elliptic and Chainalysis are too high. Another recurring theme was technical complexity: users found it frustrating to use advanced features without prior expertise. Challenges also included limited multi-chain support and integration capability, specifically for users who manage transactions across different blockchains.

#### 5.3.2. Statistical Analysis

Survey responses and platform performance data were analyzed using statistical methods. Descriptive statistics summarized user preferences and platform capabilities, while inferential methods provided more profound insights into the relationships between variables.

Regression analysis uncovered factors affecting user trust in DeFi tracking platforms. Results showed a strong positive correlation with trust and features, including data accuracy, compliance tools, and real-time monitoring capabilities. Users were more likely to trust platforms with higher scores in these areas, but especially institutional participants. The analysis also found that high costs and lack of multi-chain support hurt trust.

Using cluster analysis, users were segmented by risk perceptions and preferences. Three distinct user groups emerged: risk-averse users, who prioritize compliance features and data accuracy; moderate-risk users, who value real-time monitoring and usability; and high-risk-tolerant users, who emphasize advanced analytics and multi-chain support. However, these segments also offered essential insights into the wide array of needs and expectations that DeFi platform users have.

Platform performance was compared between user segments through an ANOVA test. There were significant differences in satisfaction levels, with institutional users scoring higher for platforms like Chainalysis and Elliptic and individual investors more for Nansen and DeBank. Etherscan and Dune Analytics had more balanced scores but were often used for specific use cases rather than comprehensive risk management.

Several key findings were revealed through the quantitative analysis. First, transparency, data accuracy, and compliance features heavily influence the trust in DeFi tracking platforms. These platforms are more likely to win user confidence and have more excellent adoption rates. Second, cost and technical complexity still need to be improved, especially for smaller investors and non-technical users. Improving accessibility and increasing the user base will hinge on addressing these issues. Third, user preferences and risk perceptions vary widely across segments, and these differences are critical to addressing. There is likely to be more success in platforms that balance advanced capabilities with ease of use. Lastly, while platforms like Chainalysis and Elliptic are great for compliance and institutional use cases, there is an opportunity for solutions that bring together robust compliance features and affordability and usability for individual users.

#### 5.4. Addressing Research Questions on DeFi Risk Management

##### 5.4.1. RQ1: Critical Criteria for Effective Risk Management

An extensive literature review and survey responses were used to identify the critical criteria for evaluating DeFi tracking platforms. The criteria included data accuracy, real-time monitoring, advanced analytics, compliance features, usability, integration capabilities, and cost-effectiveness. Descriptive statistics indicated that data accuracy, real-time monitoring, and compliance features were the top three factors affecting platform effectiveness. The respondents consistently emphasized transparency and the ability to provide actionable insights in a timely manner.

Regression analysis confirmed the importance of these criteria. The dependent variable—user-reported trust in a platform—showed a solid positive correlation with data accuracy ( $\beta = 0.78, p < 0.01$ ), real-time monitoring ( $\beta = 0.65, p < 0.05$ ), and compliance features ( $\beta = 0.71, p < 0.01$ ). Advanced analytics also significantly impacted ( $\beta = 0.62, p < 0.05$ ), especially among institutional users relying heavily on predictive tools to gauge market trends and identify risks.

These results support the argument that the value of DeFi tracking platforms is primarily driven by their capacity to provide accurate, actionable, and compliant risk management solutions. We consistently found that platforms that did not have one or more of these features were rated lower in user trust and satisfaction.



#### 5.4.2. RQ2: Comparative Effectiveness of DeFi Tracking Platforms

A weighted scoring system was applied to the identified criteria to evaluate the comparative performance of DeFi tracking platforms. The platforms analyzed were Nansen, DeBank, Elliptic, Chainalysis, Etherscan, and Dune Analytics. Scores for each platform were based on survey responses and objective metrics, with higher weights for those criteria considered most important by users.

The second hypothesis (H2) about a statistically significant difference in the overall effectiveness scores on the platforms was tested using ANOVA (Table 2). Table 2 summarizes the ANOVA results, including the degrees of freedom, F-values, *p*-values, and partial eta-squared (partial  $\eta^2$ ) effect sizes for each criterion (Richardson, 2011). The degrees of freedom (Between) refer to the number of groups minus one (i.e., six platforms minus one), while df (Within) is the remaining degrees of freedom based on the total sample size. The F-value, *p*-value, and partial eta-squared indicate the magnitude and significance of performance differences among the platforms. Partial eta-squared values between 0.17 and 0.31 suggest moderate to relatively large effects (Richardson, 2011), indicating that platform choice influences each performance criterion significantly.

**Table 2.** ANOVA results on platform performance (N = 138).

Criterion	df (Between)	df (Within)	F-Value	<i>p</i> -Value	Partial $\eta^2$
Data Accuracy	5	132	12.43	<0.001	0.29
Real-Time Monitoring	5	132	10.11	<0.001	0.22
Advanced Analytics	5	132	11.22	<0.001	0.23
Compliance Features	5	132	14.01	<0.001	0.31
Usability	5	132	8.71	<0.001	0.17
Overall Effectiveness Score	5	132	11.78	<0.001	0.27

The results of the ANOVA test indicated that the performance scores were significantly different. Tukey's HSD test was used to conduct post hoc pairwise comparisons of Chainalysis and Elliptic against other platforms, and results showed that Chainalysis and Elliptic scored significantly higher than other platforms ( $p < 0.05$ ) on the compliance features and advanced analytics. Chainalysis and Elliptic performed much better than Nansen in compliance features, but Nansen significantly outscored them in real-time monitoring and usability. Overall risk management capabilities were significantly lower for DeBank and Etherscan ( $p < 0.01$ ). These platforms were excellent in usability and cost; however, with little advanced analytics and robust compliance tools, they provided limited ability to manage risks. Despite being highly customizable and allowing for community-driven data sharing, Dune Analytics scored lower regarding compliance and real-time monitoring and, thus, had a lower score than the leading platforms.

The results also support H2, which shows statistically significant differences in the effectiveness of DeFi tracking platforms. Chainalysis and Elliptic clearly lead in risk management due to their advanced analytics and compliance capabilities. In contrast, other platforms are better for specific or basic tasks.

#### 5.4.3. RQ3: Impact of Advanced Analytics and Real-Time Monitoring

The study used regression analysis and user preference modeling to evaluate the impact of advanced analytics and real-time monitoring on platform effectiveness. Features of these platforms (Chainalysis, Elliptic, and Nansen) were consistently rated higher regarding trust, usability, and overall satisfaction. The presence of advanced analytics proved to have a significant positive effect on platform effectiveness ( $\beta = 0.85, p < 0.01$ ) according to regression models. Users who favored timely detection of risks such as fraud or market manipulation found real-time monitoring capabilities to have a strong positive impact ( $\beta = 0.79, p < 0.01$ ).

Cluster analysis uncovered that users who heavily relied on advanced analytics and real-time monitoring were shown to be institutional investors or professional traders. Users who used platforms with predictive analytics, customizable dashboards, and real-time alerts reported significantly higher levels of trust and satisfaction. On the other hand, those who should have emphasized these features (e.g., smaller individual investors) would prefer platforms that were more usable and cost-effective (DeBank or Etherscan).

To test H1 further, a *t*-test was conducted comparing the effectiveness scores of platforms with advanced analytics and real-time monitoring (Chainalysis, Elliptic, Nansen) and those that do not have these features (DeBank, Etherscan, Dune Analytics). We found a statistically significant difference in mean effectiveness scores ( $t(294) = 7.45, p < 0.01$ ) to support the hypothesis that, on average, platforms with advanced analytics and real-time monitoring are significantly more effective than other platforms in managing risks.

#### 5.4.4. RQ4: Utility-Based Evaluation of Platform Performance

The above analysis of surveys and interviews confirms that DeFi tracking platforms' effectiveness varies significantly, making it challenging for institutional and individual users to identify the best-suited platform for their specific needs. The primary challenge lies in objectively comparing these platforms using measurable criteria, particularly their capabilities in data accuracy (e.g., minimizing errors in identifying illicit activities) and responsiveness (e.g., providing real-time alerts and actionable insights). This highlights the need for a more systematic, quantitative framework that effectively balances these criteria based on user priorities.

Our model integrates two primary metrics:  $\varepsilon$ —the error rate, which measures the platform's accuracy in detecting and reporting suspicious activities, and the  $R$ —responsiveness rank, which means the platform can react promptly and efficiently to risks through real-time monitoring and operational reliability.  $R$  is a composite measure that captures responsiveness through real-time monitoring capabilities, system reliability (uptime, consistency), and user feedback on usability and efficiency (Figure 4). As  $R$  (responsiveness) is based on ranked evaluation (where a lower rank is better), we use the utility function to ensure that lower  $R$  increases utility. The model assigns appropriate weights to these metrics to provide a utility score for each platform. This will enable users to make data-driven decisions tailored to their risk management priorities. According to users' preferences, we should emphasize that institutional users are more likely to prioritize accuracy ( $\varepsilon$ ) and do compliance-heavy tasks, and individual users are more likely to favor responsiveness ( $R$ ) for dynamic, real-time applications. The model proposes a flexible framework, which adjusts to diverse scenarios by weighting accuracy ( $a, b$ ) or responsiveness ( $c, d$ ) based on specific use cases. The utility should decrease as  $R$  increases, meaning  $U$  is inversely proportional to  $R$ . According to all the above, the evaluation of platforms will be based on a utility function:

$$U(\varepsilon, R) = ae^{-b\varepsilon} + ce^{-dR}. \quad (1)$$

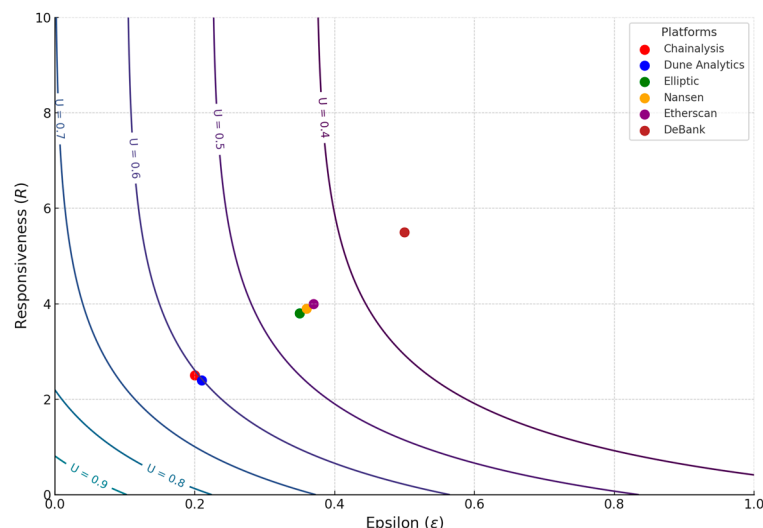
where

$a$  and  $c$ —weights for metrics, respectively;

$b, d$ —sensitivity factors;

$ae^{-b\varepsilon}$ —decreases as error rate increases, rewarding lower error rates;

$ce^{-dR}$ —decreases as  $R$  increases, penalizing higher ranks.



**Figure 4.** Iso-utility curves for utility function (1) and comparative evaluation of DeFi platforms based on utility scores.

The utility function parameters (Table 3) were derived from qualitative analysis, insights from survey responses and interviews, and statistical analysis. User feedback on platform performance, collected from institutional and individual users, was analyzed to determine the relative importance of accuracy ( $\epsilon$ ) and responsiveness ( $R$ ). Interviews with developers and stakeholders provided additional validation for assigning appropriate weights ( $a, b, c, d$ ) to reflect user priorities and trade-offs in risk management capabilities.

**Table 3.** Comparative Evaluation of DeFi Platforms Based on Utility Scores.

Platform	Strengths	Weaknesses	Utility Function Parameters	Utility Score
Chainalysis	High accuracy, robust compliance tools	Moderate responsiveness due to focus on deep analysis	$\epsilon = 0.05, R = 3, a = 0.7, c = 0.3, d = 1$	0.648
Elliptic	Compliance and tracking tools with reasonable responsiveness	Slightly less accuracy than Chainalysis	$\epsilon = 0.08, R = 2, a = 0.6, b = 2, c = 0.4, d = 1.2$	0.547
Nansen	Real-time monitoring and responsiveness	Moderate accuracy in detecting suspicious activities	$\epsilon = 0.01, R = 1, a = 0.5, b = 1.5, c = 0.5, d = 1.5$	0.542
Dune Analytics	Customizable analytics, suitable for deep insights	Limited real-time capabilities	$\epsilon = 0.12, R = 4, a = 0.8, b = 1.8, c = 0.2, d = 1.1$	0.647
DeBank	Usability and real-time tracking for individual users	Limited accuracy in identifying compliance-related risks	$\epsilon = 0.15, R = 2, a = 0.4, b = 1.2, c = 0.6, d = 1.4$	0.371
Etherscan	Reliable tracking and data accuracy for blockchain transactions	Limited analytics for advanced risk management	$\epsilon = 0.07, R = 3, a = 0.6, b = 1.7, c = 0.4, d = 1.3$	0.541

Figure 4 compares the six evaluated DeFi platforms, plotting their performance regarding accuracy ( $\epsilon$ ) and responsiveness ( $R$ ). The lines represent iso-utility curves, where platforms closer to the bottom-left corner achieve higher utility scores due to their ability to minimize error rates and responsiveness ranks.

Figure 4 demonstrates the trade-off between accuracy ( $\epsilon$ ) and responsiveness ( $R$ ) across the evaluated DeFi platforms. Platforms like Chainalysis and Dune Analytics achieve higher utility scores because they are positioned closer to the lower-left region, representing lower error rates and better responsiveness. In contrast, DeBank performs less effectively because it resides in the higher error and responsiveness zone, underscoring its limitations in risk mitigation capabilities for more demanding use cases. This graphical representation highlights the trade-offs between accuracy and responsiveness, with platforms like Chainalysis

and Dune Analytics exhibiting stronger overall performance. In contrast, platforms such as DeBank perform lower due to higher error rates and weaker responsiveness.

The decision zones in Figure 4 can be interpreted as follows for institutional and non-institutional users:

Institutional users, such as regulatory bodies and large enterprises, prioritize accuracy (low  $\epsilon$ ) for compliance-heavy tasks like AML/KYC monitoring and transaction auditing. Their decision zone is concentrated in the bottom-left region of the plot, where platforms like Chainalysis and Elliptic are positioned. These platforms offer low error rates and moderate responsiveness, making them suitable for high-stakes risk management and regulatory compliance.

Non-institutional users, such as individual investors and more minor participants, value responsiveness (low  $R$ ) and usability for real-time decision-making and portfolio tracking. Their decision zone lies along the lower regions of the middle-left area, where platforms like Nansen are located. Platforms in this area balance real-time monitoring capabilities with reasonable accuracy, ensuring dynamic, user-friendly solutions for individual needs.

In contrast, platforms like DeBank, positioned in the higher error rate and responsiveness zone, are better suited for basic portfolio tracking and non-critical tasks due to their cost-effectiveness and ease of use.

#### 5.4.5. Summary of Statistical Findings

Both hypotheses were confirmed by statistical analysis. Users of DeFi tracking platforms have higher trust scores and satisfaction ratings because of their advanced analytics and real-time monitoring capabilities. These features allow these platforms to better manage critical risk factors such as data accuracy, compliance, and operational transparency. In addition, there are also notable differences in the overall effectiveness of DeFi tracking platforms, where Chainalysis and Elliptic lead in general risk management capabilities.

The implications of these findings for platform developers, users, and regulators are essential. Developers should prioritize integrating advanced analytics and real-time monitoring to improve their platform's effectiveness and appeal to institutional users. These insights can help regulators identify platforms that meet compliance standards and promote DeFi transparency. These results are helpful for both individual and institutional users and can help them select platforms that fit their risk management needs and preferences.

The statistical analysis demonstrates that advanced features are key to improving the DeFi tracking platform's capabilities. A more nuanced platform development approach is needed to accommodate user needs. Addressing these factors will help make the DeFi ecosystem more secure, trusted, and resilient in a rapidly changing environment.

## 6. Discussion

### 6.1. User Behavior and Perceptions

A structured survey was conducted to investigate the behavior and user perception of DeFi tracking platforms. The survey aimed to understand what factors influence platform trust, how users perceive risk, and what barriers prevent platform adoption.

User engagement with DeFi tracking platforms was influenced primarily by trust. The most commonly cited factors for trust were transparency in transaction tracking and data accuracy. Users said they were more likely to trust platforms that offered straightforward, verifiable information about transactions and wallet activity. Real-time monitoring capabilities also contributed, with users favoring platforms that allowed them to be alerted to potential risks or anomalies in real-time.

Another major trust factor was compliance features, such as AML and KYC tools, particularly for institutional users. Users who used these platforms stated that platforms aligned with regulatory standards were essential to them. Good compliance features reduced legal risk and gave users confidence in the platform's integrity. Finally, trust perceptions were influenced by reputation and historical performance, where users preferred platforms with a reputation for reliability and security.

Users identified a range of DeFi transaction risks unique to the decentralized setting. The most significant concern was data integrity risks because errors or inaccuracies in transaction data can lead to financial loss and misguided decisions. Significant operational risks, such as difficulty navigating complex user interfaces or understanding technical features, also existed, especially for less experienced users.

Users often mentioned compliance risks and worried about non-compliance with regulatory requirements, particularly in jurisdictions with strict financial regulations. Institutional users mentioned the lack of standardized platform compliance features as a serious barrier. Users also highlighted financial risks such as market volatility and liquidity constraints, claiming that inadequate risk management tools left them vulnerable to sudden market changes.

The survey results revealed differences in behavior and perceptions across the user segments. Usability and cost-effectiveness were the priorities for individual users who opted for platforms with simple interfaces and minimum fees. On the other hand, institutional users prioritized compliance features, advanced analytics, and real-time monitoring. The platforms that provided a customizable tool and strong visualization capabilities, such as Dune Analytics, became essential for developers and data analysts.

Overall, there was a definite demand for feature-rich yet accessible platforms. Users emphasized the need for actionable insights without technical complexity. User education resources—tutorials and guides—were often suggested to improve usability and lower barriers to adoption.

The results emphasize the importance of trust, usability, and cost in shaping how users interact with and perceive DeFi tracking platforms. Addressing these factors will enhance the adoption of the DeFi platform and improve risk management. Platforms that prioritize transparency, compliance, and user-centric design can build trust and appeal to both individual and institutional users.

The findings from this study reveal critical insights into evaluating DeFi tracking platforms through the utility-based model. The model effectively highlights the trade-offs between accuracy and responsiveness, providing a structured approach to compare platforms based on user priorities. For instance, platforms like Chainalysis and Elliptic achieved higher utility scores due to their robust compliance tools and low error rates, aligning with institutional needs. In contrast, while cost-effective and user-friendly, platforms such as DeBank and Etherscan demonstrated limitations in advanced compliance features and responsiveness, making them more suitable for individual or non-critical use cases. These findings emphasize the utility function's ability to align platform evaluation with diverse user requirements and priorities, addressing challenges highlighted by [Gudgeon et al. \(2020\)](#) and [Werner et al. \(2021\)](#) regarding risk and security management in DeFi ecosystems.

This study builds on earlier frameworks by quantitatively integrating accuracy and responsiveness into a single evaluative metric compared to the existing literature. Prior studies, such as those by [Zetsche et al. \(2020\)](#) and [Sood et al. \(2023\)](#), have examined DeFi risks but often focused independently on either compliance capabilities or usability aspects. This research addresses this gap by providing a holistic approach to evaluating platforms through user-centric and technical metrics. The decision zones illustrated in



Figure 4 validate the importance of tailoring platform features to institutional and non-institutional users, supporting the notion that user-centric design is critical for fostering platform adoption and effectiveness (Jensen & Ross, 2020; Gudgeon et al., 2020). These findings provide actionable insights for improving DeFi platform design, particularly in risk mitigation, compliance integration, and real-time usability.

### 6.2. Regulatory and Economic Implications

DeFi regulation remains a challenging task because, on the one hand, decentralized systems have enormous innovation potential, and on the other, DeFi can be used for certain illicit activities like money laundering, fraud, and terrorist financing (Benson et al., 2024). The design and operation of DeFi tracking platforms are directly affected by regulatory measures, in particular, AML and KYC requirements.

One of the most noticeable impacts of regulations is integrating compliance tools within DeFi platforms. Features such as wallet attribution, transaction monitoring, and risk scoring have become fundamental for platforms to comply with AML/KYC standards (Turksen et al., 2024). Tools like Chainalysis and Elliptic provide institutional users and regulators with sophisticated compliance mechanisms. But these features tend to come with a cost. Platforms that integrate compliance tools naturally become more complex and expensive and may alienate smaller users or non-institutional participants who do not require such rigorous compliance features.

Regulatory scrutiny has also affected user experiences, as platforms must balance accessibility with legal requirements. In jurisdictions where users may be banned or have to complete additional steps to verify their identities, there is friction in the onboarding process. An example of this is institutional investors who may like to have some compliance features that provide a level of assurance against regulatory penalties. Conversely, individual users, particularly those in regions with weaker regulatory frameworks, may find these features burdensome or intrusive, reducing their willingness to adopt these platforms.

Risk events in DeFi can have a substantial economic impact, frequently leading to cascading events that affect more than just the protocols that are directly impacted. Some of the most significant events that break the DeFi ecosystem, weaken user trust, and threaten the stability of the whole sector are hacks, liquidity crises, and smart contract exploits. Hacks are some of the most visible and damaging risk events. Attacks on smart contracts are not new—in high-profile incidents like the Poly Network hack in 2021, attackers exploited vulnerabilities in smart contract code to steal millions of dollars in digital assets (Darvishi et al., 2024). In addition to the immediate financial losses for users, these events have long-term consequences for market confidence. Due to liquidity shortages and market volatility, it is common for users to withdraw en masse funds from affected platforms. Another consequence is that it can damage the reputation of the hacked platform, which can further discourage future users and investors from using the platform, thus delaying its recovery and future growth.

Another important economic challenge in DeFi is the liquidity crisis. These crises usually happen when a lot of money is taken out of a protocol, and it cannot fulfill user demands. For example, during market recessions, over-leveraged lending protocols may struggle to liquidate collateral quickly enough to cover loans, resulting in insolvency (Irresberger et al., 2024). This issue is intensified with DeFi due to the interconnected nature of the systems, with the collapse of one protocol affecting other protocols that share liquidity pools or collateral assets. This can cause cascading failures that destabilize entire ecosystems, requiring robust liquidity management and contingency planning.

Vulnerabilities in smart contracts also have major economic consequences. DeFi differs from centralized systems, where system administrators can intervene to fix mistakes or

halt operations, as the code is immutable. Vulnerabilities exploited can result in irreversible losses (Bhajanka & Pradhan, 2023). Such events also have more than just immediate economic fallout, including decreased user trust, regulatory scrutiny, and decreased token valuations for affected protocols.

The DeFi ecosystem also faces economic risks from systemic issues, such as market manipulation and price volatility. Examples of this include flash loan attacks, which take advantage of the high levels of leverage present in DeFi to manipulate the price of a token and often cause users losses of substantial sums (Kaur et al., 2023). This highlights the need to design platforms capable of detecting and mitigating such activities in real time. The economic consequences include costs of recovery and remediation. Whenever a platform is hacked or suffers from a liquidity crisis, it spends a lot of time and resources to compensate users, audit its smart contracts, and try to rebuild trust. In certain cases, platforms will use community funding or create new tokens to cover losses at the expense of existing assets and the users (Sockin & Xiong, 2023).

Despite these challenges, the economic resilience of the DeFi sector shows its potential to adapt and grow. DeFi platforms have increasingly implemented mechanisms to counter risks, including insurance protocols, multi-signature wallets, and decentralized governance systems. These innovations protect users and make the whole DeFi ecosystem more stable.

From an economic stability point of view, a balanced approach is important to encourage innovation and maintain economic stability in the DeFi sector. Collaborative efforts between regulators, platform developers, and users create an environment where innovation and stability can coexist.

### 6.3. Use of AI and ML in DeFi Risk Management

The recent evolution of DeFi tracking platforms reveals an increasing reliance on ML and AI to identify high-risk transactions, detect suspicious wallet behaviors, and simplify compliance. While the specific methods and performance metrics may differ from platform to platform, the general thrust of these approaches involves both supervised and unsupervised learning techniques to flag anomalous on-chain activities in real time.

AI/ML has already proven to be an excellent tool for tackling some of the most urgent DeFi risk management problems (Singh et al., 2023). These technologies allow us to process and analyze the vast amounts of data from decentralized systems, analyzing patterns and anomalies that may indicate potential risk. For instance, AI-powered anomaly detection systems can detect unusual real-time transaction patterns in detecting fraud, money laundering, or market manipulation. When these tools are integrated, platforms should be able to give proactive alerts and insights, reducing the probability of financial loss and building trust in the system.

ML algorithms are constructive in improving predictive capabilities (Goriparthi, 2024). They can use historical data to predict market trends, estimate the chance of liquidity crises, and estimate the effects of new threats (Chen et al., 2024). These insights allow users and platform operators to take actions, based on the insights, to prevent or mitigate the impact of volatile market conditions or technical vulnerabilities.

Supervised classification algorithms (random forests, gradient boosting machines, neural nets, etc.) are often used to label transactions as having a certain (potential) risk (Dhanawat, 2022). Trained on large datasets of historical blockchain data, these models learn what fraudulent transactions look like by using known illicit transactions as examples of fraud, market manipulation, or money laundering patterns. For example, ML-based classification methods are used by Chainalysis to score wallet addresses and transactions, and they publicly report detection accuracies as high as 90% for some well-studied fraud typologies (Agarwal et al., 2024). In parallel, Elliptic combines both classification and

anomaly detection methods (such as clustering and outlier detection via isolation forests or autoencoders) to identify suspiciously linked wallet addresses and sudden transaction spikes (Elliptic, 2024). While their published performance results are relatively high in precision (above 90% for some of the most popular blockchain platforms), they do tend to fluctuate as emerging threats, and periodic retraining of models is required in light of new patterns of illicit behavior.

Semi- and unsupervised algorithms are equally important in DeFi risk analysis when data labels are scarce or incomplete. To identify unusual groups that behave differently from normal user behavior, clustering techniques (e.g., k-means or hierarchical clustering) are employed to group addresses or transactions with similar characteristics (A. Sharma et al., 2022). Nansen admitted to using multi-dimensional clustering to identify wallet “personas”, looking for insider trading or large liquidity movements (GoogleCloud, 2024). When trained on enough labeled instances, the typical detection rate for abnormal transaction clusters exceeds 85%, but false positives are often triggered when the algorithm overfits to historical data.

While these promising results indicate that the ML methods are useful, performance can be very sensitive to blockchain throughput, data quality, and the novelty of the attack. For instance, leading compliance platforms typically report proprietary detection rates above 90% accuracy, though these numbers can vary across different chains. Furthermore, false positives, which are between 5 and 15 percent, currently remain an issue, which can decrease user confidence and increase the cost of compliance. To address this, platforms regularly retrain or fine-tune models as market volatility spikes or new attack vectors emerge.

Compliance management is another critical application of emerging technologies. Natural language processing (NLP) tools can help platforms interpret regulatory texts more easily and respond more quickly to changes in legal requirements. Moreover, with AI, blockchain forensic tools can track intricate multichain transaction flows to increase transparency and help recognize other illegitimate activities. These technologies enhance platforms’ regulatory compliance, making them more confident to institutional users and regulators. While AI-based automation and NLP methods are slowly being adopted for compliance tasks such as screening smart contract updates or quickly reviewing regulatory changes, they are mostly used for transaction monitoring. However, there is little public data on these implementations. Due to this, transparent third-party audits and open-source benchmarking are still limited, and it is difficult to compare detection rates across platforms.

We can conclude that AI and ML techniques have clear promise to improve DeFi risk management by speeding up detection, increasing the accuracy of illicit activity flags, and reducing manual workload. However, these methods still face challenges in DeFi risk management, such as limited labeled data for emerging threats, the high cost of continuous training, and a continuing issue of false positives.

#### 6.4. Study Contributions

This study presents a user-adaptive framework that integrates technical risk indicators (e.g., error rates, responsiveness metrics) with behavioral and contextual factors (e.g., user trust, platform adoption barriers). By unifying these dimensions, we address a key research gap: the existing work tends to either only address technical vulnerabilities or deal with DeFi risks in general. Additionally, our utility-based model provides a quantitative way to represent the tradeoffs between accuracy and responsiveness, and it can be tailored to suit a wide range of priority users. This framework also enables future scholarship by enabling a structured approach to compare, evaluate, and improve DeFi tracking platforms under different risk profiles and regulatory regimes.

From a practical point of view, our results provide guidelines for developers, institutional stakeholders, and individual users. Affordability and usability are best suited to smaller-scale or retail-focused contexts, while platforms with robust compliance mechanisms and sophisticated analytics are clearly suited to institutional investors and heavily regulated markets, but at a higher cost. Through this exposition of these divergences, we provide a decision-making tool to stakeholders to choose platforms that match their risk appetite, compliance needs, and budget constraints. Moreover, the results stress the need for platform enhancement strategies from multiple dimensions, urging developers to adopt a mix of advanced analytics as well as user-centric design and to embrace emerging technologies like AI and ML while keeping it cost-effective. Collectively, these insights lead to a safer, more transparent DeFi environment that can support an expanding and more diverse user base.

## 7. Conclusions and Future Directions

This research offers a detailed examination of risk management practices in the DeFi ecosystem evaluated against the effectiveness of tracking platforms, user behavior, and the broader implications, including risks and regulation. The results provide important input into both academic and practical discussions, including strengths and limitations of existing DeFi tools and actionable recommendations for stakeholders.

We analyzed six leading DeFi tracking platforms (Chainalysis, Elliptic, Nansen, Dune Analytics, DeBank, Etherscan) to understand their strengths and limitations in risk management. Using a mixed-methods approach that included a quantitative survey, qualitative interviews, and a utility-based model to evaluate accuracy and responsiveness, we discovered that platforms differ greatly in their suitability for different user groups. Platforms with solid compliance tools, such as Chainalysis and Elliptic, excel in addressing regulatory challenges but are often inaccessible to smaller users due to high costs. On the other hand, platforms such as DeBank and Etherscan focus on making products more user-friendly and cost-effective, but they do not include sophisticated analytics and compliance features, hindering their effectiveness for institutional users.

Transparent data presentation, real-time monitoring, and regulatory compliance are the most important features for building trust with users. Trust factors, such as transparency, accuracy of data, and compliance with regulations, were decisive in customers' choices. Platforms that provide real-time monitoring and customizable analytics are more likely to build user confidence and foster adoption. However, technical complexity, lack of multi-chain support, and high costs remain obstacles to broader engagement, including non-technical and smaller-scale users.

### *Limitations and Future Directions*

The mixed-methods approach captured a broad range of insights, but several constraints merit attention. First, the scope of analysis was restricted to six DeFi tracking platforms that are widely used but might not capture the entire breadth of tools in the fast-growing DeFi space. Second, we used voluntary survey responses and interviews from participants who had already engaged with DeFi, which could introduce self-selection bias. Third, performance data and user perceptions may change over time as platforms add new features or market conditions evolve, so the results may not reflect new or improved features. Finally, though our utility-based model balances accuracy and responsiveness, other metrics (user experience, multi-chain interoperability, regulatory compliance costs, etc.) could be added to the platform evaluation.

While this study presents valuable user insights, there are a few areas for future research to advance risk management in the DeFi domain. We welcome future studies on

developing holistic frameworks that incorporate technological, financial, operational, and compliance risks. These frameworks should account for the interdependencies between risks and propose adaptive strategies to mitigate risks and failures across the ecosystem.

The DeFi ecosystem grows across multiple blockchains and the ability to manage risks related to cross-chain transactions is becoming increasingly important. To fully leverage the potential of DeFi technologies, platform developers must prioritize integrating AI and ML tools into their tools. Developing user-centric solutions that balance advanced functionality with intuitive design will be critical in overcoming barriers to adoption. For example, platforms can provide customizable dashboards to simplify complex analytics and customize risk management features to a user's specific needs. Developers should also focus on creating scalable solutions that adjust the growth of the DeFi ecosystem.

Regulators have a critical role in fostering the future of the DeFi industry by defining frameworks that encourage innovation, protect users from risks, and bring the industry into compliance with laws and regulations. By collaborating with platform developers and industry stakeholders on the engagement process, regulators can form a nuanced understanding of the dynamics and challenges of the DeFi ecosystem.

Regulators need to begin creating harmonized international standards of DeFi governance to tackle cross-jurisdictional challenges. This will decrease ambiguity, allowing for DeFi platform growth worldwide while maintaining global compliance consistency. Emerging technologies will also be critical to maintaining the ecosystem's integrity, especially when it comes to monitoring activities, ensuring compliance, and leveraging emerging technologies like blockchain forensics to do so.

Effective risk management in DeFi could be successful when platform developers, regulators, and users balance each other. Developers must prioritize user-centric design and strong security measures, regulators must make their frameworks clear and adaptable, and users must be proactive about their own risks. Combining these efforts will guarantee that DeFi remains a safe, resilient, and innovative alternative to traditional financial systems.

By addressing these areas, future research can contribute to building a secure and resilient DeFi sector. The findings of this study, combined with further exploration, will inform the development of more effective tools, frameworks, and policies, uncovering the full potential of the DeFi ecosystem.

**Author Contributions:** Conceptualization, B.A. and V.B.; methodology, O.A. and O.L.; validation, B.A., O.A. and V.B.; formal analysis, B.A. and O.L.; investigation, V.B. and O.A.; resources, B.A. and V.B.; data curation, O.A. and O.L.; writing—original draft preparation, B.A. and O.A.; writing—review and editing, V.B. and O.L.; visualization, O.A. and O.L.; supervision, B.A.; project administration, B.A. and V.B.; funding acquisition, V.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Innovate UK CyberASAP grant 10139989.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Informed consent was obtained from all subjects involved in the study.

**Data Availability Statement:** The data supporting this study's findings are available from the corresponding author when it is a reasonable request.

**Acknowledgments:** The fourth author sincerely acknowledges support from the British Academy and CARA (project RaR\100676). All statements and opinions expressed in this article are solely those of the authors and do not necessarily reflect the views of the funding bodies.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

- Abakah, E. J. A., Adeabah, D., Tiwari, A. K., & Abdullah, M. (2023). Effect of Russia–Ukraine war sentiment on blockchain and FinTech stocks. *International Review of Financial Analysis*, 90, 102948. [CrossRef]
- Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, 34(2), e2255. [CrossRef]
- Aju, M., & Burrell, T. (2023). *Cryptoassets consumer research 2023 (wave 4)*. Financial conduct authority, research note. Available online: <https://www.fca.org.uk/publication/research-notes/research-note-cryptoasset-consumer-research-2023-wave4.pdf> (accessed on 12 October 2024).
- Akila, V., Nitin, M. V. S., Prasanth, I., Reddy, S., & Kumar, A. (2023). A cryptocurrency price prediction model using deep learning. In *E3S web of conferences* (Vol. 391, p. 01112). EDP Sciences.
- Almakhour, M., Sliman, L., Samhat, A. E., & Mellouk, A. (2023). A formal verification approach for composite smart contracts security using FSM. *Journal of King Saud University-Computer and Information Sciences*, 35(1), 70–86. [CrossRef]
- Aquilina, M., Frost, J., & Schrimpf, A. (2024). Decentralized finance (DeFi): A functional approach. *Journal of Financial Regulation*, 10(1), 1–27. [CrossRef]
- Aramonte, S., Huang, W., & Schrimpf, A. (2021). *DeFi risks and the decentralisation illusion*. Available online: [https://www.bis.org/publ/qtrpdf/r\\_qt2112b.htm](https://www.bis.org/publ/qtrpdf/r_qt2112b.htm) (accessed on 10 October 2024).
- Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). *Digital Finance*, 6(1), 55–95. [CrossRef]
- BeInCrypto. (2022). *How liquidity provider (LP) tokens work*. Available online: <https://beincrypto.com/learn/lp-tokens/> (accessed on 12 October 2024).
- Bekemeier, F. (2023). A primer on the insurability of decentralized finance (DeFi). *Digital Finance*, 5(3), 643–687. [CrossRef]
- Bennett, D., Mekelburg, E., & Williams, T. H. (2023). BeFi meets DeFi: A behavioral finance approach to decentralized finance asset pricing. *Research in International Business and Finance*, 65, 101939. [CrossRef]
- Benson, V., Adamyk, B., Chinnaswamy, A., & Adamyk, O. (2024). Harmonising cryptocurrency regulation in Europe: Opportunities for preventing illicit transactions. *European Journal of Law and Economics*, 57, 37–61. [CrossRef]
- Benson, V., Turksen, U., & Adamyk, B. (2023). Dark side of decentralised finance: A call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, 32(1), 80–97. [CrossRef]
- Bhajanka, V., & Pradhan, N. (2023, March 10–11). *A study on smart contract security vulnerabilities*. International Conference on Advanced Computing, Machine Learning, Robotics and Internet Technologies (pp. 105–115), Silchar, India.
- Bhambhwani, S. M., & Huang, A. H. (2024). Auditing decentralized finance. *The British Accounting Review*, 56(2), 101270. [CrossRef]
- Buthelezi, E. M. (2024). Navigating global uncertainty: Examining the effect of geopolitical risks on cryptocurrency prices and volatility in a Markov-switching vector autoregressive model. *International Economic Journal*, 38(4), 564–590. [CrossRef]
- Cedra, A. (2024). Mitigating risks in decentralized finance: A Systematic review of challenges and solutions. *International Journal of Economic Perspectives*, 18(1), 104–125.
- Chatziamanetoglou, D., & Rantos, K. (2024). Cyber threat intelligence on blockchain: A systematic literature review. *Computers*, 13(3), 60. [CrossRef]
- Chen, Z., Yan, L., Wang, H., & Adamyk, B. (2024). Improved facial expression recognition algorithm based on local feature enhancement and global information association. *Electronics*, 13(14), 2813. [CrossRef]
- Cheng, J., Tiwari, S., Khaled, D., Mahendru, M., & Shahzad, U. (2024). Forecasting Bitcoin prices using artificial intelligence: Combination of ML, SARIMA, and Facebook Prophet models. *Technological Forecasting and Social Change*, 198, 122938. [CrossRef]
- Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly detection in blockchain networks using unsupervised learning: A survey. *Algorithms*, 17(5), 201. [CrossRef]
- Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, 159, 107221. [CrossRef]
- Darvishi, I., Asare, B. T., Musa, A., Yeboah-Ofori, A., Oseni, W., & Ganiyu, A. (2024, August 19–21). *Blockchain technology and vulnerability exploits on smart contracts*. 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 160–167), Vienna, Austria.
- Dhanawat, V. (2022). Anomaly detection in financial transactions using machine learning and blockchain technology. *International Journal of Business Management and Visuals*, 5(1), 34–41.
- Elliptic. (2024). *Crypto wallet screening and monitoring*. Elliptic Lens. Available online: <https://www.elliptic.co/platform/lens> (accessed on 6 January 2025).
- Feng, Z., Li, Y., & Ma, X. (2023). Blockchain-oriented approach for detecting cyber-attack transactions. *Financial Innovation*, 9(1), 81. [CrossRef]
- Ghosh, B., Kazouz, H., & Umar, Z. (2023). Do automated market makers in DeFi ecosystem exhibit time-varying connectedness during stressed events? *Journal of Risk and Financial Management*, 16(5), 259. [CrossRef]



- GoogleCloud. (2024). *Nansen: Empowering crypto investors with blockchain data intelligence driven by Google cloud*. Available online: <https://cloud.google.com/customers/nansen> (accessed on 6 January 2025).
- Goriparthi, R. G. (2024). AI-driven predictive analytics for autonomous systems: A machine learning approach. *Revista de Inteligencia Artificial en Medicina*, 15(1), 843–879.
- Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). *The decentralized financial crisis: Attacking defi*. Available online: <https://arxiv.org/abs/2002.08099> (accessed on 17 October 2024).
- Harvey, C. R., & Rabetti, D. (2024). International business and decentralized finance. *Journal of International Business Studies*, 55, 840–863. [CrossRef]
- Hägele, S. (2024). Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review. *Electronic Markets*, 34(1), 33. [CrossRef]
- He, D., Wu, R., Li, X., Chan, S., & Guizani, M. (2023). Detection of vulnerabilities of blockchain smart contracts. *IEEE Internet of Things Journal*, 10(14), 12178–12185. [CrossRef]
- Ho, A., Darbha, S., Gorelkina, Y., & Garcia, A. (2022). *The relative benefits and risks of stablecoins as a means of payment: A case study perspective*. Bank of Canada. Available online: <https://www.bankofcanada.ca/2022/12/staff-discussion-paper-2022-21/> (accessed on 17 October 2024). [CrossRef]
- IBM. (n.d.). *What is risk management?* IBM. Available online: <https://www.ibm.com/uk-en/topics/risk-management> (accessed on 17 October 2024).
- Irresberger, F., John, K., & Saleh, F. (2024). Decentralized lending. In *The elgar companion to decentralized finance, digital assets, and blockchain technologies* (pp. 35–56). Edward Elgar Publishing.
- ISO. (2021). *ISO-ISO 31000—Risk management*. Available online: <https://www.iso.org/iso-31000-risk-management.html#:~:text=ISO%2031000,%20Risk%20management%20%E2%80%93%20G> (accessed on 12 October 2024).
- Janczyk, M., & Pfister, R. (2023). Factorial analysis of variance (ANOVA). In *Understanding inferential statistics: From A for significance test to Z for confidence interval* (pp. 127–144). Springer.
- Jensen, J. R., & Ross, O. (2020, November 26). *Managing risk in DeFi*. CEUR Workshop Proceedings, Riga, Latvia. [CrossRef]
- Jensen, J. R., von Wachter, V., & Ross, O. (2021). An introduction to decentralized finance (defi). *Complex Systems Informatics and Modeling Quarterly*, 26, 46–54. [CrossRef]
- Johnson, C. (2024). Decentralized finance (DeFi): Opportunities and risks in the global financial ecosystem. *Business, Marketing, and Finance Open*, 1(2), 53–64.
- Kaur, G., Habibi Lashkari, A., Sharafaldin, I., & Habibi Lashkari, Z. (2023). Smart contracts and defi security and threats. In *Understanding cybersecurity management in decentralized finance: Challenges, strategies, and trends* (pp. 91–111). Springer International Publishing.
- Khalfaoui, R., Gozgor, G., & Goodell, J. W. (2023). Impact of Russia-Ukraine war attention on cryptocurrency: Evidence from quantile dependence analysis. *Finance Research Letters*, 52, 103365. [CrossRef]
- Kirvesoja, V. (2022). *Advantages and disadvantages of decentralized financial (DeFi) services*. Available online: <https://jyx.jyu.fi/handle/123456789/81722> (accessed on 22 October 2024).
- Koprivec, F., Kržmanc, G., Škrjanc, M., Kenda, K., & Novak, E. (2021). Screening tool for anti-money laundering supervision. In *Big data and artificial intelligence in digital finance* (pp. 233–251). Springer. [CrossRef]
- Kshetri, N. (2021). Blockchain and sustainable supply chain management in developing countries. *International Journal of Information Management*, 60, 102376. [CrossRef]
- Levi, S. D., & Lipton, A. B. (2018). *An introduction to smart contracts and their potential and inherent limitations*. Available online: <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> (accessed on 12 October 2024).
- Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi). *SSRN Electronic Journal*, 4104550, 1–67. [CrossRef]
- Milk Road. (2023). *Crypto staking rewards: Best staking platform rates 2023*. Available online: <https://milkroad.com/staking> (accessed on 12 October 2024).
- Mitchell, R. (2022). *DeFi-ing the rules: Five opportunities and five risks of decentralized finance*. CFA Institute Enterprising Investor. Available online: <https://blogs.cfainstitute.org/investor/2022/06/07/defi-ing-the-rules-five-opportunities-and-five-risks-of-decentralized-finance/> (accessed on 10 November 2024).
- Oi, R. (2023). *2022's Devastating crypto breaches: Multi-million dollar hacks shake the industry*. Fintech Singapore. Available online: <https://fintechnews.sg/69446/crypto/2022s-devastating-cryptocurrency-breaches-multi-million-dollar-hacks-shake-the-industry/> (accessed on 10 November 2024).
- Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*, 33(1), 37. [CrossRef]
- Richardson, J. (2011). Eta squared and partial eta squared as measures of effect size in educational research. *Educational Research Review*, 6(2), 135–147. [CrossRef]

- Schär, F. (2021). *Decentralized Finance: On blockchain- and smart contract-based financial markets*. Available online: <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> (accessed on 15 November 2024).
- Sharma, A., Patel, N., & Gupta, R. (2022). Enhancing customer segmentation through AI: Analyzing clustering algorithms and deep learning techniques. *European Advanced AI Journal*, 11(8), 1–23. Available online: <https://eaaij.com/index.php/eaaij/article/view/31/31>.
- Sharma, P., Jindal, R., & Borah, M. D. (2023). A review of smart contract-based platforms, applications, and challenges. *Cluster Computing*, 26(1), 395–421. [CrossRef]
- Singh, K., Hasan, M., & Rajendran, R. P. (2023). Opportunities and challenges of AI/ML in finance. In *The impact of AI innovation on financial sectors in the era of industry 5.0* (pp. 238–260). IGI Global.
- Sockin, M., & Xiong, W. (2023). Decentralization through tokenization. *The Journal of Finance*, 78(1), 247–299. [CrossRef]
- Sood, A., Sinha, S., & Garg, S. (2023). Risk analysis in decentralized finance (DeFi): A fuzzy-AHP approach. *Journal of Banking and Financial Technology*, 25, 13. [CrossRef]
- Sun, T., & Yu, W. (2020). A formal verification framework for security issues of blockchain smart contracts. *Electronics*, 9(2), 255. [CrossRef]
- Trozze, A., Kleinberg, B., & Davies, T. (2024). Detecting DeFi securities violations from token smart contract code. *Financial Innovation*, 10(1), 78. [CrossRef]
- Turksen, U., Benson, V., & Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI. *Journal of Banking Regulation*, 25, 359–377. [CrossRef]
- Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Regulatory frameworks for decentralized finance (DEFI): Challenges and opportunities. *GSC Advanced Research and Reviews*, 19(2), 116–129. [CrossRef]
- Vistra. (2022). *Decentralised finance: Understanding the benefits, risks and challenges of DeFi*. Available online: <https://www.vistra.com/insights/decentralised-finance-understanding-benefits-risks-and-challenges-defi> (accessed on 20 November 2024).
- Weingärtner, T., Fasser, F., Reis Sá da Costa, P., & Farkas, W. (2023). Deciphering DeFi: A comprehensive analysis and visualization of risks in decentralized finance. *Journal of Risk and Financial Management*, 16(10), 454. [CrossRef]
- Werner, S. M., Perez, D., & Gudgeon, L. (2021, September 23–25). SoK: *Decentralized finance (DeFi)*. 3rd ACM Conference on Advances in Financial Technologies, Vienna, Austria. [CrossRef]
- Weston, G. (2021). *Decentralized exchanges (DEX) risks that you can't ignore*. 101 blockchains. Available online: <https://101blockchains.com/decentralized-exchanges-risks/> (accessed on 15 November 2024).
- Weston, G. (2022). *DeFi insurance—Simply explained*. 101 blockchains. Available online: <https://101blockchains.com/defi-insurance/> (accessed on 10 November 2024).
- Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: New challenges for compliance. *Journal of Financial Crime*, 30(1), 97–113. [CrossRef]
- Wu, J., Liu, J., Zhao, Y., & Zheng, Z. (2021). Analysis of cryptocurrency transactions from a network perspective: An overview. *Journal of Network and Computer Applications*, 190, 103139. [CrossRef]
- www.coso.org. (2023). *Guidance on enterprise risk management*. Available online: <https://www.coso.org/guidance-erm> (accessed on 17 November 2024).
- Xiong, X., Wang, Z., Cui, T., Knottenbelt, W., & Huth, M. (2023). Market misconduct in decentralized finance (DeFi): Analysis, regulatory challenges and policy implications. *arXiv*, arXiv:2311.17715.
- Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, 6(2), 172–203. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.