BEHAVIOR-CENTRIC MULTICLASS DETECTION OF FRAUD AND PHISHING IN ETHEREUM-BASED DEFI TRANSACTIONS USING DEEP TABULAR LEARNING

Ava Ameri

A THESIS SUBMITTED TO
THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF ARTS
IN INFORMATION SYSTEMS & TECHNOLOGY

YORK UNIVERSITY
TORONTO, ONTARIO

May 2026

Acknowledgement

I would like to express my deepest gratitude to my supervisor, Prof. Arash Habibi Lashkari, for his invaluable guidance, support, patience, and encouragement throughout this journey. I am deeply thankful to my family, especially my mother and brother, for their unwavering love, support, and encouragement. I also dedicate this work to the loving memory of my father, whose presence, values, and inspiration remain with me always.

Abstract

Decentralized Finance (DeFi) introduces security risks because its open, permissionless, and pseudonymous design enables fraud and phishing. This thesis first analyzes 284 DeFi platforms to identify common architectural and functional characteristics, including governance, interoperability, lending, staking, and security features. Building on this ecosystem analysis, it develops a behavior-centric multiclass detection framework for Ethereum transaction data that distinguishes legitimate, fraud, and phishing activities within a shared feature space. The framework harmonizes phishing and fraud datasets through feature alignment and preprocessing, then evaluates Logistic Regression, Support Vector Machine, Random Forest, TabNet, GANDALF, and NODE under identical conditions. Results show that deep tabular models outperform traditional baselines, with NODE achieving the strongest overall performance, particularly for minority malicious classes. Feature importance analysis identifies gas usage, nonce behavior, transaction frequency, and wallet activity as key indicators. The findings support scalable, behavior-based DeFi threat detection.

Contents

List of Tables

List of Figures

1 Introduction

Decentralized Finance (DeFi) has become one of the most significant applications of blockchain technology, offering financial services such as trading, lending, borrowing, staking, yield generation, and asset management without relying on traditional centralized intermediaries. Through smart contracts and public blockchain infrastructure, DeFi enables open participation, transparent execution, and direct user control over digital assets. However, the same characteristics that make DeFi attractive also introduce serious security challenges. Its permissionless, pseudonymous, and highly automated nature allows malicious actors to exploit users, protocols, and transaction mechanisms through fraud, phishing, and other forms of abuse.

As the DeFi ecosystem continues to expand, its structure has become increasingly complex. Platforms differ in their economic models, governance mechanisms, revenue structures, cross-chain capabilities, and security features. This diversity makes it difficult to compare platforms systematically or understand how architectural choices may influence functionality and risk exposure. At the same time, malicious activities in DeFi often emerge through repeated behavioral patterns rather than isolated events. These patterns may involve transaction frequency, gas usage, nonce behavior, wallet activity, token interactions, and repeated account-level actions. Therefore, effective DeFi security analysis requires both an ecosystem-level understanding of platform design and a data-driven approach for detecting malicious transaction behavior.

To address these needs, this thesis first conducts a large-scale comparative study of 284 DeFi platforms. The platforms are organized into major operational categories and evaluated using a unified set of functional criteria. This analysis provides a structured view of the DeFi ecosystem and highlights how different platform designs support functionality, interoperability, governance, and risk management.

Building on this study, the thesis proposes a behavior-centric multiclass machine learning framework for detecting Ethereum-based DeFi attacks. Instead of treating fraud and phishing as separate binary classification tasks, the proposed framework integrates legitimate, fraud, and phishing transaction records into a unified three-class classification problem. This formulation better reflects real-world DeFi environments, where multiple malicious behaviors may coexist and must be distinguished from both benign activity and one another.

The proposed framework evaluates both conventional machine learning models and deep tabular learning architectures. Logistic Regression, Support Vector Machine (SVM), and Random Forest are used as baseline models, while TabNet, GANDALF, and NODE are used to examine the effectiveness of advanced tabular learning methods. In this thesis, TabNet is considered an attentive and interpretable deep learning architecture for tabular data. GANDALF refers to the Gated Adaptive Network for Deep Automated Learning of Features, and NODE refers to Neural Oblivious Decision Ensembles. The models are compared using accuracy, balanced accuracy, macro-averaged precision, macro-averaged recall, macro F1-score, confusion matrices, and feature importance analysis.

The results show that deep tabular models provide stronger and more balanced performance than conventional baselines, with NODE achieving the best overall results. Feature importance analysis further shows that gas usage, nonce-related statistics, and transaction frequency are among the most important behavioral indicators for distinguishing legitimate, fraud, and phishing transactions. Overall, this thesis contributes both

an ecosystem-level understanding of DeFi platform functionality and a practical machine learning framework for automated DeFi threat detection.

2 Literature Review

Qin *et al.* [1] trace the origins of centralized financial systems to early institution-based forms of exchange in which trusted authorities governed monetary transactions, custody, and enforcement. They describe Centralized Finance (CeFi) as a layered financial ecosystem in which intermediaries manage asset custody, transaction execution, and compliance, while users typically interact only with the service layer and remain detached from the underlying institutional and operational mechanisms. Building on this perspective, Kim *et al.* [2] situate CeFi within a broader macroeconomic context and emphasize that centralized financial systems play a fundamental role in capital allocation, economic coordination, and institutional stability.

Wieandt *et al.* [3] and Smith *et al.* [4] further argue that CeFi depends on trusted intermediaries, legal enforcement, and regulatory oversight. In such systems, trust is institutional rather than computational, and security is maintained largely through centralized governance, auditing, consumer-protection frameworks, and accountability mechanisms. These characteristics distinguish CeFi from decentralized financial models, in which many of these functions are shifted away from institutions and toward protocol rules and distributed verification.

The emergence of blockchain introduced the technical foundation for this shift. Wüst and Gervais [5] distinguish between permissionless blockchains, such as Bitcoin and Ethereum, and permissioned systems, such as Hyperledger and Corda, and compare these architectures with conventional centralized databases. Their analysis highlights trade-offs involving transparency, public verifiability, privacy, integrity, and performance. They argue that blockchain architectures are most appropriate in multi-party settings where participants do not fully trust one another and no universally trusted administrator exists. Their decision methodology, summarized in Figure 1, provides a structured basis for determining when blockchain is a justified technical solution.

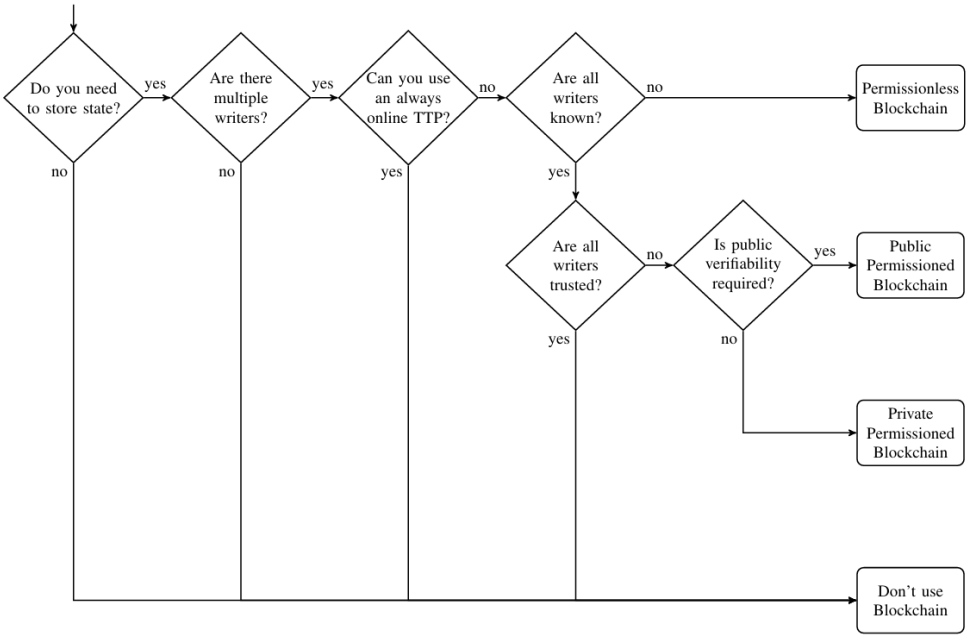


Figure 1: Decision flowchart for assessing whether blockchain is an appropriate technical solution.

Within this context, Wieandt *et al.* [3] define Decentralized Finance (DeFi) as the provision of financial services through automated blockchain-based protocols without centralized intermediaries. They identify transparency, openness, and user sovereignty as central properties of DeFi systems. These properties allow participants to inspect protocol logic, retain direct control over assets, and access financial services without depending on custodial institutions. However, they also imply that responsibility for correct interaction and asset security shifts more directly to protocol design and end users.

Qin *et al.* [1] also emphasize that the boundary between CeFi and DeFi is not always binary. They propose a structured framework for differentiating CeFi, DeFi, and hybrid services based on custody, censorship potential, and the degree of control centralization. Their framework formalizes decentralization as a multi-dimensional concept rather than a simple binary property. The decision process shown in Figure 2 therefore provides a useful conceptual basis for understanding how architectural differences translate into different operational assumptions, trust models, and threat surfaces.

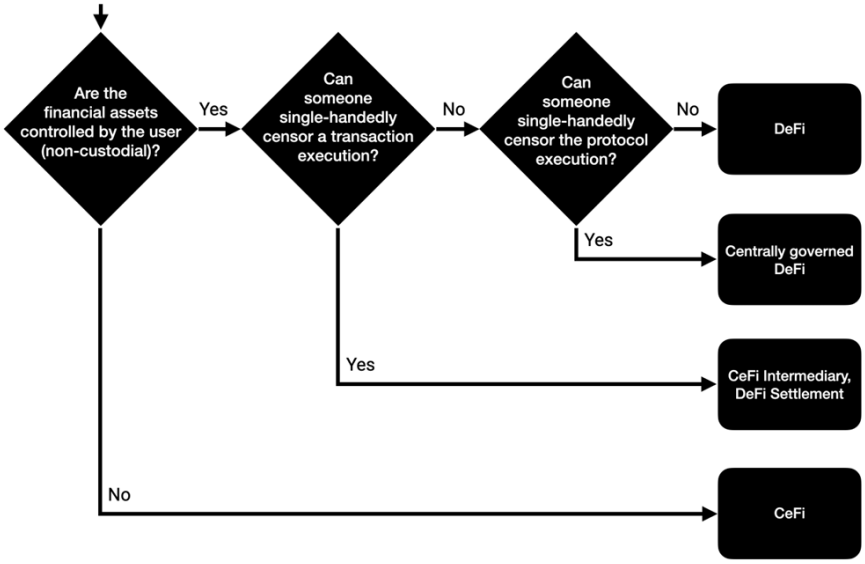


Figure 2: Decision process for classifying CeFi, DeFi, and hybrid services.

2.1 Comparison of CeFi and DeFi

The comparison between CeFi and DeFi reveals fundamental differences in intermediation, execution logic, transparency, and user responsibility. In CeFi, financial services are delivered through centralized institutions that manage custody, enforce rules, and mediate transactions. In DeFi, many of these functions are encoded into smart contracts and executed on distributed blockchain networks, thereby reducing reliance on intermediaries while increasing dependence on protocol correctness and user behavior.

John *et al.* [6] describe the Protocol for Loanable Funds (PLF) as a foundational DeFi primitive for decentralized lending and borrowing. In such systems, rules for collateralization, liquidation, and interest accrual are encoded directly into smart contracts and executed deterministically on-chain. This structure enables permissionless participation and composability across services, but it also transfers operational responsibility

from institutions to protocols and users. Son *et al.* [7] further examine the relationship between PLF-based lending and traditional bank-based lending, showing that DeFi can operate as an alternative mechanism of capital intermediation rather than merely a technological extension of existing finance.

Another important distinction lies in how transaction costs and execution priorities are handled. Johnson *et al.* [8] and Martin *et al.* [9] note that CeFi users typically experience transaction fees indirectly through institutional service structures, whereas DeFi users must pay explicit network fees that influence transaction inclusion and execution timing. These fees play a crucial role in allocating network resources and constraining spam, meaning that transaction processing in DeFi is shaped by protocol-level economic mechanisms that are largely abstracted away in CeFi.

Lashkari *et al.* [10] and Lopez *et al.* [11] also emphasize differences in control and execution semantics. DeFi systems generally provide transaction atomicity, such that operations are either executed fully or reverted entirely. By contrast, CeFi systems often involve intermediary-managed workflows, asynchronous settlement, or institution-dependent reconciliation processes. Similarly, CeFi users typically surrender direct asset control to custodial institutions, whereas DeFi depends on user-managed wallets and private keys. This shift from custodial trust to self-custody substantially changes both the operational model and the security burden placed on participants.

Transparency represents another major point of contrast. HajiHosseinKhani *et al.* [12] explain that DeFi transparency is reinforced by the public availability of smart-contract code and transaction histories, which enables independent inspection and verification. In CeFi, by contrast, transparency is generally mediated through audits, disclosures, and institutional reporting. HajiHosseinKhani *et al.* [13] further note that DeFi's permissionless and peer-to-peer architecture allows systems to operate continuously without institutional time constraints, unlike conventional financial infrastructures that remain tied to organizational workflows and regulated operating schedules.

These structural differences can also be understood through a broader theory of financial intermediation. Jakab and Kumhof [14] examine whether banks primarily act as money brokers or as creators of credit, thereby clarifying the conceptual distance between centralized balance-sheet-based finance and protocol-driven liquidity allocation. As blockchain-based systems mature, DeFi increasingly reproduces and extends conventional financial functions through automation, transparency, and composability. At the same time, this transition expands the attack surface by exposing users more directly to technical risks, interface manipulation, and protocol misuse.

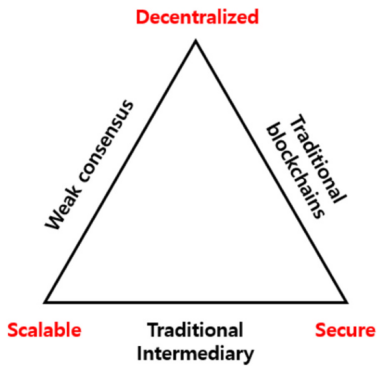


Figure 3: Conceptual trade-off among key blockchain system objectives.

In summary, CeFi and DeFi differ not only in technical implementation but also in the distribution of trust, accountability, and operational risk. CeFi concentrates responsibility within institutions, whereas DeFi re-distributes it across protocols, networks, and users. This shift is central to understanding why security challenges in DeFi often emerge in forms that differ substantially from those in traditional finance.

2.2 Phishing Scams on Ethereum Networks

Phishing scams on Ethereum networks have received significant attention because blockchain ecosystems are open, permissionless, and highly dependent on direct user interaction. Mouncey and Ciobotaru [15] show that phishing attacks have adapted to DeFi-specific interaction patterns, often exploiting user trust through malicious interfaces, deceptive links, and impersonation of legitimate platforms. Their findings indicate that phishing risk is amplified by persuasive social cues, platform engagement, and low user awareness, while participation in anti-phishing training varies across delivery formats. Figure 4 summarizes the reported likelihood of user interaction with different training types.

	Not likely	Unlikely	Neutral	Likely	Very Likely
Likelihood of interacting with Games					
N	16	15	22	15	5
Percentage (%)	21.9	20.5	30.1	20.5	6.85
Likelihood of interacting with classroom teaching					
N	16	16	14	21	6
Percentage (%)	21.9	21.9	19.2	28.8	8.22
Likelihood of interacting with own research					
N	14	12	17	18	12
Percentage (%)	19.2	16.4	23.3	24.7	16.4

Note. Total N size = 73.

Figure 4: Likelihood of interacting with different types of phishing training.

Greco *et al.* [16] examine how warning-message design influences user susceptibility to phishing by varying both the timing of warnings and the inclusion of explanatory content. Their results demonstrate that interface design choices significantly affect whether users engage in risky actions. Likewise, Zheng *et al.* [17] study phishing detection in a realistic email-filtering environment and show that experiments based on complete emails yield more reliable insight into detection behavior than simplified screenshot-based settings. Birthriya *et al.* [18] and Alkhalil *et al.* [19] further broaden this discussion by surveying spear-phishing strategies,

defense mechanisms, and lifecycle-based attack anatomy, reinforcing that phishing is best understood as a multi-stage and adaptive threat rather than an isolated event.

Emails	Condition 1	Condition 2	t	p-value
All	noExplanation_aggregate	explanation_aggregate	1.923	**.055**
	after_noExplanation	after_explanation	−0.413	.680
	before_noExplanation	before_explanation	0.342	.733
	baseline_noExplanation	baseline_explanation	2.940	**.004**
True positive	noExplanation_aggregate	explanation_aggregate	1.352	.177
	after_noExplanation	after_explanation	−0.610	.542
	before_noExplanation	before_explanation	0.382	.702
	baseline_noExplanation	baseline_explanation	2.158	**.032**
False positive	noExplanation_aggregate	explanation_aggregate	2.817	**.005**
	after_noExplanation	after_explanation	0.462	.645
	before_noExplanation	before_explanation	0.195	.846
	baseline_noExplanation	baseline_explanation	3.725	**.000**

Figure 5: Pairwise comparison between warning-message experimental conditions with and without explanation.

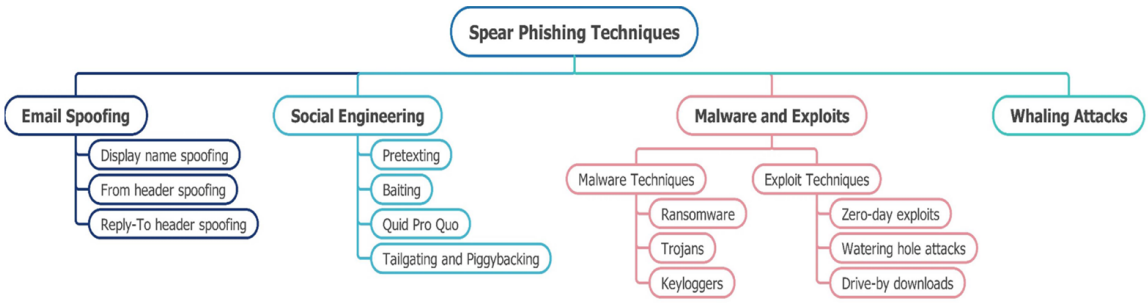


Figure 6: Classification of spear-phishing techniques.

Against this background, phishing in DeFi is particularly dangerous because users interact directly with wallets, smart contracts, and web interfaces without the protective mediation typically present in centralized systems. As a result, the consequences of social engineering, interface spoofing, and deceptive transaction prompts are often immediate and irreversible.

Phishing detection on Ethereum has evolved from classical graph-based learning to more advanced temporal, behavioral, and multi-source deep-learning frameworks. A central theme across this literature is that phishing activity is not adequately characterized by isolated wallet statistics alone. Instead, researchers increasingly model phishing through transaction topology, temporal dynamics, behavioral sequences, and, more recently, auxiliary off-chain information.

Yuan *et al.* [20] formulate Ethereum phishing detection as a node-classification problem on a transaction graph constructed from labeled phishing accounts and historical transaction records. Their framework proceeds in three main stages. First, they construct a directed transaction network from on-chain interactions. Second, they learn address representations using node2vec so that local structural properties and neighborhood relationships can be preserved in the embedding space. Third, they use a one-class SVM to distinguish phishing accounts from normal accounts under severe class imbalance. A major contribution of this study is its demonstration that phishing behavior is strongly reflected in graph structure rather than merely in simple transaction statistics such as time or transferred value. By modeling the networked nature of malicious activity, their method shows that structurally informed representations can improve phishing detection in Ethereum environments.

Wu *et al.* [21] extend this line of work by proposing trans2vec, a transaction-aware network embedding method specifically designed for Ethereum transaction networks. Their key insight is that conventional graph embedding methods treat edges too uniformly and therefore fail to capture the financial meaning of transactions. To address this limitation, trans2vec incorporates both transaction amount and timestamp into biased random-walk sampling. This design enables the embedding process to emphasize value-sensitive and time-sensitive relationships, both of which are important in financial crime analysis. The intuition behind this method is illustrated in Figure 7, where the transaction network representation highlights how neighborhood transitions can be guided by temporal and monetary attributes rather than by topology alone. Their results show that integrating such transaction-specific information improves phishing detection performance, especially under the heterogeneous and highly imbalanced conditions that characterize real Ethereum data.

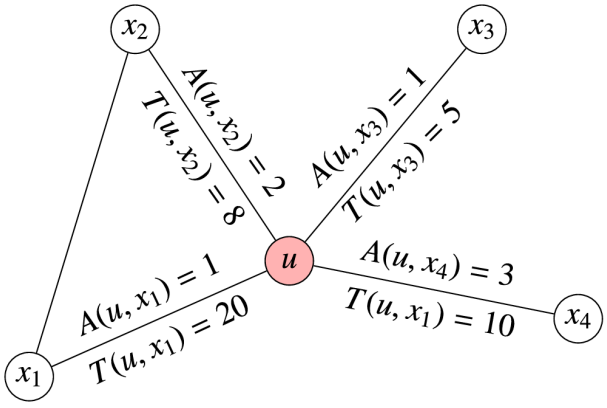


Figure 7: Illustration of an Ethereum transaction network.

Wen *et al.* [22] propose LBPS, a hybrid deep-learning architecture that combines temporal sequence modeling with learned representations from engineered account features. Their framework integrates an LSTM-FCN module, which captures time-series patterns from transaction histories, with a BP neural network that models relationships among derived transaction and state features. One of the notable aspects of their work is the construction of fixed-length time-series samples through a sliding-window strategy, which both standardizes sequential input and helps alleviate class imbalance by generating multiple training samples from phishing accounts. The overall architecture of LBPS is shown in Figure 8, where the interaction between sequential modeling and feature-based learning is clearly illustrated. In addition, the feature categories used in the model are summarized in Table 1, which describes the transaction, state, and transfer attributes extracted from the EPS dataset. This study is important because it shows that phishing behavior may be captured not only through graph connectivity but also through temporal evolution and feature interactions within wallet activity.

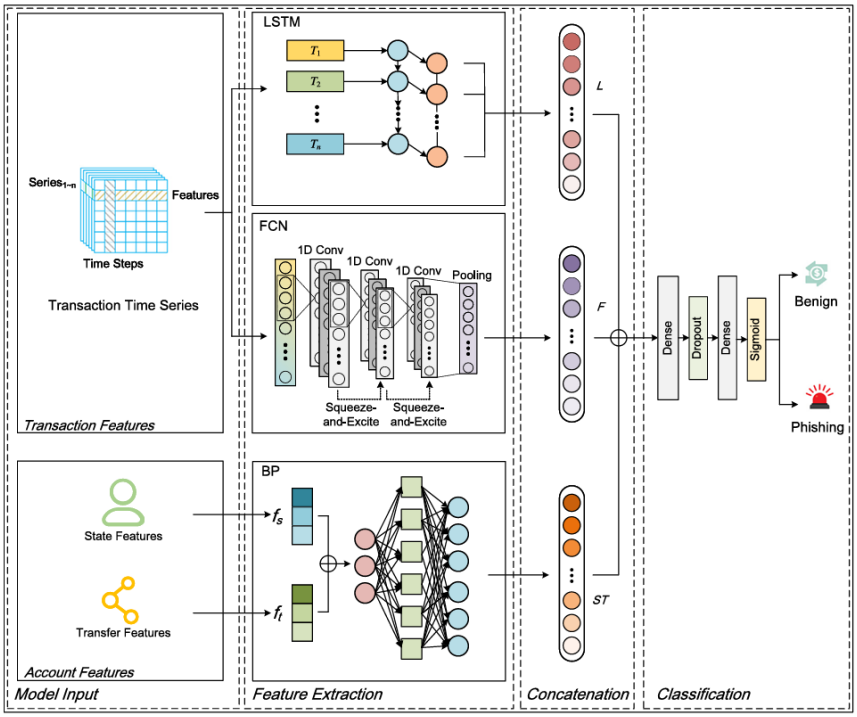


Figure 8: The structure of proposed LBPS model.

Category	Name
Transaction Features	Timestamp of transaction Ether amount of transaction Transfer direction of transaction Gas price ratio of transaction
State Features	Balance of account Number of transactions involved Ether amount received Ether amount sent Ratio of Ether received to Ether sent
Transfer Features	Number of transactions out Number of transactions in Ratio of the number of transactions in to the number of transactions out Mean of Ether in transactions in Mean of Ether in transactions out Ratio of average Ether in transactions in to the average Ether in transactions out

Table 1: Description of features in EPS-dataset.

Li *et al.* [23] propose TA-Struc2Vec, a graph-learning approach designed to capture both structural homogeneity and transaction-amount homogeneity in financial transaction networks. Their work builds on the observation that malicious actors may display similar relational behavior even when they are not directly adjacent in the graph. By extending structural-similarity-based embedding with transaction-value information, their method allows nodes with comparable financial behavior to be mapped closer together in the representation space. This is particularly useful in fraud analysis, where attackers may operate independently while still exhibiting similar behavioral structures. After learning the embeddings, Li *et al.* apply standard classifiers such as SVM and logistic regression for fraud detection. Their results suggest that structure-aware and amount-aware representations can better capture latent fraud patterns than purely topological embeddings.

Wang *et al.* [24] address a limitation of many earlier methods by modeling time as a continuous signal rather than as a set of discretized snapshots. They propose PDTGA, a temporal graph attention network for phishing detection in Ethereum transaction graphs. Their method jointly models node features, edge features, temporal encodings, and evolving neighborhood interactions using an attention mechanism inspired by Temporal Graph Attention Networks (TGAT). A major contribution of this work is its recognition that phishing activity often exhibits short-lived and bursty temporal behavior, which may be obscured when time is handled too coarsely. By incorporating temporal proximity directly into the attention process, PDTGA provides a more expressive framework for distinguishing suspicious accounts based on how and when they interact with the network.

Farrugia *et al.* [25] demonstrate that strong phishing and illicit-account detection can also be achieved through carefully designed account-level behavioral features, without requiring explicit graph representation learning. They compile a labeled Ethereum dataset containing illicit and normal accounts and train XGBoost classifiers on transaction-history-derived features. Their analysis shows that a relatively small set of variables, including activity duration, balance-related measures, and received-value characteristics, contributes strongly to classification performance. This work is important because it shows that aggregate behavioral summaries can still be highly predictive in Ethereum fraud detection, particularly when feature engineering is carefully aligned with financially meaningful account activity.

Kumar *et al.* [26] similarly investigate abnormal-account detection using classical machine-learning algorithms based on extracted behavioral features. Their work frames phishing detection as a binary classification problem and explores how wallet behavior can be transformed into predictive features for downstream modeling. Although such approaches are less structurally expressive than graph-based methods, they remain important because they provide simpler baselines and more interpretable decision paths. Their study reinforces the broader conclusion that phishing accounts often exhibit measurable deviations in transactional behavior that can be captured even with relatively conventional classifiers.

Gunathilaka *et al.* [27] introduce DeFiTrust, a more recent framework that moves beyond purely on-chain information by combining transaction events with off-chain social-media signals. Their approach derives temporal features from ERC-20 event logs and fuses them with sentiment embeddings extracted from token-related online content. The resulting representation is then passed to a neural classifier for malicious-token detection. A particularly important contribution of this work is its emphasis on explainability. The authors employ Integrated Gradients to identify which transaction-derived and sentiment-derived features contribute most strongly to the model's decisions. The overall design of the framework is shown in Figure 9, which visually summarizes the two-stream architecture and the fusion process between on-chain and off-chain signals. This study is especially relevant because it reflects a growing trend in fraud detection toward multi-source evidence integration and greater interpretability.

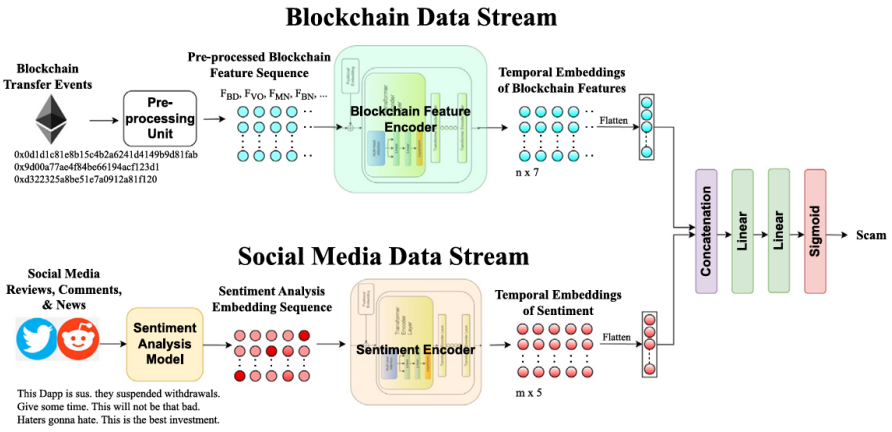


Figure 9: Overview of the DeFiTrust framework.

Overall, the phishing-detection literature on Ethereum shows a clear progression from topology-based representation learning toward richer frameworks that integrate temporal dynamics, behavioral structure, feature engineering, and external contextual signals. Earlier graph-based methods demonstrate that phishing is embedded in the relational structure of transaction networks, while later temporal and hybrid models show that the timing, sequence, and context of interactions are equally important. Despite these advances, persistent challenges remain, including severe class imbalance, incomplete ground-truth labels, and the adaptive behavior of adversaries. These challenges continue to limit the robustness and generalizability of phishing-detection systems in real-world decentralized environments.

2.3 Fraud Scams in CeFi and DeFi

Fraud detection in financial systems has evolved differently in centralized and decentralized settings because the underlying operational assumptions are fundamentally different. In CeFi, financial institutions have historically relied on their access to customer records, transaction histories, and internal compliance systems to detect suspicious activity. This environment supports strong visibility and centralized control, but it also makes fraud prevention highly dependent on institutional infrastructure and predefined monitoring rules.

Smith *et al.* [4] explain that early fraud-detection systems in CeFi were dominated by threshold-based checks and hand-crafted rules. These systems were effective for identifying well-known fraud signatures, such as unusually large transactions or obvious deviations from expected account behavior. However, their rule-driven nature also made them brittle when attackers changed tactics or when normal user behavior evolved over time. Their discussion is important because it highlights the limitations of static fraud rules in dynamic financial environments.

Johnson *et al.* [8] describe the transition from traditional rule-based monitoring toward machine-learning-driven fraud-detection pipelines. Their work emphasizes that modern fraud-detection systems increasingly rely on high-volume transactional and behavioral data to support real-time risk scoring, continuous monitoring, and automated alert generation. Rather than depending solely on predefined rules, these systems learn statistical patterns from historical data and can therefore adapt more effectively to emerging fraud behaviors. This shift marks a major transformation in CeFi fraud detection, from deterministic screening toward

data-driven predictive modeling.

Lopez *et al.* [11] further discuss the role of Neural Networks (NNs) and Deep Learning (DL) in modern financial fraud detection. They argue that these methods are well suited for modeling non-linear dependencies, high-order feature interactions, and subtle behavioral variations that conventional rule-based systems may miss. Their analysis suggests that AI-driven approaches can improve the detection of complex fraud scenarios, including coordinated abuse, identity theft, and laundering-related activity. At the same time, their discussion implies that increasing model complexity also introduces practical concerns related to interpretability, model validation, and deployment reliability.

Kim *et al.* [2] add an important critical perspective by noting that the use of AI in fraud detection, while promising, also raises concerns about bias, fairness, privacy, and regulatory accountability. Their work highlights that improved predictive performance does not automatically translate into trustworthy deployment. In centralized financial systems, where automated decisions may affect customers directly, the quality of fraud detection must be considered alongside explainability, compliance, and responsible governance. This observation is particularly relevant when comparing CeFi with DeFi, since both environments face fraud risks but differ substantially in the institutional mechanisms available to manage them.

In DeFi, fraud detection becomes more complex because activity unfolds in an open, pseudo-anonymous, and highly composable environment. Unlike CeFi, where transactions are mediated by institutions, DeFi transactions are executed through wallets, smart contracts, and decentralized protocols. As a result, fraud can emerge not only from suspicious user behavior but also from vulnerabilities in contract logic, exploitative transaction sequences, and manipulative protocol interactions.

Chen *et al.* [28] show that smart-contract vulnerabilities remain a major source of financial loss in DeFi. Their work motivates fraud-detection approaches that move beyond simple code inspection and instead reason about semantics, execution behavior, and the structural properties of smart contracts. This is important because many DeFi fraud incidents are rooted in technical weaknesses that can be exploited at scale once contracts are deployed.

Hu *et al.* [29] demonstrate that large-scale pretrained models can be adapted for Ethereum fraud detection. By applying transformer-based representation learning to blockchain data, their work reflects a broader shift toward learned feature extraction rather than purely manual engineering. This direction is especially valuable in DeFi, where the volume and heterogeneity of on-chain data make it difficult to rely only on handcrafted signals.

Jin *et al.* [30] further argue that self-supervised and behavior-aware representation learning is particularly useful when labeled fraud data are limited. Their work highlights a common challenge in DeFi fraud detection: adversaries evolve quickly, while reliable labels remain scarce. Self-supervised approaches are therefore attractive because they can exploit the abundance of unlabeled blockchain interactions to learn richer representations before downstream fraud classification.

Wu *et al.* [31] show that many DeFi fraud cases arise not from isolated malicious code but from transaction sequences and protocol-level economic manipulations. Their work is especially important because it expands the scope of fraud detection beyond individual contracts or wallets and toward multi-step exploit behavior. Taken together, these studies make clear that DeFi fraud detection requires methods capable of reasoning

across multiple layers of evidence, including code, transaction flow, user behavior, and protocol interaction.

2.4 DeFi Transaction Lifecycle

DeFi transactions follow a structured lifecycle that typically includes creation, verification, mining, and confirmation [32, 33, 34]. Although this lifecycle provides transparency and auditability, each stage also introduces distinct security considerations that influence how fraud can emerge and how detection systems should be designed.

Al-E'mari *et al.* [32] provide an important foundation for studying DeFi transactions by introducing labeled transaction data that can be used for empirical analysis. Their work supports the view that realistic fraud detection requires datasets reflecting actual transaction flow, rather than idealized or heavily simplified examples. This is particularly valuable for lifecycle-based analysis because it allows researchers to study how malicious behavior appears at different stages of execution.

John *et al.* [33] examine the economic foundations of Ethereum and explain how fees, incentives, and inclusion priority influence transaction behavior. Their discussion is relevant to the transaction lifecycle because many adversarial strategies exploit precisely these economic mechanisms. For example, gas pricing and competition for block inclusion can affect the timing and sequencing of fraudulent actions. Their work therefore helps situate DeFi fraud not only as a technical phenomenon but also as an economically driven one.

Imran *et al.* [34] discuss consensus mechanisms and scalability constraints in blockchain systems. Their analysis shows that throughput limitations, resource competition, and consensus design all shape how transactions move from initiation to confirmation. This is important because real-time fraud detection must operate within these same constraints. Detection systems cannot be designed independently of the network conditions under which suspicious transactions occur.

In the creation phase, users initiate transactions through wallets or decentralized applications by specifying recipient addresses, gas fees, and transfer amounts [32, 35]. Luo *et al.* [35] emphasize that fraud patterns may vary across project lifecycle stages, which implies that monitoring should begin as early as the transaction creation stage. After a transaction is signed, it is broadcast to the network, preserving cryptographic integrity and authenticating the sender [36, 33, 37]. Hoch *et al.* [36] frame DeFi as an ecosystem of strategic interactions shaped by incentives, while Tjäder and Ulrich [37] point out that user-side responsibility and governance ambiguity can increase exposure to fraud even when protocol logic is formally specified.

During the **verification** phase, peer nodes check whether the transaction is valid by confirming signatures, balances, and structural correctness [38, 36]. Salah *et al.* [38] note that the open and composable nature of DeFi increases both innovation and risk, which means that basic validation is not sufficient to prevent sophisticated malicious behavior. Once verified, transactions enter the mempool and await prioritization, typically influenced by gas fees.

In the mining or block-inclusion phase, transactions are incorporated into blocks through the network's consensus mechanism. Imran *et al.* [34] and Jia *et al.* [39] discuss the differences between Proof-of-Work and Proof-of-Stake systems and show how these differences influence transaction processing. Kaplan *et al.* [40] and Turillazzi *et al.* [41] explain that once a block is propagated and accepted across the network,

transactions reach the confirmation stage. At this point, they become part of the blockchain record. Although this process improves transparency and auditability, it does not eliminate fraud risk. Instead, it relocates many risks to user interaction, wallet behavior, protocol composition, and transaction semantics.

Overall, the DeFi transaction lifecycle provides a useful conceptual structure for understanding where fraud can emerge and how detection systems may intervene. Rather than viewing fraud as a single event, lifecycle-oriented analysis highlights that risk can arise during user initiation, network validation, economic prioritization, or final execution. This perspective is particularly useful for designing transaction-level detection systems that aim to identify suspicious behavior before losses are fully realized.

2.5 DeFi Transaction Security

Research on DeFi transaction security can be organized according to the level at which fraud evidence is analyzed: smart-contract level, transaction level, and multi-level. This organization is useful because fraud in DeFi does not arise from a single source. Instead, it may originate in contract logic, transaction behavior, protocol composition, or interactions across these layers.

2.5.1 Smart-Contract Level

At the smart-contract level, some studies focus on direct fraud or vulnerability detection from deployed code, while others provide broader systematic analyses of attack surfaces and security failures.

Trozze *et al.* [42] investigate securities-related fraud in DeFi by analyzing smart-contract opcode features. They train a Random Forest classifier to distinguish projects that may be involved in securities violations from those that are not. Their work is important because it demonstrates that low-level code characteristics can provide signals relevant to higher-level regulatory and fraud-related concerns. Rather than treating smart contracts purely as software artifacts, they show that contract structure can also be examined through a compliance and fraud-detection lens.

Ren *et al.* [43] propose LookAhead, a transformer-based architecture designed to detect malicious patterns in vulnerable DeFi contracts. Their approach leverages large contract datasets and combines multiple classifiers and meta-classifiers to improve detection robustness. A key contribution of this work is its attempt to model deeper structural and semantic cues in smart-contract logic, rather than relying solely on shallow handcrafted features. This makes the method particularly relevant for sophisticated attacks that cannot be identified through simple pattern matching.

Gan *et al.* [44] introduce DeFiAligner, which combines symbolic execution and LLM-based reasoning to detect semantic mismatches between project documentation and deployed smart contracts. This perspective is valuable because fraud in DeFi may stem not only from code-level vulnerabilities but also from discrepancies between claimed protocol behavior and actual implementation. By checking whether contract execution semantics align with documentation, their framework expands fraud analysis into the domain of semantic inconsistency and deceptive project representation.

Chen *et al.* [45] propose FlashSyn, an automated framework for synthesizing and validating candidate flash-loan attacks in a forked blockchain environment. Instead of relying on labeled attack data, FlashSyn systematically generates possible exploit sequences using approximation and interpolation techniques. This

work is important because it illustrates the value of counterexample-driven attack discovery. In DeFi settings, where exploit opportunities may arise from protocol composition and unforeseen interactions, automated synthesis provides a practical method for surfacing vulnerabilities before attackers exploit them.

Sun *et al.* [46] provide a broader systematic analysis through their Rug Pull Analysis Framework (RPAF). Their work includes a literature review, a reconstructed dataset, an evaluation of detection tools, and, most importantly, a taxonomy of 34 root causes of rug pulls. This taxonomy is referenced in Table 2, which provides a structured overview of the different drivers behind rug-pull attacks. The table is useful because it organizes the causes of rug pulls into a form that can support both analysis and future detection design. Rather than viewing rug pulls as a single type of event, the taxonomy highlights the diversity of conditions and mechanisms that can lead to this class of fraud.

Categories	Type	Root Cause	Scholar Paper (SL)	Grey Literature (GL)	Losses
Simple Rug Rull	LP Drain	—	SL- [2], SL- [1], SL- [3]	GL- [16], GL- [17], GL- [18], GL- [19], GL- [20], GL- [21], GL [22], GL- [23], GL- [24], GL- [25], GL- [26], GL- [27], GL- [28], GL- [29], GL- [30], GL- [31]	$5,223,217
Sell Rug Pull	Token Distribution	—	SL- [7], SL- [1], SL- [8]	GL- [22], GL- [30]	$60,587,545
SC Trap Doors	Token Generation	Mint	SL- [32], SL- [13], SL- [1]	GL- [33], GL- [34], GL- [35]	$19,465,791
		Hidden Mint	SL- [4], SL- [8]	GL- [36]	
	Destroy Token	—	SL- [32]	GL- [34]	
		Burn*	—	GL- [35]	
	Transaction Limitation	Transfer Block	SL- [32], SL- [4], SL- [1], SL- [5]	GL- [33], GL- [37]	$127,500
		Trading Cooldown	SL- [32]	GL- [37]	
		Sale-Restrict	SL- [13], SL- [2], SL- [5], SL- [38], SL- [39]	GL- [36], GL- [40], GL- [16], GL- [17], GL- [19], GL- [20], GL- [21], GL- [22], GL- [34], GL- [23], GL- [24], GL- [25], GL- [26], GL- [27], GL- [28], GL- [29], GL- [30], GL- [35]	
		Freeze Account	SL- [32]	—	
		Transaction Number or Amount Limitation	SL- [39]	GL- [36], GL- [33], GL- [37]	
		Whitelist	SL- [7], SL- [39]	GL- [36], GL- [37]	
		Blacklist	SL- [7], SL- [39]	GL- [36], GL- [33], GL- [35], GL- [37]	
	Fee	Fee Modification	SL- [4], SL- [5], SL- [39]	GL- [36], GL- [37]	$60,000
		High Sell Fee	SL- [39]	GL- [34], GL- [35], GL- [37]	
		High Buy Fee	SL- [39]	GL- [34], GL- [35]	
		Advance-Fee	SL- [13], SL- [8]	—	
		Hidden Fee	SL- [39]	—	
	Funds Manipulation	Balance Modification	SL- [4]	GL- [36], GL- [37]	$2,015,574
		Fake Money Transfer	SL- [41]	—	
		Arbitrarily Transfer	SL- [32], SL- [8]	GL- [36], GL- [42]	
	Ownership Fraud	Fake Ownership Renounce	SL- [4], SL- [41]	GL- [36]	
		Ownership Transfer*	—	GL- [43]	
		Hidden Owner*	—	GL- [33], GL- [37]	
	Unverified Contract*	—	—	GL- [42]	$1,913,898
	External Call*	—	—	GL- [36], GL- [44], GL- [35]	$7,779,182
	Proxy	—	SL- [45]	GL- [37]	$39,686
	Vulnerability	—	SL- [1]	GL- [34], GL- [46]	$10,000
LP Manipulation	Liquidity Pool Block	—	SL- [4]	GL- [36]	
	Fake LP Lock*	—	—	GL- [47]	
	Wash-Trading	—	SL- [14], SL- [8]	—	
	Pump and Dump	—	SL- [2], SL- [14], SL- [3]	GL- [40], GL- [16], GL- [17], GL- [18], GL- [19], GL- [20], GL- [21], GL- [23], GL- [24], GL- [25], GL- [26], GL- [27], GL- [28], GL- [29]	
	Hedge	—	SL- [14]	—	
Counterfeit Token	—	—	SL- [38], SL- [8], SL- [48]	—	
Combination	—	—	SL- [14]	—	$1,742,786

Table 2: Taxonomy of rug pull root causes.

Xue *et al.* [47] review Ethereum-based DeFi fraud from a broader security perspective. They identify inherited financial risks, architectural weaknesses, and development-related vulnerabilities, and they discuss future research directions such as on-chain interception and integrated prevention mechanisms. Their work is useful because it positions smart-contract fraud within a larger ecosystem of financial and technical risk rather than treating it solely as a code-analysis problem.

Qian *et al.* [48] focus on smart-contract vulnerability detection and automated repair. Their study categorizes major attack types, analyzes representative incidents, and evaluates how existing tools perform in identifying and repairing vulnerabilities. This work is particularly relevant because robust DeFi security requires not only detecting flaws but also understanding how they can be corrected in practical settings.

Rabetti *et al.* [49] examine the role of auditing in improving trust, transparency, and security in DeFi. They emphasize the limitations of traditional auditing in environments characterized by rapid protocol evolution, cross-protocol interaction, and continuous deployment. Their discussion supports the need for more automated, AI-assisted, and continuously updated auditing practices.

2.5.2 Transaction Level

At the transaction level, the literature includes classical machine-learning methods, deep-learning methods, hybrid models, and interpretable non-learning-based frameworks. This body of work is especially important because many DeFi fraud events are visible directly in transaction behavior, even when contract code alone does not reveal obvious malicious intent.

Aziz *et al.* [50] investigate anti-money-laundering-style detection in Ethereum using machine-learning techniques under limited feature settings. Their work demonstrates that strong predictive performance can still be achieved when the selected features capture essential transactional behavior. This is important because it shows that even relatively compact transaction summaries can be effective when carefully aligned with fraud-related patterns.

In a related study, Aziz *et al.* [51] apply LightGBM to Ethereum fraud detection and show that gradient-boosted tree models remain highly competitive for structured blockchain data. Their results highlight the continuing relevance of classical tabular-learning methods in a field increasingly dominated by graph and deep-learning approaches. The importance of this work lies in showing that strong baselines should not be overlooked when they offer good performance with lower complexity and better interpretability.

Ravindranath *et al.* [52] focus specifically on the class-imbalance problem that pervades DeFi fraud detection. They evaluate oversampling strategies such as SMOTENC, ADASYN, and K-Means SMOTE in combination with machine-learning classifiers. Their contribution is important because fraud datasets are typically dominated by benign transactions, and naive training can therefore bias models toward the majority class. By studying how rebalancing techniques affect detection, they provide practical guidance for improving fraud sensitivity in rare-event settings.

Taher *et al.* [53] propose a voting-based ensemble framework combined with explainable AI techniques. Their work emphasizes that detection performance alone is not sufficient in operational environments; users and analysts also need interpretable explanations for why a transaction or wallet is flagged as suspicious. This study is important because it addresses the trade-off between predictive accuracy and actionable transparency, which remains a major challenge in real-world deployment.

Wang *et al.* [54] introduce DeFiGuard, a GNN-based framework for detecting price manipulation attacks by transforming Ethereum transactions into cash-flow graphs. These graphs capture relational flow structure that is difficult to model using flat features alone. The overall architecture of DeFiGuard is shown in Figure 10, which helps clarify how raw transaction data are converted into graph representations for downstream fraud

detection. This visualization is particularly useful because it shows how graph learning is integrated into the system pipeline. The study demonstrates that explicitly modeling relational and cash-flow structure can improve the identification of manipulation patterns in decentralized markets.

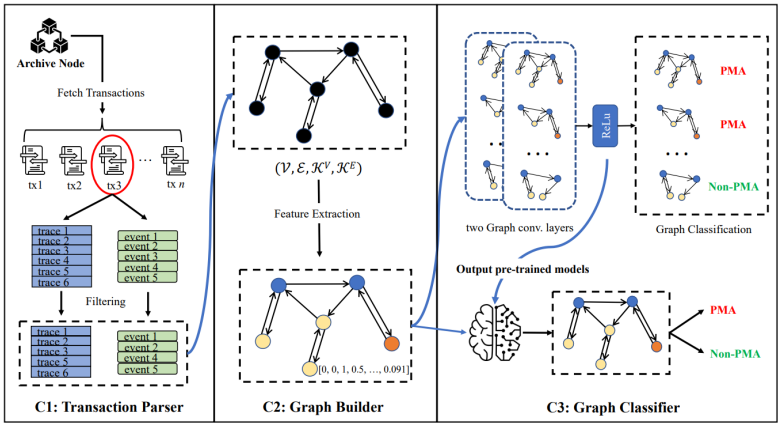


Figure 10: High-level architecture of DeFiGuard for price manipulation detection.

Kanezashi *et al.* [55] compare homogeneous and heterogeneous graph neural networks on Ethereum transaction data. Their study shows that explicitly modeling different node and edge types can provide a richer representation of on-chain interactions. This is important in blockchain environments because transactions often involve different categories of entities and relations that cannot be adequately captured by a single undifferentiated graph structure.

Tan *et al.* [56] build a labeled transaction network using crawled fraud and legitimate addresses and then apply a graph convolutional network informed by transaction volume and structural information. Their work demonstrates that fraud behavior can be detected more effectively when node attributes are combined with graph connectivity. This study contributes to the growing consensus that transaction networks contain meaningful structural signals that should not be ignored in Ethereum fraud analysis.

Tan *et al.* [57] extend their earlier work by proposing an enhanced deep-learning framework that mines transaction behaviors from the public Ethereum ledger. In addition to network construction, they introduce a transaction-behavior-based embedding method before applying graph convolution for classification. Their contribution is important because it moves beyond raw graph structure and incorporates richer behavioral representations into the node-learning process.

An *et al.* [58] introduce Finsformer, a transformer-based model with a cluster-attention mechanism for financial-attack detection. Their central idea is that similar transaction records can be grouped into localized behavioral regimes before attention is applied. This allows the model to focus more effectively on subtle local patterns that may be diluted under global attention alone. The study is important because it shows how sequence modeling in fraud detection can be refined to better capture clustered behavioral regularities.

Jia *et al.* [59] propose TLMG4Eth, a hybrid framework that combines machine-learning and deep-learning ideas by converting numerical transaction records into sentence-like representations and integrating them with graph-based views of wallet interactions and attribute similarity. This work is significant because it reflects a broader trend toward multi-view learning, where structured numeric data, relational graphs, and

representation-learning techniques are combined to improve fraud detection.

Wu *et al.* [31] propose DEFIRANGER, a non-learning-based framework that detects price manipulation through Cash Flow Tree (CFT) analysis. Instead of relying on black-box models, DEFIRANGER reconstructs raw transaction traces into interpretable cash-flow structures and then identifies high-level DeFi actions such as swaps, transfers, and protocol interactions. The pipeline is illustrated in Figure 11, which shows how raw traces are transformed into semantically meaningful CFT representations. This visualization is especially important because it makes clear how the framework lifts low-level transaction events into interpretable financial behavior. DEFIRANGER demonstrates that mechanism-aware and transparent approaches remain highly valuable, particularly in settings where interpretability is critical.

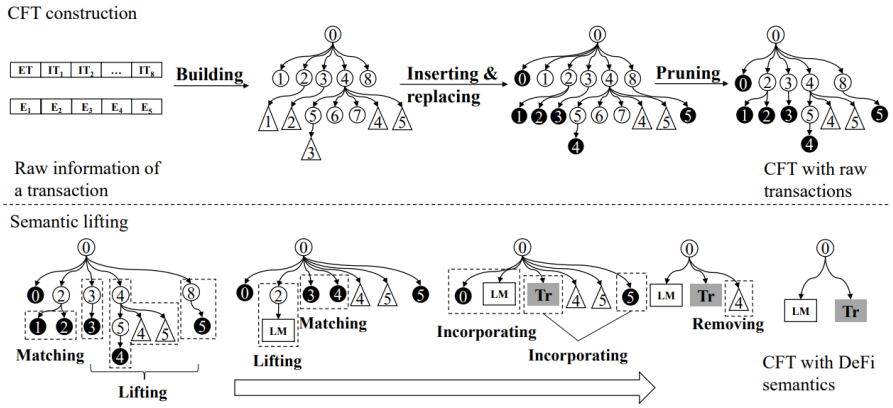


Figure 11: Overview of Cash Flow Tree (CFT) construction and semantic lifting in DeFiRanger.

2.5.3 Multi-Level

At the multi-level, studies integrate evidence across smart contracts, transactions, protocols, and wallets. This line of work is especially important because many DeFi fraud incidents are not confined to a single analytical layer. Instead, they emerge from interactions across code, user activity, and protocol composition. Norouzi *et al.* [60] propose a machine-learning framework for identifying fraud wallets associated with phishing, Ponzi schemes, and money laundering. Their work combines recursive feature elimination with cross-validation and Random Forest feature importance to select informative variables before classification. This is important because wallet-level fraud detection often suffers from noisy and high-dimensional feature spaces, and careful feature selection can improve both performance and interpretability.

Wang *et al.* [61] introduce DeFiScanner, a deep-learning framework that integrates global transaction context with local internal-operation features to detect logic vulnerabilities in DeFi smart contracts. Their contribution lies in showing that local contract behavior is often insufficient when analyzed in isolation. By incorporating broader contextual information from surrounding transactions, their model captures risk signals that single-view approaches may miss.

Palaiokrassas *et al.* [62] propose a cross-chain fraud-detection framework that combines DNNs, XGBoost, and a fine-tuned LLM across multiple protocols and blockchain environments. Their study is particularly

relevant because it addresses the challenge of generalization across heterogeneous ecosystems. As DeFi increasingly spans multiple chains and interoperable services, cross-chain detection becomes an important direction for future research.

Palaiokrassas *et al.* [63] focus on DeFi credit risk by predicting wallet liquidations using DeFi-specific transactional signals. Although their primary task is risk prediction rather than explicit fraud classification, the work remains relevant because liquidation behavior, abnormal leverage, and suspicious transactional patterns may overlap with malicious or exploitative activity. Their study shows that fraud detection and financial risk modeling can share common behavioral foundations.

Mothukuri *et al.* [64] present a multi-model AI framework that produces a project-level "TrustScore" by integrating LLM-based smart-contract auditing, anomaly detection, price monitoring, and sentiment analysis. This work is important because it reflects a broader shift toward holistic project-level risk assessment rather than single-point fraud classification. In complex DeFi environments, such integrated scoring frameworks may provide a more practical picture of overall project trustworthiness.

Kitzler *et al.* [65] analyze the complexity of DeFi compositions in which multiple protocols interact within a single transaction. They develop an algorithm to decompose nested protocol calls into interpretable building blocks. This work is valuable because it addresses one of the core challenges of DeFi security: the fact that risk often arises from protocol interaction rather than from any single component in isolation.

Xie *et al.* [66] propose DeFort, a behavior-driven framework for detecting price manipulation attacks. Their model identifies abnormal transactions, implicated functions, attackers, and victims by explicitly modeling manipulative behavior. This work is important because it focuses not merely on classification but also on attack reconstruction and attribution.

Wang *et al.* [67] introduce BLOCKEYE, a real-time attack-detection system that combines symbolic reasoning with monitoring of key service states such as asset prices. Their work is significant because it shows how real-time monitoring and policy-aware analysis can be integrated to identify attacks while they unfold, rather than only after forensic investigation.

Luo *et al.* [68, 35] provide a lifecycle-oriented taxonomy of DeFi fraud and review detection approaches across different project stages. Their framework is summarized visually in Figure 12, which shows how fraud types can be organized along the project lifecycle. This figure is valuable because it makes clear that fraud in DeFi is not confined to a single moment of system operation. Instead, different fraud risks become more prominent at different stages of project evolution, from launch and growth to maturity and decline. This lifecycle perspective supports the design of stage-aware fraud detection and monitoring systems.

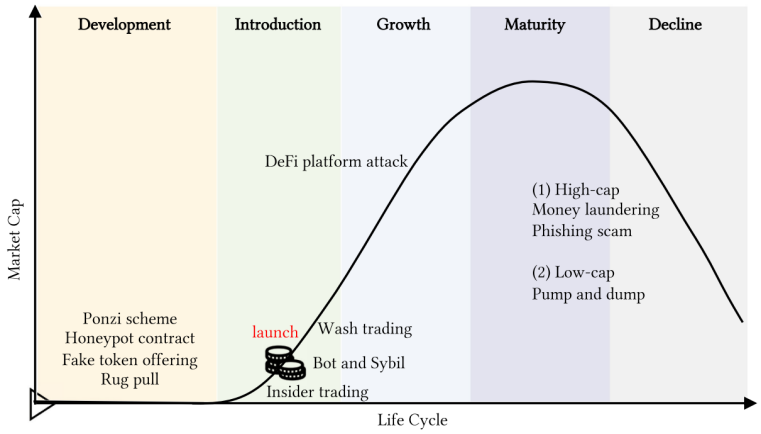


Figure 12: DeFi frauds along the project lifecycle.

Overall, the literature shows that DeFi fraud detection spans several analytical levels, from smart-contract code and transaction flow to wallet behavior, protocol composition, and cross-chain interaction. Nevertheless, transaction-level analysis remains the most widely used in practice because it is broadly applicable even when smart-contract information is incomplete or when attacks manifest directly through behavioral patterns. At the same time, many existing methods depend heavily on historical wallet activity, which limits their ability to identify zero-day attacks, such as malicious behavior that appears in a wallet's earliest observed transactions. Moreover, increasingly complex models may achieve strong predictive performance at the cost of lower interpretability and operational transparency. These limitations motivate the development of more systematic, practical, and early-stage fraud-detection approaches for analyzing DeFi transactions.

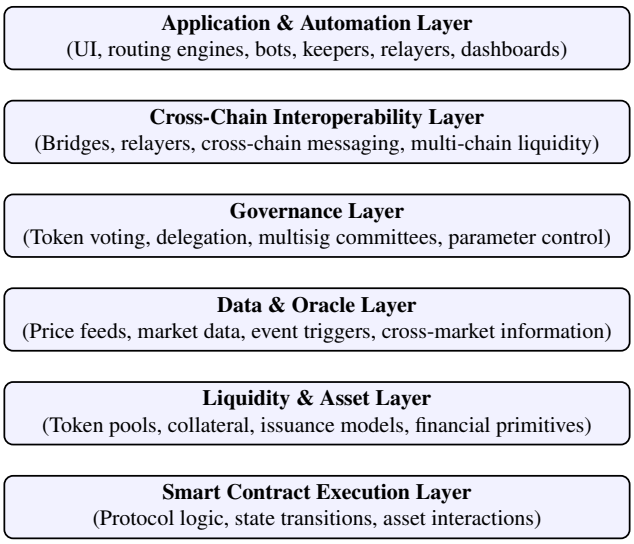


Figure 13: General architecture of DeFi platforms, illustrating six interconnected layers that support protocol functionality and influence security properties.

3 Broad Study

This section presents a detailed study of 284 DeFi platforms through a comparative architectural and functional analysis of the DeFi ecosystem. Over time, DeFi has evolved into a broad and heterogeneous landscape encompassing decentralized exchanges, lending and borrowing markets, stablecoin systems, derivative protocols, yield optimization platforms, governance frameworks, and supporting infrastructure services. Although these platforms differ significantly in purpose, economic model, and implementation, they also exhibit recurring architectural components and operational patterns that enable systematic comparison. To provide this broader perspective, the section identifies common architectural layers, establishes functional evaluation criteria, and organizes the analyzed platforms into major operational categories. The aim is not only to compare the services offered by different platforms, but also to examine how underlying architectural choices influence functionality, interoperability, governance, and exposure to risk.

3.1 Functional Evaluation Criteria

To present the study systematically, this section next establishes the functional benchmarks used to compare the 284 platforms analyzed. These criteria are intended to capture the core services commonly implemented across the DeFi ecosystem while providing a standardized and transparent framework for comparing platforms with diverse designs, economic models, and technical architectures. Each platform was evaluated against these criteria using a marking system to ensure consistency, transparency, and evidence-based assessment. For each functionality, a platform was marked YES and assigned +1 when clear evidence confirmed that the service is provided; marked NO and assigned 0 when evidence showed that the service is not provided; and marked NA with no score assigned when the absence of reliable or verifiable information prevented assigning a mark. This scoring approach prevents over-attribution of features, reduces methodological bias, and enables meaningful quantitative comparison across platforms. The 15 functionalities adopted as

evaluation benchmarks are described as follows:

- **Decentralized Exchange (DEX) Logic:** Core exchange functions, including token swaps, automated market makers (AMMs), and order book systems [69].
- **Lending or Borrowing Mechanics:** Protocols supporting peer-to-peer or pool-based lending, borrowing, and interest-earning mechanisms [69].
- **Yield Generation:** Opportunities for users to earn through liquidity mining, yield farming, and auto-compounding strategies [70].
- **Staking and Reward Systems:** Locking of assets for network or governance purposes, with associated incentives and returns [69].
- **Stable Asset Support:** Incorporation of stablecoins to reduce volatility and provide predictable settlement values [69].
- **Derivatives Trading:** On-chain access to futures, options, and synthetic assets, expanding opportunities for hedging and speculation [69].
- **Real-World Asset Tokenization:** Conversion of tangible assets such as real estate, commodities, or securities into blockchain-based tokens [71].
- **Cross-Chain Interoperability:** Ability to interact seamlessly with multiple blockchains, thereby enabling broader liquidity and asset mobility [72].
- **NFT Integration:** Tools for creating, trading, and applying non-fungible tokens (NFTs) in contexts such as ownership, collateralization, or utility [69].
- **Identity or Reputation Modeling:** Use of decentralized identity (DID), reputation scoring, or KYC modules to establish transactional trust [71].
- **Governance:** On-chain voting mechanisms, decentralized autonomous organization (DAO) participation, and control over protocol parameters [73].
- **Fi Mechanics:** Gamified finance, including play-to-earn models, reward loops, and the integration of NFT-based game assets [74].
- **Privacy or Security:** Mechanisms for safeguarding users, including anonymity, encryption, secure channels, and zero-knowledge proof protocols [69, 75].
- **AI-Enhanced Capabilities:** Application of artificial intelligence for risk assessment, fraud or anomaly detection, and automated strategy design [74].
- **Risk Management or Insurance:** Services offering protection against smart contract vulnerabilities, protocol failures, or extreme volatility [69].

By evaluating DeFi platforms across these 15 core functionalities, this section develops a unified analytical lens for systematically identifying both similarities and divergences in platform behavior. As the DeFi ecosystem expands rapidly, platforms increasingly offer overlapping services while pursuing distinct economic and revenue models [69, 71]. Without a structured classification framework, meaningful comparison becomes complex and conceptually inconsistent. For that reason, the broad study organizes platforms according to their underlying value logic and revenue mechanisms, thereby enabling systematic, transparent, and comparable analysis across heterogeneous designs [70].

Within this section, the 284 analyzed platforms are organized into eight proposed categories, each reflecting a distinct operational and economic archetype within the DeFi landscape: Decentralized Exchanges (DEXs) and AMMs, Lending and Borrowing Protocols, Stablecoin and Asset-Pegged Systems, Derivatives and Synthetic Asset Protocols, Yield Optimization and Auto-Compounding Platforms, Zero-Fee or Subsidized Transaction Models, Insurance or Coverage-Based Protocols, and Auxiliary and Multi-Service Platforms (e.g., RWA tokenization, identity-layer protocols, governance-focused systems).

This structured grouping not only prevents redundant comparisons but also highlights how economic design choices shape the implementation and adoption of functionalities across the ecosystem [71, 73]. Within each category, relevant platforms are evaluated against the 15 proposed benchmarks, ensuring that the assessment remains unbiased toward any single design philosophy and instead reflects the full breadth of systemic capabilities. The resulting evaluation tables indicate whether each platform supports each benchmark, enabling both within-category consistency checks and cross-category comparative insights [69].

The following subsections present each of the eight platform categories in detail. For each category, we summarize its functional characteristics, evaluate the platforms within that group, and identify both the strongest-performing platform in the category and the overall top-performing platform demonstrating the broadest functional coverage [69, 70].

3.2 Protocol Revenue Sharing

We begin the category-level analysis with platforms that distribute a portion of the protocol's fees or revenues to token holders, liquidity providers (LPs), or other participants. This model incentivizes long-term engagement, aligns user interests with protocol growth, and creates an ecosystem where platform success directly benefits its stakeholders [69, 71]. By rewarding contributors through revenue sharing, these platforms introduce a sustainable alternative to short-term, speculative models and ensure that value creation is closely tied to active participation in the protocol [70, 73].

3.2.1 Technical Architecture of Protocol Revenue Sharing

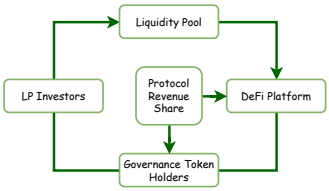
Protocol Revenue Sharing (PRS) platforms implement a smart-contract-driven mechanism that redistributes a portion of protocol-generated fees, such as trading fees, lending interest, liquidation penalties, and staking yields, to stakeholders. Their architecture is centered on three tightly integrated components: revenue accumulation, treasury governance, and distribution execution. Revenue accumulation contracts collect fees from various protocol subsystems (e.g., swaps, borrow interest, arbitrage modules), normalize them into a common accounting unit, and periodically transfer them to a treasury module. The treasury contract

maintains the aggregated revenue pool and specifies allocation rules, such as the proportions allocated to liquidity providers, governance token holders, insurance funds, or ecosystem reserves. Distribution is executed through a dedicated smart-contract layer that computes user shares based on stake, lock duration, or governance weight, using deterministic accounting formulas embedded in the protocol specification [76].
User eligibility is tracked by staking or locking contracts, which maintain on-chain records of user balances, timestamps, and reward multipliers. During distribution epochs, the distribution contract queries these state variables to calculate proportional entitlements. Some protocols incorporate oracle modules to value heterogeneous revenue components or convert multi-asset fee streams into a unified payout denomination. Governance contracts govern fee parameters, reward intervals, emission schedules, and treasury allocation policies, making PRS platforms susceptible to governance misconfiguration or capture. The architectural coupling between revenue-producing protocol modules, treasury systems, and staking logic shapes the security boundary of PRS platforms, where vulnerabilities in any upstream subsystem may propagate into reward manipulation, treasury misallocation, or systemic economic imbalance [76]. Figure 14(a)shows the architecture of this category.

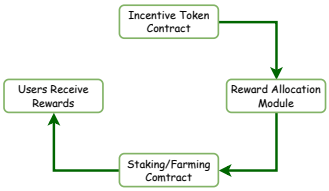
3.2.2 Platforms of Protocol Revenue Sharing

This section briefly lists and explains the platforms in this category.

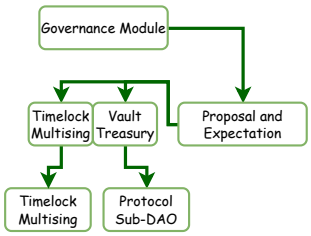
- **dForce [77]**: It is a modular DeFi platform offering lending, synthetic assets, and stablecoin protocols. It emphasizes interoperability and cross-chain functionality to enhance liquidity and composability across ecosystems.
- **Horizon Protocol [78]**: It enables the creation and trading of synthetic assets backed by collateral pools. It provides exposure to real-world and digital assets with decentralized governance and transparent on-chain settlements.
- **Frankencoin [79]**: It is a decentralized stablecoin protocol that allows users to mint tokens against various forms of collateral. Its design prioritizes long-term price stability through flexible collateralization and market-driven incentives.
- **Midas [80]**: It is a yield optimization protocol that automates investment strategies across DeFi platforms. It maximizes returns through dynamic allocation and compounding while simplifying portfolio management for users.
- **Aave [81]**: It is a decentralized lending and borrowing protocol that facilitates interest-earning deposits and collateralized loans. It introduced innovations such as flash loans and credit delegation to expand DeFi applications.
- **Synthetix [82]**: It is a protocol for issuing and trading synthetic assets representing fiat currencies, commodities, and indices. It leverages decentralized oracles and collateral-backed models to ensure accurate asset price tracking.



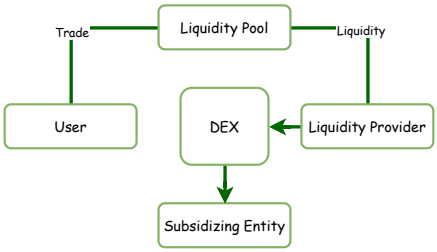
(a) Technical Architecture of Protocol Revenue Sharing



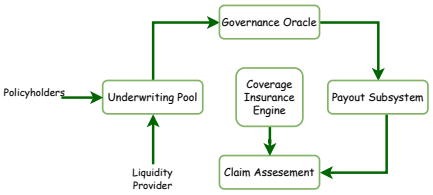
(b) Technical Architecture of Token-Based Incentivization Platforms



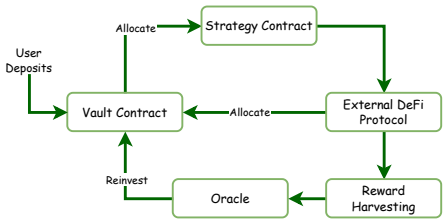
(c) Technical Architecture of Treasury-Governed DAOs



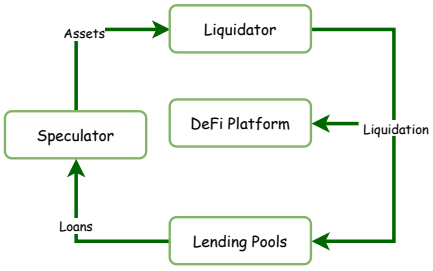
(d) Technical Architecture of Zero-Fee or Subsidized Models



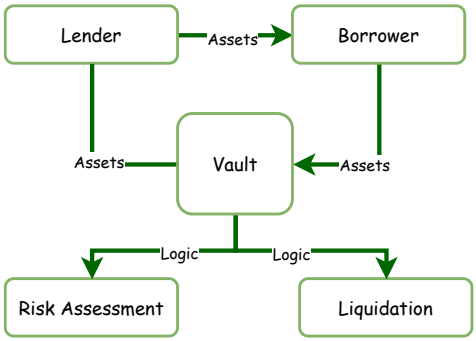
(e) Technical Architecture of Insurance and Coverage-Based Platforms



(f) Technical Architecture of Yield Optimization



(g) Speculation or Leverage-Driven



(h) Service Fee-Based Tools

Figure 14: Distribution of 284 DeFi platforms across eight categories. The figure illustrates concentration in revenue-sharing and utility-service models, reflecting where current development efforts and user demand are most strongly aligned.

- **Chainge [83]**: It is a cross-chain DeFi aggregator and decentralized exchange that enables seamless asset transfers. It focuses on interoperability and security through decentralized custody and multi-chain liquidity support.
- **Parrot Protocol [84]**: It is a DeFi network built on Solana that includes a stablecoin (PAI), non-custodial lending, and margin trading via a vAMM. It emphasizes unlocking value locked in LP tokens through collateralized borrowing and composable financial primitives.
- **MANTRA [85]**: It is a community-governed DeFi ecosystem that provides lending, staking, and launchpad services. It incorporates decentralized governance to enhance transparency and user participation in risk management.
- **UniLend Finance [86]**: It is a permissionless protocol combining spot trading with lending services. It allows any ERC-20 token to be listed, broadening access to liquidity and decentralized financial products.
- **Mimo [87]**: It is a decentralized platform focused on stablecoin issuance and lending. It allows users to mint stablecoins by locking collateral and provides efficient mechanisms for managing stable liquidity.
- **hope.money [88]**: It is a decentralized finance ecosystem designed to provide stablecoin issuance and yield services. It emphasizes sustainability by integrating lending, borrowing, and treasury-backed stability features.
- **Larix [89]**: It is a lending protocol on the Solana blockchain that supports a wide range of digital assets. It leverages Solana's scalability to deliver efficient lending, collateralization, and interest-earning services.
- **Synthetify [90]**: It is a Solana-based protocol for synthetic asset issuance and trading. It offers fast, low-cost transactions and enables users to gain exposure to real-world assets without direct ownership.
- **Abracadabra [91]**: It is a lending protocol that allows users to borrow its stablecoin, MIM, against interest-bearing tokens. It introduces novel collateral types and expands DeFi composability by leveraging yield-bearing assets.
- **Mass (MASS) [92]**: It is a mobile-centric DeFi platform integrating trading, on/off ramp, limit orders, and access to on-chain/off-chain data in a unified app. Its design streamlines interactions across multiple chains and protocols.
- **QuickSwap [93]**: It is a decentralized exchange built on Polygon, providing fast and low-cost token swaps. It mirrors Uniswap's automated market maker model while leveraging Polygon's scalability for improved efficiency.
- **Angle Protocol [94]**: It is a decentralized stablecoin protocol specializing in collateralized and delta-neutral mechanisms. It ensures stability by balancing collateral positions with hedging strategies and supporting multi-asset backing.

- **Euler Finance [95]**: It is a lending protocol designed for long-tail assets. It enables permissionless token listing and risk-adjusted borrowing, and introduces isolated lending markets to mitigate systemic risk.
- **Fringe Finance [96]**: It is a decentralized money market and margin trading platform designed to unlock capital spread in crypto assets regardless of market capitalization. It supports lending, borrowing, margin trading, staking, and LP token collateralization, with features including partial liquidations, multi-chain support, and atomic repayments.
- **Maple Finance [97]**: It is a decentralized credit protocol providing undercollateralized lending to institutional borrowers. It combines on-chain transparency with professional credit assessment through pool delegates.
- **Venus Protocol [98]**: It is a lending and borrowing platform on Binance Smart Chain. It supports the issuance of algorithmic stablecoins and provides efficient collateralized lending across a wide range of digital assets.
- **Sushi [99]**: It is a decentralized exchange and DeFi ecosystem that evolved from Uniswap's AMM model. It extends functionality through lending, yield farming, and cross-chain integration under a community-governed framework.
- **Silo Finance [100]**: It is a lending protocol that creates isolated markets for each asset. This design minimizes systemic risk while enabling permissionless token listing for collateral and borrowing.
- **Wombat Exchange [101]**: It is a multi-chain decentralized exchange focused on stablecoin swaps. It offers low-slippage trading, efficient liquidity pools, and cross-chain interoperability for stable assets.
- **ShapeShift DAO [102]**: It is a community-owned DeFi platform enabling cross-chain asset swaps. It emphasizes decentralization, open-source development, and integration with multi-chain wallets and protocols.
- **Ooki Protocol [103]**: It is a decentralized finance protocol combining lending, borrowing, margin trading, staking, and community governance. It supports permissionless listings, AI-driven features, and multi-chain integrations, and distributes a portion of its revenue to OOKI stakers as staking rewards.
- **Mai (Qi Dao Protocol) [104]**: It is a decentralized stablecoin platform on Polygon. It allows users to mint stablecoins against collateralized assets at no interest.
- **Goldfinch [105]**: It is a decentralized credit protocol enabling real-world lending without requiring crypto collateral. It bridges on-chain capital with off-chain businesses through trust-based credit assessment.
- **Meld [106]**: It is a decentralized protocol that aims to integrate crypto and fiat banking services by allowing users to borrow fiat against crypto collateral, with features such as "genius loans" that automatically reduce principal over time.

- **Lido [107]**: A liquid staking protocol that enables users to stake assets such as ETH or SOL and receive derivative tokens. These tokens can be used across DeFi, increasing liquidity and capital efficiency.
- **Cream Finance [108]**: It is a lending protocol that supports long-tail crypto assets. It extends liquidity to less-common tokens while also offering borrowing, lending, and yield-optimization features.
- **Mintera [109]**: It is a DeFi protocol focused on sustainable finance. It integrates climate-positive initiatives to provide yield opportunities while supporting carbon offset and green projects.
- **TrueFi [110]**: It is an unsecured lending protocol that combines decentralized governance with credit assessment. It enables capital-efficient lending by allowing trusted borrowers to access loans without full collateralization.
- **Notional [111]**: It is a fixed-rate lending and borrowing protocol. It introduces time-bound fTokens to provide predictable yields and borrowing costs, enhancing stability within the DeFi ecosystem.
- **Compound [112]**: It is a widely adopted lending protocol that allows users to supply assets and earn variable interest or borrow against collateral. It introduced algorithmic interest rate models in DeFi.
- **SmartCredit.io [113]**: It is a lending protocol designed for fixed-income loans. It emphasizes borrower-lender relationships by providing personal lending markets alongside automated risk management.
- **Marinade Finance [114]**: It is a Solana-based liquid staking protocol. It issues mSOL tokens representing staked SOL, which can be used in DeFi applications to enhance liquidity and composability.
- **Bancor [115]**: It is an automated market maker protocol that introduced liquidity pools and single-sided staking. It features impermanent loss protection and enables decentralized token swaps with built-in liquidity.
- **Jet Protocol [116]**: It is a Solana-based lending platform focusing on efficiency and scalability. It provides collateralized borrowing and lending services with governance driven by its community.
- **Beanstalk [117]**: It is an algorithmic stablecoin protocol that maintains price stability through supply adjustments rather than collateralization. It incentivizes participants via credit-based mechanisms to balance supply and demand.
- **mStable [118]**: It is a DeFi protocol focused on stablecoin aggregation and yield optimization. It provides low-slippage swaps, lending, and interest-bearing products for stable assets.
- **Carbonable [119]**: It is a DeFi platform linking blockchain finance with carbon offset initiatives. It tokenizes environmental projects, enabling investors to support sustainability while accessing yield opportunities.
- **Open Dollar (ODG) [120]**: It is a lending protocol that enables users to borrow stablecoins against crypto collateral. It emphasizes stability and scalability through efficient collateral management mechanisms.

- **Tarot [121]**: It is a decentralized lending protocol specializing in leveraged yield farming. It allows users to supply liquidity with leverage while dynamically managing risks through collateralized positions.
- **Brú Finance [122]**: It is a decentralized credit protocol connecting DeFi liquidity with real-world assets. It focuses on tokenizing commodities and on supply chain financing to broaden access to capital.
- **Quicksilver [123]**: It is a liquid staking protocol for the Cosmos ecosystem. It enables staking of native tokens and the issuance of liquid derivatives that can be used across IBC-enabled chains.
- **Liquity [124]**: It is a decentralized borrowing protocol that issues the LUSD stablecoin against ETH collateral. It operates with zero-interest loans and ensures system stability through a stability pool and automated liquidations.
- **Veda [125]**: A DeFi protocol that provides decentralized credit and liquidity management. It emphasizes permissionless access to credit markets and integrates automated risk-adjusted lending strategies.
- **bemo [126]**: It is a liquid staking protocol built on NEAR Protocol. It allows users to stake NEAR tokens and receive derivative assets that can be used across DeFi applications to increase liquidity.
- **Stader [127]**: It is a multi-chain liquid staking protocol that provides modular staking infrastructure. It enables users to stake assets across supported blockchains and receive liquid derivatives for use in DeFi.
- **Davos Protocol [128]**: It issues a stablecoin backed by staked assets and yield-generating strategies. It focuses on preserving stability while allowing collateral to continue earning yield.
- **StakeWise [129]**: It is a liquid staking protocol for Ethereum that tokenizes staking rewards separately from principal deposits. This dual-token model enhances transparency and flexibility in the management of staked assets.
- **Yield Protocol [130]**: It offers fixed-rate lending and borrowing using tokenized debt instruments called fyTokens. It provides predictable returns and borrowing costs, reducing interest rate volatility in DeFi.
- **Lara Protocol [131]**: It is a DeFi lending system that allows undercollateralized loans based on credit risk assessment. It aims to extend access to credit while maintaining risk-adjusted stability.
- **Wildcat [132]**: It is a protocol for decentralized credit markets that introduces configurable lending pools. It empowers issuers to design tailored markets while ensuring transparency and automated enforcement of terms.
- **Raydium [133]**: It is an automated market maker and liquidity provider on Solana. It integrates with Serum's order book, combining AMM liquidity with centralized exchange-like trading efficiency.

- **Timeswap [134]**: A decentralized lending and borrowing protocol that operates without oracles. It employs a three-variable automated market maker model to enable permissionless, trust-minimized credit markets.
- **Rocket Pool [135]**: It is a decentralized Ethereum staking protocol designed for both node operators and smaller stakers. It enables pooled staking with liquid staking tokens while maintaining decentralization.
- **Router Protocol [136]**: It is an interoperability solution enabling cross-chain asset transfers. It focuses on secure, efficient bridging across multiple blockchains to enhance liquidity mobility.
- **Port Finance [137]**: It is a money market protocol on Solana that supports variable interest rate lending and borrowing. It leverages Solana's scalability to provide efficient liquidations and real-time risk management.
- **Hubble [138]**: It is a Solana-based protocol issuing the USDH stablecoin against crypto collateral. It emphasizes capital efficiency by allowing users to earn yield on deposited collateral while minting stablecoins.
- **Mayan Finance [139]**: It is a cross-chain swapping protocol built on Solana. It enables trustless, efficient asset transfers across multiple chains with low fees and minimal slippage.
- **Unit Protocol [140]**: A decentralized borrowing system that enables the issuance of the USDP stablecoin against various crypto assets. It prioritizes inclusivity by supporting long-tail tokens as collateral.
- **Ribbon Finance [141]**: It is a structured products protocol offering automated options strategies. It provides users with sustainable yield through options vaults while abstracting away technical complexity.
- **Solend [142]**: It is a lending and borrowing platform on Solana designed for scalability. It supports collateralized lending through community-driven governance and adjustments to risk parameters.
- **Badger Finance [143]**: It is a DeFi protocol focused on bringing Bitcoin into DeFi. It provides vaults and lending products to unlock liquidity and yield opportunities for tokenized Bitcoin.
- **Circle Yield [144]**: It is a regulated crypto yield product offered by Circle. It provides fixed-term USDC lending to institutional borrowers, ensuring transparency and compliance with financial standards.
- **Morpho [145]**: It is a peer-to-peer layer built on top of lending protocols like Aave and Compound. It improves capital efficiency by matching lenders and borrowers directly while remaining compatible with the underlying liquidity pools.
- **Ankr Liquid Staking [146]**: It is a multi-chain staking solution that issues liquid staking tokens. It enables stakers to retain liquidity and deploy assets across DeFi while earning staking rewards.

- **Minterest [147]**: It is a lending protocol designed to capture and redistribute all revenue to its users. It automates interest, liquidation, and fee capture, creating a self-sustaining incentive model for participants.
- **Term Finance [148]**: It is a fixed-term lending protocol that matches borrowers and lenders through periodic auctions. It ensures transparent rate discovery and predictable borrowing costs in DeFi markets.
- **Tectonic Finance [149]**: It is a lending and borrowing platform on Cronos. It provides money market functionality with cross-chain asset support, enabling users to earn passive yield or access liquidity.
- **Veno Finance [150]**: It is a liquid staking protocol on Cronos that issues liquid staking tokens. It enhances capital efficiency by enabling stakers to participate in DeFi and earn staking rewards.

In summary, the protocol revenue-sharing category illustrates how fee redistribution can support robust, multi-service ecosystems that balance user incentives with long-term sustainability. Platforms in this category tend to integrate a wide range of financial primitives, including DEX logic, lending, yield generation, staking, derivative markets, and cross-chain capabilities, highlighting their ambition to operate as comprehensive DeFi hubs rather than single-purpose products. The comparative analysis shows that the strongest performers deploy revenue sharing not merely as a reward mechanism but as an architectural foundation that supports governance, privacy safeguards, and systemic utility. At the same time, the category reveals inherent trade-offs: the sustainability of reward flows depends heavily on continuous protocol usage, and platforms must carefully calibrate economic parameters to avoid dilution or misaligned incentives. Compared to other models, revenue-sharing systems tend to exhibit the broadest feature coverage, yet they face greater complexity in coordinating incentives across diverse service modules. As DeFi matures, these platforms demonstrate how shared economic participation can reinforce decentralization while enabling scalable, multi-functional architectures. This category, therefore, sets a benchmark for operational breadth, though its economic interdependencies also introduce unique security challenges.

3.3 Token-Based Incentivization

The next category in the broad study includes platforms that rely on token rewards to incentivize participation rather than directly redistributing protocol revenues. These systems reward users with native tokens, which can typically be staked, traded, or used within the ecosystem for governance and utility purposes. This approach has become common in DeFi because it supports user acquisition, liquidity growth, and ecosystem expansion by aligning participation with token-based incentives [69, 71, 70].

3.3.1 Technical Architecture of Token-Based Incentivization Platforms

Token-based incentivization platforms employ a smart-contract architecture that stimulates user participation, liquidity formation, and protocol engagement through programmable token rewards. Their core design integrates token-minting logic, reward-distribution contracts, and stake-tracking mechanisms, which collectively implement an endogenous incentive system aligned with the platform's economic objectives. At

Table 3: Platforms – Protocol Revenue Sharing Category

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
dForce	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	YES	13
Horizon Protocol	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	13
Frankencoin	YES	YES	YES	YES	YES	NA	YES	YES	NO	YES	YES	NO	YES	NO	YES	11
Aave	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES	YES	NO	YES	NO	YES	11
Synthetix	YES	YES	YES	YES	YES	YES	YES	YES	NO	NO	YES	NO	YES	NO	YES	11
Chainge	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	11
Midas	NO	YES	YES	YES	YES	NA	YES	YES	NO	YES	NA	NO	YES	YES	YES	10
Parrot Protocol	YES	YES	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	10
MANTRA	YES	YES	YES	YES	YES	NO	YES	YES	NO	NO	YES	NO	YES	NO	YES	10
UniLend Finance	YES	YES	YES	YES	YES	NO	NO	NO	YES	NO	YES	NO	YES	YES	YES	10
Mimo	YES	YES	YES	YES	YES	NO	YES	YES	YES	NO	YES	NO	NO	NO	YES	10
Larix	NO	YES	YES	YES	YES	NO	YES	NO	YES	NO	YES	NO	YES	NO	YES	9
Synthetify	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	YES	NO	NO	NO	YES	9
Abracadabra	NO	YES	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
QuickSwap	YES	NO	YES	YES	NO	YES	NO	YES	NO	NO	YES	YES	NO	YES	YES	9
Angle	NO	YES	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Euler Finance	YES	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Fringe Finance	NO	YES	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Maple Finance	NO	YES	YES	YES	YES	NO	YES	YES	NO	NO	YES	NO	YES	NO	YES	9
hope.money	YES	YES	YES	YES	YES	YES	NA	NA	NO	NO	YES	NO	NO	NO	YES	8
Mass Protocol	YES	NA	NA	NO	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	8
Venus Protocol	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Sushi	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
Silo Finance	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Wombat Exchange	YES	NO	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
ShapeShift DAO	YES	YES	NO	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Ooki Protocol	NO	YES	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	NO	YES	YES	8
Mai (Qi Dao Protocol)	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Goldfinch	NO	YES	YES	YES	NO	NO	YES	NO	NO	YES	YES	NO	YES	NO	YES	8
Meld	NO	YES	YES	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Lido	NO	YES	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Cream Finance	YES	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	8
Mintera	NO	YES	YES	YES	YES	NO	NO	NA	YES	NO	YES	NO	YES	NO	YES	8
Ribbon Finance	NO	YES	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	NO	NO	YES	8
TrueFi	NO	YES	YES	YES	YES	NO	NO	NO	NO	YES	YES	NO	NO	NA	YES	7
Notional	NO	YES	YES	YES	YES	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	7
Compound	NO	YES	YES	NO	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	7
SmartCredit.io	NO	YES	YES	YES	NO	NO	NO	NO	NO	YES	NO	NO	YES	YES	YES	7
Marinade Finance	NO	YES	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Bancor	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Jet Protocol	NO	YES	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Beanstalk	YES	NO	YES	YES	YES	NO	NO	NO	YES	NO	YES	NO	NO	NO	YES	7
mStable	YES	YES	YES	YES	YES	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	7
Carbonable	NO	NO	YES	YES	NO	NO	YES	NO	YES	NO	YES	NO	YES	NO	YES	7
Open Dollar (ODG)	NO	YES	YES	NO	YES	NO	NO	YES	YES	NO	YES	NO	NO	NO	YES	7
Tarot	NO	YES	YES	NO	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Brú Finance	NO	YES	YES	NO	YES	NO	YES	YES	NO	NO	YES	NO	NO	NO	YES	7
Port Finance	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	7
Unit Protocol	YES	YES	YES	YES	YES	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	7
Minterest	NO	YES	YES	NO	YES	NO	NO	YES	YES	NO	YES	NO	NO	NO	YES	7
Quicksilver	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	6
Liquity	NO	YES	YES	NO	YES	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	6
bemo	NO	YES	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	6
Stader	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	6
Davos Protocol	NO	YES	YES	NO	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	6
StakeWise	NO	YES	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	6
Yield Protocol	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	NO	YES	6
Hubble	NO	YES	YES	YES	YES	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	6
Solend	NO	YES	YES	YES	YES	NO	NO	NA	NO	NO	YES	NO	NO	NO	YES	6
Morpho	NO	YES	YES	NO	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	6
Term Finance	NO	YES	YES	NO	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	6
Veda	NO	NO	YES	NA	YES	NO	NA	YES	NO	NO	NO	NO	YES	NO	YES	5
Lara Protocol	NO	NO	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	5
Wildcat	NO	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	YES	NO	YES	5
Raydium	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	5
Timeswap	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	YES	NO	NO	NO	YES	5
Rocket Pool	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	5
Router Protocol	YES	NO	NO	NO	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	5
Badger Finance	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	5
Tectonic Finance	NO	YES	YES	NO	YES	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	5
Mayan Finance	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	4
Circle Yield	NO	YES	YES	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	4
Ankr Liquid Staking	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	YES	4
Veno Finance	NO	NO	YES	YES	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO	YES	4

the foundation of this architecture lies the incentive token contract, which encodes minting rules, emission schedules, vesting constraints, and governance roles. Incentive distribution is mediated by reward allocator contracts, which compute payouts based on user activity parameters, such as liquidity provision, transaction volume, staking duration, or governance participation, and disburse rewards according to deterministic, on-chain formulas [151].

A complementary staking or farming module records user deposits and locks assets or LP tokens, enabling the protocol to evaluate participation levels and proportionally adjust rewards. Some designs incorporate performance-based multipliers or time-dependent boost factors, implemented through state-tracking variables recorded in staking contracts. Oracle modules may be used to normalize reward valuations across heterogeneous assets or to prevent reward exploitation during volatile market periods. Protocol governance oversees emission parameters, reward curves, token supply ceilings, and vesting schedules, making governance integrity a central determinant of incentive stability [151]. Fig. 14(b) shows the architecture of this category.

3.3.2 Platforms of Token-Based Incentivization

This section briefly lists and explains the platforms in this category.

- **Hakka Finance [152]**: It is a DeFi ecosystem offering diverse financial products with user incentives driven by its native token. Token rewards encourage participation across prediction markets, asset management, and lending services.
- **Shade Protocol [153]**: It is a privacy-preserving DeFi platform built on Secret Network. It incentivizes users through token rewards tied to its stablecoin and DeFi applications, aligning growth with protocol adoption.
- **Katana [154]**: It is a decentralized exchange on Ronin that distributes governance tokens to liquidity providers. This token-based incentivization mechanism strengthens user engagement and ecosystem liquidity.
- **CrossCurve [155]**: It is a DeFi platform enabling stable asset swaps and liquidity provision across chains. Users are incentivized with native tokens that can be staked or traded to secure additional rewards.
- **CVI Finance [156]**: It is a volatility index platform that incentivizes users through its governance token. Rewards are distributed for staking, liquidity provision, and trading activities tied to crypto volatility indices.
- **Trader Joe [157]**: It is a comprehensive decentralized trading platform on Avalanche with support for token swaps, lending, yield farming, and concentrated liquidity through its Liquidity Book AMM model.

- **Biswap [158]**: It is a decentralized exchange on Binance Smart Chain that incentivizes users through token rewards for trading, liquidity provision, and referrals. Its model reinforces growth in token liquidity and adoption.
- **KyberSwap [159]**: It is a multi-chain DEX aggregator and liquidity platform. Token incentives are distributed to liquidity providers and stakers, ensuring that governance participation aligns with liquidity growth.
- **StellaSwap [160]**: It is a decentralized exchange on Moonbeam designed for Polkadot's ecosystem. It relies on token rewards to incentivize liquidity provision, trading activity, and governance participation.
- **Preon Finance [161]**: It is a DeFi protocol enabling overcollateralized stablecoin issuance. Users receive token-based incentives for supplying collateral and providing liquidity, thereby strengthening demand for the platform's native token.
- **Beethoven X [162]**: It is a decentralized exchange and investment platform built on Balancer technology. It incentivizes liquidity providers by distributing token rewards through liquidity pools and yield farming strategies.
- **Nolus [163]**: It is a DeFi protocol offering leveraged lending and borrowing services. Users are rewarded with native tokens for supplying liquidity and participating in protocol governance.
- **Defx [164]**: It is a decentralized exchange and Layer-1 blockchain built for perpetual futures (up to $25\times$ leverage in regular mode, and even higher in "Degen" mode). It operates with a central limit order book (CLOB), a delta-neutral liquidity vault (Liquidity Engine), and integrates yield, trading fees, and liquidation profits as revenue streams to liquidity providers.
- **Curve Finance [165]**: It is a decentralized exchange optimized for stablecoin trading. Its token model incentivizes liquidity providers and governance participants through staking and reward mechanisms.
- **Alium Finance [166]**: It is a cross-chain decentralized exchange that introduces a hybrid liquidity model combining centralized and decentralized liquidity sources to mitigate fragmentation across blockchains. It incentivizes liquidity providers through token rewards and supports cross-chain swaps to enhance accessibility.
- **WigoSwap [167]**: It is a decentralized exchange on Fantom that relies on token incentives to reward liquidity providers and traders. Its model also integrates gamified staking features to boost user engagement.
- **Aldrin [168]**: A decentralized exchange on Solana that offers spot and futures trading. Users earn rewards in the native token for liquidity provision and staking, aligning participation with platform development.

- **DODO [169]**: A decentralized exchange that employs a proactive market-maker model. Token rewards incentivize liquidity provision, governance participation, and ecosystem activities across multiple chains.
- **Saber [170]**: It is a stablecoin and wrapped asset exchange on Solana. Liquidity providers are incentivized with token rewards, which can be staked or farmed for additional yield.
- **Lifinity [171]**: It is an automated market maker on Solana that optimizes liquidity with oracle-based pricing. It distributes token incentives to liquidity providers, reinforcing long-term liquidity stability.
- **Saddle Finance [172]**: It is a decentralized exchange optimized for stablecoin and pegged asset swaps. It incentivizes liquidity providers with native token rewards to maintain deep liquidity and low-slippage trades.
- **zkSwap Finance [173]**: It is a layer-2 automated market maker protocol leveraging zk-Rollups for high throughput and low fees. Liquidity providers are rewarded with token incentives to support ecosystem participation and scalability.
- **Loopring [174]**: It is a layer-2 protocol enabling high-throughput decentralized exchanges. Token incentives reward users for liquidity provision, staking, and protocol governance, aligning growth with adoption.
- **Balancer [175]**: It is an automated portfolio manager and decentralized exchange. Its token model incentivizes liquidity providers and governance participants through staking and liquidity mining rewards.
- **HorizonDEX [176]**: It is a decentralized exchange platform that uses token rewards to encourage liquidity provision and trading activity. It integrates governance mechanisms to align incentives with protocol sustainability.
- **MelegaSwap [177]**: It is a decentralized exchange that rewards liquidity providers and traders with native tokens. Its incentive structure supports token staking, yield farming, and governance participation.
- **VVS Finance [178]**: It is an automated market maker on Cronos. It relies on token incentives to reward liquidity provision, farming, and staking, boosting user participation in the ecosystem.
- **Atrix [179]**: It is a decentralized exchange and liquidity provider on Solana. Users are rewarded with tokens for contributing liquidity, which can be further staked for additional yield.
- **Velodrome [180]**: It is a decentralized exchange built on Optimism. It distributes token rewards to liquidity providers and governance participants, promoting sustainable growth within the Optimism ecosystem.

- **Paraswap [181]**: It is a decentralized exchange aggregator optimizing token swaps across multiple platforms. Token-based incentives encourage user participation in governance and ecosystem engagement.
- **Convex Finance [182]**: It is a yield optimization protocol built on Curve Finance. It distributes token rewards to liquidity providers and stakers, enhancing incentives for long-term participation.
- **STRKFarm [183]**: It is a staking and yield farming platform that relies on token incentives. Users earn rewards for providing liquidity and staking, reinforcing demand for its governance token.
- **Uniswap [184]**: It is a leading decentralized exchange utilizing an automated market maker model. Token incentives are distributed to liquidity providers and governance participants through the native UNI token.
- **CroSwap [185]**: It is a decentralized exchange on Cronos. It incentivizes liquidity provision and trading through token rewards that can also be staked or farmed for additional yield.
- **Hegic [186]**: It is an options trading protocol that uses token rewards to encourage liquidity provision and governance. Users are incentivized to supply liquidity to support decentralized options markets.
- **Invariant [187]**: It is a decentralized exchange on Solana designed for efficient token swaps. It distributes token rewards to liquidity providers, aligning user incentives with ecosystem liquidity growth.
- **Hundred Finance [188]**: It is a lending and borrowing protocol operating across multiple chains. Token-based rewards incentivize liquidity provision, collateral supply, and governance participation.
- **Mercurial Finance [189]**: It is a Solana-based stable asset exchange. It incentivizes liquidity providers with token rewards, supporting dynamic vaults for efficient stablecoin trading.
- **Treble [190]**: It is a DeFi protocol that incentivizes users with native token rewards for providing liquidity and engaging with platform services. Its model strengthens ecosystem participation and token demand.
- **RBX [191]**: It is a decentralized finance hub offering swaps, staking, and token launch services. It relies on token incentives to reward users for liquidity provision and active governance involvement.
- **Moox Protocol [192]**: It is a decentralized exchange that incentivizes liquidity provision through token rewards. Its model promotes user participation in trading and governance activities.
- **Orca [193]**: It is an automated market maker on Solana known for its user-friendly interface. It distributes token rewards to liquidity providers, reinforcing liquidity depth and ecosystem engagement.
- **Amply Finance [194]**: It is a DeFi protocol that offers yield opportunities through farming and staking. Token rewards are central to incentivizing liquidity provision and platform participation.
- **Minu Swap [195]**: It is a decentralized exchange where liquidity providers and traders earn token rewards. Incentives are designed to boost liquidity and encourage ecosystem growth.

- **Sphere [196]**: It is a DeFi platform that rewards users with governance tokens for participation in liquidity and staking activities. Its model aligns token demand with protocol expansion.
- **Cope [197]**: It is a Solana-based project that uses token incentives to reward ecosystem participants. Users engage in staking and governance activities that strengthen the protocol's long-term utility.
- **Bebop [198]**: It is a decentralized trading platform focusing on efficient asset swaps. Token rewards incentivize liquidity provision and user activity, promoting ecosystem adoption.
- **Quarry [199]**: It is a protocol for yield farming on Solana. It distributes token incentives to liquidity providers and stakers, simplifying the process of earning rewards from DeFi applications.
- **Starbase [200]**: It is a decentralized platform that supports token creation, fundraising, and governance. Users are incentivized with native tokens for participation in ecosystem development and governance activities.
- **PawSwap [201]**: It is a decentralized exchange designed for community-driven ecosystems. Token rewards are provided to liquidity providers and traders, encouraging engagement and liquidity growth.

Collectively, token-based incentivization platforms demonstrate how emission-driven economies shape user engagement, liquidity provision, and protocol growth across DeFi. These systems typically combine staking, lending, governance participation, and gamified components to attract users, relying on well-designed reward schedules to sustain activity and align behaviors. The analysis shows that although many platforms offer broad functionality, their reliance on token emissions introduces volatility in long-term participation, particularly when reward structures overshadow underlying utility. Compared to revenue-sharing models, incentivization platforms offer fewer integrated financial services but compensate by promoting community engagement through rapid bootstrapping and accessible earning mechanisms. However, the category also highlights structural limitations: token rewards alone cannot guarantee sustainable liquidity, and poorly calibrated emissions may lead to economic instability or decreased user retention. Despite these challenges, the strongest systems in this category effectively combine financial primitives with thoughtfully engineered incentive loops, illustrating how token economics can reinforce governance participation, liquidity depth, and user activity. This category thus occupies a unique position between functional breadth and behavioral engineering, setting the stage for the vulnerabilities associated with incentive mechanisms.

3.4 Treasury-Governed DAOs

Another category identified in this broad study includes platforms that channel protocol value into a treasury governed collectively by a DAO. Rather than distributing value directly to users, these systems pool resources and redeploy them through governance-approved decisions for ecosystem development, incentives, and other strategic purposes [71, 69, 70].

Table 4: Platforms - Token-Based Incentivization

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
Hakka Finance	YES	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	NO	YES	12
Shade Protocol	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	11
Katana	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	11
CrossCurve	YES	NO	YES	YES	YES	NO	NO	YES	YES	NA	YES	NO	YES	YES	YES	10
CVI Finance	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	NA	NO	YES	10
Trader Joe	YES	YES	YES	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	10
Biswap	YES	NO	YES	YES	NO	NO	NO	YES	YES	YES	YES	YES	YES	NO	YES	10
KyberSwap	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	YES	YES	10
StellaSwap	YES	NO	YES	YES	YES	NO	NO	YES	YES	YES	YES	NO	YES	NO	YES	10
Preon Finance	NO	YES	YES	YES	YES	NO	NO	YES	YES	YES	YES	NO	YES	NO	YES	10
Beethoven X	YES	NO	YES	YES	YES	NO	NO	YES	YES	YES	YES	NO	YES	NO	YES	10
Nolus	NO	YES	YES	YES	YES	NO	NA	YES	NO	NO	YES	NO	YES	YES	YES	9
Defx	YES	NO	YES	YES	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Curve Finance	YES	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Alium Finance	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	YES	YES	NO	YES	9
WigoSwap	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	YES	YES	NO	YES	9
Aldrin	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
DODO	YES	NO	YES	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	9
Saber	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
Lifinity	YES	NO	YES	YES	YES	NO	NO	YES	YES	YES	YES	NO	NO	NO	YES	9
Saddle Finance	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
zkSwap Finance	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
Loopring	YES	NO	YES	YES	YES	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	9
Balancer	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
HorizonDEX	YES	NO	YES	YES	NA	NO	NO	NA	YES	YES	YES	NO	YES	NO	YES	8
MelegaSwap	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
VVS Finance	YES	NO	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Atrix	YES	NO	YES	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Velodrome	YES	NO	YES	YES	NO	NO	NO	NO	YES	YES	YES	NO	YES	NO	YES	8
Paraswap	YES	NO	YES	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Convex Finance	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Uniswap	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Hegic	NO	NO	YES	YES	YES	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	8
Invariant	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	NO	NO	YES	NO	YES	8
STRKFarm	NO	YES	YES	YES	YES	NO	NO	NA	YES	YES	NO	NO	NA	NO	YES	7
CroSwap	YES	NO	YES	YES	NA	NO	NO	YES	YES	YES	NO	NO	NA	NO	YES	7
Hundred Finance	NO	YES	YES	YES	NO	NO	NO	YES	NO	NA	YES	NO	YES	NO	YES	7
Mercurial Finance	YES	NO	YES	NA	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Treble	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
RBX	YES	NO	YES	YES	NO	NO	NO	YES	NO	YES	NO	NO	YES	NO	YES	7
Orca	YES	NO	YES	YES	NO	NO	NO	NO	NO	YES	YES	NO	YES	NO	YES	7
Amply Finance	NO	YES	YES	YES	YES	NO	NO	NO	NO	YES	NO	NO	YES	NO	YES	7
Moox Protocol	YES	NO	YES	YES	NO	NO	NO	NA	NO	YES	NO	YES	NA	NO	YES	6
Minu Swap	YES	NO	YES	YES	NO	NO	NO	NA	NO	YES	NO	NO	YES	NO	YES	6
Sphere	NO	YES	YES	YES	NO	NO	NA	NA	NO	NO	YES	NO	YES	NO	NO	5
Bebop	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	NO	YES	NO	YES	5
Cope	NO	NO	YES	YES	NO	NO	NA	NO	YES	NO	NO	YES	NA	NA	NO	4
Quarry	NO	NO	YES	YES	NO	NO	NO	NA	NO	NO	NO	NO	NA	NO	YES	3
Starbase	YES	NO	NO	NA	NO	NO	NO	NO	NO	YES	NO	NO	NA	NO	YES	3
PawSwap	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	YES	NO	NO	NO	NO	3

3.4.1 Technical Architecture of Treasury-Governed DAOs

Treasury-governed Decentralized Autonomous Organizations (DAOs) rely on a modular smart-contract architecture that coordinates collective decision-making, fund management, and operational execution without centralized intermediaries. Their design typically integrates three core components: governance modules, treasury or vault systems, and proposal-execution frameworks. The governance module administers token-weighted or role-based voting procedures, maintains quorum and threshold rules, enforces delegation logic, and records decisions immutably on-chain. Treasury contracts safeguard protocol funds, commonly denominated in native tokens, stablecoins, or yield-bearing assets, and expose controlled interfaces for deposit, withdrawal, and budget allocation. DAO actions are mediated by a proposal-and-execution engine, in which participants submit spending requests, parameter changes, or strategic initiatives as executable transactions. Upon successful governance approval, the execution engine interacts with the treasury or downstream protocol modules to implement the authorized action [202].

Advanced implementations incorporate timelock contracts, which introduce mandatory execution delays to mitigate governance attacks, and multisignature safeguards, which provide an additional layer of verification for high-risk transactions. Some architectures introduce modular sub-DAOs or working groups, each with specialized treasuries under the broader governance protocol. Oracle systems may be integrated to verify off-chain conditions or budget triggers, though such dependencies increase the DAO's attack surface. Because treasury governance directly controls protocol funds and operational parameters, its architectural security

hinges on the integrity of votes, resistance to governance capture, the correctness of proposal execution, and robust treasury access controls. This model enables scalable, transparent, community-driven resource allocation but simultaneously exposes the protocol to strategic manipulation and governance-based exploits [202]. Figure 14(c) shows the architecture of this category.

3.4.2 Platforms of Treasury-Governed DAOs

This section briefly lists and explains the platforms in this category.

- **1inch [203]**: A decentralized exchange aggregator governed by a DAO. Treasury revenues are allocated by token holders to support ecosystem development, liquidity incentives, and protocol improvements.
- **PieDAO [204]**: A decentralized asset management collective that creates tokenized index funds whose protocol-managed treasury is governed by the DAO. Revenues collected are deployed via governance-approved mechanisms to support liquidity, incentives, and community programs.
- **BarnBridge [205]**: A DeFi protocol offering structured financial products. Its DAO treasury manages revenues to fund ecosystem incentives, risk management strategies, and protocol development.
- **Reflexer Finance [206]**: Issuer of the RAI stablecoin. DAO-led treasury governance ensures sustainable growth by allocating resources to development, liquidity strategies, and community-driven initiatives.
- **PlutosDAO [207]**: A cross-chain synthetic asset protocol governed by its DAO. Treasury-controlled revenues are used to fund incentives, support liquidity, and expand ecosystem adoption.

In conclusion, treasury-governed DAOs represent a governance-centric economic model in which value is accumulated, stewarded, and redeployed through decentralized decision-making processes rather than distributed directly to users. The platforms in this category offer moderate functional coverage but excel in treasury allocation mechanisms, governance proposals, strategic budgeting, and community-driven development. Unlike revenue-sharing or token-incentive models, treasury-oriented systems prioritize long-term ecosystem sustainability over short-term yield, emphasizing transparency, accountability, and collective ownership. The comparative analysis shows that while DAOs in this category offer fewer financial primitives, they compensate with deep governance infrastructure and structured reinvestment strategies. This creates an operational environment suited for protocol evolution, risk management, and strategic incentive design, albeit at the cost of narrower functional utility. Treasury-governed DAOs, therefore, highlight a fundamentally different philosophy of value generation, one rooted in shared capital pools and collective decision rights.

Table 5: Platforms - Treasury-Governed DAOs

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
1inch	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
PieDAO	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
BarnBridge	NO	NO	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	NO	NO	YES	8
Reflexer Finance	NO	YES	NO	YES	YES	NO	NO	NA	NO	YES	YES	NO	YES	NO	YES	7
PlutosDAO	NO	NO	YES	YES	NO	NO	NO	NO	NO	YES	YES	NO	YES	NO	YES	6

3.5 Zero-Fee or Subsidized Models

The broad study also includes platforms that seek adoption by removing fees or heavily subsidizing transactions. These systems typically rely on alternative revenue models, treasury support, or external incentives instead of conventional fee extraction. Their main objective is to reduce friction, improve accessibility, and make on-chain participation more attractive, especially for small-scale users and early adopters [69, 71, 70].

3.5.1 Technical Architecture of Zero-Fee or Subsidized Models

Zero-fee or subsidized DeFi models depart from conventional fee-based exchange or liquidity frameworks by removing, reducing, or externally funding transaction costs. Their design typically integrates three primary components: a subsidy-financing module, a fee-override execution engine, and a liquidity coordination layer that maintains market operations despite suppressed fee revenues. In these architectures, the DEX or protocol's execution layer is configured to bypass standard swap-fee deductions, while the subsidy module, funded by protocol treasuries, token emissions, strategic partnerships, or external sponsors, compensates liquidity providers (LPs) for the absence of fee income. The liquidity layer aggregates and tracks LP stakes, adjusts reward formulas, and provides real-time liquidity states to the execution engine [208].
Some implementations employ token-based emissions as substitutes for fees, rewarding LPs with governance or utility tokens whose emission curves are encoded in smart-contract schedules. Others rely on treasury-driven reimbursements or sponsorship mechanisms, in which a governing entity periodically allocates funds to maintain LP incentives and ensure liquidity depth. Because fee subsidies distort natural market-clearing mechanisms, oracle modules may be used to track effective costs, slippage thresholds, and subsidy burn rates. Governance contracts determine funding frequencies, emission decay rates, and sustainability constraints, rendering governance integrity critical to the model's long-term viability. Although zero-fee architectures can accelerate early-stage adoption and reduce user friction, their dependence on external subsidies exposes the protocol to sustainability risks, treasury depletion, and incentive misalignment if subsidy mechanisms are improperly calibrated [208]. Figure 14(d) shows the architecture of this category.

3.5.2 Platforms of Zero-Fee or Subsidized Models

This section briefly lists and explains the platforms in this category.

- **Jupiter [209]**: Built on Solana, the liquidity aggregator offers zero-fee swaps. It subsidizes transactions by routing through optimized liquidity sources, improving accessibility for small-scale traders.
- **PoolTogether [210]**: A no-loss savings protocol where users deposit funds into prize pools. Instead of charging fees, yields are pooled to reward participants through prize drawings, subsidizing user participation.
- **CowSwap [211]**: Operating as a decentralized exchange aggregator, it eliminates trading fees through batch auctions. It leverages miner-extractable value (MEV) protection to subsidize transactions and improve execution prices.

- **Matcha [212]**: Built on the 0x Protocol, this decentralized exchange aggregator provides zero-fee trading by sourcing liquidity across multiple DEXs and subsidizing user costs through optimized routing.

- **Slingshot [213]**: Designed as a decentralized trading platform that offers gas-fee subsidies for users. It enhances accessibility by combining zero-fee swaps with competitive aggregation across liquidity sources.

Overall, the zero-fee or subsidized models category underscores the role of cost-efficiency as a strategic differentiator in DeFi. Platforms in this space reduce or eliminate transaction fees by relying on treasury subsidies, liquidity incentives, MEV-resistant routing, or innovative batch-execution mechanisms. This model significantly lowers the barrier to entry for smaller users and enhances accessibility, making these platforms attractive alternatives to high-fee environments. However, the analysis reveals significant structural limitations: most platforms in this category lack advanced features such as real-world asset tokenization, NFT utilities, GameFi components, or AI-driven enhancements, thereby constraining their integration into the broader ecosystem. Furthermore, reliance on subsidies or external incentive sources raises sustainability concerns, particularly when treasury reserves are finite or market conditions shift. Despite these challenges, the strongest performers in this category successfully combine foundational financial primitives, such as DEX logic, cross-chain routing, staking, and identity modeling, with efficient execution layers. The category highlights how fee minimization can coexist with functional versatility, positioning zero-fee systems as key enablers of user growth. Their architectural choices also surface specific risks related to routing manipulation and MEV interactions.

Table 6: Platforms – Zero-Fee or Subsidized Models Category

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
Jupiter	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	11
PoolTogether	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	NO	YES	10
CowSwap	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	7
Matcha	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	NO	YES	NO	YES	6
Slingshot	YES	NO	NO	NA	NO	NO	NO	YES	YES	YES	NO	NO	NO	NO	YES	5

3.6 Insurance or Coverage-Based

Another major category in the broad study consists of platforms that pool user premiums and provide coverage against risks such as smart contract exploits, exchange failures, and extreme volatility. These systems play an important role in reducing uncertainty across the DeFi ecosystem and in supporting broader participation by introducing decentralized forms of risk mitigation [69, 71, 70, 214].

3.6.1 Technical Architecture of Insurance and Coverage-Based

Insurance and coverage-based DeFi platforms implement decentralized risk pooling and claims processing mechanisms through a modular smart-contract architecture designed to protect against protocol failures, security breaches, market anomalies, and other on-chain events. Architecturally, these systems are organized into three principal modules: the underwriting pool, the coverage issuance engine, and the claims assessment and payout subsystem. The underwriting pool aggregates capital contributed by liquidity providers or stakers

who commit funds to back risk exposures in exchange for yield, premiums, or governance rights. Each underwriting pool is parameterized by coverage capacity, risk coefficients, lock-up constraints, and exposure diversification rules, which are encoded directly in the pool contract [215].

Coverage issuance is handled by dedicated smart contracts that allow users to purchase policies specifying a coverage target (e.g., a lending protocol, DEX, or bridge), coverage duration, insured amount, and premium rate. These parameters are evaluated using pricing functions derived from historical risk, pool capacity, and protocol-level indicators. Claims assessment is performed through one of three architectural models: governance-based adjudication, oracle-triggered automated payouts, or hybrid models that combine decentralized voting with verifiable incident data. In governance-driven systems, token holders evaluate claims proposals and authorize payouts via quorum-based voting. In oracle-driven models, predefined events, such as smart contract exploits or peg deviations, trigger deterministic payout logic [215].

The payout subsystem withdraws funds from the underwriting pool in accordance with predefined settlement rules, ensuring that liquidity providers bear losses in proportion to their stakes. Governance contracts oversee premium curves, risk parameters, dispute mechanisms, and treasury reserves, shaping the platform's solvency and resilience under correlated-risk environments. Because these architectures depend on secure oracle inputs, reliable adjudication mechanisms, and well-calibrated economic incentives, insurance protocols face distinctive risks, including oracle manipulation, governance capture, fraudulent claims, and undercapitalization during systemic events [215]. Figure 14(e) shows the architecture of this category.

3.6.2 Platforms of Insurance and Coverage-Based

This section briefly lists and explains the platforms in this category.

- **Bumper Finance [216]**: Provides decentralized protection against price volatility. Users pay premiums to secure a protected price floor for assets, with pooled funds covering losses.
- **Neptune Mutual [217]**: Offers parametric insurance for DeFi protocols and exchanges. Premiums are pooled into cover markets, and claims are resolved through on-chain governance.
- **DSLA Protocol [218]**: Enables users to hedge against performance risks such as service downtime or yield fluctuations. Premium pools compensate covered parties when agreed conditions are not met.
- **B.Protocol [219]**: Enhances DeFi lending platforms with backstop liquidity. Users contribute funds to a shared pool that protects against liquidations while earning protocol fees.
- **InsurAce [220]**: A multi-chain insurance protocol offering coverage against smart contract hacks, stablecoin depegs, and exchange failures. Premiums are pooled to support claim payouts and ecosystem stability.
- **Tidal Finance [221]**: Provides customizable insurance pools where users set parameters for risk and coverage. Premium revenues are shared collectively to backstop losses across DeFi applications.
- **Nexus Mutual [222]**: A decentralized insurance mutual offering coverage for smart contract exploits and exchange risks. Members contribute to a shared capital pool that pays out validated claims.

- **Ease (EASE) [223]**: A decentralized DAO-based "Uninsurance" protocol where users deposit into yield-generating vaults and coverage is activated only if a security incident occurs. There is no upfront premium; losses are shared across participants via protocol mechanisms.
- **OpenCover [224]**: Aggregates decentralized insurance products into a unified interface. Premiums are allocated to coverage pools, enabling users to access diversified protection against DeFi risks.

In summary, insurance and coverage-based platforms fill a critical gap in the DeFi ecosystem by providing mechanisms to mitigate risks arising from smart-contract exploits, liquidity failures, price crashes, and cross-protocol dependencies. Although their functional breadth is narrower than that of multi-purpose platforms, their architecture is notably sophisticated, incorporating underwriting pools, coverage issuance engines, risk-pricing systems, and incident-adjudication frameworks. The analysis shows that leading platforms effectively balance yield generation, staking, cross-chain capabilities, governance, and privacy protections while prioritizing capital efficiency and claim reliability. Their design reinforces trust, an essential prerequisite for institutional and mainstream adoption, by offering decentralized alternatives to traditional insurance systems. However, the category also highlights systemic challenges: oracle dependencies, undercapitalization risks, and governance-based claim adjudication can all introduce inconsistencies or vulnerabilities. When viewed alongside the other categories, insurance platforms appear less diversified but more specialized, playing an indispensable role in stabilizing the broader DeFi landscape.

Table 7: Platforms – Insurance or Coverage-Based Category

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
Bumper Finance	NO	NO	YES	YES	YES	YES	NO	NO	NO	YES	YES	NO	YES	YES	YES	9
Neptune Mutual	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	YES	NO	YES	NO	YES	9
DSLA	NO	NO	YES	YES	NO	NO	NO	YES	YES	YES	YES	NO	NA	YES	YES	8
B.Protocol	NO	YES	YES	YES	NO	NO	NA	YES	NO	YES	YES	NO	YES	NO	YES	8
InsurAce	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Tidal Finance	NO	NO	YES	YES	NO	NO	NA	YES	NO	YES	YES	NO	YES	NO	YES	7
Nexus Mutual	NO	NO	YES	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	7
ease (EASE)	NO	NO	YES	YES	NO	NO	NO	NA	NO	YES	YES	NO	YES	NO	YES	6
OpenCover	NO	NO	NO	NO	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	5

3.7 Yield Optimization

The broad study next considers platforms focused on yield optimization, that is, protocols that aggregate, reallocate, and compound user deposits across multiple strategies in order to maximize returns. By automating complex yield-farming and reinvestment logic, these platforms make advanced strategies more accessible to a wider user base [69, 71, 70].

3.7.1 Technical Architecture of Yield Optimization

Yield optimization platforms automate the deployment of user assets across multiple DeFi protocols to maximize returns through compounding, reward harvesting, and strategy rotation. Their architecture is typically organized around three core smart-contract modules: the vault contract, the strategy module, and the reward harvesting and reinvestment subsystem. The vault contract serves as an asset-aggregation layer, pooling user deposits and issuing vault-specific share tokens representing proportional ownership of the underlying assets. The vault maintains state variables for Net Asset Value (NAV), total shares, and strategy allocations, enabling transparent accounting and proportional withdrawal logic [225].

External deployment logic is encoded in modular strategy contracts, each defining a specific yield-generating pathway such as lending, liquidity provision, staking, or liquidity mining. Strategies interact autonomously with external DeFi protocols and expose standardized interfaces for depositing, withdrawing, reporting performance, and estimating expected annualized returns. This modularity allows platforms to run multiple simultaneous strategies while dynamically reallocating capital based on performance, gas efficiency, and risk constraints. A dedicated reward harvesting subsystem periodically collects incentive tokens or accumulated interest from deployed strategies and executes auto-compounding operations by swapping, staking, or reinvesting rewards back into the vault to increase share value [225].

To ensure robustness, yield optimizers frequently integrate oracle modules for asset valuation, slippage estimation, and cross-protocol pricing, while governance contracts regulate strategy whitelisting, performance fee parameters, and emergency pause mechanisms. Although this architecture provides enhanced capital efficiency and automation, it also introduces layered dependency risk across underlying protocols, amplifying vulnerabilities related to liquidation cascades, strategy malfunction, oracle inaccuracies, and composability failures [225]. Figure 14(f) shows the architecture of this category.

3.7.2 Platforms of Yield Optimization

This section briefly lists and explains the platforms in this category.

- **Snowball [226]**: A yield optimization protocol on Avalanche that automates compounding strategies. It reallocates user deposits across farms to maximize returns while minimizing manual intervention.
- **Jones DAO [227]**: provides structured yield strategies for options markets. It automates hedging and yield generation, making advanced derivatives strategies accessible to users.
- **Clip Finance [228]**: A multi-chain yield optimizer that reallocates assets across protocols. It uses automated strategies to optimize yields while simplifying cross-chain portfolio management.
- **Yield Yak [229]**: A yield aggregator on Avalanche offering auto-compounding strategies. It improves efficiency by routing assets to high-yield farms and automatically reinvesting rewards.
- **Metronome Synth [230]**: A yield optimization protocol combining synthetic assets with automated farming. It allows users to maximize returns by allocating collateral into yield-bearing strategies.
- **Tenderize [231]**: enables liquid staking derivatives with auto-compounding yield. Users stake assets and receive tokenized derivatives that can be used in DeFi while accruing staking rewards.
- **Alchemix [232]**: A self-repaying loan protocol that channels collateral into yield strategies. The yield generated automatically pays down debt, combining borrowing and yield optimization.
- **Ratio Finance [233]**: A Solana-based protocol offering overcollateralized stablecoins and yield optimization. It reallocates collateral into farming strategies to enhance capital efficiency.
- **Shell Protocol [234]**: provides composable stablecoin and liquidity strategies. It automates yield opportunities by routing assets into optimized liquidity pools and farming positions.

- **Yearn Finance [235]**: One of the earliest yield aggregators, automating yield farming through its Vaults. It reallocates deposits across protocols and compounds rewards to maximize efficiency.
- **Stake DAO [236]**: A yield optimizer that aggregates strategies across multiple DeFi protocols. It automates staking, farming, and rebalancing while allowing users to participate in DAO governance.
- **HyperJump [237]**: A multi-chain yield farming and automated market maker protocol that reallocates user deposits into farms to maximize returns across supported ecosystems.
- **Penguin Finance [238]**: A yield optimization platform on Avalanche. It automates compound interest strategies through its yield-farming products while offering gamified features to enhance user engagement.
- **Kamino Finance [239]**: A Solana-based yield optimizer designed for concentrated liquidity positions. It automates rebalancing and compounding strategies to maximize efficiency for liquidity providers.
- **Idle Finance [240]**: A protocol for optimizing yields on stablecoins and tokens. It reallocates deposits across lending protocols and offers risk-adjusted tranches to suit user preferences.
- **Goat Protocol [241]**: A yield optimization platform that automates cross-chain farming strategies. It reallocates liquidity dynamically to capture the highest yields across multiple networks.
- **Origin Ether [242]**: provides a liquid staking derivative for ETH that accrues staking yield. It allows users to retain liquidity while participating in yield strategies across DeFi.
- **Jasper Vault [243]**: A yield aggregator offering automated vault strategies. It channels user deposits into diversified farming opportunities to optimize returns while reducing management complexity.
- **YieldFi [244]**: A yield farming platform that automates reward harvesting and compounding. It distributes optimized strategies to users, simplifying access to sustainable DeFi yields.
- **Cropper Finance [245]**: A Solana-based yield optimizer. It enables auto-compounding and allocation of user deposits into high-yield farms to maximize return efficiency.
- **Antfarm Finance [246]**: A yield optimization platform that reallocates liquidity across automated strategies. It maximizes user returns by dynamically balancing capital across high-yield pools.
- **Compound Blue [247]**: extends Compound's lending model with optimized strategies. It channels user deposits into curated markets while automating yield accrual and reinvestment.
- **Friktion [248]**: A structured yield protocol on Solana offering automated options strategies. It provides diversified vaults that generate optimized risk-adjusted returns for depositors.
- **Ovix (0vix) [249]**: A lending and yield optimization platform on Polygon. It reallocates assets through money markets to optimize yield opportunities while supporting cross-chain liquidity.

- **Sonne Finance [250]**: A lending protocol on Optimism that enables yield optimization through collateralized lending markets. Users earn optimized returns by supplying assets into its liquidity pools.
- **Rebalance Finance [251]**: automates portfolio reallocation across DeFi strategies. It maximizes yield through continuous optimization while maintaining target risk profiles.
- **Crema Finance [252]**: A Solana-based liquidity protocol offering optimized yield for concentrated liquidity positions. It automates rebalancing and compounding to increase capital efficiency.
- **Pickle Finance [253]**: A yield aggregator that optimizes farming strategies through automated vaults. It reallocates user funds across protocols to enhance yield and reduce complexity.
- **EarnPark [254]**: A yield optimization platform that automates compounding strategies for stablecoins and tokens. It reallocates liquidity to farms with competitive yields to maximize efficiency.
- **Dual Finance [255]**: A protocol offering structured products and yield optimization strategies. It enables users to earn optimized returns through options-based vaults and automated strategies.
- **Teahouse [256]**: A yield optimization protocol offering actively managed vault strategies. It reallocates user deposits across DeFi opportunities to generate consistent, risk-adjusted returns.
- **xToken Terminal [257]**: provides automated yield strategies for governance tokens and liquidity positions. It simplifies staking and liquidity management through structured optimization products.
- **Mellow Protocol [258]**: A modular yield optimization platform that enables custom strategy vaults. It automates allocation and compounding, making advanced yield farming accessible to users.
- **Koi Finance [259]**: A cross-chain yield optimizer that reallocates liquidity across multiple networks. Tokenized vaults allow users to capture competitive yields with minimal manual effort.
- **Hord [260]**: offers tokenized asset baskets and yield optimization strategies. It automates portfolio management, enabling users to access diversified yield opportunities through DeFi indices.
- **Menthol Protocol [261]**: A sustainable yield platform that automates carbon offset strategies. It combines yield optimization with environmental sustainability by allocating revenues to green initiatives.
- **Tulip Protocol [262]**: A Solana-based yield aggregation protocol (formerly known as SolFarm). It auto-compounds farming rewards and reallocates liquidity across high-yield pools to maximize user returns.
- **BracketX [263]**: provides structured products and yield optimization strategies using volatility trading. It automates options-based strategies to deliver risk-adjusted yield opportunities.
- **Harvest Finance [264]**: A multi-chain yield aggregator that deploys automated strategies across DeFi protocols. It harvests and compounds rewards to optimize user returns.

- **Beefy Finance [265]**: A leading multi-chain yield optimizer. It offers automated vaults that reallocate and compound assets, maximizing returns while simplifying farming strategies.
- **NillaConnect [266]**: A cross-chain yield optimizer that automates the allocation of user assets. It streamlines access to farming opportunities by compounding returns across supported networks.
- **Lagoon [267]**: A DeFi protocol providing automated yield strategies. It reallocates liquidity into optimized pools and compounds rewards to maximize user efficiency.
- **MorFi [268]**: A yield optimization platform that distributes user deposits into multiple farming strategies. It automates harvesting and reinvestment to enhance long-term returns.
- **Francium [269]**: A Solana-based yield aggregator offering leveraged yield farming. It reallocates user assets into high-yield strategies, compounding rewards to optimize returns.
- **TokensFarm [270]**: A yield farming-as-a-service platform. It enables projects to launch farming campaigns while optimizing the distribution of rewards to liquidity providers.
- **Filet Finance [271]**: A staking and yield optimization protocol for Filecoin. It automates delegation and compounding, allowing users to earn optimized yields from storage mining.
- **maxAPY [272]**: A multi-chain yield optimizer that aggregates high-yield opportunities. It auto-compounds rewards and reallocates liquidity to maximize annualized returns.
- **Reaper Farm [273]**: A Fantom-based yield optimization platform. It automates compounding strategies across multiple DeFi protocols to maximize yields for users.

Taken together, yield optimization platforms illustrate how automation, composability, and integration of cross-protocol strategies can maximize capital efficiency for users. These systems abstract the complexity of yield farming by deploying modular vaults, strategy contracts, and auto-compounding engines that interact autonomously with multiple DeFi protocols. The strongest platforms exhibit broad functional coverage spanning staking, lending, cross-chain operations, NFT utilities, governance, GameFi, and AI-assisted optimization, demonstrating a high level of architectural sophistication. However, this breadth also introduces layered dependency risk: since yield optimizers depend on numerous external protocols, failures such as liquidation cascades, oracle inaccuracies, or strategy malfunctions propagate quickly and amplify systemic instability. Compared to revenue-sharing or token-incentive models, yield optimizers are more functionally diverse but also significantly more exposed to composability risks. Their role within the DeFi ecosystem is therefore twofold: to provide accessible, high-performance yield aggregation while also bearing the risks of the protocols they leverage.

3.8 Speculation or Leverage-Driven Platforms

The broad study also identifies a category of platforms whose revenues are driven primarily by trading fees, funding rates, and leveraged speculation. These protocols attract high-volume traders and offer advanced trading instruments, including perpetual swaps, options, and structured derivatives [69, 71, 70].

Table 8: Platforms – Yield Optimization Platforms Category

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
Snowball	YES	YES	YES	YES	YES	NA	NO	YES	YES	NO	YES	YES	YES	YES	YES	12
Jones DAO	YES	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	11
Clip Finance	NO	NO	YES	YES	NO	NA	YES	YES	YES	NO	YES	NO	YES	YES	YES	9
Yield Yak	YES	NO	YES	YES	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
Metronome Synth	NO	YES	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	YES	YES	9
Tenderize	YES	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Alchemix	NO	YES	YES	YES	YES	NA	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Ratio Finance	NO	YES	YES	YES	YES	NO	NO	NA	NO	NO	YES	NO	YES	YES	YES	8
Shell Protocol	YES	NO	YES	YES	NO	NO	NO	YES	YES	NA	YES	NO	YES	NO	YES	8
Yearn Finance	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Stake DAO	NO	NO	YES	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
HyperJump	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	NO	YES	YES	NO	YES	8
Penguin	YES	NO	YES	YES	NO	NO	NO	NO	YES	NO	YES	YES	YES	NO	YES	8
Kamino Finance	YES	YES	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Idle Finance	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Goat Protocol	NO	NO	YES	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
Origin Ether	NO	YES	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Jasper Vault	NO	NO	YES	YES	NO	YES	NO	YES	YES	NO	NO	NO	YES	YES	YES	8
YieldFi	NO	NO	YES	YES	YES	NO	NA	YES	YES	NO	NO	NO	YES	NO	YES	7
Cropper Finance	YES	NO	YES	YES	NO	NO	NO	NA	YES	NO	YES	NO	YES	NO	YES	7
Antfarm Finance	YES	NO	YES	YES	NO	NO	NO	YES	NO	NA	YES	NO	YES	NO	YES	7
Compound Blue	NO	YES	YES	NO	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Friktion	NO	YES	YES	NO	NO	YES	NO	YES	YES	NO	NO	NO	YES	NO	YES	7
Rebalance Finance	NO	NO	YES	YES	NO	NO	YES	YES	NO	NO	NO	NO	YES	YES	YES	7
Crema Finance	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	NO	NO	YES	NO	YES	7
Pickle Finance	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
EarnPark	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	YES	YES	7
Ovix	NO	YES	YES	YES	NO	NO	NO	NA	NO	NA	YES	NO	YES	NO	YES	6
Sonne Finance	NO	YES	YES	YES	NO	NO	NO	NA	NO	NA	YES	NO	YES	NO	YES	6
Dual Finance	NO	YES	YES	YES	NO	YES	NO	NA	NO	NO	YES	NO	NO	NO	YES	6
xToken Terminal	NO	YES	YES	NA	NO	NO	NO	YES	YES	NO	NO	NO	YES	NO	YES	6
Mellow Protocol	NO	NO	YES	YES	NO	NA	NO	YES	YES	NO	NO	NO	YES	NO	YES	6
Koi Finance	YES	NO	YES	YES	NO	NO	NO	NA	NO	NO	YES	NO	YES	NO	YES	6
Hord	NO	NO	YES	YES	NO	NO	NO	YES	NO	NA	YES	NO	YES	NO	YES	6
Menthol Protocol	NO	NO	YES	YES	NO	NO	NO	YES	YES	NA	YES	NO	NO	NO	YES	6
Tulip	NO	YES	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	6
Harvest Finance	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	6
Beefy Finance	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	6
Teahouse	NO	NO	YES	NA	NO	NO	NO	YES	YES	NA	NO	NO	YES	NA	YES	5
BracketX	NO	NO	YES	YES	NO	YES	NO	NA	NO	NA	NO	NO	YES	NO	YES	5
NillaConnect	NO	YES	YES	NO	NA	NO	NO	YES	NO	NA	NO	NO	YES	NO	YES	5
Lagoon	NO	NO	YES	NO	NO	NO	NO	YES	NO	NO	YES	NO	YES	NA	YES	5
Francium	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	5
TokensFarm	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	5
Filet Finance	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	5
maxAPY	NO	NO	YES	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	YES	YES	5
Reaper Farm	NO	NO	YES	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	4
MorFi	YES	NO	YES	NA	NO	NO	NO	NA	NO	NA	NO	NO	NA	NO	YES	3

3.8.1 Technical Architecture of Speculation or Leverage-Driven

Speculation- and leverage-driven DeFi platforms implement architectures that enable users to take amplified exposure to asset price movements through perpetual futures, margin trading, leveraged tokens, or synthetic-leverage pathways. Their design typically integrates four tightly coupled modules: collateral and margin management, position-tracking and funding-rate engines, price-oracle subsystems, and liquidation executors. Collateral contracts lock user assets and compute real-time collateralization ratios using oracle-provided prices. The position-tracking engine maintains long and short positions, updates leverage multipliers, and enforces continuous funding-rate transfers between opposing market sides in perpetual-futures architectures. Oracle modules supply time-synchronized reference prices that govern mark-to-market valuation, liquidation thresholds, and risk checks [274].

When a position's notional value exceeds safe leverage parameters, the liquidation subsystem initiates automated deleveraging or full liquidation, often allowing third-party liquidators to repay debt or close positions in exchange for incentives. Some architectures separate the execution and settlement layers, in which trades are matched off-chain while settlement and state updates occur on-chain, thereby improving latency but increasing dependence on trusted sequencers. Governance contracts determine leverage caps, maintenance margins, insurance fund allocations, and liquidation penalties, making the platform highly sensitive to governance integrity, oracle reliability, and the correctness of funding rate equations. The architectural interdependence among leverage, collateral, price oracles, and liquidation logic introduces systemic risks, including cascading liquidations, oracle-driven insolvency, and strategic price manipulation in thin-liquidity

markets [274]. Figure 14(g) shows the architecture of this category.

3.8.2 Platforms of Speculation or Leverage-Driven

This section briefly lists and explains the platforms in this category.

- **Vela Exchange [275]**: A decentralized perpetuals trading platform offering synthetic asset markets, isolated margin, and liquidity provision capabilities. It captures revenue from trading fees and funding rates on leveraged positions.
- **UniDex [276]**: A decentralized exchange aggregator supporting leveraged trading. It combines liquidity aggregation with perpetual contracts to capture revenue from fees and speculative positions.
- **Polynomial Protocol [277]**: Automates options and perpetual strategies on Optimism. It generates revenue through trading fees while providing users with structured exposure to derivatives markets.
- **Parcl [278]**: A decentralized real estate derivatives platform enabling speculation on property price indices. It monetizes through trading activity and funding rates in synthetic real estate markets.
- **PowerDEX [279]**: A decentralized derivatives exchange offering leveraged positions. Its revenue model is based on transaction fees and funding payments from perpetual trading.
- **dYdX [280]**: A leading decentralized derivatives exchange supporting perpetual swaps with high leverage. It earns revenues from trading fees and funding rates while serving professional-grade traders.
- **Zeta Markets [281]**: A Solana-based derivatives protocol offering perpetuals and options. It captures revenue from funding payments and trading fees across leveraged positions.
- **Concordex [282]**: A decentralized exchange on Concordium focusing on derivatives. It enables leveraged trading and generates revenue from trading fees and funding mechanisms.
- **Contango [283]**: A decentralized derivatives protocol offering fixed-maturity futures. It derives revenues from trading activity and funding spreads, catering to speculative trading demand.
- **Evo Exchange [284]**: A cross-chain, interblockchain DEX using MPC technology for native asset trading. It combines trading, liquidity, and derivatives across chains, generating revenue from trading fees.
- **Dopex [285]**: A decentralized options protocol that provides automated options vaults and leveraged strategies. It generates revenue from trading fees and option premiums.
- **Drift [286]**: A Solana-based decentralized exchange offering perpetual swaps with leverage. Revenues are derived from trading fees and funding rates within its on-chain order book.
- **Deri Protocol [287]**: Supports perpetual futures, options, and volatility trading. It monetizes through transaction fees and funding payments across leveraged derivatives markets.

- **Lyra [288]**: An options trading protocol built on Optimism. It generates income from option premiums and fees while enabling leveraged speculation in decentralized options markets.
- **SynFutures [289]**: A decentralized derivatives platform offering perpetual futures for any ERC-20 token. It derives revenue from trading fees and leveraged speculation.
- **Kwenta [290]**: A decentralized exchange for perpetual futures built on Optimism. It derives revenue from trading fees and funding rates, serving advanced traders with leverage.
- **GMX [291]**: A decentralized perpetual exchange supporting high-leverage trading of significant assets. It generates revenue from trading fees and funding payments, with a focus on low-slippage execution.
- **Thetanuts Finance [292]**: A structured products protocol offering automated options strategies. Its revenue model is based on option premiums and derivatives trading fees.
- **Opium [293]**: A derivatives protocol enabling customizable financial contracts (options, perpetuals, structured products). It derives revenue from trading fees and derivative premiums.
- **Rage Trade [294]**: A perpetual futures exchange on Arbitrum. It captures revenue from trading fees and funding rates, supporting advanced strategies with leveraged positions.
- **Kromatika Finance [295]**: A decentralized trading platform enabling limit orders and perpetual swaps. It generates revenue from trading fees and supports leveraged trading strategies.
- **RubyDex [296]**: A decentralized derivatives exchange offering perpetual contracts. Its fee-based model monetizes leveraged trading and high-volume speculative activity.
- **LN Exchange [297]**: A decentralized exchange supporting perpetual futures. Revenues are derived from trading fees and funding rates tied to leveraged positions.
- **FutureSwap [298]**: A decentralized perpetuals exchange with customizable leverage. It derives revenue from trading fees and funding payments on leveraged trades.
- **Siren [299]**: A decentralized options trading platform. It derives revenue from option premiums and trading fees, enabling leveraged speculation in digital assets.
- **Gearbox [300]**: A leverage protocol that provides composable leveraged credit accounts. It monetizes through borrowing fees while enabling leveraged strategies across DeFi protocols.
- **Opyn [301]**: A decentralized derivatives platform focused on options. It generates revenue through option premiums and trading fees within its on-chain markets.
- **Alpha Homora [302]**: A leveraged yield farming and lending protocol. Revenues are sourced from borrowing fees and funding rates associated with leveraged farming strategies.

- **Perpetual Protocol [303]**: A decentralized exchange for perpetual futures. It captures trading fees and funding payments, offering leveraged trading with on-chain transparency.
- **SEIF Finance [304]**: A derivatives exchange designed for perpetual contracts and leveraged products. It earns revenues through transaction fees and funding mechanisms tied to trading activity.
- **Carbon DeFi [305]**: A decentralized trading protocol enabling custom on-chain limit and range orders. It generates revenue from trading fees while supporting speculative trading strategies.
- **Panoptic [306]**: A perpetual options protocol built on Uniswap v3. It monetizes through fees on leveraged options positions, offering continuous exposure to volatility markets.
- **FCON DEX [307]**: A decentralized exchange supporting leveraged perpetual swaps. Its fee-based model captures revenues from trading activity and funding payments.
- **Apricot Finance [308]**: A Solana-based lending and leverage protocol. It generates revenue from borrowing fees and enables leveraged yield-farming strategies.
- **OptionBlitz [309]**: A decentralized platform for options and binary derivatives. It derives revenue from option premiums and transaction fees associated with leveraged contracts.
- **Optix [310]**: An options trading protocol that automates structured derivatives strategies. It monetizes through fees on option premiums and leveraged speculative activity.

Speculation or leverage-driven platforms embody the high-risk, high-reward segment of DeFi by offering derivatives, perpetual swaps, leveraged positions, and synthetic assets. These platforms require robust pricing mechanisms, deep liquidity, responsive execution layers, and reliable oracle systems. The comparative assessment shows that leading platforms cover core services such as staking, lending, derivatives, cross-chain functionality, and NFT-based utilities while optimizing their infrastructure for active traders. Their architecture is distinct from that of other categories owing to the central role of collateral management, margining systems, funding-rate mechanisms, and liquidation engines. Although this makes the category essential for sophisticated financial use cases, it also exposes it to oracle manipulation, liquidity mismatches, and extreme sensitivity to price volatility. Compared to yield-optimization or revenue-sharing categories, leverage-driven systems offer narrower functionality but significantly greater financial complexity.

3.9 Service Fee-Based Tools

The final category in this broad study includes platforms and tools that provide specialized services, such as dashboards, analytics, APIs, and risk monitoring, and that generate revenue through fees or subscriptions rather than through core financial activity. These systems serve as infrastructure, coordination, and monitoring layers that support broader DeFi adoption [69, 71].

Table 9: Platforms – Speculation or Leverage-Driven Category

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
Vela Exchange	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	NO	YES	NO	YES	12
UniDex	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	YES	NA	YES	11
Polynomial Protocol	YES	YES	YES	YES	YES	YES	NO	NO	YES	YES	YES	NO	YES	NO	YES	11
Parcl	YES	YES	YES	NO	YES	YES	YES	NA	YES	NO	YES	NO	YES	NO	YES	10
dYdX	YES	YES	YES	YES	NO	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	10
PowerDEX	YES	NO	YES	YES	YES	YES	NA	YES	NO	NA	YES	NO	YES	NO	YES	9
Zeta Markets	YES	NO	YES	YES	NO	YES	NO	YES	YES	NA	YES	NO	YES	NA	YES	9
Concordex	YES	YES	YES	YES	NO	YES	NO	NA	NO	YES	YES	NO	YES	NO	YES	9
Contango	NO	YES	YES	YES	NO	YES	NO	YES	YES	NA	YES	NO	YES	NO	YES	9
Evo Exchange	YES	YES	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NA	YES	9
Dopex	NO	NO	YES	YES	YES	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	9
Drift	YES	YES	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	9
Deri Protocol	NO	NO	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	YES	YES	9
Lyra	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	9
SynFutures	NO	NO	YES	YES	NO	YES	NO	YES	YES	YES	YES	NO	YES	NO	YES	9
Kwenta	NO	NO	YES	YES	YES	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	9
GMX	YES	NO	YES	YES	NO	YES	NO	YES	NO	NA	YES	NO	YES	NO	YES	8
Thetanuts Finance	NO	YES	YES	YES	NO	YES	NO	YES	NO	NA	YES	NO	YES	NO	YES	8
Opium	NO	NO	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
Rage Trade	YES	NO	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Kromatika Finance	YES	NO	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
FutureSwap	NO	NO	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
Siren	NO	NO	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	YES	YES	8
RubyDex	YES	NO	NO	NO	NO	YES	NA	YES	YES	YES	NO	NO	YES	NA	YES	7
LN Exchange	YES	NO	YES	NA	NO	YES	YES	NA	NO	NO	YES	NO	YES	NO	YES	7
Gearbox	NO	YES	YES	YES	NO	NA	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Opyn	NO	NO	YES	NO	YES	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Alpha Homora	NO	YES	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Perpetual Protocol	NO	NO	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Carbon (Carbon DeFi)	YES	NO	YES	NO	NO	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	7
Panoptic	NO	NO	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	7
SEIF FINANCE	YES	NO	NA	NA	NO	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	6
FCON DEX	YES	NO	YES	YES	NO	NO	NO	YES	NA	NO	NO	NO	YES	NO	YES	6
Apricot Finance	NO	YES	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	6
OptionBlitz	NO	NO	YES	YES	NO	YES	NO	NA	NO	NA	YES	NO	NO	NO	YES	5
Optix	NO	NA	YES	NO	NO	YES	NO	YES	NO	NA	NO	NO	NO	NO	YES	4

3.9.1 Technical Architecture of Service Fee-Based

Service fee-based tools in DeFi encompass a broad class of protocols that provide analytical, operational, monitoring, or automation services in exchange for usage-based fees. Their architecture is organized into three core subsystems: data acquisition and processing, service execution logic, and fee settlement modules. Data acquisition layers collect on-chain or cross-protocol state via event listeners, indexers, or oracle-fed data streams, and normalize it into structured representations for downstream computation. The service execution layer hosts specialized logic, such as on-chain risk scoring, transaction-simulation engines, compliance verifiers, automated rebalancers, or security-analysis modules, either implemented entirely on-chain or via hybrid off-chain computation anchored by on-chain verification proofs [311].

The fee-settlement subsystem enforces a deterministic compensation scheme for tool execution, typically using pay-per-use micropayments, subscription models, or fee flows rebated as gas. Smart contracts maintain metering variables that track resource usage (e.g., simulation calls, security checks, or monitoring intervals) and release funds via escrowed or direct-payment channels. Governance modules regulate pricing curves, service tiers, authorized tool upgrades, and treasury allocation for tool maintenance and development. Some service-fee-based architectures also incorporate staking or bonding-based security mechanisms, in which service providers must lock value to ensure honest execution, thereby linking economic security to operational integrity [311].

The architectural coupling between data ingestion, computation, and fee enforcement introduces unique risks: oracle manipulation can distort analytical outputs; faulty computation modules may produce incorrect risk assessments; and misconfigured fee mechanisms may lead to underfunded services or exploitation of tool-execution pathways. Nevertheless, the model provides a scalable, cost-effective foundation for delivering advanced DeFi services, including auditing, analytics, monitoring, and compliance [311]. Figure 14(h) shows the architecture of this category.

3.9.2 Platforms of Service Fee-Based

This section briefly lists and explains the platforms in this category.

- **IX Swap [312]**: A liquidity and trading platform for tokenized securities and real-world assets. It generates revenue through service fees on token issuance, custody, and liquidity provisioning.
- **Holdstation [313]**: A DeFi wallet and trading platform integrating perpetuals and asset management. It monetizes via service fees on trading, portfolio tools, and premium features.
- **Enzyme Finance [314]**: An on-chain asset management protocol offering customizable investment vaults. It charges service fees for vault creation, management, and performance monitoring.
- **RhinoFi [315]**: A layer-2 DeFi hub (formerly DeversiFi) providing swaps, yield, and cross-chain services. Revenues are derived from transaction service fees and bridging operations.
- **dHEDGE [316]**: A decentralized asset management platform enabling users to follow or create strategies. It generates service fees through performance-based charges on managed portfolios.
- **Furucombo [317]**: A DeFi tool that simplifies strategy building through a drag-and-drop interface. It monetizes by charging service fees on bundled transactions and advanced automation features.
- **Dolomite [318]**: A margin trading and portfolio management platform. It collects service fees on margin positions, lending services, and portfolio utilities.
- **CoinStats [319]**: A crypto portfolio management and analytics tool. Its revenue model relies on subscription fees for premium analytics and API-based portfolio services.
- **Delio [320]**: A crypto asset management and lending service. It generates revenue through service fees for custody, asset management tools, and lending activities.
- **Legato [321]**: A protocol on Move-based blockchains (e.g., Sui) offering fixed-rate vaults for liquid stakers. As staking APYs fluctuate, it enables users to lock in rewards via service fees on vault operations.
- **FlowX [322]**: A decentralized trading dashboard and analytics tool. It monetizes by charging service fees for advanced portfolio insights, API integrations, and premium features.
- **Maxbid Pro [323]**: A DeFi execution tool providing automated bidding and trading optimization. Revenues are derived from service fees for advanced order execution and strategy automation.
- **De.Fi [324]**: A security and analytics platform offering a crypto antivirus and yield monitoring dashboard. It generates fees through premium subscriptions and API access for institutional users.
- **Multichain [325]**: A cross-chain bridge and interoperability protocol that enables token transfers across blockchains. It generates revenue through service or bridge fees on cross-chain transactions.

- **Solrise Finance [326]**: A Solana-based asset management platform. It monetizes via service fees charged on fund creation, portfolio management, and performance metrics.
- **TheStandard.io [327]**: A decentralized protocol offering stablecoin issuance and asset management. It collects service fees on vault operations, borrowing, and collateral management.
- **Tokenlon [328]**: A decentralized exchange and settlement layer built on 0x Protocol. It generates revenue through service fees on swaps and settlement transactions.
- **Hedgehog [329]**: A DeFi portfolio manager and trading tool. It derives revenue from service fees for asset rebalancing, analytics, and premium trading features.
- **Interport Finance [330]**: A cross-chain DEX aggregator. Its service-fee model is tied to routing transactions and to providing interoperability across liquidity sources.
- **Soldex [331]**: A decentralized exchange on Solana that integrates AI-driven trading strategies. It generates service fees from swaps and advanced trading tools offered to users.
- **OpenOcean [332]**: A multi-chain DEX aggregator that provides optimal routing for token swaps. Its revenue model is based on service fees from aggregated trades and cross-chain transactions.
- **Degen Wallet [333]**: A DeFi wallet offering multi-chain support and built-in trading utilities. It monetizes through service fees on swaps, transfers, and integrated services.
- **0x [334]**: A decentralized exchange protocol providing infrastructure for token trading and liquidity aggregation. It generates revenues through service fees on API usage and transaction settlement.
- **AirSwap [335]**: A peer-to-peer decentralized trading protocol. It collects service fees from token swaps and provides infrastructure for secure, gas-efficient transactions.
- **Avata [336]**: A DeFi infrastructure platform offering risk management and analytics tools. It monetizes by charging fees for portfolio monitoring, APIs, and reporting services.
- **Crypto Valley Exchange [337]**: An exchange integrating regulated services with DeFi tools. Its revenue model is based on service fees from trading and asset management.
- **DZap [338]**: A DeFi execution tool that simplifies multi-step transactions into single-click operations. It collects service fees on bundled transactions and automation utilities.
- **Marginly [339]**: A DeFi margin trading and portfolio management tool. Its revenue model is based on service fees from leveraged trading and advanced portfolio services.
- **Akropolis [340]**: Provides yield optimization and financial primitives. It monetizes through service fees on vaults, asset management, and integrations.
- **Augur [341]**: A decentralized prediction market platform. It generates revenue through service fees on market creation, participation, and settlement.

- **Integral [342]**: A decentralized exchange optimized for large trades with minimal slippage. It monetizes through service fees on settlement and liquidity usage.
- **Router Nitro [343]**: A cross-chain liquidity aggregation protocol. It monetizes by charging fees on routed transactions.
- **Pika Protocol [344]**: Offers derivatives and perpetual futures trading. It collects service fees on leveraged transactions and efficient rollup execution.
- **Clipper [345]**: A DEX optimized for retail traders. It charges service fees on low-slippage swaps across curated pools.
- **DeGate [346]**: A layer-2 decentralized exchange built on zk-rollups. Its revenue model relies on service fees tied to trading transactions.
- **Dexed Finance [347]**: A decentralized trading and portfolio management tool. It generates revenue through service fees for swaps, portfolio analytics, and premium execution services.
- **Rubicon [348]**: A decentralized order book exchange on Optimism. It earns service fees on order execution and liquidity provision.
- **Erasure [349]**: A decentralized data marketplace generating fees from uploads, staking, and marketplace transactions.
- **Mangrove [350]**: A DEX protocol with programmable order books. It monetizes through service fees on trades and execution features.
- **Polymarket [351]**: A decentralized prediction and information market platform. It collects service fees from market creation and settlement.
- **Ave AI [352]**: A DeFi analytics and trading assistant platform that monetizes via subscription fees for advanced analytics and automation.
- **Metavisor [353]**: A yield and portfolio optimization tool for institutions, monetizing via service fees for strategy automation and treasury management.
- **LI.FI [354]**: A cross-chain liquidity aggregator offering APIs and SDKs. Its revenue model is based on routing service fees.
- **Keep Network [355]**: Provides privacy-focused infrastructure such as tBTC. It generates service fees from integrations and cryptographic tools.
- **Rocko [356]**: A DeFi infrastructure and portfolio management service that monetizes through fees on trading utilities and analytics.
- **Bamboo Relay [357]**: A decentralized order-book exchange built on the 0x protocol. It monetizes by charging service fees on order matching and settlement.

- **Ubik Capital [358]**: A validator and staking service provider generating revenue through fees for delegation and infrastructure.
- **Metrom [359]**: A DeFi analytics and monitoring platform. It charges fees for advanced risk monitoring, portfolio insights, and integration services.
- **ByBarter [360]**: A decentralized peer-to-peer trading platform that earns fees on swaps and escrow utilities.
- **PropellerSwap [361]**: A decentralized swap and liquidity routing platform. It monetizes through service fees on token swaps and through integrated liquidity-routing features.
- **Earnifi [362]**: A notification tool for unclaimed airdrops and rewards. It generates subscription-based revenue for premium alerts.
- **BetDEX Exchange [363]**: A decentralized sports betting exchange charging service fees on wagers and settlements.
- **Swoop Exchange [364]**: A DeFi trading aggregator monetizing via service fees on token swaps.
- **Duel Duck [365]**: A gamified DeFi prediction platform earning service fees from user wagers and gameplay interactions.
- **Droidex [366]**: A decentralized exchange aggregator supporting cross-chain swaps. It collects service fees on routed trades and advanced execution services.
- **Sprintcheckout [367]**: A crypto payment and checkout tool. It generates revenue through transaction and integration service fees for online merchants.

Finally, service-fee-based tools constitute a vital infrastructure layer within the DeFi ecosystem, providing middleware services such as routing, execution automation, identity modeling, asset management, privacy modules, and cross-chain functionality. Unlike other categories that focus on end-user financial products, platforms in this segment deliver operational utility that supports both users and protocols. The analysis shows that leading tools offer balanced functional coverage, combining DEX logic, support for derivatives, governance mechanisms, privacy protections, and infrastructure services. Their strength lies not in specialization but in enabling the broader ecosystem to operate more efficiently, securely, and transparently. However, because these platforms depend heavily on automation systems, oracle feeds, RPC nodes, relayers, and cross-chain executors, they exhibit heightened infrastructure-dependency risk. Compared to categories driven by token economics or leverage structures, service tools underpin interoperability, usability, and risk management across DeFi. Their intermediary role is critical to ecosystem reliability while exposing them to distinct vulnerabilities.

Table 10: Platforms – Service Fee-Based Tools Category

	DEX	Lending/Borrowing	Yield	Staking	Stablecoin	Derivatives	Real-World Asset	Cross-Chain	NFT	Identity and wallet	Governance	GameFi	Privacy and security	AI	DeFi infrastructure	MARK
IX Swap	YES	YES	YES	YES	NO	NO	YES	YES	YES	YES	YES	NO	YES	NO	YES	11
Holdstation	YES	NO	YES	YES	NO	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	11
Enzyme Finance	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	NO	YES	NO	YES	11
RhinoFi	YES	YES	YES	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	10
dHEDGE	YES	YES	YES	YES	NO	YES	NO	YES	YES	NO	YES	NO	YES	NO	YES	10
Furucombo	YES	YES	YES	YES	NO	NO	NO	YES	YES	NA	YES	NO	YES	NO	YES	9
Dolomite	YES	YES	YES	YES	NO	NA	NO	YES	YES	NO	YES	NO	YES	NO	YES	9
CoinStats	YES	NO	YES	YES	NO	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	9
Delio	YES	YES	YES	YES	NO	NO	NA	YES	YES	NO	NO	NO	YES	YES	NO	8
Legato	YES	NO	YES	YES	NO	YES	NA	NO	NO	NO	YES	NO	YES	YES	YES	8
Maxbid Pro	YES	YES	YES	YES	NO	YES	NA	YES	NO	NO	NO	NO	YES	NO	YES	8
De.Fi	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	NO	NO	YES	YES	YES	8
Multichain	NO	NO	YES	YES	YES	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
Solrise Finance	YES	NO	YES	YES	NO	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	8
TheStandard.io	NO	YES	YES	YES	YES	NO	NO	NO	YES	NO	YES	NO	YES	NO	YES	8
Tokenlon	YES	NO	YES	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	8
Hedgehog	YES	NO	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Interport Finance	YES	NO	YES	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
OpenOcean	YES	NO	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	8
Degen Wallet	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	8
0x	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
AirSwap	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	8
Avata	YES	YES	NO	YES	NO	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	8
FlowX	YES	NO	YES	YES	NO	NO	NA	NA	YES	NA	YES	NO	YES	NO	YES	7
Soldex	YES	NO	YES	YES	NO	NA	NO	NA	NO	NO	YES	NO	YES	YES	YES	7
Crypto Valley Exchange	NO	NO	NO	NO	YES	YES	NO	YES	YES	NA	YES	NO	YES	NO	YES	7
DZap	YES	NO	YES	NO	NO	NO	NA	YES	YES	NO	NO	NO	YES	YES	YES	7
Marginly	YES	YES	YES	NA	NO	YES	NO	YES	NO	NO	NO	NO	YES	NO	YES	7
Akropolis	NO	YES	YES	YES	YES	NO	NO	NO	NO	NO	YES	NO	YES	NO	YES	7
Augur	NO	NO	YES	YES	NO	YES	NO	NO	NO	YES	YES	NO	YES	NO	YES	7
Integral	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Router Nitro	YES	NO	YES	NO	NO	NO	NO	YES	YES	NO	YES	NO	YES	NO	YES	7
Pika Protocol	NO	NO	YES	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Clipper	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
DeGate	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Dexed	NO	NO	YES	YES	NO	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	7
Rubicon	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Erasure	NO	NO	YES	YES	NO	NO	NO	NO	NO	YES	YES	NO	YES	YES	YES	7
Mangrove	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	7
Polymarket	NO	NO	NO	YES	NO	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	7
Ave AI	NO	NO	YES	YES	NO	NO	NO	YES	YES	YES	NO	NO	YES	NO	YES	7
Metavisor	NO	NO	YES	YES	NO	NO	NO	YES	NO	NA	YES	NO	YES	NO	YES	6
Keep Network	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	6
Rocko	NO	YES	YES	NO	NO	NO	NO	YES	NO	YES	NO	NO	YES	NO	YES	6
LLFI	YES	NO	NO	NO	YES	NO	NA	YES	NO	NA	NO	NO	YES	NO	YES	5
Ubik Capital	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	5
Metrom	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	5
ByBarter	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	NO	NO	YES	NO	YES	5
Bamboo Relay	YES	YES	NA	NO	NA	NO	NO	NO	NO	NO	NO	NO	YES	NO	YES	4
PropellerSwap	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	4
Earnifi	NO	NO	NO	NO	NO	NO	NO	YES	YES	NO	NO	NO	YES	NO	YES	4
BetDEX Exchange	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	YES	NO	YES	NO	YES	4
Swoop Exchange	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	4
Duel Duck	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	YES	YES	NO	YES	4
Droidex	YES	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	YES	4
Sprintcheckout	NO	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	YES	YES	4

3.10 Comparative Insights from Category-Wise and Overall Platform Performance

This subsection synthesizes the category-level results to identify cross-category performance patterns and highlight structural differences across DeFi revenue models. Beyond category-level comparisons, Figure 15 provides a consolidated view of the final performance scores for all 284 evaluated platforms. This figure highlights not only the strongest representatives within each category but also the relative ranking of platforms across the broader ecosystem. Multi-functional platforms such as dForce and Horizon Protocol consistently achieve the highest aggregate scores, confirming that broad integration of financial primitives, cross-chain capabilities, governance, and privacy mechanisms is strongly correlated with systemic strength. Conversely, platforms with narrower design goals, including insurance systems, treasury-governed DAOs, and zero-fee models, tend to fall in the mid-to-low scoring ranges, reflecting the trade-off between specialization and functional breadth. Overall, the distribution underscores how category orientation constrains achievable performance ceilings and reveals a clear distinction between holistic financial ecosystems and single-purpose service architectures.

The comparative evaluation of 284 DeFi platforms across eight distinct categories further reveals significant variation in both functional coverage and strategic orientation. Each category reflects a different approach to value generation, governance, and ecosystem design, illustrating the diversity and specialization that characterize the decentralized finance landscape. As shown in Figure 15, protocol revenue sharing (74 platforms) and service fee-based tools (57 platforms) constitute the most substantial segments, followed by token-based incentivization (50), yield optimization platforms (48), speculation or leverage-driven models (36), insurance or coverage-based systems (9), and both treasury-governed DAOs and zero-fee or subsidized models (5 each). This distribution underscores a concentration of development efforts toward revenue-sharing and utility-based service architectures, while capital-efficient insurance and zero-fee models remain comparatively niche.

Within the protocol revenue-sharing category, dForce and Horizon Protocol stand out as the strongest performers, each achieving 13 of the 15 benchmark functionalities. Their extensive functional integration, including DEX logic, lending and borrowing, yield generation, staking, stablecoins, derivatives, real-world asset tokenization, cross-chain interoperability, privacy protections, and AI-enhanced mechanisms, positions them at the forefront of this model. In the token-based incentivization category, Hakka Finance leads with 12 of the 15 evaluated benchmarks [152]. Although the platform combines lending, staking, governance, and GameFi components within a reward-driven token economy, it lacks real-world asset tokenization, identity modeling, and AI-based tools.

Treasury-governed DAOs such as MakerDAO and BadgerDAO prioritize capital pooling and protocol-controlled value allocation rather than broad functional diversification. Their primary systemic strength lies in robust treasury management and mechanisms that reinforce long-term stability. However, this focus on financial stewardship results in a comparatively narrower service scope when contrasted with multifunctional DeFi ecosystems. Among zero-fee or subsidized models, Jupiter demonstrates the strongest performance, achieving 11 of the 15 benchmark functionalities [209]. Its integration of lending, staking, support for stablecoins, derivatives, cross-chain functionality, and privacy measures provides a robust operational foundation, albeit without real-world asset tokenization, NFT integration, or AI enhancements.

Within the insurance or coverage-based category, Bumper Finance and Neptune Mutual emerge as leading representatives [216, 217]. Both prioritize risk-protection mechanisms while offering yield generation, staking, and governance features. However, their selective functional coverage, most notably the absence of real-world asset tokenization and full AI integration, constrains their broader systemic capabilities. Yield optimization platforms exhibit similar variation, with Snowball achieving the highest functional coverage at 12 of the 15 assessed benchmarks [226]. The platform combines lending, staking, stablecoin operations, cross-chain interoperability, NFT features, governance, GameFi components, and AI-driven optimization tools, forming a comprehensive service suite.

For speculation or leverage-driven systems, Vela Exchange leads with 12 of the 15 benchmarks. Its functional coverage, spanning lending, staking, derivatives, cross-chain interoperability, and NFT functionality, aligns with the needs of active trading and leveraged strategies. However, it omits real-world asset tokenization and AI augmentation. Finally, in the service fee-based tools category, IX Swap, Holdstation, and Enzyme Finance achieve balanced performance, each meeting 11 of the 15 benchmarks [312, 313, 314]. These platforms provide user-facing financial infrastructure through fee-for-service models, integrating core DeFi components such as lending, derivatives, governance, and privacy safeguards, while differing in their support for cross-chain, NFT, and AI capabilities.

Taken together, the category-level and overall scoring analyses reveal a clear pattern: platforms offering comprehensive multi-service ecosystems consistently outperform narrowly focused systems across categories. This indicates that functional integration, rather than category type alone, is a primary determinant of platform strength and ecosystem utility. At the same time, specialized platforms deliver targeted value within their domains, underscoring the diversity of strategic orientations within DeFi. Beyond these functional and architectural differences, an important observation is that none of the evaluated platforms or protocol models can be regarded as inherently resilient to major DeFi attack vectors, including flash loan attacks, rug pulls, phishing, fraud, oracle manipulation, reentrancy, governance exploits, bridge attacks, and MEV-related threats. Although many platforms advertise security, privacy, governance, or risk-management features, their publicly available documentation does not provide concrete evidence of resistance to the identified attack classes, nor does it present comprehensive and validated solutions for mitigating them in practice. This gap between functional richness and demonstrated security resilience highlights an important limitation of the current DeFi ecosystem.

In conclusion, this thesis focuses its detailed empirical analysis on phishing and fraud attacks because they are among the most common and practically relevant threats in DeFi, and because they are supported by available datasets that enable systematic analysis and model development. This focus allows the study to move from broad ecosystem-level comparison to a more data-driven investigation of two attack classes that are both prevalent and empirically tractable.

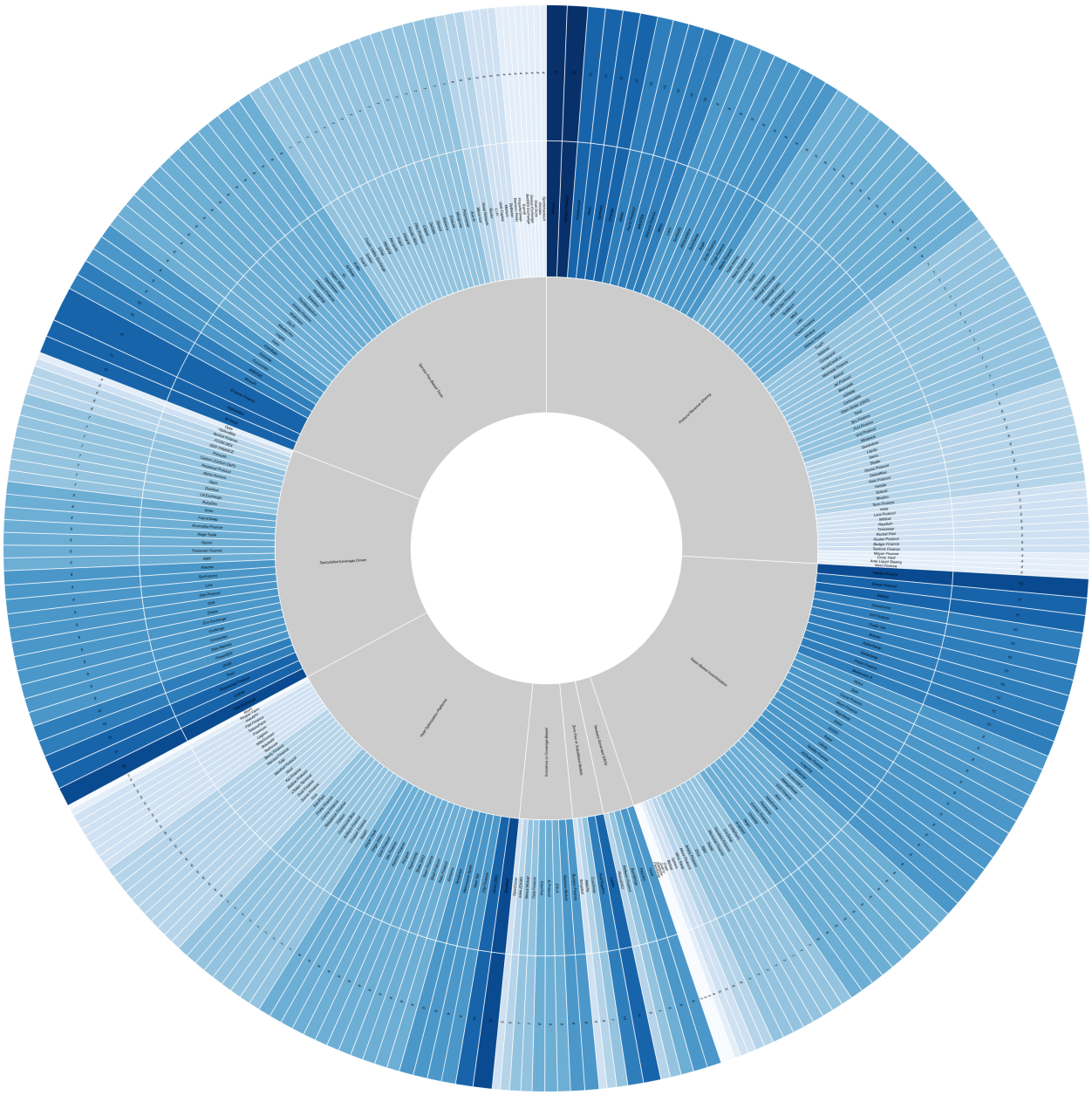


Figure 15: Final performance scores across all evaluated platforms. Higher scores reflect broader functional coverage and deeper systemic integration, enabling cross-category comparison of platform maturity and capability.

4 Proposed Model

This section presents the proposed learning framework for detecting malicious activity in Ethereum-based DeFi transactions. In the final design of this thesis, the phishing and fraud datasets are not treated as two separate binary problems. Instead, they are integrated into a unified classification framework in which each record is assigned one of three mutually exclusive labels: benign, phishing, or fraud. Accordingly, the problem addressed in this work is most precisely formulated as a multiclass classification task over a merged blockchain dataset. This unified formulation allows the models to learn not only how to separate malicious activity from legitimate behavior, but also how to distinguish between different categories of attacks within a shared feature space.

The proposed framework consists of four main phases. First, the phishing and fraud datasets are integrated through schema alignment and label harmonization to be represented in a common tabular structure. Second, domain-relevant blockchain features are extracted from the raw transaction records to build a classifier-ready feature matrix. Third, the resulting features are processed and normalized through a shared preprocessing pipeline to improve numerical stability and ensure comparability across models. Finally, the processed data are used to train and evaluate three deep tabular learning models, namely: TabNet, NODE, and GANDALF, together with three conventional baseline classifiers: Logistic Regression, SVM, and Random Forest.

This unified feature-level learning design is particularly well-suited to blockchain security analysis because malicious behavior is rarely captured by a single raw field. Rather, phishing and fraud patterns typically emerge from combinations of transaction statistics, wallet activity, temporal behavior, gas consumption signals, token interactions, and account-level attributes. By mapping all observations into a common structured representation and evaluating multiple learning paradigms under identical data conditions, the framework supports a rigorous comparison of model behavior for multiclass DeFi attack detection. The overall pipeline of the proposed framework is illustrated in Fig. 16.

4.1 Dataset Integration and Label Harmonization

Before model training, the phishing and fraud datasets are integrated into a single learning corpus. This step is necessary because the two sources originate from different attack contexts and may differ in structure, naming conventions, or available attributes. To enable joint learning, their records are mapped into a common schema, and their labels are harmonized into the three target classes used in this thesis: benign, phishing, and fraud.

This integration stage is methodologically important for two reasons. First, it converts two security datasets into one unified benchmark, allowing all models to be trained and evaluated under the same data distribution. Second, it enables the study to move beyond simple malicious-versus-benign discrimination and instead address a more informative multiclass setting in which the classifier must also distinguish between different forms of malicious behavior. The result is a more realistic experimental framework for blockchain security analysis, since practical security systems often need to identify the category of an attack rather than merely detect its existence.

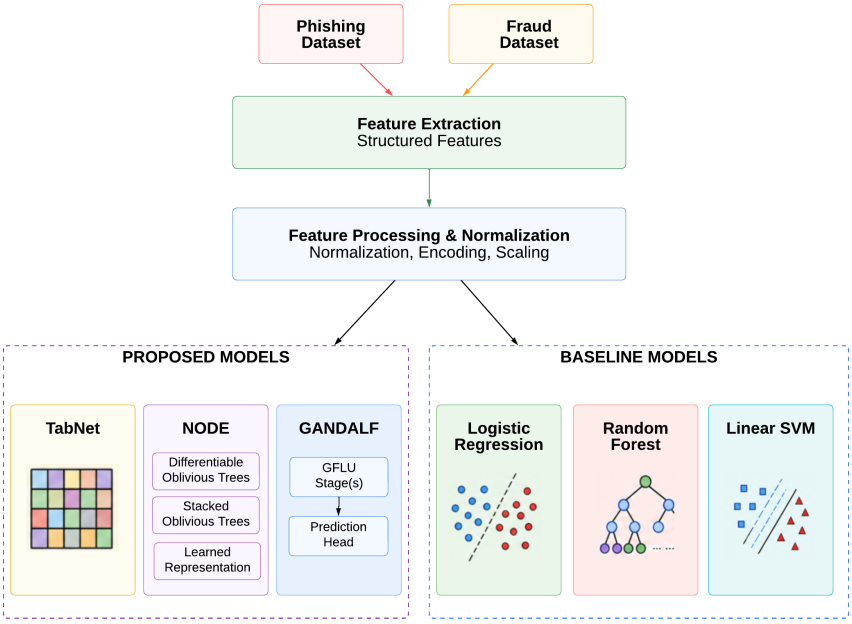


Figure 16: Overall proposed multiclass framework.

4.2 Feature Extraction and Schema Alignment

After integration, the raw blockchain records are transformed into structured tabular features that summarize the behavior of each transaction, wallet, or account instance. Rather than relying directly on raw logs, the proposed framework constructs a domain-informed feature space that captures transactional, temporal, and behavioral properties relevant to malicious activity detection.

The extracted features are designed to represent various aspects of blockchain behavior, including transaction frequency, transferred value, gas usage, token movement, activity timing, wallet interaction patterns, and account-level historical statistics. Because phishing and fraud typically manifest as subtle combinations of such signals, the feature extraction stage provides the semantic foundation required for effective learning. In addition, schema alignment ensures that the extracted variables from the merged datasets remain consistent in meaning and format, thereby preserving a common representation across all observations.

The resulting feature matrix serves as the shared input to all deep and traditional classifiers used in this thesis. This common input space is essential for fair comparison, since any observed performance differences can then be attributed more directly to the learning architectures rather than to differences in feature construction.

4.3 Feature Processing and Normalization

Following feature extraction, the merged feature matrix is passed through a shared preprocessing pipeline. This stage is required because blockchain-derived tabular features may contain missing values, invalid numeric entries, infinite values, outliers, or substantial scale variation across variables. Without proper preprocessing, such issues can negatively affect optimization stability and reduce the reliability of model comparisons.

Accordingly, the feature processing stage converts the input variables into a consistent numeric representation, handles missing or infinite values, and applies normalization where appropriate. This ensures that the input space is numerically stable and that all models are trained on the same cleaned representation. The use of a unified preprocessing pipeline across all classifiers is a key methodological choice in this work, because it reduces confounding factors and makes the comparative evaluation more rigorous.

4.4 Classification Model Training and Evaluation

In the final stage, the processed feature matrix is used to train and evaluate both deep learning and conventional machine learning classifiers. The primary emphasis of this thesis is on three deep architectures specialized for structured data: TabNet, NODE, and GANDALF. These models were selected because they represent three different but complementary strategies for learning from tabular inputs. To contextualize their performance, three conventional baselines are also included: Logistic Regression, Support Vector Machine, and Random Forest.

All models are trained on the same merged multiclass dataset and evaluated under the same experimental conditions. Since the task involves three classes, performance should be assessed using metrics appropriate for multiclass classification, including overall accuracy, macro-averaged precision, macro-averaged recall, macro-averaged F1-score, class-wise results, confusion matrices, and, when probabilistic outputs are available, multiclass ROC-AUC. This evaluation design ensures that model performance is measured not only in terms of overall correctness, but also in terms of balance across the phishing, fraud, and benign classes.

4.4.1 TabNet

TabNet is a deep neural architecture designed specifically for tabular learning. Instead of processing all features uniformly, it uses a sequence of decision steps in which the model selectively attends to the most informative subset of variables at each stage [368]. This selective mechanism is implemented using sparse, dynamically generated attentive masks for each input sample.

The architecture is composed primarily of feature transformers and attentive transformers. At each decision step, the attentive transformer determines which input dimensions should receive emphasis, while the feature transformer computes the latent representation associated with that selected subset. The outputs of several decision steps are then aggregated to produce the final representation used for prediction. Because the feature masks are sparse and instance-specific, TabNet offers both predictive flexibility and interpretability. A conceptual illustration of the TabNet workflow is shown in Fig. 17.

In the context of this thesis, TabNet is particularly suitable because phishing and fraud patterns often depend on a relatively small set of highly informative blockchain features. By adaptively focusing on different feature subsets for different samples, TabNet can model heterogeneous malicious behaviors while also providing insight into which variables are most influential during prediction.

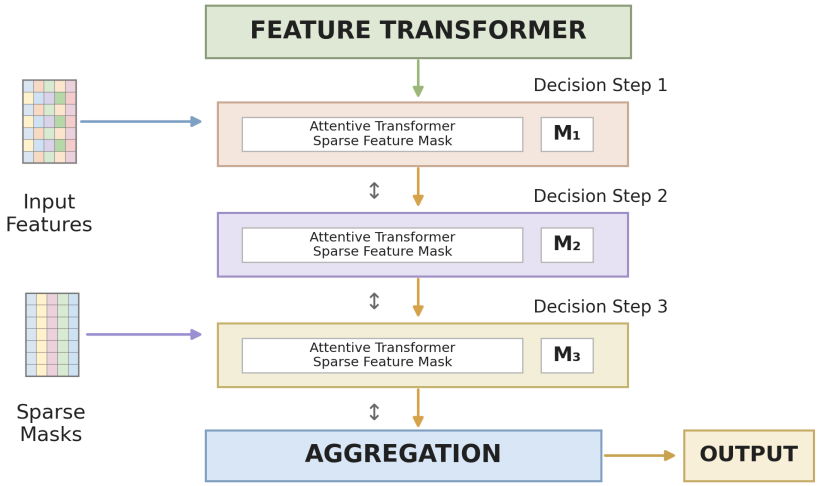


Figure 17: TabNet architecture. At each decision step, an attentive transformer produces a sparse feature mask, a feature transformer learns the corresponding representation, and the decision outputs are aggregated before multiclass prediction.

4.4.2 NODE

NODE combines the inductive bias of tree-based learning with the optimization benefits of differentiable neural networks [369]. Its core building block is the oblivious decision tree, in which all nodes at the same depth share the same split criterion. This structured constraint makes the model well-suited to threshold-based feature interactions commonly found in tabular data.

Unlike conventional tree ensembles, NODE is fully differentiable and can be trained end-to-end using gradient-based optimization. Multiple oblivious trees are grouped into ensembles, and one or more NODE layers may be stacked to learn increasingly rich feature interactions. The leaf responses from these trees are concatenated to form a learned tabular representation, which is then passed to the output layer for final prediction. Figure 18 presents the NODE structure used conceptually in this work.

NODE is a strong candidate for blockchain attack detection because suspicious behavior often emerges only when several variables jointly satisfy threshold-like conditions. For example, attack patterns may depend on simultaneous irregularities in transaction value, gas behavior, wallet history, or temporal activity. NODE is especially effective in such settings because it can capture non-linear and higher-order feature interactions while retaining a tree-inspired representation bias.

4.4.3 GANDALF

GANDALF is a deep tabular architecture built around Gated Feature Learning Units (GFLUs) [370]. Rather than relying on sparse sequential attention or tree-style routing, GANDALF learns tabular representations through staged gated transformations that decide how input information should be preserved, suppressed, or updated across successive layers.

Each GFLU applies feature-wise gating operations to the input representation. Conceptually, these operations include a learned feature mask together with reset, update, and candidate-state components that pro-

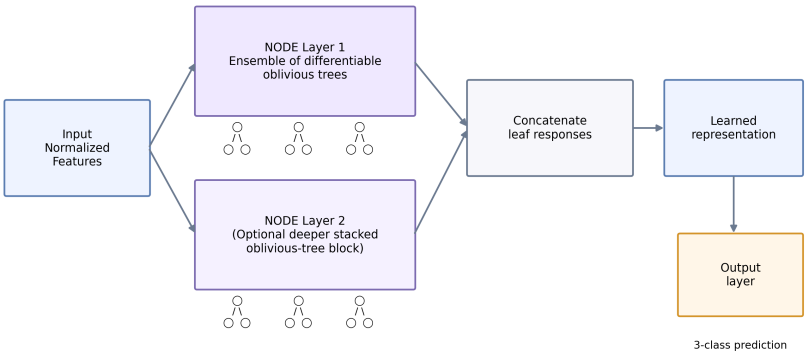


Figure 18: NODE architecture. Input features pass through one or more ensembles of differentiable oblivious decision trees, whose leaf responses are concatenated into a learned representation and mapped to a three-class output layer.

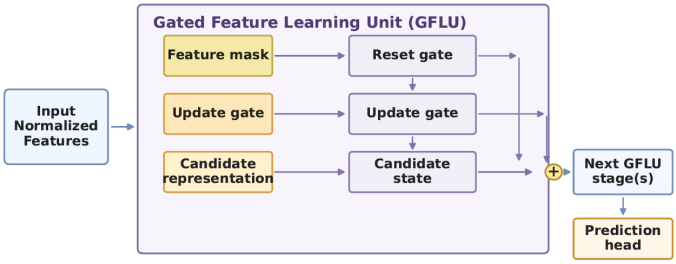


Figure 19: GANDALF architecture. Stacked Gated Feature Learning Unit (GFLU) stages iteratively refine the normalized feature representation through masking and gating operations before the final three-class prediction head.

gressively refine the feature representation passed to the next stage. Through repeated GFLU stages, the model constructs a latent representation that emphasizes informative dimensions while attenuating noisy or less relevant signals. The resulting representation is then fed to a final prediction head, as illustrated in Fig. 19.

This architecture is well aligned with the objectives of the present study because the merged blockchain feature set contains many engineered variables of unequal predictive value. GANDALF is therefore a meaningful addition to the comparison framework, as it tests whether progressive gated feature refinement can improve discrimination among benign, phishing, and fraud behaviors in a structured DeFi setting.

4.4.4 Baseline Models

To complement the deep tabular architectures, three widely used conventional classifiers are included as baselines: Logistic Regression, SVM, and Random Forest. These models provide a strong methodological reference point and help determine whether the deep architectures offer a meaningful advantage on the merged multiclass dataset.

Logistic Regression serves as a linear baseline, indicating how well the engineered blockchain feature space separates the three classes using a simple decision function. SVM is included because of its strong perfor-

mance in high-dimensional classification settings and its ability to model more complex class boundaries depending on the selected formulation. Random Forest is a tree-based ensemble baseline that can naturally capture non-linear feature interactions and typically performs well on structured tabular data without requiring the same degree of sensitivity to feature scaling as linear models.

Together, these baselines strengthen the comparative design by showing whether improvements obtained by TabNet, NODE, or GANDALF arise from genuinely more expressive tabular learning mechanisms rather than from the feature engineering stage alone.

4.5 Comparative Design Rationale

The selection of TabNet, NODE, and GANDALF provides a strong basis for comparison because the three models reflect different architectural philosophies for deep tabular learning. TabNet emphasizes sequential sparse attention, NODE emphasizes differentiable tree-structured partitioning, and GANDALF emphasizes progressive gated feature refinement. Evaluating these models on the same merged feature space and under the same preprocessing conditions enables a fair and informative comparison of how different deep learning biases respond to blockchain-derived structured data.

Including Logistic Regression, Support Vector Machine, and Random Forest further strengthens the experimental design by establishing reference performance levels using standard machine learning methods. This makes it possible to determine not only which deep model performs best, but also whether deep tabular learning yields a meaningful advantage over conventional classifiers for multiclass DeFi attack detection.

More broadly, the proposed framework serves not only as a predictive pipeline but also as an experimental testbed for understanding whether different learning paradigms generalize across multiple forms of malicious blockchain activity within a unified classification problem.

In summary, the proposed model formulates DeFi attack detection as a unified multiclass tabular learning problem in which phishing, fraud, and benign behaviors are learned jointly from a merged and harmonized blockchain dataset. The framework integrates dataset alignment, domain-driven feature extraction, shared preprocessing, and comparative model training within a single experimental pipeline. By combining three specialized deep tabular architectures with strong traditional baselines under identical conditions, the proposed design provides both a practical detection framework and a rigorous basis for analyzing the suitability of different learning strategies for multiclass blockchain security classification.

5 Experiments and Results

This chapter presents the experimental design and evaluation results of the proposed multiclass DeFi attack detection framework. As discussed in Chapter 4, the phishing and fraud datasets were not treated as independent binary tasks. Instead, they were merged into a unified three-class classification problem, where each transaction record was labeled as legitimate, fraud, or phishing. This setting reflects a more realistic blockchain security scenario in which multiple malicious behaviors coexist in the same transaction space and must be distinguished from each other as well as from benign activity.

The experiments were designed to evaluate both predictive performance and feature-level behavior across different model families. Three deep tabular learning models, namely TabNet, NODE, and GANDALF, were compared with three conventional machine learning baselines: Logistic Regression, SVM, and Random Forest. All models were trained and tested under the same data split and preprocessing conditions to ensure a fair comparison. In addition to classification performance, feature importance analysis was conducted to identify the most influential blockchain attributes and to examine whether different learning paradigms converge toward similar behavioral signals.

5.1 Datasets

This study was conducted using two publicly available Ethereum-based DeFi transaction datasets collected at the Behavior-Centric Cybersecurity Center (BCCC): BCCC-DeFiPhishingTrans-2025 and BCCC-DeFiFraudTrans-2025. Rather than treating these datasets as two separate binary classification benchmarks, they were integrated into a unified multiclass dataset in order to better reflect realistic DeFi threat detection scenarios, where multiple malicious behaviors coexist within the same transaction space.

The first dataset, BCCC-DeFiPhsihingTrans-2025, contains both legitimate and phishing transaction records. The version used in this thesis includes 3,395,828 legitimate samples and 1,215,171 phishing samples. The second dataset, *BCCC-DeFiFraudTrans-2025*, was developed as a comprehensive DeFi fraud analysis dataset, containing wallet- and transaction-level information collected from Etherscan. It contains 1,026,867 transaction records labeled as either legitimate or fraud and is associated with 9,374 unique wallet addresses. According to the dataset description, its labels were further validated through anomaly detection, consistency checks, and duplicate removal during the original construction process.

Because the two datasets were prepared independently, their schemas were not directly identical. Therefore, prior to integration, the feature sets of both datasets were compared and aligned through column matching and feature mapping. Each dataset initially contained 170 attributes; however, only the subset of features common to all sources was retained after alignment. Following this process, duplicate, redundant, and non-overlapping attributes were removed, resulting in a unified feature space of 148 features. This common 148-feature representation was used as the final tabular input space for all models evaluated in this thesis.

After feature alignment, all records were relabeled under a shared multiclass encoding scheme:

- **0**: legitimate
- **1**: fraud

- **2**: phishing

Using this labeling strategy, fraud, phishing, and legitimate DeFi transaction records were merged into a single consolidated dataset. Duplicate samples were then removed from the merged dataset to avoid duplicate observations after integration. The resulting dataset was shuffled using a fixed random seed to ensure reproducibility and subsequently partitioned into training, validation, and test sets using a stratified **70%/15%/15%** split, as summarized in Table 11, thereby preserving the class proportions across all partitions.

Table 11: Dataset split used in the multiclass experiments.

Subset	Number of Samples	Number of Features
Training	3,946,506	148
Validation	845,680	148
Test	845,680	148

To prepare the data for model training, a shared preprocessing pipeline was applied to all partitions. Non-numeric values were coerced to numeric wherever possible; missing and infinite values were handled systematically; extreme numerical values were clipped to reduce instability caused by outliers; and constant columns were removed. Finally, all remaining input features were stored in 32-bit floating-point format, while labels were cast to integer format. This unified preprocessing pipeline ensured numerical stability, supported more memory-efficient training, and made comparisons across models consistent and reproducible.
The class distribution in the training set is presented in Table 12. As expected, the data are imbalanced, with legitimate transactions forming the majority class, phishing samples the second-largest group, and fraud the smallest. This imbalance makes macro-level evaluation metrics particularly important, since overall accuracy alone may overestimate model quality.

Table 12: Training set class distribution.

Class	Label	Count
Legitimate	0	3,033,731
Fraud	1	62,155
Phishing	2	850,620

5.1.1 Dataset Evaluation Criteria

To evaluate model performance under class imbalance, multiple complementary metrics were employed:

- **Accuracy**: the overall fraction of correctly classified samples.
- **Macro Precision**: the average precision across classes, treating each class equally.
- **Macro Recall**: the average recall across classes, treating each class equally.
- **Macro F1-score**: the harmonic mean of macro precision and macro recall.

- **Balanced Accuracy**: the mean recall over all classes.
- **ROC-AUC**: reported where probability estimates were available.

Because the dataset is imbalanced, macro-averaged scores and balanced accuracy were considered more informative than accuracy alone. In addition, confusion matrices were used to illustrate the detailed error distribution among legitimate, fraud, and phishing transactions.

The statistical distribution of fraudulent and phishing transactions was examined at both the transaction level and the wallet level because malicious blockchain activity is often unevenly distributed across addresses. In the final aligned dataset, the transaction-level class distribution shows a clear imbalance among legitimate, fraud, and phishing records. Legitimate transactions form the majority class, phishing transactions represent the second-largest group, and fraud transactions form the smallest class. In the training set, there are 3,033,731 legitimate transactions, 62,155 fraud transactions, and 850,620 phishing transactions, corresponding to 76.87%, 1.57%, and 21.55% of the training data, respectively. The same distribution is preserved in the validation and test sets, where each split contains 650,086 legitimate transactions, 13,319 fraud transactions, and 182,275 phishing transactions. This stratified distribution ensures that all classes are consistently represented across the experimental splits while preserving the natural imbalance of blockchain-based malicious activity datasets. However, because fraudulent and phishing activities may be concentrated in repeated transactions from a limited number of wallets, the wallet-level distribution is also important for understanding whether malicious behavior is broadly distributed or concentrated among recurring wallet addresses.

Possible wallet overlap across the train, validation, and test splits was also considered as part of the leakage analysis. Since Ethereum wallets can appear in multiple transactions, a transaction-level split may result in some wallet addresses appearing in more than one split. However, this does not directly create label leakage in the proposed framework because raw wallet addresses are not used as categorical model inputs. The models are trained on numerical behavioral and transaction-level features, including gas usage, nonce-related behavior, transaction frequency, and wallet activity patterns, rather than address identifiers. Therefore, the model is not designed to memorize specific wallets, but to learn behavioral differences among legitimate, fraud, and phishing activities. Any wallet overlap is therefore treated as a limitation of transaction-level evaluation rather than direct contamination of the labels. Temporal leakage was also considered by ensuring that no future-derived labels, post-event indicators, or target-dependent attributes were intentionally introduced during feature construction. Since the extracted features represent observable blockchain transaction behavior, the current experimental design remains suitable for evaluating behavior-centric malicious activity detection. A stricter wallet-disjoint or fully chronological split can be considered as future robustness analysis, but the current setting is still valid because it avoids direct address-based memorization and focuses on general transaction behavior.

5.2 New Augmented Dataset

The main contribution of this work lies in integrating the phishing and fraud datasets into a unified multiclass analytical setting. Instead of evaluating phishing detection and fraud detection separately, both malicious categories were aligned into a common feature-level representation. This produced a more challenging

and realistic learning problem, as the models were required to both separate malicious transactions from legitimate ones and distinguish phishing from fraud within the malicious transaction space.
This merged formulation better reflects real blockchain environments, where multiple attack types coexist and often share overlapping behavioral traits. It also enables feature importance analysis to reveal whether the same transaction-level signals are informative across different forms of DeFi abuse.

5.3 Performance Results

Table 13 summarizes the test-set performance of all six evaluated models. Overall, the results show a clear separation between the conventional baselines and the deep tabular models. Among the baseline methods, Random Forest achieved the strongest performance, reaching an accuracy of 0.9963 and a macro F1-score of 0.9685. In contrast, Logistic Regression and Linear SVM achieved lower macro precision and macro F1-scores, despite maintaining relatively high recall. This suggests that although the linear models detected many minority-class instances, they did so at the cost of more false positives and weaker class separation, especially for the fraud class.
Among the deep tabular models, NODE achieved the best overall performance, with a test accuracy of 0.9987, macro precision of 0.9911, balanced accuracy of 0.9953, and macro F1-score of 0.9932. GANDALF closely followed NODE, while TabNet also delivered very strong results, albeit slightly below NODE and GANDALF. These results indicate that the deep tabular architectures were more effective at modeling the nonlinear and overlapping behavioral patterns present in the multiclass DeFi transaction space.

Table 13: Overall test performance comparison of all evaluated models.

Model	**Accuracy**	**Macro Precision**	**Macro Recall**	**Balanced Accuracy**	**Macro F1**	**ROC-AUC**
Logistic Regression	0.9369	0.7314	0.9678	0.9678	0.7859	0.9900
Linear SVM	0.9561	0.7926	0.9399	0.9399	0.8465	–
Random Forest	0.9963	0.9442	0.9979	0.9979	0.9685	1.0000
TabNet	0.9980	0.9842	0.9920	0.9920	0.9880	–
GANDALF	0.9984	0.9883	0.9953	0.9953	0.9918	–
NODE	**0.9987**	**0.9911**	0.9953	0.9953	**0.9932**	–

The weighted-average results further confirm the strength of the best-performing models. NODE achieved a weighted F1-score of 0.9987, followed by GANDALF with 0.9984 and TabNet with 0.9980, while Random Forest reached 0.9964. This indicates that the deep models not only maintained excellent overall performance on the dominant legitimate class, but also preserved strong discrimination ability on the minority malicious classes. Since the dataset is highly imbalanced, these weighted and macro-level results together provide a more reliable picture of model quality than accuracy alone.
A class-wise analysis shows that fraud was the most difficult category across all models, which is expected given its substantially smaller representation in the training set. Even so, the strongest models achieved very high fraud recall, specifically 0.9893 for NODE, 0.9897 for GANDALF, and 0.9803 for TabNet. This is particularly important in blockchain security, where failing to identify minority-malicious transactions may lead to significant practical risks. At the same time, the phishing and legitimate classes were also classified

with near-perfect consistency by the best models, indicating that the learned decision boundaries generalized well across both majority and minority classes.

Confusion Matrix Analysis

The confusion matrices provide further insight into the error structure of the evaluated models. In general, the best-performing models made very few mistakes, and the remaining errors were concentrated primarily between legitimate and phishing transactions. Fraud was separated with particularly high sensitivity, and cross-confusion between fraud and phishing was almost entirely eliminated in the strongest models. This pattern suggests that fraud transactions occupy a more distinct region of the learned feature space, whereas legitimate and phishing transactions exhibit greater behavioral overlap.

NODE produced the strongest confusion matrix overall, shown in Table 14. Out of 13,319 fraud samples in the test set, only 142 were misclassified as legitimate, and none were misclassified as phishing. For the legitimate and phishing classes, the number of errors was also extremely small relative to the test-set size, confirming the strong balanced performance already reflected in the macro metrics.

Table 14: Confusion matrix for NODE on the test set.

True / Predicted	Legitimate	Fraud	Phishing
Legitimate	649,592	338	156
Fraud	142	13,177	0
Phishing	461	0	181,814

GANDALF, shown in Table 15, achieved performance very close to NODE. It slightly reduced fraud-to-legitimate errors compared with NODE, but introduced a very small number of fraud-to-phishing and phishing-to-fraud misclassifications. Nevertheless, the total number of errors remained extremely low, confirming GANDALF as one of the most reliable models in the study.

Table 15: Confusion matrix for GANDALF on the test set.

True / Predicted	Legitimate	Fraud	Phishing
Legitimate	649,303	434	349
Fraud	131	13,182	6
Phishing	457	6	181,812

TabNet also performed strongly, as shown in Table 16, although its error counts were slightly higher than those of NODE and GANDALF. In particular, it produced more legitimate-to-fraud and phishing-to-legitimate errors than the other two deep models. Even so, its confusion matrix still demonstrates very strong class separation overall, particularly for the fraud class.

For comparison, the confusion matrices of the baseline models further illustrate the performance gap between conventional classifiers and deep tabular learning methods. Logistic Regression, presented in Table 17, achieved very high fraud recall, but at the expense of many legitimate transactions being incorrectly classified as fraud or phishing. This behavior is consistent with its lower macro precision and shows that the model was less selective in its decision boundaries.

Table 16: Confusion matrix for TabNet on the test set.

True / Predicted	Legitimate	Fraud	Phishing
Legitimate	649,172	609	305
Fraud	262	13,057	0
Phishing	536	1	181,738

Table 17: Confusion matrix for Logistic Regression on the test set.

True / Predicted	Legitimate	Fraud	Phishing
Legitimate	598,849	31,215	20,022
Fraud	89	13,230	0
Phishing	2,044	1	180,230

Linear SVM, shown in Table 18, reduced some of the excessive fraud predictions seen in Logistic Regression, but still produced substantial confusion between legitimate and phishing transactions and a noticeably larger number of fraud-to-legitimate errors than the stronger models.

Table 18: Confusion matrix for Linear SVM on the test set.

True / Predicted	Legitimate	Fraud	Phishing
Legitimate	616,592	12,275	21,219
Fraud	1,565	11,754	0
Phishing	2,074	0	180,201

Random Forest, given in Table 19, was substantially stronger than the two linear baselines and came much closer to the deep models. It perfectly detected all fraud transactions in the test set, but still made more legitimate-to-fraud and phishing-to-legitimate errors than NODE, GANDALF, and TabNet. This explains why Random Forest remained the strongest conventional baseline, yet still fell slightly behind the best deep tabular models on macro-level measures.

Taken together, the confusion matrices confirm the ranking observed in Table 13. The deep tabular models produced the most balanced error profiles, with NODE delivering the strongest overall trade-off between minority-class sensitivity and low false-positive behavior. GANDALF closely matched this performance, while TabNet remained highly competitive. Among the baseline models, Random Forest emerged as the most effective conventional method, whereas Logistic Regression and Linear SVM were less robust to class imbalance and overlapping feature distributions.

Figure 20 provides a visual summary of the overall comparison across all models in terms of accuracy, macro F1-score, and balanced accuracy. The figure highlights the consistent advantage of the deep tabular approaches over the baseline methods. Figure 21 complements this comparison by presenting the normalized confusion matrices of the three best-performing models, allowing their residual error patterns to be compared more directly.

Table 19: Confusion matrix for Random Forest on the test set.

True / Predicted	Legitimate	Fraud	Phishing
Legitimate	647,324	2,656	106
Fraud	0	13,319	0
Phishing	401	0	181,874

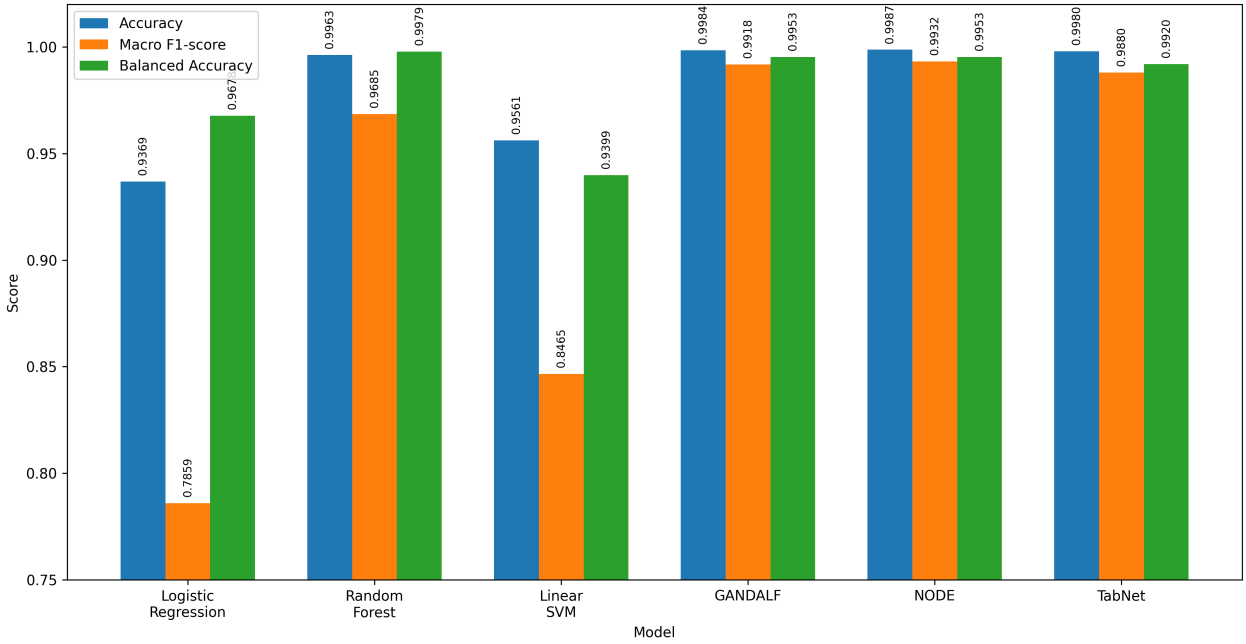


Figure 20: Comparison of accuracy, macro F1-score, and balanced accuracy across all evaluated models.

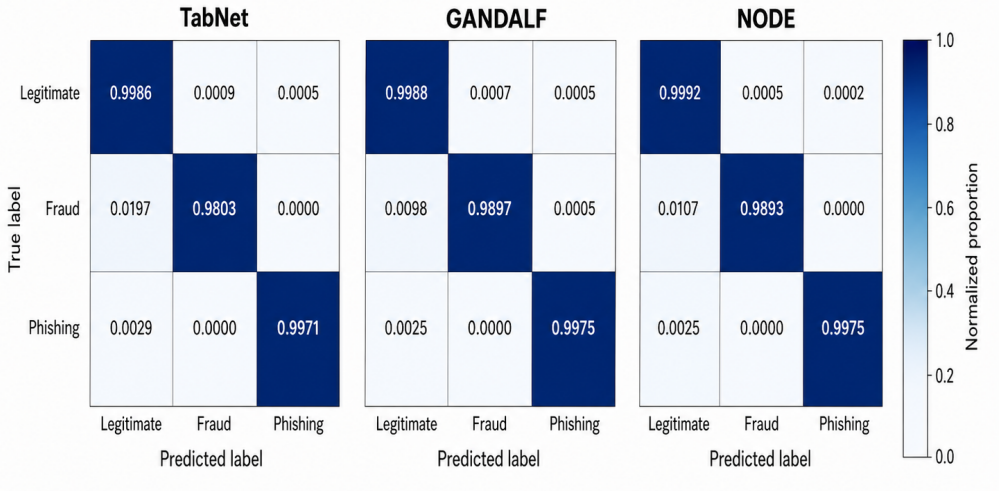


Figure 21: Normalized confusion matrices for TabNet, GANDALF, and NODE.

5.4 Top-Ranked Features

Feature importance analysis was used to identify the blockchain transaction attributes that contributed most to classification performance. Because different model families expose importance differently, model-specific ranking methods were used. For the linear models, absolute coefficient magnitudes were used; for Random Forest, impurity-based importance was used; and for the deep tabular models, permutation importance on the validation set was employed.

Tables 20 and 21 summarize the top-ranked features of the evaluated models.

Table 20: Top-ranked features for the deep tabular models.

TabNet	**GANDALF**	**NODE**
addr_gas_used.gas_used_sum	addr_num_transaction	addr_nonce.nonce_max
erc721_Is_Zero_Divisor	addr_nonce.nonce_sum	addr_num_transaction
addr_cumulativeGasUsed.cumulativeGasUsed_sum	addr_values.values_max	addr_nonce.nonce_mean
addr_num_transaction	addr_gas_used.gas_used_mean	addr_gas_used.gas_used_stdev
addr_gas_used.gas_used_mean	addr_nonce.nonce_median	addr_cumulativeGasUsed.cumulativeGasUsed_max
addr_nonce.nonce_mean	addr_nonce.nonce_mean	addr_cumulativeGasUsed.cumulativeGasUsed_median
addr_nonce.nonce_median	erc721_Symbol_Length	addr_gas_used.gas_used_mean
addr_nonce.nonce_sum	erc721_Unique_Chars_Name	addr_values.values_min
addr_gas_used.gas_used_median	total_gas_cost	addr_nonce.nonce_median
addr_values.values_max	erc721_Name_Entropy	addr_nonce.nonce_min

Table 21: Top-ranked features for the baseline models.

Logistic Regression	**Random Forest**	**Linear SVM**
addr_number_of_unique_from_address	addr_gas_used.gas_used_mean	addr_number_of_unique_to_address
addr_gas_used.gas_used_max	addr_cumulativeGasUsed.cumulativeGasUsed_stdev	addr_number_of_unique_from_address
addr_number_of_to_address	log_removed	addr_number_of_to_address
addr_number_of_from_address	addr_nonce.nonce_median	addr_gas_used.gas_used_cv
addr_num_transaction	gas_efficiency	length_transaction_hash
length_transaction_hash	addr_cumulativeGasUsed.cumulativeGasUsed_cv	is_contract_creation
addr_number_of_unique_to_address	gas_price_ratio	addr_nonce.nonce_cv
addr_gas_used.gas_used_mean	addr_number_of_to_address	addr_number_of_errors
addr_gas_used.gas_used_stdev	addr_nonce.nonce_variance	transaction_hash
effective_gas_price	addr_gas_used.gas_used_median	erc721_TokenQuantity

A comparison of the feature rankings reveals several important patterns. First, no single feature appears in the top-10 list of all six models, which suggests that each model family captures a somewhat different view of the transaction space. However, several features recur consistently across multiple models:

- `addr_gas_used.gas_used_mean` appears in **five** of the six models.
- `addr_num_transaction` appears in **four** models.
- `addr_nonce.nonce_median` appears in **four** models.
- `addr_number_of_to_address` and `addr_nonce.nonce_mean` each appear in **three** models.

These recurring features strongly suggest that account activity level, nonce behavior, and gas usage statistics are among the most reliable indicators of malicious DeFi behavior in the merged dataset. In other words, the best-performing models do not rely on isolated token-level signals alone; rather, they learn from repeated transaction behavior, temporal wallet activity, and execution-cost characteristics. Across the deep tabular models, `addr_num_transaction`, `addr_gas_used.gas_used_mean`, `addr_nonce.nonce_mean`, and `addr_nonce.nonce_median` emerged as the most consistently important features, indicating that transaction activity, gas usage behavior, and nonce-related statistics play a central role in discriminating between the target classes. This convergence is especially meaningful because the deep models use different internal learning mechanisms, yet still focus on similar behavioral cues. Therefore, these features can be regarded as the best overall feature signals in the proposed framework.

At the same time, each model also highlighted some distinctive features. TabNet placed high importance on `erc721_Is_Zero_Divisor` and cumulative gas statistics; GANDALF emphasized several ERC-721 textual characteristics such as symbol length and name entropy; and NODE focused more strongly on nonce extrema and cumulative gas distributions. This indicates that while a common behavioral core exists, different model architectures also uncover complementary views of malicious transaction behavior.

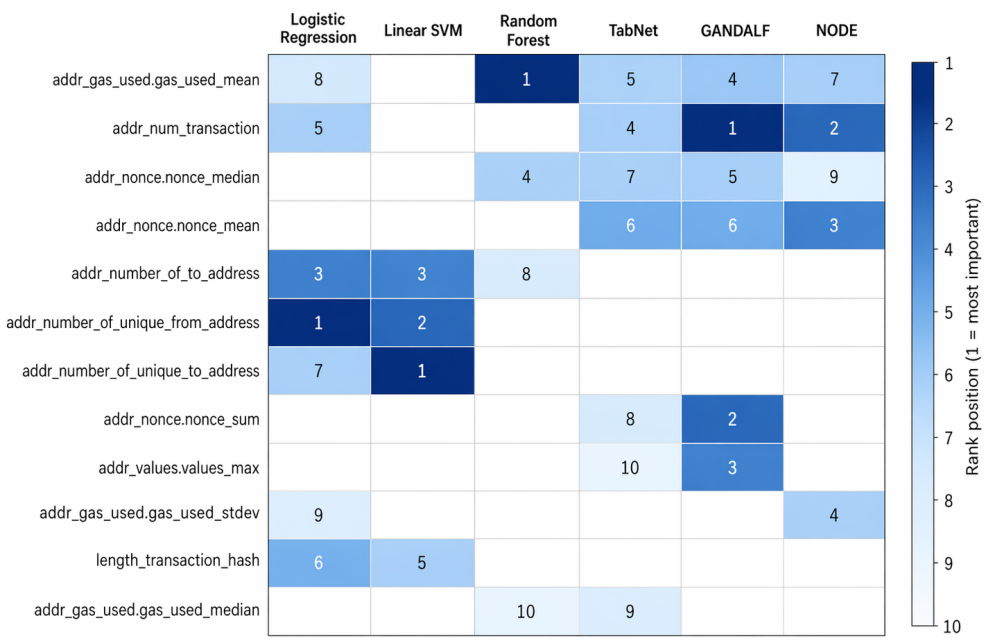


Figure 22: Comparison of the top-ranked features across all evaluated models.

5.5 Class-wise Behavioral Profiling

The feature rankings provide useful insight into the behavioral differences among the three classes. Legitimate transactions tend to follow more regular and broadly distributed operational patterns, whereas phishing and fraud samples exhibit greater irregularities in wallet-level activity statistics. In particular, nonce-related features, gas consumption summaries, and transaction count features appear repeatedly among the most

informative variables, suggesting that malicious accounts differ from benign ones not only in isolated transaction values but also in repeated transactional behavior over time.

Fraud appears to be especially separable when models capture highly structured behavioral signals. This is reflected in the very high fraud recall of Random Forest, GANDALF, and NODE. Phishing transactions are also detected with very high performance, but the confusion matrices indicate that the remaining errors occur more often between phishing and legitimate classes than between phishing and fraud. This suggests that some phishing behaviors partially resemble benign usage patterns at the feature level, especially when observed only through aggregated statistics.

Another important observation is that the strongest models rely on both account-level and transaction-level signals. Features such as `addr_num_transaction`, `addr_nonce.*`, and `addr_gas_used.*` capture persistent wallet behavior, while token- and gas-related attributes capture more local interaction dynamics. This combination seems essential for robust multiclass discrimination.

5.6 Zero-Day Detection Scenario

Although the present experiments were conducted in a supervised multiclass setting, the results also offer useful implications for zero-day DeFi threat analysis. In particular, the fact that the best-performing models consistently relied on broad behavioral features rather than attack-specific identifiers suggests that they may generalize better to unseen malicious patterns than models that depend primarily on narrow signatures.

Features related to transaction frequency, nonce evolution, gas consumption summaries, and cumulative activity statistics are not tied to one specific phishing or fraud template. Instead, they reflect higher-level behavioral properties of suspicious accounts. This makes them promising candidates for early warning systems and anomaly-aware blockchain monitoring pipelines.

Nevertheless, true zero-day detection cannot be claimed solely from the current experiments, because all evaluated classes were present during training. A dedicated zero-day protocol would require withholding one attack subtype or one temporal segment during training and then evaluating whether the model can still identify previously unseen malicious behavior. Such an evaluation is left for future work, but the present findings suggest that the proposed multiclass framework provides a strong foundation for that direction.

In summary, the experimental results demonstrate that deep tabular learning is highly effective for multiclass DeFi threat detection. NODE achieved the strongest overall results, followed closely by GANDALF and TabNet, while Random Forest remained the strongest conventional baseline. The feature analysis further showed that wallet activity, nonce behavior, and gas-related statistics form the most stable and informative signals across model families. Together, these findings support the effectiveness of the proposed unified learning framework for practical blockchain security analysis.

6 Analysis and Discussion

This chapter provides a deeper interpretation of the results presented in Chapter 5. Rather than only reporting model performance, this chapter analyzes the behavioral meaning of the most important features, examines how different models respond to multiclass DeFi attack detection, discusses the computational implications of the proposed framework, and highlights the practical relevance of the results for real-world blockchain security systems.

A key contribution of this thesis is the construction of a unified multiclass learning framework in which legitimate, fraud, and phishing DeFi transactions are analyzed together in a shared feature space. This makes the analysis more realistic than in isolated binary classification settings, since operational blockchain monitoring systems must simultaneously distinguish among multiple forms of malicious behavior. The results show that the strongest models learn behavioral signatures associated with abnormal wallet activity, transaction sequencing, gas consumption patterns, and contract interaction statistics. These findings are important not only for classification performance but also for interpretability and practical deployment.

6.1 Interpretation of the Most Important Features

The feature importance analysis revealed that the most influential variables are not arbitrary numeric attributes, but rather behavior-oriented descriptors that characterize how an address interacts with the Ethereum blockchain over time. Across the evaluated models, several features repeatedly emerged as highly informative, particularly those related to transaction count, gas usage, nonce progression, cumulative gas usage, and selected token-level attributes.

Figure 22 compares the top-ranked features across all evaluated models, while Figure 23 shows how often the most important features appeared among the top rankings of different classifiers. These visualizations demonstrate that certain features are consistently useful regardless of whether the model is linear, tree-based, or deep tabular.

Gas-Related Features

Among the most consistently important variables, `addr_gas_used.gas_used_mean` was particularly significant. This feature reflects the average gas consumed by an address across its transactions and captures the typical computational footprint of that address. In Ethereum-based systems, gas usage is closely tied to the complexity and type of smart contract interaction. Normal users often exhibit a relatively varied and application-driven gas usage profile, depending on whether they are transferring tokens, interacting with DeFi protocols, approving contracts, or swapping assets. In contrast, malicious activity often produces more systematic or anomalous gas patterns. Fraud schemes, automated exploit scripts, and wallet-draining behaviors may involve repeated contract calls with similar gas characteristics or unusually extreme gas costs. Therefore, this feature acts as a compact summary of an address's execution behavior and is a strong indicator of whether its interaction pattern is consistent with legitimate use.

Other gas-related attributes such as `addr_gas_used.gas_used_sum`, `addr_gas_used.gas_used_median`, and `addr_gas_used.gas_used_stdev` further enrich this picture. The total gas consumed over a series of trans-

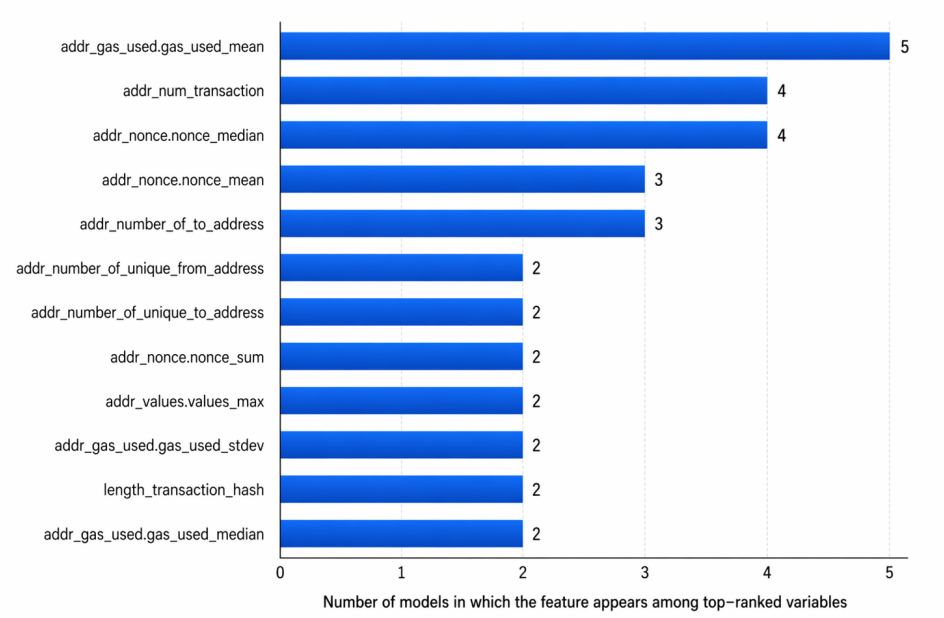


Figure 23: Frequency of occurrence of the most important features across all models. Features that repeatedly appear among the top-ranked variables provide evidence of stable behavioral relevance in multiclass DeFi attack detection.

actions captures cumulative execution intensity, while the median and standard deviation describe the central tendency and variability of that behavior. A malicious address may show either unusually stable behavior, reflecting repeated scripted actions, or unusually irregular behavior, reflecting attempts to exploit or interactions with many different contracts. This explains why gas-related attributes appeared not only in the deep models but also in the stronger baseline models.

Transaction Count Features

The feature `addr_num_transaction` is another major indicator of behavioral intensity. This attribute summarizes how active a wallet is within the observed data. It is particularly useful because many forms of malicious DeFi behavior involve repeated or concentrated activity. Fraudulent wallets may conduct bursts of transactions associated with rug-pull preparation, laundering, or repeated interactions with malicious contracts. Likewise, phishing-related wallets may accumulate repeated inflows and outflows tied to victim accounts. By contrast, legitimate user behavior is often more heterogeneous and less systematically concentrated. As a result, transaction count functions as a high-level signature of wallet behavior and helps distinguish ordinary users from malicious actors.

This feature is also important from a practical perspective because it is intuitively interpretable. A fraud analyst or blockchain investigator can easily understand why an address with abnormal activity volume may be suspicious. Thus, it not only improves classification but also enhances the explainability of the framework.

Nonce Features

Nonce-based features, including addr_nonce.nonce_mean, addr_nonce.nonce_median, addr_nonce.nonce_sum, addr_nonce.nonce_max, and addr_nonce.nonce_min, were especially prominent in NODE and GANDALF. The nonce in Ethereum reflects the sequence number of outgoing transactions from an address, and therefore indirectly captures temporal ordering, transaction progression, and wallet maturity.
These features are powerful because they allow tabular models to absorb part of the sequential nature of blockchain activity without explicitly using a temporal sequence model. For example, an attacker-controlled address may show highly regular or rapidly increasing nonce behavior due to scripted automation, bot-driven interaction, or coordinated exploit execution. Legitimate user behavior, on the other hand, tends to be more irregular and context-dependent. Thus, nonce statistics provide strong evidence about how an address behaves over time, making them highly effective for distinguishing malicious from benign activity.

Cumulative Gas and Value Features

Features such as addr_cumulativeGasUsed_sum, addr_cumulativeGasUsed_max, and addr_values_max are also important because they summarize broader account-level activity beyond individual transactions. Cumulative gas features reflect the overall computational cost associated with an address, while value features capture the scale and distribution of transferred assets. Malicious behavior is often not defined by a single event, but by how activity accumulates over time. Fraud addresses may repeatedly transact in specific value ranges or incur abnormally high cumulative gas costs due to repetitive contract interactions. Therefore, these features help the models learn persistent behavioral signatures rather than isolated point anomalies.

ERC-721 Metadata Features

Some model-specific features, particularly those emphasized by GANDALF and TabNet, were related to ERC-721 metadata, such as erc721_Symbol_Length, erc721_Unique_Chars_Name, erc721_Name_Entropy, and erc721_Is_Zero_Divisor. These features are useful because scam tokens and suspicious NFT-related assets often exhibit unusual naming conventions, low-quality metadata, or irregular symbol structures. For example, highly random names, abnormal character distributions, or suspiciously short or long symbols may indicate deceptive or automatically generated tokens. Such features therefore provide complementary evidence that goes beyond wallet behavior and extends into asset-level semantics.

Discussion of Common and Best Overall Features

Overall, the strongest and most stable features can be grouped into three broad categories:

1. **Activity features:** transaction counts and address-level interaction statistics
2. **Execution-cost features:** gas usage summaries and cumulative gas measures
3. **Sequential behavior features:** nonce-based statistics

Among these, the best overall features across models are:

- addr_gas_used.gas_used_mean
- addr_num_transaction
- addr_nonce.nonce_mean
- addr_nonce.nonce_median

These features are especially valuable because they are not tied to one narrow attack signature. Instead, they capture general behavioral irregularities that are likely to remain relevant even when attack tactics evolve.

6.2 Zero-Day Attack Analysis Across Baseline Models

Although the present work does not implement a strict zero-day experimental setup in which one malicious subtype is withheld during training, the results still provide useful insights into model robustness and generalization. In particular, the relative behavior of the baseline models suggests how different learning paradigms respond when malicious behavior is represented in a shared feature space with overlapping characteristics. Figure 24 compares the baseline models in terms of balanced accuracy and macro F1-score. The figure shows that Logistic Regression and Linear SVM perform noticeably worse than Random Forest, indicating that linear decision boundaries are insufficient for capturing the full complexity of multiclass DeFi attack behavior.

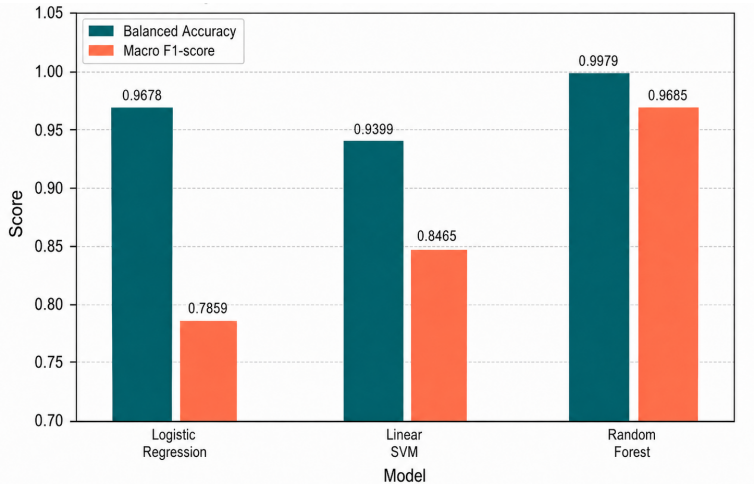


Figure 24: Comparative performance of the baseline models in terms of balanced accuracy and macro F1-score. Random Forest substantially outperforms Logistic Regression and Linear SVM, indicating the importance of nonlinear feature interactions.

Logistic Regression achieved reasonable recall but much lower precision, especially for the minority malicious class. This means that it tended to overpredict suspicious activity and generated more false positives. In real-world settings, such behavior would burden analysts with an excessive volume of alerts and reduce operational trust in the system. Linear SVM improved somewhat on this behavior, but its overall macro-level performance remained clearly below that of the nonlinear methods.

Random Forest emerged as the strongest baseline because it can model nonlinear interactions between blockchain features. This is important because malicious DeFi behavior is rarely defined by a single field. Rather, it emerges from combinations of gas usage, nonce progression, address-level counts, and token-related signals. The stronger performance of Random Forest suggests that any future zero-day detection extension of this work would likely benefit from models that capture nonlinear and interaction-based structure rather than relying on fixed linear separations.

6.3 Class-wise Feature Attribution and Behavioral Signatures

One of the main benefits of the multiclass formulation is that it allows the three classes to be analyzed as distinct behavioral categories. Rather than only distinguishing malicious from benign transactions, the framework learns to separate legitimate, fraud, and phishing patterns within a common feature space. Figure 25 presents the class-wise F1-scores of the evaluated models.

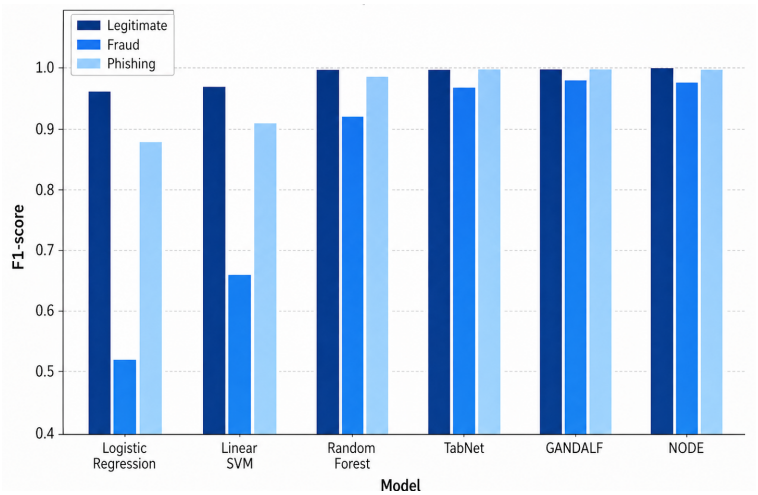


Figure 25: Class-wise F1-score comparison across all evaluated models. The strongest models maintain high performance across legitimate, fraud, and phishing classes, with the most noticeable performance gap appearing in the fraud class for weaker baselines.

Legitimate Class

The legitimate class was recognized with extremely high precision and recall by the strongest models. This suggests that benign DeFi behavior occupies a relatively stable, well-structured region of the feature space. Legitimate addresses likely exhibit more natural variation in their transaction counts, gas usage, and nonce progression, but remain broadly consistent with ordinary DeFi operations. This makes them easier to learn as a reference class.

Fraud Class

The fraud class is especially interesting because it is the smallest class, but still highly separable for the best-performing models. This indicates that fraud transactions exhibit a distinctive behavioral signature.

Fraud-related activity often includes repeated contract interactions, unusual transaction volumes, suspicious value transfer patterns, and characteristic gas or nonce behavior. As a result, even though fraud is relatively rare, it forms a relatively compact malicious region in the feature space. This explains why Random Forest, GANDALF, and NODE all achieved very strong fraud recall.

Phishing Class

Phishing was also detected with very high performance, but it was the malicious class most likely to overlap with legitimate activity. This is visible in the confusion matrices, where the remaining errors more often involve phishing being confused with legitimate rather than fraud. A likely explanation is that phishing-related transactions can more closely mimic ordinary wallet behavior, especially when observed in aggregate statistics. For example, a phishing victim may approve a malicious contract or transfer assets in ways that resemble normal user interaction at a coarse-grained feature level. This makes phishing behavior more diffuse in the shared feature space.
Figure 21 illustrates the normalized confusion matrices for the three best-performing deep tabular models.

6.4 Computational Efficiency

In practical blockchain security applications, model performance must be considered together with computational cost. A model that is highly accurate but prohibitively slow to train or deploy may be less useful than a slightly weaker model that can be retrained frequently and integrated into operational pipelines.
Figure 26 illustrates the trade-off between predictive performance and computational efficiency across the evaluated models. This type of graph is especially useful because it visualizes not only which model is best in absolute terms, but which model offers the best balance between effectiveness and cost.

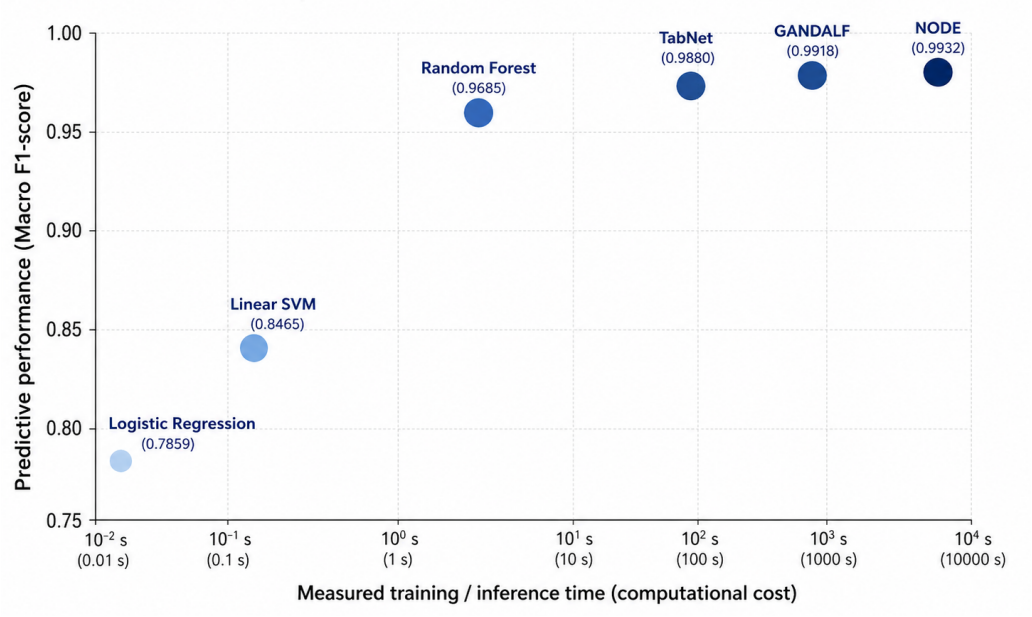


Figure 26: Illustrative trade-off between predictive performance and computational cost across the evaluated models. Replace the plotted values with the measured training or inference times for each model.

From an operational perspective, NODE is the best choice when maximum predictive quality is required. However, if a production setting demands frequent retraining, lower latency, or reduced resource usage, a model such as GANDALF or Random Forest may offer a more favorable balance. This distinction is important in practice because fraud detection pipelines are often updated as new malicious behaviors emerge.

6.5 Feature Dimensionality and Computational Cost Analysis

The final aligned feature space contains 148 numerical features. This dimensionality is moderate: it is rich enough to capture wallet-level behavior, gas-related execution characteristics, and token-level descriptors, yet still tractable for large-scale tabular learning.

However, when combined with millions of samples, even 148 features produce significant computational demands. The preprocessing pipeline therefore plays a critical role in the feasibility of the framework. By coercing non-numeric values into numeric form, handling missing and infinite values, clipping extreme values, and converting all features to float32, the framework reduces memory usage while maintaining sufficient numerical precision for effective training.

Figure 27 groups the most important features by category, showing that not all 148 features contribute equally. A relatively small subset of activity, gas, and nonce features accounts for much of the predictive power. This suggests that future studies on feature pruning or dimensionality reduction may reduce costs while preserving most of the classification performance.

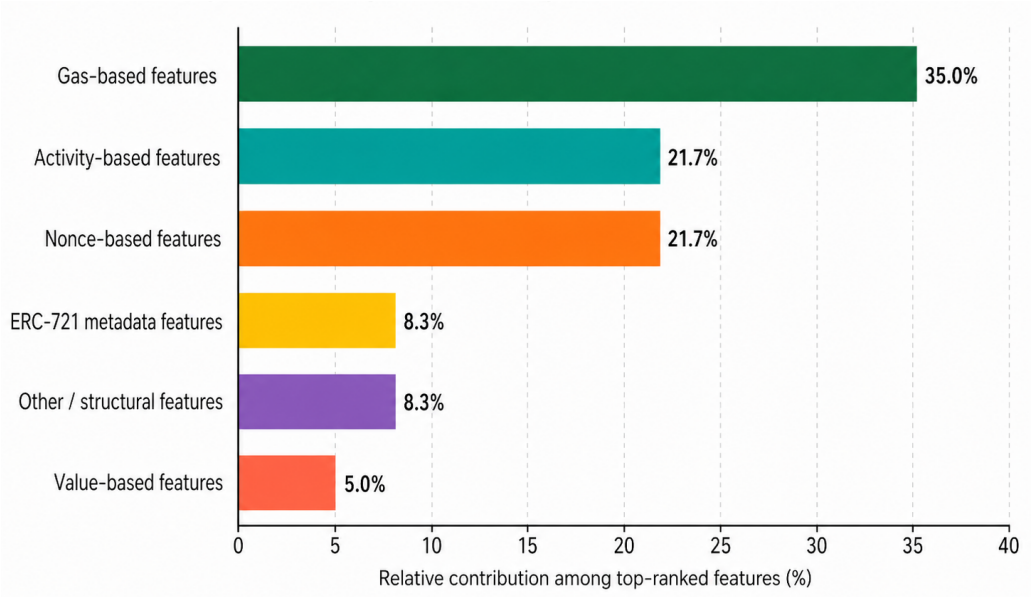


Figure 27: Relative importance of major feature groups in the multiclass DeFi detection framework. The figure highlights the dominant role of activity, gas, and nonce-based features.

6.6 Comparative Performance Evaluation

The overall comparison of the six evaluated models yields several important conclusions. First, the multiclass DeFi detection problem is not adequately captured by linear models. Logistic Regression and Linear

SVM provide useful baselines, but their lower macro precision and macro F1-scores indicate that the merged blockchain feature space contains nonlinear relationships that simple linear boundaries cannot model effectively.

Second, Random Forest establishes a strong conventional baseline and confirms the importance of nonlinear feature interactions. Third, deep tabular models yield the strongest overall results, demonstrating that richer representation learning is particularly useful for multiclass DeFi attack detection. Figure 28 summarizes the comparative performance of all evaluated models.

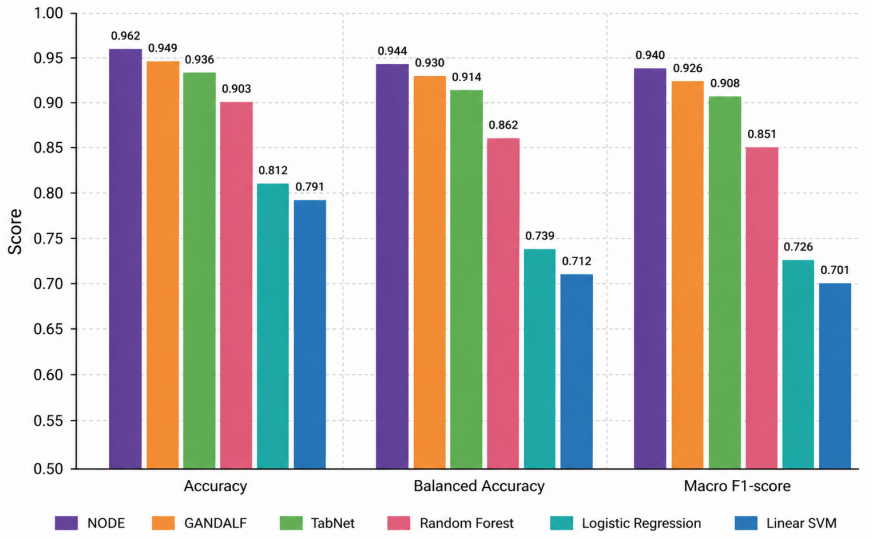


Figure 28: Overall comparative performance of all evaluated models in terms of accuracy, balanced accuracy, and macro F1-score.

Among the deep models, NODE achieved the best overall predictive performance. This suggests that its architecture is especially effective at capturing the subtle interactions among wallet activity, gas usage, and sequential behavior that characterize fraud and phishing transactions. GANDALF followed closely and can be interpreted as the most balanced deep model, particularly if efficiency considerations are incorporated. TabNet also performed strongly and contributed useful interpretability insights, even if its final metrics were slightly lower than those of NODE and GANDALF.

The final ranking observed in this thesis is:

$$\text{NODE} > \text{GANDALF} > \text{TabNet} > \text{Random Forest} > \text{Linear SVM} > \text{Logistic Regression}.$$

This ranking should be understood within the context of the aligned 148-feature multiclass benchmark proposed in this work. Within that setting, the results clearly support the use of deep tabular learning for practical Ethereum-based DeFi attack detection.

6.7 Industrial Relevance and Practical Use of the Proposed Framework

One of the most important implications of this work is its practical applicability to blockchain security operations. The proposed multiclass framework is not only an academic classification system but also supports

several real-world use cases.

Exchange and Custodial Wallet Risk Screening

Cryptocurrency exchanges and wallet providers can use the model as a pre-screening layer for addresses or transactions. Instead of relying solely on blacklists or manually curated rules, they can incorporate behavioral analytics into transaction monitoring. Addresses exhibiting fraud-like or phishing-like characteristics can be flagged for additional verification, restricted withdrawals, or manual review.

AML and Compliance Monitoring

Compliance teams can use the framework as a prioritization tool in anti-money-laundering workflows. Multiclass predictions help analysts distinguish between different suspicious profiles rather than simply labeling activity as risky or non-risky. This is operationally useful because phishing-related behavior and fraud-related behavior may require different investigation workflows.

SOC and Threat Hunting

Blockchain intelligence teams and security operation centers can use the model outputs to triage large volumes of transactions more efficiently. Rather than manually reviewing massive transaction logs, analysts can focus first on the highest-risk wallets and transactions identified by the classifier. Because the top features are behaviorally interpretable, the alerts are more explainable and actionable.

Fraud Investigation and Forensics

The framework can also support post-incident investigation. If a wallet is classified as fraud-like, investigators can inspect its interaction history, gas profile, value patterns, and neighboring wallets to reconstruct the attack path. If it is classified as phishing-like, analysts may instead focus on malicious approval behavior, token traps, or deceptive contract interactions.
Industry relevance stems from three main strengths of the framework:

1. it delivers very strong multiclass detection performance;
2. it relies on interpretable behavioral features rather than only opaque signatures;
3. it can serve as a scalable screening and prioritization layer in existing blockchain monitoring pipelines.

Therefore, the practical value of this thesis lies not only in achieving high classification accuracy but also in demonstrating how behavioral machine learning can support more proactive and explainable DeFi security analytics.
This chapter interpreted the experimental results from a behavioral, computational, and practical perspective. The most important features were shown to capture meaningful properties of wallet activity, gas usage, transaction ordering, and token metadata. Fraud emerged as the most behaviorally distinctive malicious class, while phishing remained the malicious class most likely to overlap with legitimate activity. Among

the evaluated methods, deep tabular models provided the strongest overall results, with NODE achieving the best predictive performance. Finally, the discussion showed that the proposed framework has clear industrial relevance for exchange monitoring, compliance workflows, threat hunting, and blockchain forensic analytics.

7 Conclusion

This thesis examined the security challenges and structural complexity of the decentralized finance ecosystem, with a particular focus on fraud and phishing detection in Ethereum-based DeFi transactions. The work was motivated by the rapid growth of DeFi platforms and the increasing sophistication of malicious activities that exploit the open, pseudonymous, and automated nature of blockchain-based financial systems.

The first part of the thesis presented a broad comparative study of 284 DeFi platforms. By organizing platforms into major functional and economic categories and evaluating them through standardized criteria, the study provided a systematic view of the DeFi ecosystem. This analysis showed that DeFi platforms vary significantly in their support for lending, borrowing, staking, yield generation, governance, cross-chain interoperability, privacy, insurance, and infrastructure services. It also demonstrated that broader functional coverage does not necessarily imply stronger security resilience, since many platforms still lack clear evidence of protection against major DeFi attack vectors.

The second part of the thesis proposed a unified multiclass machine learning framework for DeFi attack detection. By integrating legitimate, fraud, and phishing records into a shared feature space, the framework moved beyond separate binary classification tasks and addressed a more realistic detection problem. Three conventional machine learning models, namely Logistic Regression, Support Vector Machine, and Random Forest, were used as baselines. These baselines were compared with three deep tabular learning models, namely TabNet, GANDALF, and NODE. All six models were evaluated under the same preprocessing and experimental conditions.

The experimental results demonstrated that deep tabular learning models outperform conventional baselines in terms of balanced accuracy and macro F1-score. Among all evaluated models, NODE achieved the strongest overall performance, followed closely by GANDALF and TabNet. The confusion matrix results further confirmed that the best-performing models were able to detect minority malicious classes with very few errors, which is especially important in security applications where missed attacks can have significant consequences.

Feature importance analysis showed that transaction-level behavioral indicators play a central role in DeFi attack detection. In particular, gas usage statistics, nonce-based features, transaction frequency, and account-level activity patterns were repeatedly identified as important predictors across different models. These findings suggest that malicious DeFi behavior can be detected not only through direct attack signatures, but also through broader behavioral patterns captured from blockchain transaction data.

Overall, this thesis contributes a structured analysis of the DeFi ecosystem and a practical data-driven framework for detecting fraud and phishing activity. The results provide useful insights for researchers, platform developers, and security practitioners working to improve the reliability and trustworthiness of decentralized financial systems. Future work may extend this framework by incorporating temporal sequence modeling, graph-based transaction relationships, real-time monitoring, and cross-chain data to improve adaptability against evolving DeFi threats.

Bibliography

[1] K. Qin, L. Zhou, Y. Afonin, L. Lazzaretti, and A. Gervais, "Cefi vs. defi–comparing centralized to decentralized finance," *arXiv preprint arXiv:2106.08157*, 2021.

[2] J. Kim and S. Yoon, "Ai bias in financial fraud detection," *Financial Technology and Ethics*, vol. 11, no. 3, pp. 215–228, 2022.

[3] A. Wieandt and L. Heppding, "Centralized and decentralized finance: Coexistence or convergence?," in *The Fintech disruption: How financial innovation is transforming the banking industry*, pp. 11–51, Springer, 2023.

[4] J. Smith and R. Patel, "The evolution of rule-based fraud detection in cefi," *Journal of Financial Security*, vol. 10, no. 3, pp. 123–134, 2022.

[5] K. Wüst and A. Gervais, "Do you need a blockchain?," in *2018 crypto valley conference on blockchain technology (CVCBT)*, pp. 45–54, IEEE, 2018.

[6] K. John, L. Kogan, and F. Saleh, "Smart contracts and decentralized finance," *Annual Review of Financial Economics*, vol. 15, no. 1, pp. 523–542, 2023.

[7] J. Son and D. Ryu, "Competitive dynamics between decentralized and centralized finance lending markets," *International Review of Financial Analysis*, vol. 96, p. 103699, 2024.

[8] R. Johnson and H. Lee, "Machine learning in financial fraud detection," *Finance Technology Journal*, vol. 15, no. 2, pp. 67–79, 2023.

[9] P. Martin and Q. Liu, "Advancements in unsupervised learning for cefi fraud detection," *Computational Economics*, vol. 30, no. 4, pp. 401–414, 2022.

[10] A. H. Lashkari, S. Hajihosseinkhani, J. Duarte, I. Lopez, Z. H. Lashkari, and S. Rios-Aguilar, "Advanced genetic algorithm and penalty fitness function for enhancing defi security and detecting ethereum fraud transactions," *Blockchain: Research and Applications*, p. 100376, 2025.

[11] A. Lopez *et al.*, "The role of neural networks in fraud detection," *Journal of Artificial Intelligence in Finance*, vol. 8, no. 1, pp. 44–58, 2023.

[12] S. HajiHosseinKhani, A. H. Lashkari, and A. M. Oskui, "Unveiling smart contract vulnerabilities: Toward profiling smart contract vulnerabilities using enhanced genetic algorithm and generating benchmark dataset," *Blockchain: Research and Applications*, vol. 6, no. 2, p. 100253, 2025.

[13] S. HajiHosseinKhani, A. H. Lashkari, and A. M. Oskui, "Unveiling vulnerable smart contracts: Toward profiling vulnerable smart contracts using genetic algorithm and generating benchmark dataset," *Blockchain: Research and Applications*, p. 100171, 2023.

[14] Z. Jakab and M. Kumhof, "Banks are not intermediaries of loanable funds—facts, theory and evidence," 2018.

[15] E. Mouncey and S. Ciobotaru, "Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness," *Journal of Economic Criminology*, vol. 7, p. 100125, 2025.

[16] F. Greco, G. Desolda, P. Buono, and A. Piccinno, "Enhancing phishing defenses: The impact of timing and explanations in warning for email clients," *Computer Standards & Interfaces*, p. 103982, 2025.

[17] S. Zheng and I. Becker, "Presenting suspicious details in {user-facing} e-mail headers does not improve phishing detection," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pp. 253–271, 2022.

[18] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and prevention of spear phishing attacks: A comprehensive survey," *Computers & Security*, p. 104317, 2025.

[19] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, p. 563060, 2021.

[20] Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang, and X. Zhang, "Detecting phishing scams on ethereum based on transaction records," in *2020 IEEE international symposium on circuits and systems (ISCAS)*, pp. 1–5, IEEE, 2020.

[21] J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, "Who are the phishers? phishing scam detection on ethereum via network embedding," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 2, pp. 1156–1166, 2020.

[22] T. Wen, Y. Xiao, A. Wang, and H. Wang, "A novel hybrid feature fusion model for detecting phishing scam on ethereum using deep neural network," *Expert Systems with Applications*, vol. 211, p. 118463, 2023.

[23] R. Li, Z. Liu, Y. Ma, D. Yang, and S. Sun, "Internet financial fraud detection based on graph learning," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 3, pp. 1394–1401, 2022.

[24] L. Wang, M. Xu, and H. Cheng, "Phishing scams detection via temporal graph attention network in ethereum," *Information Processing & Management*, vol. 60, no. 4, p. 103412, 2023.

[25] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the ethereum blockchain," *Expert Systems with Applications*, vol. 150, p. 113318, 2020.

[26] N. Kumar, A. Singh, A. Handa, and S. K. Shukla, "Detecting malicious accounts on the ethereum blockchain with supervised learning," in *Cyber Security Cryptography and Machine Learning: Fourth International Symposium, CSCML 2020, Be'er Sheva, Israel, July 2–3, 2020, Proceedings 4*, pp. 94–109, Springer, 2020.

[27] M. Gunathilaka, S. Wickramanayake, and H. D. Bandara, "Defitrust: A transformer-based framework for scam defi token detection using event logs and sentiment analysis," *Expert Systems with Applications*, vol. 251, p. 123913, 2024.

[28] D. Chen, L. Feng, Y. Fan, S. Shang, and Z. Wei, "Smart contract vulnerability detection based on semantic graph and residual graph convolutional networks with edge attention," *Journal of Systems and Software*, vol. 202, p. 111705, 2023.

[29] S. Hu, Z. Zhang, B. Luo, S. Lu, B. He, and L. Liu, "Bert4eth: A pre-trained transformer for ethereum fraud detection," in *Proceedings of the ACM Web Conference 2023*, pp. 2189–2197, 2023.

[30] C. Jin, J. Zhou, C. Xie, S. Yu, Q. Xuan, and X. Yang, "Enhancing ethereum fraud detection via generative and contrastive self-supervision," *arXiv preprint arXiv:2408.00641*, 2024.

[31] S. Wu, D. Wang, J. He, Y. Zhou, L. Wu, X. Yuan, Q. He, and K. Ren, "Defiranger: Detecting price manipulation attacks on defi applications," 2021.

[32] S. Al-E'mari, M. Anbar, Y. Sanjalawe, and S. Manickam, "A labeled transactions-based dataset on the ethereum network," in *International Conference on Advances in Cyber Security*, pp. 61–79, Springer, 2020.

[33] K. John, B. Monnot, P. Mueller, F. Saleh, and C. Schwarz-Schilling, "Economics of ethereum," *Available at SSRN 4783695*, 2024.

[34] M. Imran, B. Yao, W. Ali, A. Akhunzada, M. K. Azhar, M. Junaid, and U. Iqbal, "Research perspectives and challenges of blockchain for data-intensive and resource-constrained devices," *IEEE Access*, vol. 10, pp. 38104–38122, 2022.

[35] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "Ai-powered fraud detection in decentralized finance: A project life cycle perspective," *ACM Computing Surveys*, vol. 57, no. 4, pp. 1–38, 2024.

[36] E. Hoch, "The defi ecosystem game: Proof-via-simulations," in *The International Conference on Mathematical Research for Blockchain Economy*, pp. 285–314, Springer, 2024.

[37] O. Tjäder and L. Ulrich, "The great defi dilemma: How stakeholders can navigate the uncertain waters of decentralised finance adoption: An explorative study," 2023.

[38] M. Salah *et al.*, "Decentralized finance (defi) on blockchain: Current landscape and future trends," *Journal of Innovative Technologies*, vol. 6, no. 1, pp. 1–13, 2023.

[39] F. Jia, J. Zheng, and F. Li, "Decentralized intelligence in gamefi: Embodied ai agents and the convergence of defi and virtual ecosystems," *arXiv preprint arXiv:2412.18601*, 2024.

[40] B. Kaplan, V. F. Benli, and E. A. Alp, "Blockchain based decentralized lending protocols: A return analysis between s&p 500 and defi assets," *JOEEP: Journal of Emerging Economies and Policy*, vol. 8, no. 1, pp. 360–378, 2023.

[41] A. Turillazzi, A. Tsamados, E. Gencc, M. Taddeo, and L. Floridi, "Decentralised finance (defi): a critical review of related risks and regulation," *Available at SSRN*, 2023.

[42] A. Trozze, B. Kleinberg, and T. Davies, "Detecting defi securities violations from token smart contract code," 2023.

[43] S. Ren, T. Tu, J. Liu, D. Wu, and K. Ren, "Lookahead: Preventing defi attacks via unveiling adversarial contracts," 2024.

[44] R. Gan, L. Zhou, L. Wang, K. Qin, and X. Lin, "Defialigner: Leveraging symbolic analysis and large language models for inconsistency detection in decentralized finance," in *6th Conference on Advances in Financial Technologies (AFT 2024)*, Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024.

[45] Z. Chen, S. M. Beillahi, and F. Long, "Flashsyn: Flash loan attack synthesis via counter example driven approximation," in *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, pp. 1–13, 2024.

[46] D. Sun, W. Ma, L. Nie, and Y. Liu, "Sok: Comprehensive analysis of rug pull causes, datasets, and detection tools in defi," 2024.

[47] Y. Xue, D. Fan, S. Su, J. Fu, N. Hu, W. Liu, and Z. Tian, "A review on the security of the ethereum-based defi ecosystem.," *CMES-Computer Modeling in Engineering & Sciences*, vol. 139, no. 1, 2024.

[48] P. Qian, R. Cao, Z. Liu, W. Li, M. Li, L. Zhang, Y. Xu, J. Chen, and Q. He, "Empirical review of smart contract and defi security: vulnerability detection and automated repair," *arXiv preprint arXiv:2309.02391*, 2023.

[49] D. Rabetti, "Auditing decentralized finance (defi) protocols," in *Proceedings of the Conference on Decentralized Finance (DEFI) Protocols*, vol. 15, pp. 1–58, 2023.

[50] R. M. Aziz, M. F. Baluch, S. Patel, and P. Kumar, "A machine learning based approach to detect the ethereum fraud transactions with limited attributes," *Karbala International Journal of Modern Science*, 2022.

[51] R. M. Aziz, M. F. Baluch, S. Patel, and A. H. Ganie, "Lgbm: a machine learning approach for ethereum fraud detection," *International Journal of Information Technology*, vol. 14, no. 7, pp. 3321–3331, 2022.

[52] V. Ravindranath, M. Nallakaruppan, M. L. Shri, B. Balusamy, and S. Bhattacharyya, "Evaluation of performance enhancement in ethereum fraud detection using oversampling techniques," *Applied Soft Computing*, vol. 161, p. 111698, 2024.

[53] S. S. Taher, S. Y. Ameen, and J. A. Ahmed, "Advanced fraud detection in blockchain transactions: An ensemble learning and explainable ai approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12822–12830, 2024.

[54] D. Wang, B. Wu, X. Yuan, L. Wu, Y. Zhou, and H. Cui, "Defiguard: A price manipulation detection service in defi using graph neural networks," 2024.

[55] H. Kanezashi, T. Suzumura, X. Liu, and T. Hirofuchi, "Ethereum fraud detection with heterogeneous graph neural networks," *arXiv preprint arXiv:2203.12363*, 2022.

[56] R. Tan, Q. Tan, P. Zhang, and Z. Li, "Graph neural network for ethereum fraud detection," in *2021 IEEE international conference on big knowledge (ICBK)*, pp. 78–85, IEEE, 2021.

[57] R. Tan, Q. Tan, Q. Zhang, P. Zhang, Y. Xie, and Z. Li, "Ethereum fraud behavior detection based on graph neural networks," *Computing*, vol. 105, no. 10, pp. 2143–2170, 2023.

[58] H. An, R. Ma, Y. Yan, T. Chen, Y. Zhao, P. Li, J. Li, X. Wang, D. Fan, and C. Lv, "Finsformer: A novel approach to detecting financial attacks using transformer and cluster-attention," *Applied Sciences*, vol. 14, no. 1, p. 460, 2024.

[59] Y. Jia, Y. Wang, J. Sun, Y. Liu, Z. Sheng, and Y. Tian, "Ethereum fraud detection via joint transaction language model and graph representation learning," *arXiv preprint arXiv:2409.07494*, 2024.

[60] B. Norouzi, "Enhancing fraudulent account detection on the ethereum blockchain: A novel feature selection approach and comparative analysis of machine learning algorithms," master's thesis, Bishop's University, August 2023. https://www.ubishops.ca/wp-content/uploads/norouzi20230801.pdf.

[61] B. Wang, X. Yuan, L. Duan, H. Ma, C. Su, and W. Wang, "Defiscanner: Spotting defi attacks exploiting logic vulnerabilities on blockchain," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1577–1588, 2022.

[62] G. Palaiokrassas, S. Scherrers, I. Ofeidis, and L. Tassiulas, "Leveraging machine learning for multi-chain defi fraud detection," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 678–680, IEEE, 2024.

[63] G. Palaiokrassas, S. Scherrers, E. Makri, and L. Tassiulas, "Machine learning in defi: Credit risk assessment and liquidation prediction," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 650–654, IEEE, 2024.

[64] V. Mothukuri, R. M. Parizi, J. L. Massa, and A. Yazdinejad, "An ai multi-model approach to defi project trust scoring and security," in *2024 IEEE International Conference on Blockchain (Blockchain)*, pp. 19–28, IEEE, 2024.

[65] S. Kitzler, F. Victor, P. Saggese, and B. Haslhofer, "Disentangling decentralized finance (defi) compositions," 2022.

[66] M. Xie, M. Hu, Z. Kong, C. Zhang, Y. Feng, H. Wang, Y. Xue, H. Zhang, Y. Liu, and Y. Liu, "Defort: Automatic detection and analysis of price manipulation attacks in defi applications," in *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis*, pp. 402–414, 2024.

[67] B. Wang, H. Liu, C. Liu, Z. Yang, Q. Ren, H. Zheng, and H. Lei, "Blockeye: Hunting for defi attacks on blockchain," in *2021 IEEE/ACM 43rd international conference on software engineering: companion proceedings (ICSE-companion)*, pp. 17–20, IEEE, 2021.

[68] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "Ai-powered fraud detection in decentralized finance: A project life cycle perspective," *ACM Computing Surveys*, 2023.

[69] S. M. Werner, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, "Sok: Decentralized finance (defi)," *arXiv preprint arXiv:2404.11281*, 2024.

[70] R. Zhang, S. Xiong, and B. Zhao, "Similarities and differences in defi protocols: A comparative study," *arXiv preprint arXiv:2404.00034*, 2024.

[71] F. Schär, "Decentralized finance: On blockchain- and smart contract-based financial markets," *Journal of Financial Stability*, vol. 50, p. 100–106, 2021.

[72] A. Unknown, "A dynamic taxonomy of defi protocols," *SSRN Electronic Journal*, 2024.

[73] P. Amores, M. Hernández, and D. Castillo, "Blockchain governance in decentralized finance," *arXiv preprint arXiv:2311.01433*, 2023.

[74] T. Gupta, R. Sharma, and R. Kumar, "Ai-powered fraud detection in defi ecosystems," *arXiv preprint arXiv:2308.15992*, 2023.

[75] U.S. Department of the Treasury, "Illicit finance risk assessment of decentralized finance." https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf, 2023.

[76] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, "An analysis of uniswap markets," 2021.

[77] dForce Team, "dforce: Modular defi protocols." https://dforce.network, 2024. Accessed: 2025-10-02.

[78] Horizon Protocol Team, "Horizon protocol: Synthetic asset platform." https://horizonprotocol.com, 2024. Accessed: 2025-10-02.

[79] Frankencoin Team, "Frankencoin: Decentralized stablecoin protocol." https://frankencoin.com, 2024. Accessed: 2025-10-02.

[80] CoinMarketCap Academy, "What is midas investments (midas)? offering the highest yields on btc, eth, and usdt." https://coinmarketcap.com/academy/article/what-is-midas-investments-midas-offering-the-highest-yields-on-btc-eth-and-usdt, 2022. Accessed: 2025-10-06.

[81] Aave Team, "Aave protocol whitepaper v1.0," tech. rep., Aave, 2020. Accessed: 2025-10-06.

[82] Synthetix Team, "Synthetix: Synthetic asset protocol." https://synthetix.io, 2024. Accessed: 2025-10-02.

[83] Chainge Finance Team, "Chainge: Cross-chain defi aggregator." https://chainge.finance, 2024. Accessed: 2025-10-02.

[84] Parrot Protocol Team, "Parrot protocol documentation." https://doc.parrot.fi/guide/, 2024. Accessed: 2025-10-06.

[85] MANTRA Team, "Mantra: Community-governed defi ecosystem." https://mantrachain.io, 2024. Accessed: 2025-10-02.

[86] UniLend Team, "Unilend: Permissionless spot trading and lending." https://unilend.finance, 2024. Accessed: 2025-10-02.

[87] Mimo Labs, "Mimo: Decentralized stablecoin and lending platform." https://mimo.capital, 2024. Accessed: 2025-10-02.

[88] Hope.money Team, "Hope.money protocol documentation." https://docs.hope.money/, 2024. Accessed: 2025-10-06.

[89] Larix Team, "Larix: Solana-based lending protocol." https://projectlarix.com, 2024. Accessed: 2025-10-02.

[90] Synthetify Team, "Synthetify: Solana-based synthetic asset protocol." https://synthetify.io, 2024. Accessed: 2025-10-02.

[91] Abracadabra Team, "Abracadabra: Interest-bearing collateralized lending." https://abracadabra.money, 2024. Accessed: 2025-10-02.

[92] Alchemy / Mass Team, "Mass: Defi mobile platform." https://www.alchemy.com/dapps/mass, 2025. Accessed: 2025-10-06.

[93] QuickSwap Team, "Quickswap: Decentralized exchange on polygon." https://quickswap.exchange, 2024. Accessed: 2025-10-06.

[94] Angle Protocol Team, "Angle protocol documentation." https://angle.money, 2024. Accessed: 2025-10-06.

[95] Euler Finance Team, "Euler finance: Permissionless lending for long-tail assets." https://www.euler.finance, 2024. Accessed: 2025-10-06.

[96] Fringe Finance Team, "Fringe finance platform documentation." https://docs.fringe.fi/, 2024. Accessed: 2025-10-06.

[97] Maple Finance Team, "Maple finance: Institutional credit protocol." https://maple.finance, 2024. Accessed: 2025-10-06.

[98] Venus Protocol Team, "Venus protocol: Decentralized money market on bnb chain." https://app.venus.io, 2024. Accessed: 2025-10-06.

[99] Sushi DAO, "Sushi: Multichain defi ecosystem." https://sushi.com, 2024. Accessed: 2025-10-06.

[100] Silo Finance Team, "Silo finance: Isolated lending markets." https://www.silo.finance, 2024. Accessed: 2025-10-06.

[101] Wombat Exchange Team, "Wombat exchange: Multichain stablecoin dex." https://www.wombat.exchange, 2024. Accessed: 2025-10-06.

[102] ShapeShift DAO, "Shapeshift dao: Cross-chain defi platform." https://shapeshift.com, 2024. Accessed: 2025-10-06.

[103] CoinMarketCap, "Ooki protocol (ooki) — coinmarketcap." https://coinmarketcap.com/currencies/ooki-protocol/, 2025. Accessed: 2025-10-06.

[104] Qi Dao Team, "Mai (qi dao): Polygon-based stablecoin protocol." https://www.mai.finance, 2024. Accessed: 2025-10-06.

[105] Goldfinch Finance Team, "Goldfinch: Real-world credit protocol." https://goldfinch.finance, 2024. Accessed: 2025-10-06.

[106] Coinbureau Editorial Team, "Meld protocol: Defi banking on cardano." https://coinbureau.com/review/meld-protocol/, 2023. Accessed: 2025-10-06.

[107] Lido Team, "Lido: Liquid staking protocol." https://lido.fi, 2024. Accessed: 2025-10-06.

[108] Cream Finance Team, "Cream finance: Defi lending protocol." https://cream.finance, 2024. Accessed: 2025-10-06.

[109] Mintera Team, "Mintera: Sustainable defi protocol." https://mintera.io, 2024. Accessed: 2025-10-06.

[110] TrueFi Team, "Truefi: Uncollateralized lending protocol." https://truefi.io, 2024. Accessed: 2025-10-06.

[111] Notional Finance Team, "Notional: Fixed-rate lending and borrowing." https://notional.finance, 2024. Accessed: 2025-10-06.

[112] Compound Labs, "Compound protocol whitepaper," tech. rep., 2019. Accessed: 2025-10-06.

[113] SmartCredit.io Team, "Smartcredit.io: Fixed-income lending platform." https://smartcredit.io, 2024. Accessed: 2025-10-06.

[114] Marinade Finance Team, "Marinade finance: Solana liquid staking protocol." https://marinade.finance, 2024. Accessed: 2025-10-06.

[115] Bancor Team, "Bancor: Automated market maker and liquidity protocol." https://bancor.network, 2024. Accessed: 2025-10-06.

[116] Jet Protocol Team, "Jet protocol: Solana-based lending platform." https://jetprotocol.io, 2024. Accessed: 2025-10-06.

[117] Beanstalk Farms, "Beanstalk: Algorithmic stablecoin protocol." https://bean.money, 2024. Accessed: 2025-10-06.

[118] mStable Team, "mstable: Stablecoin aggregation and yield platform." https://mstable.org, 2024. Accessed: 2025-10-06.

[119] Carbonable Team, "Carbonable: Sustainable defi and carbon offset platform." https://carbonable.io, 2024. Accessed: 2025-10-06.

[120] Open Dollar Team, "Open dollar: Collateralized stablecoin lending protocol." https://www.opendollar.com, 2024. Accessed: 2025-10-06.

[121] Tarot Team, "Tarot: Leveraged yield farming and lending protocol." https://www.tarot.to, 2024. Accessed: 2025-10-06.

[122] Brú Finance Team, "Brú finance: Real-world asset tokenization and credit protocol." https://bru.finance, 2024. Accessed: 2025-10-06.

[123] Quicksilver Team, "Quicksilver: Liquid staking for cosmos ecosystem." https://quicksilver.zone, 2024. Accessed: 2025-10-06.

[124] Liquity Team, "Liquity protocol whitepaper," tech. rep., 2021. Accessed: 2025-10-06.

[125] Veda Finance Team, "Veda finance: Decentralized credit and liquidity management." https://veda.finance, 2024. Accessed: 2025-10-06.

[126] bemo Team, "bemo: Liquid staking on near protocol." https://bemo.finance, 2024. Accessed: 2025-10-06.

[127] Stader Labs, "Stader: Multi-chain liquid staking platform." https://staderlabs.com, 2024. Accessed: 2025-10-06.

[128] Davos Protocol Team, "Davos protocol: Yield-backed stablecoin." https://www.davos.xyz, 2024. Accessed: 2025-10-06.

[129] StakeWise Team, "Stakewise: Dual-token liquid staking protocol." https://stakewise.io, 2024. Accessed: 2025-10-06.

[130] Alchemy / Yield Protocol Team, "Yield protocol: Fixed-rate lending and borrowing dapp." https://www.alchemy.com/dapps/yield-protocol, 2025. Accessed: 2025-10-06.

[131] Lara Protocol Team, "Lara protocol: Undercollateralized credit markets." https://laraprotocol.com, 2024. Accessed: 2025-10-06.

[132] Wildcat Finance Team, "Wildcat: Configurable decentralized credit markets." https://wildcat.finance, 2024. Accessed: 2025-10-06.

[133] Raydium Team, "Raydium: Amm and order book integration on solana." https://raydium.io, 2024. Accessed: 2025-10-06.

[134] Timeswap Labs, "Timeswap: Oracle-free lending and borrowing protocol." https://timeswap.io, 2024. Accessed: 2025-10-06.

[135] Rocket Pool Team, "Rocket pool: Decentralized ethereum staking protocol." https://rocketpool.net, 2024. Accessed: 2025-10-06.

[136] Router Protocol Team, "Router protocol: Cross-chain liquidity infrastructure." https://www.routerprotocol.com, 2024. Accessed: 2025-10-06.

[137] Port Finance Team, "Port finance: Solana money market protocol." https://port.finance, 2024. Accessed: 2025-10-06.

[138] Hubble Protocol Team, "Hubble protocol: Usdh stablecoin and collateralized borrowing." https://hubbleprotocol.io, 2024. Accessed: 2025-10-06.

[139] Mayan Finance Team, "Mayan finance: Cross-chain swaps on solana." https://mayan.finance, 2024. Accessed: 2025-10-06.

[140] Unit Protocol Team, "Unit protocol: Usdp stablecoin and borrowing system." https://unit.xyz, 2024. Accessed: 2025-10-06.

[141] Ribbon Finance Team, "Ribbon finance: Structured products and options vaults." https://www.ribbon.finance, 2024. Accessed: 2025-10-06.

[142] Solend Team, "Solend: Solana lending and borrowing protocol." https://solend.fi, 2024. Accessed: 2025-10-06.

[143] Badger DAO, "Badger finance: Bitcoin yield and liquidity protocol." https://badger.finance, 2024. Accessed: 2025-10-06.

[144] Circle Team, "Circle yield: Institutional crypto yield product." https://www.circle.com/en/yield, 2024. Accessed: 2025-10-06.

[145] Morpho Labs, "Introducing morpho: The peer-to-peer layer on lending protocols." https://morpho.org/blog/introducing-morpho/, 2024. Accessed: 2025-10-06.

[146] Ankr Team, "Ankr: Multi-chain liquid staking solution." https://www.ankr.com, 2024. Accessed: 2025-10-06.

[147] Minterest Team, "Minterest: Revenue-sharing lending protocol." https://minterest.com, 2024. Accessed: 2025-10-06.

[148] Term Finance Team, "Term finance: Fixed-term lending via auction markets." https://term.finance, 2024. Accessed: 2025-10-06.

[149] Tectonic Finance Team, "Tectonic finance: Cross-chain money market on cronos." https://tectonic.finance, 2024. Accessed: 2025-10-06.

[150] Veno Finance Team, "Veno finance: Liquid staking on cronos." https://veno.finance, 2025. Accessed: 2025-10-06.

[151] C. Fisch, C. Masiak, S. Vismara, and Y. Zhang, "Initial coin offerings: Financing growth with cryptocurrency token sales," *Journal of Corporate Finance*, vol. 62, p. 101–186, 2019.

[152] Hakka Finance Team, "Hakka finance: Decentralized financial ecosystem." https://hakka.finance, 2025. Accessed: 2025-10-06.

[153] Shade Protocol Team, "Shade protocol: Privacy-preserving defi on secret network." https://shadeprotocol.io, 2025. Accessed: 2025-10-06.

[154] Ronin / Katana Team, "Katana: Decentralized exchange on ronin." https://katana.roninchain.com, 2025. Accessed: 2025-10-06.

[155] CrossCurve Finance Team, "Crosscurve: Cross-chain stable asset exchange." https://crosscurve.fi, 2025. Accessed: 2025-10-06.

[156] CVI Finance Team, "Cvi finance: Crypto volatility index platform." https://cvi.finance, 2025. Accessed: 2025-10-06.

[157] Trader Joe Team / Avalanche Builder Hub, "Trader joe integration on avalanche builder." https://build.avax.network/integrations/trader-joe, 2025. Accessed: 2025-10-06.

[158] Biswap Team, "Biswap: Decentralized exchange on bsc." https://biswap.org, 2025. Accessed: 2025-10-06.

[159] KyberSwap Team, "Kyberswap: Multi-chain dex aggregator." https://kyberswap.com, 2025. Accessed: 2025-10-06.

[160] StellaSwap Team, "Stellaswap: Defi hub on moonbeam." https://stellaswap.com, 2025. Accessed: 2025-10-06.

[161] Preon Finance Team, "Preon finance: Collateralized stablecoin protocol." https://preon.finance, 2025. Accessed: 2025-10-06.

[162] Beethoven X Team, "Beethoven x: Defi investment platform on balancer tech." https://beets.fi, 2025. Accessed: 2025-10-06.

[163] Nolus Team, "Nolus: Leveraged lending and borrowing protocol." https://nolus.io, 2025. Accessed: 2025-10-06.

[164] Defx Team, "Defx: Decentralized exchange layer 1 for perpetual futures." https://defx.com/, 2025. Accessed: 2025-10-06.

[165] Curve Finance Team, "Curve finance: Stablecoin amm and governance." https://curve.fi, 2025. Accessed: 2025-10-06.

[166] Alium Finance Team, "Alium finance: Introducing hybrid dex liquidity to address liquidity limitations." https://aliumswap.medium.com/alium-finance-introducing-hybrid-dex-liquidity-to-address-liquidity-limitations-13d2f2f85558, 2021. Accessed: 2025-10-06.

[167] WigoSwap Team, "Wigoswap: Gamified dex on fantom." https://wigoswap.io, 2025. Accessed: 2025-10-06.

[168] Alchemy / Aldrin Team, "Aldrin: Solana dex and derivatives platform dapp." https://www.alchemy.com/dapps/aldrin, 2025. Accessed: 2025-10-06.

[169] DODO Team, "Dodo: Proactive market maker (pmm) dex." https://dodoex.io, 2025. Accessed: 2025-10-06.

[170] Saber Team, "Saber: Stablecoin and wrapped asset exchange on solana." https://saber.so, 2025. Accessed: 2025-10-06.

[171] Lifinity Team, "Lifinity: Oracle-based amm on solana." https://lifinity.io, 2025. Accessed: 2025-10-06.

[172] Saddle Finance Team, "Saddle finance: Stablecoin and pegged-asset amm." https://saddle.finance, 2025. Accessed: 2025-10-06.

[173] zkSwap Finance Team, "zkswap finance: zk-rollup amm protocol." https://www.zkswap.finance/, 2025. Accessed: 2025-10-06.

[174] Loopring Team, "Loopring: Layer-2 protocol for high-throughput dexs." https://loopring.org, 2025. Accessed: 2025-10-06.

[175] Balancer Team, "Balancer: Automated portfolio manager and dex." https://balancer.fi, 2025. Accessed: 2025-10-06.

[176] HorizonDEX Team, "Horizondex: Token-incentivized dex." https://horizondex.io, 2025. Accessed: 2025-10-06.

[177] Alchemy / MelegaSwap Team, "Melegaswap: Bnb chain dex and yield platform dapp." https://www.alchemy.com/dapps/melegaswap, 2025. Accessed: 2025-10-06.

[178] VVS Finance Team, "Vvs finance: Amm on cronos." https://vvs.finance, 2025. Accessed: 2025-10-06.

[179] Atrix Team, "Atrix: Solana dex and liquidity provider." https://atrix.finance, 2025. Accessed: 2025-10-06.

[180] Velodrome Team, "Velodrome: Dex on optimism with token incentives." https://velodrome.finance, 2025. Accessed: 2025-10-06.

[181] Alchemy / Paraswap Team, "Paraswap: Dex aggregator dapp." https://www.alchemy.com/dapps/paraswap, 2025. Accessed: 2025-10-06.

[182] Convex Finance Team, "Convex finance: Yield optimization built on curve." https://convexfinance.com, 2025. Accessed: 2025-10-06.

[183] Crossmint / STRKFarm Team, "Strkfarm: Yield farming platform on crossmint ecosystem." https://www.crossmint.com/ecosystem/strkfarm, 2025. Accessed: 2025-10-06.

[184] Hayden Adams et al., "Uniswap whitepaper: A constant product market maker." https://uniswap.org/whitepaper.pdf, 2020. Accessed: 2025-10-06.

[185] Alchemy / CroSwap Team, "Croswap: Cronos dex dapp." https://www.alchemy.com/dapps/croswap, 2025. Accessed: 2025-10-06.

[186] Hegic Protocol Team, "Hegic: On-chain options protocol." https://www.hegic.co, 2025. Accessed: 2025-10-06.

[187] Invariant Finance Team, "Invariant: Efficient dex on solana." https://invariant.app, 2025. Accessed: 2025-10-06.

[188] Hundred Finance Team, "Hundred finance: Cross-chain lending protocol." https://hundred.finance, 2025. Accessed: 2025-10-06.

[189] Mercurial Finance Team, "Mercurial finance: Stable asset exchange on solana." https://mercurial.finance, 2025. Accessed: 2025-10-06.

[190] CoinGecko, "Treble (tre) — coingecko." https://www.coingecko.com/en/coins/treble, 2025. Accessed: 2025-10-06.

[191] RBX Team, "Rbx: Multi-chain defi hub." https://rbx.ae, 2025. Accessed: 2025-10-06.

[192] Alchemy / Moox Protocol Team, "Moox protocol: Dex dapp." https://www.alchemy.com/dapps/moox, 2025. Accessed: 2025-10-06.

[193] Orca Team, "Orca: Solana automated market maker." https://www.orca.so, 2025. Accessed: 2025-10-06.

[194] Amply Finance Team, "Amply finance: Yield and staking protocol." https://amply.finance, 2025. Accessed: 2025-10-06.

[195] Alchemy / Minu Swap Team, "Minu swap: Dex dapp." https://www.alchemy.com/dapps/minu-swap, 2025. Accessed: 2025-10-06.

[196] Sphere Finance Team, "Sphere finance: Governance and staking platform." https://sphere.finance, 2025. Accessed: 2025-10-06.

[197] Cope Team, "Cope: Token incentive ecosystem on solana." https://cope.mirror.xyz, 2025. Accessed: 2025-10-06.

[198] Bebop Team, "Bebop: Decentralized asset trading platform." https://bebop.xyz, 2025. Accessed: 2025-10-06.

[199] Alchemy / Quarry Team, "Quarry: Yield farming protocol dapp." https://www.alchemy.com/dapps/quarry, 2025. Accessed: 2025-10-06.

[200] CoinMarketCap, "Starbase (star) — coinmarketcap." https://coinmarketcap.com/currencies/starbase/, 2025. Accessed: 2025-10-06.

[201] SunCrypto / PawSwap Team, "Pawswap token (paw) info — suncrypto." https://suncrypto.in/price/paw, 2025. Accessed: 2025-10-06.

[202] S. Hassan, P. De Filippi, and W. Reijers, "Decentralized autonomous organizations (daos): Taxonomy, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 11780–11799, 2022.

[203] 1inch Network Team, "1inch network documentation." https://1inch.io, 2025. Accessed: 2025-10-06.

[204] PitchBook / PieDAO, "Piedao: Tokenized index funds and dao governance." https://pitchbook.com/profiles/company/437592-70overview, 2025. Accessed: 2025-10-06.

[205] BarnBridge Team, "Barnbridge whitepaper," tech. rep., BarnBridge, 2021. Accessed: 2025-10-06.

[206] Reflexer Labs, "Reflexer finance documentation (rai stablecoin)." https://reflexer.finance, 2025. Accessed: 2025-10-06.

[207] Alchemy / PlutosDAO Team, "Plutosdao: Synthetic asset protocol dapp." https://www.alchemy.com/dapps/plutosdao, 2025. Accessed: 2025-10-06.

[208] J. Xu, Y. Zhou, and S. Wang, "Transaction fee mechanism design for blockchain systems," in *Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 83–93, ACM, 2022.

[209] Jupiter Team, "Jupiter aggregator: Zero-fee swaps on solana." https://jup.ag, 2025. Accessed: 2025-10-06.

[210] PoolTogether Team, "Pooltogether protocol documentation." https://pooltogether.com, 2025. Accessed: 2025-10-06.

[211] CowSwap Team, "Cowswap: Mev-protected batch auction protocol." https://cowswap.exchange, 2025. Accessed: 2025-10-06.

[212] 0x Labs / Matcha Team, "Matcha: Decentralized exchange aggregator." https://matcha.xyz, 2025. Accessed: 2025-10-06.

[213] Slingshot Finance Team, "Slingshot: Gas-fee subsidized defi trading platform." https://slingshot.finance, 2025. Accessed: 2025-10-06.

[214] Y. Chen, A. Li, and K. Xu, "Decentralized insurance in defi: Risk modeling, governance, and future challenges," 2023. Accessed: 2025-10-06.

[215] S. Wang, X. Xu, and Z. Zhang, "Defirisk: A classification and analysis of risks in decentralized finance," in *IEEE International Conference on Blockchain*, pp. 45–54, IEEE, 2023.

[216] Bumper Finance Team, "Bumper finance: Decentralized asset protection protocol." https://bumper.fi, 2025. Accessed: 2025-10-06.

[217] Alchemy / Neptune Mutual Team, "Neptune mutual: Defi insurance dapp." https://www.alchemy.com/dapps/neptune-mutual, 2025. Accessed: 2025-10-06.

[218] Alchemy / DSLA Protocol Team, "Dsla protocol: Risk hedging dapp." https://www.alchemy.com/dapps/dsla, 2025. Accessed: 2025-10-06.

[219] B.Protocol Team, "B.protocol: Backstop liquidity and liquidation protection." https://bprotocol.org, 2025. Accessed: 2025-10-06.

[220] InsurAce Team, "Insurace: Multi-chain defi insurance platform." https://www.insurace.io, 2025. Accessed: 2025-10-06.

[221] Tidal Finance Team, "Tidal finance: Customizable defi insurance pools." https://tidal.finance, 2025. Accessed: 2025-10-06.

[222] Nexus Mutual Team, "Nexus mutual: Decentralized insurance mutual." https://nexusmutual.io, 2025. Accessed: 2025-10-06.

[223] OpenCover / Ease Team, "Ease: Decentralized uninsurance protocol." https://opencover.com/ease/, 2025. Accessed: 2025-10-06.

[224] OpenCover Team, "Opencover: Aggregated defi insurance protocol." https://opencover.com, 2025. Accessed: 2025-10-06.

[225] R. Zhang, J. Chen, and Y. Wang, "On the security and performance of yield farming in decentralized finance," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–9, IEEE, 2022.

[226] Snowball Team, "Snowball: Automated yield optimization on avalanche." https://snowball.network, 2025. Accessed: 2025-10-06.

[227] Jones DAO Team, "Jones dao: Structured yield strategies for options." https://jonesdao.io, 2025. Accessed: 2025-10-06.

[228] Clip Finance Team, "Clip finance: Cross-chain yield aggregation." https://clip.finance, 2025. Accessed: 2025-10-06.

[229] Yield Yak Team, "Yield yak: Auto-compounding yield aggregator." https://yieldyak.com, 2025. Accessed: 2025-10-06.

[230] Metronome Team, "Metronome synth: Yield optimization with synthetic assets." https://metronome.io, 2025. Accessed: 2025-10-06.

[231] Tenderize Team, "Tenderize: Liquid staking and auto-compounding protocol." https://tenderize.me, 2025. Accessed: 2025-10-06.

[232] Alchemix Team, "Alchemix: Self-repaying loans via yield strategies." https://alchemix.fi, 2025. Accessed: 2025-10-06.

[233] Ratio Finance Team, "Ratio finance: Stablecoins and yield optimization on solana." https://ratio.finance, 2025. Accessed: 2025-10-06.

[234] Shell Protocol Team, "Shell protocol: Composable stablecoin and yield strategies." https://shellprotocol.io, 2025. Accessed: 2025-10-06.

[235] Yearn Finance Team, "Yearn finance: Automated yield aggregator." https://yearn.finance, 2025. Accessed: 2025-10-06.

[236] Stake DAO Team, "Stake dao: Multi-protocol yield optimization and governance." https://stakedao.org, 2025. Accessed: 2025-10-06.

[237] DappRadar / HyperJump Team, "Hyperjump (fi) — dappradar amm yield farming." https://dappradar.com/dapp/hyperjump-fi-amm-yieldfarm, 2025. Accessed: 2025-10-06.

[238] Penguin Finance Team, "Penguin finance: Gamified yield optimization on avalanche." https://penguinfinance.org, 2025. Accessed: 2025-10-06.

[239] Kamino Finance Team, "Kamino finance: Concentrated liquidity and auto-compounding on solana." https://kamino.finance, 2025. Accessed: 2025-10-06.

[240] Idle Finance Team, "Idle finance: Risk-adjusted yield optimization." https://idle.finance, 2025. Accessed: 2025-10-06.

[241] DeFiLlama / Goat Protocol Team, "Goat protocol — defillama overview." https://defillama.com/protocol/goat-protocol, 2025. Accessed: 2025-10-06.

[242] Origin Protocol Team, "Origin ether (oeth): Liquid staking derivative for eth." https://originprotocol.com/osea, 2025. Accessed: 2025-10-06.

[243] Jasper Vault Team, "Jasper vault: Automated vault-based yield aggregator." https://jaspervault.io, 2025. Accessed: 2025-10-06.

[244] YieldFi Team, "Yieldfi: Automated yield farming and compounding." https://yieldfi.app, 2025. Accessed: 2025-10-06.

[245] Cropper Finance Team, "Cropper finance: Auto-compounding yield optimizer on solana." https://cropper.finance, 2025. Accessed: 2025-10-06.

[246] Antfarm Finance Team, "Antfarm finance: Dynamic liquidity allocation for yield optimization." https://antfarm.finance, 2025. Accessed: 2025-10-06.

[247] Compound Blue Team, "Compound blue: Optimized lending and yield strategies." https://compound.finance, 2025. Accessed: 2025-10-06.

[248] Alchemy / Friktion Team, "Friktion: Structured yield dapp on solana." https://www.alchemy.com/dapps/friktion, 2025. Accessed: 2025-10-06.

[249] CoinGecko / Ovix Team, "0vix protocol (0vix) — coingecko." https://www.coingecko.com/en/coins/0vix-protocol, 2025. Accessed: 2025-10-06.

[250] Sonne Finance, "Sonne finance: Yield optimization on optimism." https://sonne.finance, 2025. Accessed: 2025-10-06.

[251] Alchemy / Rebalance Finance Team, "Rebalance finance: Portfolio optimization dapp." https://www.alchemy.com/dapps/rebalance, 2025. Accessed: 2025-10-06.

[252] Crema Finance, "Crema finance: Concentrated liquidity and yield optimization." https://crema.finance, 2025. Accessed: 2025-10-06.

[253] Pickle Finance Team, "Pickle finance: Automated yield farming vaults." https://pickle.finance, 2025. Accessed: 2025-10-06.

[254] EarnPark, "Earnpark: Automated yield optimization for stablecoins and tokens." https://earnpark.com, 2025. Accessed: 2025-10-06.

[255] Dual Finance, "Dual finance: Structured products and yield strategies." https://dual.finance, 2025. Accessed: 2025-10-06.

[256] Teahouse Finance, "Teahouse: Actively managed yield optimization vaults." https://teahouse.finance, 2025. Accessed: 2025-10-06.

[257] xToken Terminal, "xtoken terminal: Automated yield strategies for governance tokens." https://xtokenterminal.io, 2025. Accessed: 2025-10-06.

[258] Mellow Protocol, "Mellow protocol: Modular yield optimization and strategy vaults." https://mellow.finance, 2025. Accessed: 2025-10-06.

[259] CoinMarketCap, "Koi finance (koi) — coinmarketcap." https://coinmarketcap.com/currencies/koi-finance/, 2025. Accessed: 2025-10-06.

[260] Hord Team, "Hord: Tokenized asset baskets and yield strategies." https://hord.app, 2025. Accessed: 2025-10-06.

[261] Alchemy / Menthol Team, "Menthol protocol: Sustainable yield dapp." https://www.alchemy.com/dapps/menthol-protocol, 2025. Accessed: 2025-10-06.

[262] CoinMarketCap / Tulip Protocol Team, "Solfarm / tulip (tulip) — coinmarketcap." https://coinmarketcap.com/currencies/solfarm/, 2025. Accessed: 2025-10-06.

[263] BracketX, "Bracketx: Structured products and options-based yield strategies." https://bracketx.fi, 2025. Accessed: 2025-10-06.

[264] Harvest Finance, "Harvest finance: Automated multi-chain yield aggregator." https://harvest.finance, 2025. Accessed: 2025-10-06.

[265] Beefy Finance, "Beefy finance: Multi-chain automated yield optimization vaults." https://beefy.finance, 2025. Accessed: 2025-10-06.

[266] Alchemy / NillaConnect Team, "Nillaconnect: Cross-chain yield optimization dapp." https://www.alchemy.com/dapps/nillaconnect, 2025. Accessed: 2025-10-06.

[267] Lagoon Finance, "Lagoon: Automated defi yield strategies." https://lagoon.finance, 2025. Accessed: 2025-10-06.

[268] MorFi Protocol, "Morfi: Automated multi-strategy yield optimization." https://morfi.io, 2025. Accessed: 2025-10-06.

[269] Francium, "Francium: Leveraged yield aggregation on solana." https://francium.io, 2025. Accessed: 2025-10-06.

[270] TokensFarm, "Tokensfarm: Yield farming as a service." https://tokensfarm.com, 2025. Accessed: 2025-10-06.

[271] Filet Finance, "Filet finance: Filecoin staking and yield optimization." https://filet.finance, 2025. Accessed: 2025-10-06.

[272] maxAPY, "maxapy: Multi-chain yield aggregation platform." https://maxapy.com, 2025. Accessed: 2025-10-06.

[273] Reaper Farm, "Reaper farm: Automated yield compounding on fantom." https://reaper.farm, 2025. Accessed: 2025-10-06.

[274] Z. Chen, Y. Li, and Y. Liu, "Empirical analysis of cryptocurrency derivatives and perpetual futures markets," *Finance Research Letters*, vol. 43, p. 101410, 2021.

[275] Vela Exchange Team, "Vela exchange knowledge base." https://docs.vela.exchange/vela-knowledge-base, 2025. Accessed: 2025-10-07.

[276] UniDex Exchange Team, "Unidex exchange overview." https://unidex.exchange, 2025. Accessed: 2025-10-07.

[277] Polynomial Protocol Team, "Polynomial protocol." https://polynomial.fi, 2025. Accessed: 2025-10-07.

[278] Parcl Labs, "Parcl real estate derivatives protocol." https://parcl.co, 2025. Accessed: 2025-10-07.

[279] AIJourn, "Powertrade / powerdex launches first-ever options on xstocks: Bringing 24/7 tokenized stock derivatives to crypto." https://aijourn.com/powertrade-powerdex-launches-first-ever-options-on-xstocks-bringing-24-7-tokenized-stock-derivatives-to-crypto/, 2025. Accessed: 2025-10-07.

[280] dYdX Foundation, "dydx exchange documentation." https://dydx.exchange, 2025. Accessed: 2025-10-07.

[281] Zeta Markets Team, "Zeta markets: Perpetual options derivatives platform." https://www.zeta.markets, 2025. Accessed: 2025-10-07.

[282] Concordex Developers, "Concordex exchange protocol overview." https://concordex.io, 2025. Accessed: 2025-10-07.

[283] Contango Team, "Contango protocol." https://contango.xyz, 2025. Accessed: 2025-10-07.

[284] Evo Exchange Team, "Evo exchange: Interblockchain decentralized exchange." https://www.alchemy.com/dapps/evo-exchange, 2025. Accessed: 2025-10-07.

[285] Crossmint / Dopex DAO, "Dopex dao: Decentralized options protocol — crossmint ecosystem." https://www.crossmint.com/ecosystem/dopex, 2025. Accessed: 2025-10-07.

[286] Drift Protocol, "Drift: On-chain derivatives exchange." https://drift.trade, 2025. Accessed: 2025-10-07.

[287] Deri Protocol, "Deri protocol documentation." https://deri.io, 2025. Accessed: 2025-10-07.

[288] Lyra Finance Team, "Lyra options trading protocol." https://app.lyra.finance, 2025. Accessed: 2025-10-07.

[289] SynFutures Labs, "Synfutures protocol overview." https://synfutures.com, 2025. Accessed: 2025-10-07.

[290] Kwenta DAO, "Kwenta derivatives exchange." https://kwenta.io, 2025. Accessed: 2025-10-07.

[291] GMX Team, "Gmx exchange documentation." https://gmx.io, 2025. Accessed: 2025-10-07.

[292] Thetanuts Finance, "Thetanuts structured products protocol." https://thetanuts.finance, 2025. Accessed: 2025-10-07.

[293] Alchemy / Opium Team, "Opium: Derivatives protocol dapp." https://www.alchemy.com/dapps/opium, 2025. Accessed: 2025-10-07.

[294] Rage Trade Team, "Rage trade perpetual exchange." https://rage.trade, 2025. Accessed: 2025-10-07.

[295] Kromatika Finance, "Kromatika protocol documentation." https://kromatika.finance, 2025. Accessed: 2025-10-07.

[296] BNBChain / RubyDex Team, "Rubydex — bnbchain dappbay." https://dappbay.bnbchain.org/detail/rubydex, 2025. Accessed: 2025-10-07.

[297] LN Exchange, "Ln exchange documentation." https://ln.exchange, 2025. Accessed: 2025-10-07.

[298] FutureSwap Team, "Futureswap protocol overview." https://futureswap.com, 2025. Accessed: 2025-10-07.

[299] Siren Protocol, "Siren options trading." https://siren.xyz, 2025. Accessed: 2025-10-07.

[300] Gearbox Foundation, "Gearbox protocol overview." https://gearbox.fi, 2025. Accessed: 2025-10-07.

[301] Coinbase Blog / Opyn Team, "Moving markets onchain: Welcoming opyn markets to coinbase." https://www.coinbase.com/en-ca/blog/moving-markets-onchain-welcoming-opyn-markets-to-coinbase, 2025. Accessed: 2025-10-07.

[302] Alpha Venture DAO, "Alpha homora protocol." https://alphaventuredao.io, 2025. Accessed: 2025-10-07.

[303] Perpetual Protocol Team, "Perpetual protocol documentation." https://perp.com, 2025. Accessed: 2025-10-07.

[304] SEIF Finance, "Seif derivatives exchange." https://seif.finance, 2025. Accessed: 2025-10-07.

[305] Carbon DeFi, "Carbon protocol overview." https://carbondefi.xyz, 2025. Accessed: 2025-10-07.

[306] Panoptic Protocol, "Panoptic perpetual options protocol." https://panoptic.xyz, 2025. Accessed: 2025-10-07.

[307] DappRadar / FCON Team, "Fcon dex — dappradar listing." https://dappradar.com/dapp/fcon-dex, 2025. Accessed: 2025-10-07.

[308] Apricot Finance, "Apricot leverage protocol." https://apricot.one, 2025. Accessed: 2025-10-07.

[309] Alchemy / OptionBlitz Team, "Optionblitz: Options binary derivatives protocol dapp." https://www.alchemy.com/dapps/optionblitz, 2025. Accessed: 2025-10-07.

[310] Optix Protocol Team, "Optix structured derivatives protocol." https://optixprotocol.com, 2025. Accessed: 2025-10-07.

[311] M. Bartoletti, F. Cucurachi, and S. Lande, "A survey of defi security: Vulnerabilities, attacks, and analysis tools," in *IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 540–559, IEEE, 2023.

[312] IX Swap Team, "Ix swap platform overview." https://ixswap.io, 2025. Accessed: 2025-10-07.

[313] Holdstation Labs, "Holdstation wallet and trading platform." https://holdstation.com, 2025. Accessed: 2025-10-07.

[314] Enzyme Finance, "Enzyme finance: On-chain asset management protocol." https://enzyme.finance, 2025. Accessed: 2025-10-07.

[315] RhinoFi Team, "Rhinofi: Layer-2 defi hub." https://rhino.fi/, 2025. Accessed: 2025-10-08.

[316] dHEDGE DAO, "dhedge: Decentralized asset management protocol." https://www.dhedge.org, 2025. Accessed: 2025-10-07.

[317] Furucombo Team, "Furucombo: Defi strategy builder." https://furucombo.app, 2025. Accessed: 2025-10-07.

[318] Dolomite Labs, "Dolomite: Margin trading and portfolio management platform." https://dolomite.io, 2025. Accessed: 2025-10-07.

[319] CoinStats Team, "Coinstats: Portfolio and analytics tool." https://coinstats.app, 2025. Accessed: 2025-10-07.

[320] Delio Global, "Delio: Digital asset management platform." https://delio.global, 2025. Accessed: 2025-10-07.

[321] Crossmint / Legato Team, "Legato: Liquid staking vaults protocol." https://www.crossmint.com/ecosystem/legato-finance, 2025. Accessed: 2025-10-08.

[322] FlowX Finance, "Flowx: Defi analytics and trading dashboard." https://flowx.finance, 2025. Accessed: 2025-10-07.

[323] Maxbid Pro Team, "Maxbid pro: Defi execution and optimization tool." https://maxbid.pro, 2025. Accessed: 2025-10-07.

[324] De.Fi Team, "De.fi: Security and analytics platform." https://de.fi, 2025. Accessed: 2025-10-07.

[325] Multichain Team, "Multichain: Cross-chain bridge protocol." https://www.multichain.com/, 2025. Accessed: 2025-10-08.

[326] Solrise Finance Team, "Solrise finance: Asset management on solana." https://solrise.finance, 2025. Accessed: 2025-10-07.

[327] TheStandard.io Team, "The standard protocol: Decentralized asset management and stablecoin issuance." https://thestandard.io, 2025. Accessed: 2025-10-07.

[328] Tokenlon Team, "Tokenlon: Decentralized exchange and settlement layer." https://tokenlon.im, 2025. Accessed: 2025-10-07.

[329] Hedgehog App Team, "Hedgehog: Defi portfolio management tool." https://hedgehog.app, 2025. Accessed: 2025-10-07.

[330] Interport Finance, "Interport: Cross-chain dex aggregator." https://interport.fi, 2025. Accessed: 2025-10-07.

[331] Soldex AI, "Soldex: Ai-driven decentralized exchange on solana." https://soldex.ai, 2025. Accessed: 2025-10-07.

[332] OpenOcean Team, "Openocean: Cross-chain dex aggregator." https://openocean.finance, 2025. Accessed: 2025-10-08.

[333] Degen Wallet Team, "Degen wallet: Multi-chain defi wallet." https://degenwallet.xyz, 2025. Accessed: 2025-10-08.

[334] 0x Labs, "0x protocol: Decentralized exchange infrastructure." https://0x.org, 2025. Accessed: 2025-10-08.

[335] AirSwap Team, "Airswap: Peer-to-peer trading protocol." https://airswap.io, 2025. Accessed: 2025-10-08.

[336] CoinMarketCap / Avata Team, "Avata network (avat) — coinmarketcap." https://coinmarketcap.com/currencies/avata-network/, 2025. Accessed: 2025-10-08.

[337] Crypto Valley Exchange, "Crypto valley exchange: Digital asset platform." https://cryptovalley.exchange, 2025. Accessed: 2025-10-08.

[338] DZap Team, "Dzap: One-click defi execution." https://dzap.io, 2025. Accessed: 2025-10-08.

[339] Alchemy / Marginly Team, "Marginly: Defi margin trading dapp." https://www.alchemy.com/dapps/marginly, 2025. Accessed: 2025-10-08.

[340] Akropolis, "Akropolis: Defi framework and yield tools." https://akropolis.io, 2025. Accessed: 2025-10-08.

[341] Augur Project, "Augur: Decentralized prediction markets." https://augur.net, 2025. Accessed: 2025-10-08.

[342] Integral, "Integral: Dex for large trades." https://integral.link, 2025. Accessed: 2025-10-08.

[343] Router Protocol Team, "Router nitro: Cross-chain liquidity aggregation." https://routerprotocol.com/nitro, 2025. Accessed: 2025-10-08.

[344] Pika Protocol, "Pika protocol: Perpetual futures." https://pikaprotocol.com, 2025. Accessed: 2025-10-08.

[345] Clipper DEX, "Clipper: Low-slippage dex for retail traders." https://clipper.exchange, 2025. Accessed: 2025-10-08.

[346] DeGate, "Degate: zk-rollup layer-2 dex." https://degate.com, 2025. Accessed: 2025-10-08.

[347] CoinGecko / Dexed Team, "Dexed (dexed) — coingecko." Accessed via CoinGecko at https://www.coingecko.com/en/coins/dexed, 2025. Accessed: 2025-10-08.

[348] Rubicon Exchange, "Rubicon: Order book dex on optimism." https://rubicon.finance, 2025. Accessed: 2025-10-08.

[349] Erasure Protocol, "Erasure: Decentralized data marketplace." https://erasure.world, 2025. Accessed: 2025-10-08.

[350] Mangrove, "Mangrove: Programmable order book dex." https://mangrove.exchange, 2025. Accessed: 2025-10-08.

[351] Polymarket Team, "Polymarket: Information and prediction markets." https://polymarket.com, 2025. Accessed: 2025-10-08.

[352] Ave AI, "Ave ai: Defi analytics and trading assistant." https://aveai.app, 2025. Accessed: 2025-10-08.

[353] Metavisor, "Metavisor: Yield and treasury optimization." https://metavisor.app, 2025. Accessed: 2025-10-08.

[354] LI.FI, "LI.FI: Cross-chain liquidity aggregator (apis and sdks)." https://li.fi, 2025. Accessed: 2025-10-08.

[355] Keep Network, "Keep network: Threshold cryptography and tbtc." https://keep.network, 2025. Accessed: 2025-10-08.

[356] Rocko Finance, "Rocko: Defi infrastructure and portfolio management." https://rocko.finance, 2025. Accessed: 2025-10-08.

[357] Alchemy / Bamboo Relay Team, "Bamboo relay: Decentralized order-book exchange dapp." https://www.alchemy.com/dapps/bamboo-relay, 2025. Accessed: 2025-10-08.

[358] Ubik Capital, "Ubik capital: Validator and staking services." https://ubik.capital, 2025. Accessed: 2025-10-08.

[359] Alchemy / Metrom Team, "Metrom: Defi analytics and monitoring dapp." https://www.alchemy.com/dapps/metrom, 2025. Accessed: 2025-10-08.

[360] ByBarter, "Bybarter: Peer-to-peer defi trading." https://bybarter.io, 2025. Accessed: 2025-10-08.

[361] Alchemy / PropellerSwap Team, "Propellerswap: Swap and liquidity routing platform dapp." https://www.alchemy.com/dapps/propellerswap, 2025. Accessed: 2025-10-08.

[362] Earnifi Team, "Earnifi: Airdrop and claim notifications." https://earni.fi, 2025. Accessed: 2025-10-08.

[363] BetDEX Labs, "Betdex: Decentralized sports betting exchange." https://betdex.com, 2025. Accessed: 2025-10-08.

[364] Swoop Exchange, "Swoop exchange: Defi trading aggregator." https://swoop.exchange, 2025. Accessed: 2025-10-08.

[365] Duel Duck, "Duel duck: Gamified defi prediction platform." https://duelduck.com, 2025. Accessed: 2025-10-08.

[366] Crossmint / Droidex, "Droidex: Decentralized exchange aggregator — crossmint ecosystem." https://crossmint-light.webflow.io/ecosystem/droidex, 2025. Accessed: 2025-10-08.

[367] Sprintcheckout Team, "Sprintcheckout: Crypto payment and checkout platform." https://sprintcheckout.com, 2025. Accessed: 2025-10-08.

[368] S. Ö. Arik and T. Pfister, "Tabnet: Attentive interpretable tabular learning," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 35, pp. 6679–6687, 2021.

[369] S. Popov, S. Morozov, and A. Babenko, "Neural oblivious decision ensembles for deep learning on tabular data," *International Conference on Learning Representations*, 2020.

[370] M. Joseph and H. Raj, "Gandalf: gated adaptive network for deep automated learning of features," *arXiv preprint arXiv:2207.08548*, 2022.

Appendices

A Appendix 1

B Appendix 2