Decentralized Finance (DeFi): A Survey

Erya Jiang∗, Bo Qin∗, Qin Wang¶, Zhipeng Wang§, Qianhong Wu†, Jian Weng‡
Xinyu Li∗, Chenyang Wang∗, Yuhang Ding∗, Yanran Zhang∗

∗Renmin University of China, China
¶University of New South Wales, Australia
§Imperial College London, UK
†Beihang University, China
‡Jinan University, China

Abstract

Decentralized Finance (DeFi) is a new paradigm in the creation, distribution, and utilization of financial services via the integration of blockchain technology. Our research conducts a comprehensive introduction and meticulous classification of various DeFi applications. Beyond that, we thoroughly analyze these risks from both technical and economic perspectives, spanning multiple layers. We point out research gaps and avenues, covering technical advancements, innovative economics, and sociology and ecology optimization.

1 Introduction

With blockchain’s rise, Decentralized Finance (DeFi) [1] has emerged as a disruptive financial paradigm in the middle of 2020 (a period known as the DeFi summer), challenging traditional finance [2]. DeFi utilizes blockchain for creating, distributing, and utilizing financial services [3], surpassing traditional finance in various aspects:

• **Trustless.** DeFi protocols eliminate centralized intermediaries like brokerages, banks, and insurance companies, which come with defects such as high costs, cumbersome processes, account opening restrictions, e.g., Know Your Customer (KYC), and lack of transparency.
• **Non-human intervention.** DeFi’s trading rules are pre-written, making automation and immutability key features [4] while running on-chain that reduces counterparty risk and eliminates the single point of failure.
• **Maximal availability.** Most DeFi products have no downtime, enabling 24/7 financial services to everyone.
• **Borderless.** DeFi enables global accessibility without being restricted by national boundaries, allowing anyone from anywhere including those from low economic levels or underserved regions to leverage its services.
• **Permissionless.** Deployed in a decentralized manner across peer-to-peer (P2P) networks, opens new opportunities for organizations, e.g., DAOs [5] to areas previously accessible only to licensed institutions.
• **Extensibility.** DeFi’s open-source nature encourages user contributions, facilitating the emergence of novel financial concepts such as flash loans [6,7].

As of Aug. 2023, the total locked value (TLV)1 in DeFi markets has reached US$40.257b, following a peak value of US$253b in Dec. 2021 (also claimed in [8]). This substantial investment has sparked numerous innovations, including decentralized exchanges (DEXs, e.g., Uniswap [9], dYdX [10]), lending (Compound [11], Aave [12]), yield aggregators (Convex [13], Harvest [14]), liquid staking (Lido [15], Rocket Pool [16]), and various other developments [1].

Previous investigations. We highlight several recent studies that have elegantly reviewed DeFi-related concepts. Wener et al. [1] conducted the first systematic studies focusing on general DeFi protocols, covering layer-based protocols and services. Moin et al. [17] classified major stablecoin designs, while Zhao et al. [18] specifically explored algorithmic stablecoins. Bartoletti et al. [19] introduced lending protocols using a formal model that describes their transitions as a state machine reflecting user interactions. Xu et al. [20] presented a general business model for a small corpus of DeFi protocols, including protocols for loanable funds, DEXs, and yield aggregators. Li et al. [21] describe the picture of confidential smart contrast that can be used for DeFi privacy. Xu et al. [22] comprehensively reviewed DEXs and their corresponding automated market maker (AMM) protocols. Erinle et al. [23] provided a comprehensive overview of cryptocurrency wallets that support DeFi services. Lastly, Zhou et al. [8] thoroughly investigated a range of attacks and incidents in the DeFi space. Additionally, a series of research works have drawn their focus on MEV extractions [24,25] and frontrunning attacks [26–28].

This paper follows the burgeoning prosperity of DeFi and extends its research horizons. We explore the mechanisms of DeFi apps and investigate the security risks from technological and economic perspectives (cf. Figure 1). In particular,

• We conduct a comprehensive statistical analysis of the literature in the DeFi field. According to the analyti-

1Data source: https://defillama.com [Aug. 2023], marked as #DefiLlama.
Risks of DeFi

We propose a DeFi classification frame based on the complexity of financial services. The frame (summarized in Table 1) classifies DeFi applications into three categories: tool level, basic functionality level, and service level. We detail the structure of DeFi applications and related research insights in each category.

We discuss the security of DeFi applications from two pillars: technical (Section 4) and economic perspectives (Section 5). Our discussions are grounded in relevant academic papers and real-world incidents, outlining a broad spectrum of DeFi risks, possible losses, implementations, and possible defenses (summarized in Table 2).

We provide information on the gap between existing DeFi realizations and the ideal state. We conclude by proposing technological, sociological, and economic research directions (Section 6).

2 Methodology

We provide the analytical approach of statistical literature analysis and outline the corresponding modeling process. The results based on quantitative and qualitative analysis will be presented in the following sections.

Our analysis started with retrieving academic papers and research articles related to DeFi from IEEE Xplore, ACM, and Springer. After keyword screening and manual checking, we obtained a total of 15,598 relevant articles.

In reviewing the existing literature, we realized that an effective way to classify the themes of existing works is based on the financial complexity of the DeFi application, as shown in Figure 2. According to this classification, DeFi applications can be classified as digital assets, wallets, oracles, and asset bridges at infrastructural level, stablecoins, lending, and exchanges at functional level, and diverse derivatives at service level. In addition, we have screened and classified the literature that offers DeFi security risk solutions.

We utilized quantitative techniques including employing descriptive statistics and other tools to establish relationships, trends, and statistical significance to analyze the data. We also employed qualitative analysis to complement the quantitative analysis. This allowed us to gain a holistic understanding of the subject matter and capture nuanced insights.

3 DeFi Applications

We conducted a statistical analysis on over 10,000 DeFi-apps-related literature pieces that we obtained.

Observation. DeFi research literature availability correlates with proximity to blockchain logic. We observe that research on DeFi tools and functionalities closely tied to blockchain emerged earlier and has more quantity. For example, digital assets research, due to the native token-blockchain consensus relationship, is the most abundant in DeFi.

Insight. Initially, DeFi research focused on fundamental tools and logic. This is because establishing a reliable and secure blockchain infrastructure was crucial during the early stages of blockchain and DeFi development. This involved core technologies like decentralized development, consensus algorithms, network security, and smart contract platforms for automated financial functions. These studies deepened the understanding of blockchain’s underlying logic, resulting in extensive literature. As the infrastructure was established, exploration and development of complex DeFi tools and applications followed. Early research mirrored the developmental process of the financial system, which begins with establishing basic tools and infrastructure before expanding to a wider range of products and services. Similarly, DeFi progressed from infrastructure construction to the research and development of diverse tools and applications.

Observation. DeFi research has seen a significant increase, especially in 2022 and 2023. These papers explore previously unexplored aspects of DeFi, such as DeFi derivatives.

Insight. The research boom in DeFi since 2022 is attributed to several factors, including the maturation and expansion of the DeFi market, technological innovations, and increased involvement of institutions and enterprises. As the DeFi market matures, there is a rising demand for diverse and complex
DeFi products, including derivatives. The validation of DeFi’s potential through industry practices has also played a role. Introduction of new technologies like Layer-2 scaling solutions, cross-chain technologies, and privacy protection has opened up new possibilities. Additionally, the participation of enterprises and the regulatory measures and resources they bring have further fueled research in DeFi.

**Observation.** Technical solutions constitute the main type of literature in the DeFi field.

**Insight.** Technical solutions being the focus of researchers and practitioners is inherent as DeFi is driven by technology practice and application. They play a key role in transforming theories into practical tools and platforms.

**Figure 3:** Trend of Research Literature on DeFi Applications (Log10 Scale): We illustrate the trends of literature related to different DeFi apps over time. Notably, literature on asset management, prediction markets, and perpetual contracts is limited, leading to overlapping lines with the horizontal axis.

**Figure 4:** Publications of Literature Type: We classify the literature into three categories: review articles (blue), empirical studies (green), and technical solutions (yellow). We summarize the distribution of different types of literature.

**Observation.** Review articles often assess from a single disciplinary perspective, restricting comprehensive evaluations.

**Insight.** DeFi encompasses multiple disciplines, including economics, information security, law, and more. When review articles lean towards a single disciplinary perspective, they tend to be influenced by specific viewpoints and limitations. This ultimately stems from the fact that authors may be influenced by their own disciplinary viewpoints, leading to a lack of understanding of other disciplines. This reflects the insufficient depth of collaboration among different disciplinary talents, highlighting the need to cultivate interdisciplinary talents with a comprehensive perspective.

**Observation.** Empirical research lacks a macro perspective and broader significance in investigating DeFi apps. Apart from empirical research in the field of digital assets, which includes market data analysis, other areas rely more on case studies investigating specific projects, resulting in a lack of macro perspectives and broader empirical investigations.

**Insight.** Due to the novelty of DeFi, empirical research in this domain faces challenges. Inconsistent definitions and unclear models complicate empirical investigations. Privacy and data protection concerns surrounding DeFi apps make it difficult to acquire sufficient data for macro perspectives and broad empirical studies. The rapid emergence of new DeFi apps and models also poses challenges in keeping up with the pace of innovation and conducting comprehensive research. Consequently, empirical research in DeFi tends to focus more on specific case studies rather than broader investigations.

### 3.1 Tools of DeFi

**Digital Asset.** Native cryptocurrencies and derivative tokens constitute the money flowing in DeFi.

**Native cryptocurrency.** Native cryptocurrency refers to the primary digital asset of a blockchain. Prominent examples include Bitcoin [29], Ethereum [30], Litecoin [31], Monero [32–34], and Zcash [35, 36], all operating on standalone blockchains and incentivized within their respective economies. These cryptocurrencies can be directly transferred on the chain that hosts them and used for paying transaction fees, serving various functions within its ecosystem.

**Derivative Token.** Many DeFi apps issue tokens representing the ownership of the assets corresponding to the app. Additionally, DeFi app-issued tokens can perform in lending [12], staking [16], and insuring [37], and be empowered to participate in governance. Tokens in physical form represent ownership of real-world assets like real estate and collectibles.

Ethereum has a wide range of token standards for various DeFi apps. The widely known ERC-20 standard is fungible and interchangeable and used for currencies, voting tokens, and pledge tokens. Other Ethereum token standards are tailored for specific scenarios, such as non-fungible token standard ERC-721 used in artwork and digital collections, and semi-fungible token standard ERC-1155 utilized in GameFi and copyright. ERC-998 is designed to combine ERC-20 and ERC-721, enabling compatibility and interoperability.
Other blockchain platforms like Binance Smart Chain (BSC), Avalanche, and Bitcoin have also introduced their own token standards, such as BEP-20, BEP-721, ARC-721, and BRC-20, following similar rules to the ERC standards.

There is controversy regarding the classification of DeFi tokens as currencies, commodities, or securities. Some DeFi tokens exhibit currency attributes, possessing wide usability and circulation, while others may be classified as securities due to their characteristics of representing ownership, dividends, or investment returns. The classification also relies on regulatory standards, which are varied across regions and continuously adjusted given the technical complexity of DeFi.

The digital asset research field within DeFi emerged early and has a wealth of literature. Quantitative and predictive research, specifically focused on the cryptocurrency market, is a significant area of study. Quantitative research employs historical market data to develop trading strategies and algorithms based on technical analysis indicators, statistical models, and machine learning methods. Predictive research, on the other hand, involves constructing forecasting models using time series analysis, machine learning, and deep learning techniques. Notably, the integration of machine learning and deep learning, along with comprehensive consideration of market characteristics and risks, are prominent features within this research field.

Wallet. A wallet is a tool for managing the keys and addresses of digital asset holders. Wallets serve to interact with the blockchain instead of storing on-chain assets. In DeFi, users can manage multiple accounts from a single wallet.

Typically, a wallet has three basic functions: recording, receiving, and transferring currencies. With the development, its functions have evolved from simple transfers to encompass multi-chain management, asset custody, and other scenarios. Numerous academic research and industry examples on the functional expansion of wallets exist. Software wallets like imToken [38], Bip [39], Wetez [40], TrustWallet [41], and hardware wallets like Ledger [42] and Trezor [43] have explored and implemented these functionalities. In the industry, multi-chain wallets are typically developed by creating interfaces for different blockchains. Some multi-chain wallets have even introduced “flash exchange” functionality, utilizing exchange rates as a medium for transactions.

Wallet security is a critical consideration, encompassing key preservation, recovery procedures, and risk mitigation. Cold wallets offer physical isolation but carry the risk of loss, while others may be classified as securities due to their characteristics of representing ownership, dividends, or investment returns. The classification also relies on regulatory standards, which are varied across regions and continuously adjusted given the technical complexity of DeFi.

Oracle. The execution of smart contracts requires meeting conditions specified in the contracts, while also requiring support from external data. Oracle provides external data sources for smart contracts on the blockchain, supplying them with data information. As of Oct. 2023, the total value of all oracles reached US$25b, with Chainlink holding nearly half of the market among more than 40 different oracles (#DefiLlama).

To ensure trustworthy on-chain data, the accuracy of data is the main concern [44]. We have observed that review articles in this field generally classify oracles based on their operational mechanisms, which can be broadly categorized into provider identity-based and voting-based oracles. Identity-based oracles involve specific implementation methods such as setting whitelists/blacklists, incorporating identity verification in transport layer protocols, or using machine learning techniques to identify reliable and cost-effective oracles [45]. MakerDao [46] is an example of this type of oracle. On the other hand, voting-based oracles incentivize providers to exhibit economically rational behavior and provide accurate data through monetary rewards and penalties. Implementation methods for voting-based oracles include peer-to-peer prediction [47, 48], reputation mechanisms [49], game-theoretic approach for price data verification [50, 51], and others.

While different approaches have been implemented, challenges remain in ensuring data security. Identity-based oracles are vulnerable to single points of failure and bribery attacks. Voting-based oracles have limited applicability due to the need for data verification, which restricts them to publicly accessible information. These oracles also face challenges like data latency and high verification costs. Furthermore, the timeliness and freshness of time-sensitive data are often overlooked in current research, creating a dilemma in balancing security and timeliness.

Asset Bridge. Heterogeneous blockchains present a challenge to achieving smooth interoperability in DeFi. An asset bridge is a solution for asset transfer and interoperability between different blockchains. In the days that have passed in 2023, the average daily trading volume of the asset bridge exceeded $214 million, with the highest daily trading volume reaching $1.232 billion (#DefiLlama), reflecting active trading activity in the business. The functioning of an asset bridge varies depending on the implementation. Atomic swaps allow the direct exchange of cryptocurrency across blockchains [52]. Ripple introduced the InterLedger protocol (ILP) in 2012, facilitating cross-ledger interactions through third-party notaries. Pegged sidechains were proposed by the Bitcoin Core development team in 2014. Interoperability platforms such as Cosmos [53] and Polkadot [54] realize cross-chain communication and interaction through relay chains or side chains. In 2015, Joseph Poon and Thaddeus Dryja conceptualized the Bitcoin Lightning Network. In 2016, BTC-Relay [55], a cross-chain solution based on a relay chain, achieved one-way cross-chain connectivity between Ethereum and Bitcoin [56]. Vitalik Buterin [57]’s effort provided an in-depth analysis of blockchain interoperability issues. Notable cross-chain DeFi applications include Thorswap [58] and Chainswap [59].
3.2 Basic Functions of DeFi

**Stablecoin.** The prices of cryptocurrencies are highly volatile, but stablecoins offer price stability as they are pegged to fiat currencies, which is exactly why stablecoins were born. As a foundational currency, stablecoins support liquidity pools, lending, insurance, and other financial activities [60], mitigating the risks associated with market fluctuations. As of Oct. 2023, the stablecoin market contains a total market capitalization of over $120b and over 100 projects (#DefiLlama).

Stablecoins circulation involves reserve, insurance, and other essential links. Methods of forming stablecoins include off-chain reserves, such as USDT [61], USDC [62], and GUSD [63], on-chain collateralization like Dai [46] and LUSD [64], and algorithmic stablecoins without collateralization such as AMPL [65], Basis [66], FRAX [67], and UST [68]. Among them, we have found that algorithmic stablecoins are a controversial object of research. While having the advantages of high transparency and low/no collateral rates, multiple algorithmic stablecoin crashes, including Luna-UST collapse in 2022 [69], have cast a shadow over this solution. To address this challenge, Klages Mundt et al. [70] propose modeling-based approaches to enhance stablecoin design and resilience, ensuring price stability even amidst market shocks. Fu et al. [71] propose a rational Ponzi model to analyze the sustainability of algorithmic stablecoins.

A critical issue we identified in stablecoin research is the lack of widely accepted definitions for stablecoins. Existing literature often lacks clarity in defining what precisely constitutes a stablecoin. While some review articles discuss various implementation approaches, they do not provide a definitive core definition. Many papers focus on highlighting the desired characteristics and advantages of an ideal stablecoin, without delving into a concrete definition. Only a few studies examine stablecoin definitions from a legislative perspective or attempt to model specific types of stablecoins.

**Lending.** DeFi lending abandons the centralized credit assessment framework but relies on recognized collateral for pooling liquidity, enabling low-cost lending and arbitrage, and improving the transferability of debt holdings. DeFi lending has a large market, with a TLV of $14.782b and 300+ Apps (#DefiLlama). It allows borrowers to engage in trading activities, while lenders can earn additional revenue via collateral rates [72]. The primary motivation for users to use DeFi lending is to obtain participation rewards, such as governance tokens. In extreme cases, investors can form a borrowing spiral [73] or leverage spiral [74] to maximize benefit.

DeFi lending apps typically involve collateralization, lending, and liquidation. Based on such a model, apps like Compound [11] and AAVE [12], enable over-collateralized, trustless DeFi lending. But out of the demand for low/zero collateralization and regulatory requirements, undercollateralized lending is born, building credit on the blockchain and setting the constraints for using the borrowed assets [75]. Solutions based on credit assessment models [76, 77] and incentive punishment mechanisms [78] are proposed, respectively. In the industry, TrueFi [79], Defi Passport [80], and CreDA [81] have carried out the practice of on-chain credit assessment.

Flash loans are DeFi’s innovative non-collateralized lending tool and have various use cases, such as arbitrage, collateral swapping, and self-liquidation [6]. Flash swaps provide similar services to flash loans within DEXs. Both flash loans and flash swaps leverage the atomicity of transactions, utilizing optimistic transfers that enable collateral-free loans or token exchange transactions as long as the loan is repaid by the end of the block (illustrated in Figure 3).

**Exchange.** In traditional exchanges, market makers summarize trades based on the seller’s request and the buyer’s offer on the order book. Decentralized exchanges (DEXs) decentralize aggregation, clearing, and market making through blockchain [82, 83]. More than 1000 apps have made DEXs the most abundant application type in DeFi, with a TLV of US$11.498b (#DefiLlama).

DEX can be divided into different models based on the implementation of trading pair discovery and order matching [84]. These models include on-chain order book model as implemented by Stellar, off-chain order book model as implemented by 0x [85], AirSwap [86], IDEX [87] and dYdX [10, 88], and non-order book model which is one of the most important innovations of DeFi. Methods of no-order book model, including reserve pool (implemented by KyberNetwork [89]) and algorithms of AMM like constant mean (adopted by Balancer [90]), constant product (adopted by Uniswap [9]), dynamic weighting(adopted by Bancor [91]) and mixed-function algorithm(adopted by the Curve Finance [92]), have been implemented in the industry. This is also one of the hottest research areas, including reviews that categorically evaluate different implementations [22, 93, 94] and specific algorithms that have been put into practice in the industry. We observe that empirical research is a kind of literature that is relatively lacking. There are some case studies on individual algorithms like [95], but there is a lack of empirical studies based on extensive data.

3.3 Services of DeFi

Inspired by traditional derivatives, DeFi offers on-chain options, asset management, and decentralized insurance by replacing traditional processes with on-chain automatic executions [3]. New financial derivatives, such as perpetuity contracts and prediction markets, have also emerged.

DeFi derivatives are a recent development in both industry and academia. However, compared to the industry’s quick implementation and over US$1.8b TLV (#DefiLlama), research on DeFi derivatives is limited, with only a few available papers. Empirical research in this field is almost non-existent, and most review articles focus on discussing the feasibility of DeFi derivatives. They emphasize the benefits compared...
to traditional solutions but lack evaluations of implemented solutions. This may be related to the novelty of the field. Additionally, there is a more substantial and earlier body of research related to DeFi insurance, possibly because of the high level of decentralization and collateral involved in the DeFi space, making risk management a crucial concern.

Furthermore, frequent DeFi incidents have raised significant concerns about the security of funds. Insurance is seen as a significant tool to mitigate risk and enhance capital security, which is why it received earlier attention and exploration. In contrast, research on other types of DeFi derivatives, such as options, perpetual contracts, and asset management, is rela-
DeFi asset management can be categorized as active or passive. Active asset management involves a professional team making investment decisions and trades, for example, Enzyme [108]’s managers or DAO members and Babylon Finance [118]’s community governance. Passive asset management such as Set [109] and Index Coop [119], on the other hand, allows users to create their own indices, structured products, and more in the form of smart contracts. Integrated platforms combine active and passive ways, offering quantitative analysis with machine learning, such as SW DAO [120], Kava DeFi Platform [121], and DAOventures [122].

DeFi insurance has the same working aspects as traditional insurance, including creation, purchase, and claim of insurance. The differences between DeFi insurance and traditional are that DeFi insurance enables all users to create their own insurance content as can be seen in Etherisc [123] and turns the decision on insurance claims into a transparent and verifiable process achieved through implementing shared pool models (e.g. Nexus Mutual [37]), social proof endorsement (e.g. VouchForMe [110]) or prediction markets (e.g. Augur [111]) and financial derivatives (e.g. oTokens [106]).

Insurance is one of the most widely studied applications in DeFi derivatives. The review literature has discussed the potential [124] and risk [125] of blockchain technology in the insurance industry and the possible application for the entire insurance process [126]. Various solutions have also been proposed including the construction of the entire framework [127] and the enhancement of efficiency [128], verifiability [129], traceability [130] and other performance.

Perpetual Contract. DeFi perpetual contracts allow participants to speculate or hedge against the price movements of an underlying asset, similar to leveraged spot trades, but without an expiration date, and use a fund fee mechanism to track the price index of the underlying asset. DeFi perpetual contracts are usually implemented as NFTs by smart contracts and can be traded in DEXs. Participants can be incentivized by providing liquidity and receiving rewards.

Prediction Market. Prediction markets involve the creation, trading, and settlement based on real-world event outcomes using smart contracts. Participants are motivated by profit-sharing for accurate predictions and liquidity rewards. The revenue in prediction markets is directly impacted by event outcomes, making it a significant incentive. To determine event outcomes, prediction markets use incentive mechanisms like reward and punishment or oracles providing real-world data. Augur [111], for example, incentivizes accurate reporting through a dispute mechanism where the winner receives the loser’s staked tokens. Omen Prediction Market [113] introduced Reality.ETH, a decentralized oracle challenging previous user results to approach the truth.

4 Technical Security Risks

We identified three types of technical security risks based on DeFi architectural design (Table 2): infrastructure layer risk, protocol layer risk, and application layer attacks.

4.1 DeFi Infrastructural Layer

Risks in Network Communication. DeFi relies on network protocols like TCP/IP, which directly impact the security of networks. Attackers can exploit vulnerabilities, manipulate messages, or control network service providers, posing risks to the security of transactions. Denial of Service (DoS) attacks pose a threat where attackers may leverage network congestion to flood the system with invalid transactions or consume excessive bandwidth and computing resources. Additionally, node transparency risks such as Eclipse attacks [131] and Sybil attacks [132] and centralized control by a few entities in
51% attacks [133] can undermine trust, security, and stability. Researchers have proposed various approaches to analyze network security, including attack graph analysis [134, 135] and mathematical models quantifying parameters like risk, vulnerability, and threats [136].

**Risks in Consensus Algorithm.** Consensus algorithms enable nodes to reach agreement on tasks such as transaction ordering, block generation, and data validation. Nodes are incentivized with block rewards and transaction fees. However, this decision-making power introduces uncertainty regarding the transactions included in a block, which can be exploited by attackers through Miner Extractable Value (MEV) [24]. While MEV can have legitimate uses, such as ensuring timely liquidation in lending protocols, facilitating accurate price formation, and arbitraging in DEX, it also creates problems for users. MEV can result in advantageous forks over the main chain [137, 138]. Attackers utilize MEV for front-running [139, 140] or sandwich attacks [27], compromising fairness [141] and colluding with nodes for profit.

**Forks.** A fork occurs when the main chain splits into two separate chains. The forked chain may have different security and stability, making it more susceptible to new vulnerabilities and attacks. This can disrupt the compatibility of smart contracts on both chains, requiring redevelopment and migration. In DeFi, chain forks can fragment markets and reduce liquidity. Users may lose funds by mistakenly operating on the wrong chain. Attackers can exploit forks to gain unearned rewards by overtaking and overwriting the main chain.

**Front-running.** Front-running attacks (cf. Figure 5a) occur when an attacker predicts or monitors a user’s transactions and submits their own transactions with higher priority, blocking others and altering outcomes for additional profit [26, 142]. They exploit blockchain transparency and transaction latency. The bZx lending platform suffered a front-running attack in Feb. 2020, where attackers borrowed assets and sold them at manipulated prices, earning significant profits. Mitigation front-running risks solutions include lightning networks for off-chain transactions, batch order processing to narrow the window and raise costs for attackers, sealed transactions to prevent eavesdropping, and fee market efficiency improvement to reduce MEV and front-running profitability [143, 144]. FaaS like Flashbots enables traders to directly send transactions to miners, aiming to reduce front-running risks and give users more control. However, Weintraub et al. [145] found that over 80% of Ethereum’s MEV occurs through Flashbots, raising questions about the feasibility of FaaS and potential competitive concerns for other participants.

**Sandwich Attack.** A sandwich attack [27] (cf. Figure 5b) is an exploitation tactic where an attacker executes counterparty trades before and after a target trade to profit from price discrepancies and illiquidity. The attacker manipulates the price by squeezing the low-cost trade between the target trade [146]. Attackers monitor DEX order books and trading activity to identify profitable opportunities and swiftly submit counterparty trades for additional revenue. The main difference between sandwich attacks and front-running attacks is the timing of target transaction execution and their respective targets. Sandwich attacks impact prices by executing counterparty trades simultaneously, causing unfair trading losses for the target trader. Front-running attacks gain an advantage by submitting trades before execution, resulting in unfair trading costs for other traders. Although confirming specific sandwich attacks can be challenging, there have been reports of numerous DeFi sandwich attacks exploiting illiquidity, price slippage, and execution delays on DEXs for additional profit.

### 4.2 DeFi Protocol Layer

Smart contracts are vital for implementing and securing DeFi functions. However, they are vulnerable to common vulnerabilities, which have been recognized by academia [147] and industry [148]. Beyond coding, improper protocol design can also introduce security risks.

**Risks in Writing Smart Contracts.** Coding errors such as arithmetic errors, conversion errors, inconsistent access control, and functional reentry are some representative vulnerabilities in smart contracts [149, 150].

**Reentry.** A reentry attack is a significant threat to smart contract security. Attackers exploit this vulnerability by repeatedly executing a specific contract function and invoking malicious contracts during each execution [151]. The attacker deploys a malicious contract with callable functions into the...

---

**Figure 5: Front-running and Sandwich Attack**
target contract and re-invokes it multiple times by calling a function of the target contract. This attack allows unauthorized access to contract funds, modifies the contract status, or performs other malicious actions. The DAO, a community-based investment and fund allocation platform, experienced a reentry attack in 2016. The attacker successfully steals millions of Ether by repeatedly calling the withdrawal function through a malicious contract. To prevent reentry attacks, the Ethereum community has implemented improvements such as a "backward transfer" mode, modifiers to restrict external contract calls, locking mechanisms, status markers, state variables, and lock flags to track and prevent re-calls of functions.

**Overflow.** Overflow is common in smart contracts and can result in unexpected money transfers, contract lockouts, or DoS. These vulnerabilities include integer overflow, array overflow, and memory overflow. Attackers exploit integer overflow to alter contract states or transfer funds. Array overflow allows attackers to access other data in a contract’s memory, leading to data tampering. Memory overflow can cause contract execution failure. In 2018, attackers exploited an integer overflow vulnerability in BeautyChain, an Ethereum-based platform, resulting in the theft of approximately $3 million in cryptocurrency. Similarly, Meerkat Finance, a BSC-based lending protocol, suffered a loss of $31 million in Mar. 2021 due to an overflow vulnerability. To prevent such vulnerabilities, developers should focus on boundary checking during coding and conduct thorough code reviews.

**Random Numbers Misuse.** Misuse of random numbers in smart contracts can lead to security and fairness issues [152][153]. Attackers exploit this vulnerability to predict or manipulate outcomes, gaining unfair advantages. In 2018, hackers manipulated the random number generator of the EOSPlay gambling contract on the EOS blockchain, receiving significant rewards. Insecure random numbers in functions like key generation compromise encryption algorithms. To prevent misuse, developers should carefully assess the need for random numbers. Verifiable generators like Blockchain-based Random Number Generators (BRNGs) and protocols like Distributed Random Number Generation (DRNG) can enhance security. Security audits and code reviews are also essential.

**Risks in Updating Smart Contracts.** Smart contract updates pose potential issues and security risks such as contract misbehavior, funds loss, contract unavailability, or reduced security. Incompatibility between new and previous versions can introduce vulnerabilities, hinder data migration, or disrupt contract dependencies. Incorrect configuration parameters or tampering can lead to contract failures or unexpected outcomes [154]. New permission mechanisms or access control rules may result in incorrect or overly permissive configurations, enabling unauthorized actions. Mismanagement of multiple contract versions can lead to inconsistencies. For instance, in April 2021, Uranium Finance on BSC suffered an attack due to neglected parameter changes during a contract upgrade. To prevent such issues, developers should plan, test, audit upgrades, establish monitoring, and rollback mechanisms to detect and mitigate problems promptly.

**Risks in Design of Protocols.** Alongside code vulnerabilities, security risks can arise from inadequate protocol design, including logical vulnerabilities, flawed economic models, insufficient risk management, and inappropriate authorization. Complex algorithms or models may overlook specific scenarios, impeding proper functionality. Economic models with inflationary, deflationary, or unfair revenue sharing may lead to revenue loss or instability. Insufficient risk management measures hinder responses to adverse events and risk mitigation. In Jun. 2021, Iron Finance faced a crisis due to its economic model when its governing token TITAN’s price collapsed. Massive selling of both TITAN and its stablecoin IRON triggered a mechanism that minted more TITAN as IRON’s price dropped, intensifying the price drop and causing a death spiral. Furthermore, flawed designs may grant administrators undue control, enabling manipulation or Rug Pull. The Compounder Finance team misused administrator privileges to replace audited contracts with malicious ones, resulting in the misappropriation of user funds.

## 4.3 DeFi Application Layer

The security risks of DeFi extend beyond the system’s internal workings to include external attacks towards asset bridges, irregular services provided by auxiliary applications like oracles, and users’ misconceptions about smart contracts.

**Risks in Cross-chain.** Cross-chain attacks exploit the mechanism of cross-chain transactions, posing risks to the security and stability of cross-chain DeFi apps. These attacks can lead to asset loss, transaction delays, and information tampering. There are two main types of cross-chain attacks: native-chain attacks and inter-chain attacks. Native-chain attacks include double-spend attacks, false proof attacks, vulnerability exploits, reverse transaction attacks, and replay attacks [178]. Inter-chain attacks encompass relay blocking and inter-chain route hijacking [181]. Payment channels may also be vulnerable to wormhole attacks, where intermediate node fees can be stolen [183]. DeFi cross-chain applications face unique security risks. Cross-chain smart contracts in DeFi apps are exposed to vulnerabilities in their own code and the calling relationship between contracts. Price manipulation attacks and repeated borrowing and lending attacks are examples of cross-chain attacks faced by DeFi apps, as seen in the case of the attack on PancakeSwap in Apr. 2021.

**Risks in Auxiliary Tools.** Auxiliary services are entities that promote efficiency but are external to the system.

**Oracle Manipulate.** Oracle manipulation by hackers involves providing false data to smart contracts, leading to improper benefits or disruption of normal operations [187]. This manipulation can result in negative consequences, including stablecoin unanchoring, malicious carry trades, forced liquidation,
and depleted protocol liquidity. Attackers target data sources by attacking API interfaces or tampering with supply chains. They provide false or inaccurate data, modify prices or offer incorrect market information. To prevent oracle manipulation, developers must prioritize secure and tamper-resistant oracles, along with incentivizing their usage. Ensuring the quality of connected markets is also crucial.

Risks of Ignorance. Users’ limited understanding of smart contracts and their associated security risks can lead to unforeseen circumstances [202]. Moreover, the shortage of security awareness makes them susceptible to phishing attacks, resulting in personal information leaks and fund theft [203]. Phishing attacks in DeFi involve impersonating legitimate entities or creating deceptive environments like fake DeFi platforms or sending fraudulent notifications to trick users into revealing sensitive information, private keys, or login credentials. For example, in Dec. 2021, Badger DAO suffered a $120 million loss due to a phishing attack involving malicious wallet requests. Similarly, in 2021, attackers stole assets by sharing fraudulent links on social media, leading users to a fake Uniswap website.

5 Economic Security Risks

DeFi economic risks stem from rational players’ actions within the ecosystem, rather than traditional vulnerabilities. Liquidity Depletion. DeFi liquidity depletion risk occurs when there is a shortage of market liquidity, causing transaction delays, price fluctuations, and market instability. Insufficient liquidity can result from adverse market conditions, increased risk sentiment, or rapid fund withdrawals. Factors like market fluctuations, falling collateral prices, or manipulation can also contribute to liquidity depletion. The Black Thursday event in Mar. 2020, involving MakerDAO, exemplifies the consequences of liquidity depletion [204]. To mitigate this risk, DeFi platforms should attract diverse liquidity providers and reduce dependency on specific sources. Incentives can be implemented to attract and retain liquidity providers [84, 205]. Additionally, DeFi applications should develop risk management strategies and contingency plans to address liquidity depletion scenarios.

Flashloan Attack. Flash loan security risks involve vulnerabilities, contracts, and attack risks associated with flash loans [7, 139]. We observed that such attacks occur frequently and can be categorized into code vulnerabilities, bid arbitrage, and price manipulation. Attackers exploit flash loans to execute sophisticated strategies that exploit smart contract vulnerabilities. Bid arbitrage manipulates transaction sequences to capitalize on arbitrage opportunities using borrowed funds. Price manipulation involves using flash loan funds for large-scale trading, influencing prices. Defending against flash loan attacks requires managing protocol security, auditing contracts, and implementing measures like transaction order restrictions, delays, or time windows.

Market Manipulation. Market manipulation artificially influences asset prices to profit. Illiquid assets pose higher risks to underlying financial products. Manipulative strategies include spoofing [206], ramping [207], bear raids, cross-market

Table 2: Concerns and Solutions in DeFi Applications and Open Research Challenges

<table>
<thead>
<tr>
<th>Affected Layers</th>
<th>Attacks</th>
<th>Incidents</th>
<th>Solutions</th>
<th>Research Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Time</td>
<td>Application</td>
<td>Loss</td>
</tr>
<tr>
<td>Network</td>
<td>Dos (DDoS) [155] [156]</td>
<td>2020/05</td>
<td>Youbi</td>
<td>N/A</td>
</tr>
<tr>
<td>Communication</td>
<td>Eclipse Attack [131] [158]</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Sybil Attack</td>
<td></td>
<td>2022/04</td>
<td>PegNet</td>
<td>0.6M USD</td>
</tr>
<tr>
<td>51% Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td>Fork [163] [139] [27]</td>
<td>2023/03</td>
<td>DODO</td>
<td>0.7M USD</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Front-running Attack [36] [142]</td>
<td>2021/10</td>
<td>Alpha Homora V2</td>
<td>40.61 ETH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Arbitrage Attack [166]</td>
<td>8 BTC</td>
</tr>
<tr>
<td>Smart Contract</td>
<td>Reentrancy [168] [151]</td>
<td>2016/06</td>
<td>TheDAO</td>
<td>3.6M ETH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2018/07</td>
<td>Bancor</td>
<td>1.2M USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2021/07</td>
<td>AnySwap</td>
<td>8M USD</td>
</tr>
<tr>
<td>Protocol</td>
<td>Rag Doll [173]</td>
<td>2021/03</td>
<td>Meerkat Finance</td>
<td>20M USD</td>
</tr>
<tr>
<td>Bridge</td>
<td>Double Spend Attack [175]</td>
<td>2020/02</td>
<td>DForce</td>
<td>2.5M USD</td>
</tr>
<tr>
<td></td>
<td>False Proof Attack [175] [177]</td>
<td>2022/02</td>
<td>Wormhole</td>
<td>1.2M ETH</td>
</tr>
<tr>
<td></td>
<td>Replay Attack [176]</td>
<td>2022/09</td>
<td>OncaBridge</td>
<td>2M ETH</td>
</tr>
<tr>
<td></td>
<td>Inter-Chain Route Hijacking [181]</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wormhole Attack [183]</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cross-chain Price Manipulation [185]</td>
<td>2023/08</td>
<td>NeoFi</td>
<td>23.5 ETH</td>
</tr>
<tr>
<td>Auxiliary Tools</td>
<td>Oracle Manipulation [187] [144]</td>
<td>2023/06</td>
<td>Theora Protocol</td>
<td>0.37M USD</td>
</tr>
<tr>
<td>Usage Method</td>
<td>Phishing Attack [183] [189]</td>
<td>2022/12</td>
<td>Bitkeep</td>
<td>8M USD</td>
</tr>
<tr>
<td>Economic Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real Collapse/Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019/09</td>
</tr>
<tr>
<td>Compound</td>
</tr>
<tr>
<td>2019/09</td>
</tr>
<tr>
<td>77M USD</td>
</tr>
<tr>
<td>194/195</td>
</tr>
<tr>
<td>Market Manipulation</td>
</tr>
<tr>
<td>2022/10</td>
</tr>
<tr>
<td>Mango</td>
</tr>
<tr>
<td>114M USD</td>
</tr>
<tr>
<td>196/197</td>
</tr>
<tr>
<td>Flashloan</td>
</tr>
<tr>
<td>various</td>
</tr>
<tr>
<td>various</td>
</tr>
<tr>
<td>various</td>
</tr>
<tr>
<td>139/7</td>
</tr>
<tr>
<td>Death Spinal</td>
</tr>
<tr>
<td>2023/05</td>
</tr>
<tr>
<td>Lasso-UST Collapse</td>
</tr>
<tr>
<td>66B USD</td>
</tr>
<tr>
<td>198/71</td>
</tr>
<tr>
<td>Ponzi and Fraud</td>
</tr>
<tr>
<td>2022/11</td>
</tr>
<tr>
<td>FTX Collapse</td>
</tr>
<tr>
<td>32B USD</td>
</tr>
<tr>
<td>199</td>
</tr>
<tr>
<td>CeFi Impact</td>
</tr>
<tr>
<td>2023/03</td>
</tr>
<tr>
<td>SVB Collapse</td>
</tr>
<tr>
<td>23B USD</td>
</tr>
<tr>
<td>200/201</td>
</tr>
</tbody>
</table>

10
manipulation, and oracle manipulation [188], which can manipulate segments or the entire market. Market manipulation has resulted in various negative impacts on the DeFi ecosystem, such as bad debts due to failure of timely liquidation, losses for liquidity providers due to false price-based payouts in synthetic assets, and depeg for algorithm stablecoins [71].

Distinguishing normal fluctuations from manipulation in DeFi is challenging due to anonymity, trading freedom, and regulatory gaps. Anonymous transactions hinder accurate tracking of participant behavior. Trading freedom and liquidity provision enable price influence through large-scale transactions or exploiting limited market depth. Regulatory gaps and the lack of mechanisms like KYC requirements hamper monitoring manipulative behavior. To reduce market manipulation risks in the DeFi market, it is necessary to strengthen regulatory compliance and enhance investor education. Monitoring tools and algorithms can detect abnormal trading patterns and manipulative behavior in a timely manner. Strengthening investor education can increase awareness of market risks, encouraging cautious participation.

**Governance Risk.** Governance and incentives can drive choices that benefit DeFi apps. However, inadequate incentives may lead token holders to prioritize external gains, potentially harming the system. Immediate governance updates can be vulnerable if malicious contract code is executed using acquired governance tokens. The Beanstalk protocol faced governance risks when an attacker accumulated tokens and proposed a malicious proposal to divert funds. In Ethereum 2.0 (post-Merge), validators face censorship pressure due to The Office of Foreign Assets Control of the US Department of the Treasury(US OFAC) sanctions on Tornado Cash [208, 209].

**Death Spiral and Instability.** Stablecoins aim to maintain a consistent value by being pegged to a fiat currency. A "death spiral" refers to a scenario where a stablecoin rapidly and uncontrollably loses its value. This decline can trigger a compounding effect, intensifying the downward spiral and eroding confidence in the stablecoin, ultimately culminating in a self-perpetuating cycle of value deterioration. The concept of a death spiral is particularly relevant in crypto stablecoins, especially algorithmic ones. An example is the depeg of UST, which led to the collapse of Luna’s value in 2022 [71, 198]. This event marked the onset of a "crypto winter," a period of prolonged market decline and reduced investor optimism.

**Ponzi and Fraud.** The Ponzi game is named after Charles Ponzi, who deceived investors with a postage stamp speculation scheme. It involves funding preexisting liabilities by issuing new debt. Ponzi schemes have infiltrated the crypto markets, especially during ICOs, IEOs, IDOs, and similar events. A recent example is the FTX collapse [199] in 2022, where SVB sold FTT tokens to Alameda, a high-frequency trading company under the same ownership, in an attempt to inflate token prices. Ponzi’s collapse extends beyond immediate losses of rug pull with far-reaching implications.

**CeFi Impact.** The crypto market has become increasingly influenced by macroeconomics, exhibiting a trajectory that parallels traditional stock markets. It is susceptible to the impacts of conventional financial crises. The SVB (Silicon Valley Bank) collapse [200,201] in early 2023 is an illustrative case. SVB, a Centralized Finance (CeFi) bank for high-tech and crypto startups, experienced a crisis that resulted in the loss of deposits. This event eroded confidence in secure crypto asset storage methods and raised concerns about asset safety.

### 6 Open Research Challenges

**Observation.** There exists a time lag between the industry and academia, as industry innovation often precedes academic research. However, the implementation of DeFi in the industry currently is primarily driven by commercial intuition, lacking comprehensive academic research in problem definition, theoretical analysis, mechanism design, and economic models. This gap hinders theoretical innovation and the timely resolution of emerging issues, limiting efficiency and sustainability.

**Gap.** The relative lag in academic research, particularly with regard to information security concerns, can result in potential inadequacies in the security assessment of newly emerging DeFi protocols. Accidents and risks that arise during the use of new technologies (emerging financial products) cannot be anticipated, forewarned, or prevented in advance, posing risks to user assets and impeding comprehensive development.

**Revenue.** Therefore, further research on DeFi requires in-depth exploration of new technologies and models, encompassing different perspectives such as information security, and game theory mechanisms, and conducting systematic evaluations that are aligned with industry practices. To bridge the gap between industry and academia, it is necessary to address the lack of research and validation tools in the academic community. Academic researchers require models, simulation tools, and data analysis capabilities to establish and validate DeFi solutions. Effective data and analysis tools are needed to collect, organize, and analyze transaction and contract data. Comprehensive security audit tools are also necessary to evaluate the security of smart contracts and protocols. Joint efforts between academia and the industry can promote the development and improvement of these tools. Academic researchers can focus on developing models and simulation tools, while the industry can provide real-time data and practical experience to support data and analysis tool development. Collaboration between the academic community and security audit teams can enhance the security of DeFi projects by jointly researching and developing security audit tools.

**Gap.** Regarding economic security concerns, the relative lag in academia has resulted in a lack of in-depth analysis and theoretical modeling of economic interactions and mechanism designs in DeFi. Firstly, the industry lacks a proper understanding of participant behavior and incentive mechanisms,
leading to product designs that heavily rely on experience and intuition. Secondly, information asymmetry and incomplete information exacerbate the industry’s limited awareness and application of existing academic research. DeFi applications lack guidance from economic equilibrium theories, leading to potential risks, instability, manipulation, attacks, and systemic risks. Inappropriate incentive structures and market imbalances undermine the achievement of economic and societal objectives, efficiency, fairness, and sustainability.

**Revenue.** The academic community should utilize analytical tools such as economic equilibrium and game theory to establish technical and economic models for DeFi applications and conduct research on game mechanism design and analysis. Progress can be made from multiple perspectives of economic modeling, mechanism design, and technical implementation, and combining theoretical analysis, practical solutions, and empirical research.

**Gap.** Regardless of the improvement in technology, security, or economics in the field of DeFi, the interdisciplinary nature of DeFi cannot be overlooked. Collaboration between economists, computer scientists, legal experts, and other stakeholders is crucial. As mentioned earlier, the limitations of a single-disciplinary perspective have been highlighted, and it has been pointed out that the core issue lies in the insufficient depth of interdisciplinary collaboration and the shortage of talent with interdisciplinary expertise.

**Revenue.** To address this issue, on one hand, it is necessary to encourage and facilitate interdisciplinary collaboration among experts from different disciplines through cross-disciplinary projects or platforms. On the other hand, it is important to cultivate talents with multidisciplinary skills required in DeFi research. Specifically, these talents need to possess expertise in areas such as blockchain, network security, code analysis, financial markets, investment analysis, risk management, and financial technology, spanning disciplines like economics, computer science, and cryptography.

In addition to the overall observations in DeFi mentioned above, there are also research gaps and challenges in specific aspects such as technological construction, sociological construction, economic construction, and ecosystem construction. We will elaborate on each of these areas (cf. Table 3).

### Table 3: Open Research Challenges

<table>
<thead>
<tr>
<th>Direction</th>
<th>Open Research Challenge</th>
<th>Literature (paper count)</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Tools</td>
<td>Definition and Model</td>
<td>283, e.g., [1]</td>
</tr>
<tr>
<td>DeFi Technical Construction</td>
<td>Performance</td>
<td>137, [210] [211] [212]</td>
</tr>
<tr>
<td></td>
<td>Function Integration Platforms</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Contract Audition</td>
<td>600, [213] [214] [215]</td>
</tr>
<tr>
<td></td>
<td>Incident Detection</td>
<td>308, [216] [217] [218]</td>
</tr>
<tr>
<td>DeFi Economy Construction</td>
<td>Sustainable Tokenomics</td>
<td>193, [219] [220] [221]</td>
</tr>
<tr>
<td></td>
<td>Balanced Incentive</td>
<td>122, [222] [223] [224]</td>
</tr>
<tr>
<td>DeFi Sociology Construction</td>
<td>Privacy</td>
<td>216, [225] [226]</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>75, [227] [228] [229]</td>
</tr>
<tr>
<td>DeFi Ecology</td>
<td>User Engagement and Education</td>
<td>11, [230] [231] [232] [233]</td>
</tr>
</tbody>
</table>

### 6.1 DeFi Technology Construction

**Functionality.** There are numerous protocols and functionalities in DeFi. Function integration platforms can provide unified access, simplifying user operations and enhancing user experience. Their goals include user-friendly interfaces, protocol integration, security, and interoperability for seamless asset and data transfers. However, these aspects have not been extensively explored by both the industry and the academic.

Research challenges for function integration platforms encompass staying updated and incorporating the developments and innovations, implementing better risk management practices to adapt to the dynamic nature of the DeFi market, conducting comprehensive security audits and vulnerability fixes, and addressing challenges related to interoperability, stability, and availability that arise from integrating multiple protocols.

**Security.** DeFi security involves analyzing attack and threat models at the network [134–136], smart contract [234] (single contract, multiple contracts, and contract audit [8]), protocol [235], and application layers [236, 237].

We found that in-depth research on DeFi network communication security, standardized evaluation, audit methods, and defense strategies is lacking. Researchers can enhance DeFi security by analyzing network topology, node communication, and protocols like authentication, access control, and secure smart contracts. Existing smart contract audit tools have limitations in detecting complex attack strategies and advanced vulnerabilities. Research is needed on tracking contract changes, conducting timely audits, and establishing security standards and best practices. Moreover, there is limited research on secure DeFi application models and security issues arising from the collaboration between different applications.

**Incident Detection and Emergency Response.** DeFi acts as an amplifier for information security issues and risks, making disaster recovery and emergency response more urgent. Currently, this is a relatively unexplored research field. Timely incident detection and handling are essential for protecting user assets and the health of DeFi. Detecting incidents based on historical data is commonly done, but real-time monitoring remains understudied. Future research should focus on developing intelligent monitoring systems that analyze data and traffic patterns, using machine learning to identify abnormal activities and risks in advance. Establishing effective incident response mechanisms, as well as post-incident cooperation and asset recovery protocols, are important research gaps.

### 6.2 DeFi Sociology Construction

**Privacy.** DeFi privacy protection aims to safeguard users’ personal information, transaction data, and financial flows from unauthorized tracking, monitoring, and access. As the user base expands, privacy concerns in DeFi become more apparent, as existing analysis techniques can de-anonymize pseudonyms and infer user identities from external informa-
tion on the blockchain [238, 239]. Existing research explores privacy-enhancing technologies such as zero-knowledge proofs (ZKPs) [240], ring signatures [33], Trusted Execution Environments (TEEs) for anonymous computation, cryptographic techniques, and mixing schemes for transaction privacy protection, as well as confidential smart contracts for data privacy protection [21, 241]. Initially applied to privacy coins like Zerocoin [242], zero-knowledge proofs (ZKPs) such as zk-SNARKs [243] and Bulletproofs [244] have been utilized to enhance transaction privacy on the blockchain. Simpler and more efficient privacy coin schemes, including mixing schemes, have also been proposed. These technologies offer improved privacy protection, data security, anonymous transactions, and smart contract verification in DeFi. However, how these technologies can adapt to the specific and complex application scenarios in DeFi, enhance performance, and achieve scalability, remains an unresolved research question. Additionally, striking a balance between anonymity and traceability to meet regulatory requirements poses significant challenges. Readers interested in exploring privacy-enhancing technologies in DeFi are recommended to refer to relevant Systematization of Knowledge (SoK) papers [245].

Compliance. Compliance in DeFi is vital for protecting funds for users, ensuring stability for the system, and preventing illegal activities such as money laundering and terrorist financing for regulators. However, the decentralized and permissionless nature of DeFi conflicts with compliance and regulation. For instance, Tornado Cash faced sanctions by the US OFAC for enabling anonymous transfers used in illicit activities. Balancing these conflicting aspects poses a challenge. Moreover, the rapid growth of DeFi requires the development of an appropriate compliance framework, including cross-border cooperation and leveraging technology for efficient processes.

6.3 DeFi Economy Construction

Sustainable Tokenomics. Token issuers should prioritize the design and implementation of a cryptocurrency or token ecosystem that promotes long-term viability, equilibrium, and positive impact. Rather than engaging in deceptive practices, their focus should be on crafting mechanisms that enhance economic stability, while incentivizing productive and sustainable behaviors among token holders, users, and participants. Initiatives should be geared towards creating enduring value for the token, rather than relying on short-term speculative gains. By contributing to a resilient token ecosystem characterized by responsible practices and sustainable growth, token issuers can foster a positive and sustainable impact.

Balanced Incentive. Incentives hold a crucial role for token investors and holders. An effective incentive mechanism should extend benefits to all participants, encompassing both regular users (utilizing mobile clients, light clients, or web browsers) and network contributors (such as miners, validators, and operators). Within the PoW consensus model, the majority of regular users often find it challenging to secure stable rewards, given their limited impact on the network. In contrast, miners wield substantial power, affording them the ability to generate MEV revenues. Meanwhile, in PoS settings, stakeholders have the opportunity to earn a steady income. However, the issuance of tokens without associated costs can lead to potential token issuance abuse. Striking a balance between incentivizing network contributors while preventing token issuance abuse is crucial. This will create a fair ecosystem where rewards align with contributions, promoting healthier and equitable participation from all stakeholders.

6.4 DeFi Ecology Construction

User Engagement and Education. User engagement and user education are crucial for the DeFi ecosystem’s growth. Low user engagement can lead to reduced liquidity, increased transaction costs, and insufficient market depth, while user ignorance can elevate the risk of fraud and attacks. Enhancing usability is paramount in addressing these challenges. The industry should prioritize creating user-friendly interfaces and streamlining processes to attract a broader user base. Additionally, effective incentive mechanisms can encourage user participation and contributions. Comprehensive and easily understandable educational resources, including textbooks, online courses and guides, must be made available. Establishing a supportive community can further bolster user education by promoting collaboration and knowledge sharing, enabling users to assist and support each other on their DeFi journey.

Conclusion. This paper presents a comprehensive literature review and proposes a classification framework based on the complexity of DeFi services. We evaluate DeFi applications and discuss their security from both technical and economic perspectives. Furthermore, we identify research gaps and future directions, exploring relevant research topics.
References


[216] Xun Sun, Xi Xiao, Wentao Xiao, Bin Zhang, Guangwu Hu, and Tian Wang. Short and distort manipulations in the cryptocurrency market: Case study, patterns and


A Foundations of DeFi

A.1 Operational Supports

Transactions. A transaction is the smallest unit in the blockchain ledger. It includes sender and receiver addresses, the number of coins involved, a unique hash value, a timestamp, transaction/gas fee, block information (block ID of the first recording block), and data payloads for execution (cf. Figure 1). Interactions with the blockchain are categorized as transfer or contract transactions. Transfer transactions involve simple coin transfers, while contract transactions interact with smart contracts. A transaction sender must be an Externally Owned Account (EOA), while the receiver can be a smart contract address or an EOA, and the transaction data field contains the required parameters for the contract function.

Block. The block is a fundamental unit of data, consisting of header and body. The header contains the previous block’s hash, current block’s ID, and Merkle root of its content, ensuring a tamper-proof chain. The block body contains transactions. Creating a new block involves propagation and validation across different nodes via consensus algorithms. A newly added block is linked in the current chain.

Chain. The chain is a series of blocks linked together using cryptographic hashes (cf. Figure 1). Each block contains a unique identifier (hash) derived from its data and the previous block’s hash. This creates a continuous and tamper-resistant chain of data known as the blockchain (conceptual milestones in 1991 [246], 2008 [29], and 2014 [247]).

Smart contracts. Smart contract constitutes a crucial element supporting DeFi protocols. Deployed on-chain, it acts as a computerized transaction protocol that transforms traditional contract terms into executable programs, maintaining logical connections between terms as a flow (see Figure 1). Smart contracts feature automatic execution, instant response, and strict enforcement, and the contracts deployed on them are tamper-proof, minimizing the chance of human intervention.

DApp. Short for decentralized applications, DApps are constructed on blockchain using smart contracts [248]. Smart contracts can be likened to code-based Lego blocks with automatic execution functions [249]. Multiple smart contracts can collaborate to achieve the intricate functionalities required by applications. DApps usually offer user interfaces, streamlining users’ interactions with the blockchain. User actions via DApps are recorded on the blockchain as transactions, executed according to pre-written smart contract rules, and verified by blockchain nodes.

A.2 DeFi Composition

Wallet. A user can manage multiple accounts from a single wallet in DeFi. Each account has three components: public key, private key, and address, as shown in Figure 2. A cryptographic algorithm generates a pair of one-to-one keys when an account is created. The private key generates the digital signature necessary for proving ownership of assets, which can be verified by the corresponding public key. An address, generated from the public key by a one-way hash function, is to DeFi what an account is to traditional finance, symbolizing a user’s on-chain identity. Since private keys are difficult to remember, the wallet developers have set up mnemonics as double insurance policy to help users memorize complex private keys. A mnemonic can be understood as a simplified version of the private key, which is generated by an algorithm that selects words from a fixed vocabulary. When the user forgets the private key, the mnemonic is used to recover it.

Figure 1: DeFi Foundations

Figure 2: Components of Wallets

The security of wallets focus on three essential links: the creation, storage, and use of private keys. The storage security of private keys can be strengthened through local storage. The security recovery of private keys can be enhanced through secret sharing and TTP. The secure usage of private keys can be
achieved through multi-factor authentication. Non-custodial wallets, such as MetaMask [99], locally store private keys, protecting them from server owners and attackers. Through academic research, the conditions for implementing secret sharing to protect private keys have evolved from relying on TTP authentication [250] or permissioned blockchains [251] to utilizing single-password systems [252] and trustless environments [253]. The industry has also developed security-enhanced wallets based on secret sharing, such as Zengo [100].

Academic research has covered different types of TTP-based wallets, e.g., [254]’s identity-based key encryption for software wallets and [255]’s recovery for hardware wallets, and considered factors like privacy, e.g., [256]’s recovery scheme with privacy protection using ZKPs. Argent [101] is one of the industry examples that utilizes TTP. Multi-factor authentication, including biometric features [257] like fingerprint [258, 259], iris, pulse [260], and behavioral features like mouse behavior [261], can help to verify the identity of user.

**Oracle.** Oracle provides external data sources for smart contracts on the blockchain, supplying them with data information. The oracle retrieves the data from off-chain data providers, typically nodes within the blockchain network, who fetch data from various public sources. The data is then sent to smart contracts of the oracle, which tasks such as packaging, verification, and cleansing of the received data. Finally, the oracle submits the updated data, allowing the user or smart contract that initiated the request to obtain.

**Stablecoin.** Stablecoins can be formed through various methods, including off-chain reserves or on-chain collateralization. Stablecoins circulate similarly to traditional finance systems, involving reserve, issuance, and other essential links. Off-chain reserved stablecoins are backed by fiat or assets like gold. Maintaining transparency and integrity of reserve assets ensures a 1:1 collateralization ratio between stablecoins and backing assets. However, these stablecoins carry risks due to centralized reserves and third-party audits. In contrast, on-chain reserve stablecoins and algorithmic stablecoins use digital assets as collateral or eliminate collateralization altogether. They are created through a transparent on-chain process with different price stabilization mechanisms. Despite their advantages, some on-chain stablecoins are prone to downfall caused by a death spiral during crises.

**Lending.** Decentralized lending protocols typically involve collateralization, lending, and liquidation. Users provide digital assets as collateral, which are aggregated into a pool that forms a reserve used for redemption. The smart contracts issue credential tokens to users, which can be used for redemption. Users’ credit for borrowing is based on the liquidity they provide, and the floating or fixed borrowing rate is determined by an interest rate contract that adjusts based on supply-borrowing dynamics according to specific interest rate models. Liquidation is triggered when a user’s debts exceed the borrowing capacity, and any participant can compete to liquidate debts and earn rewards. Some protocols distribute governance tokens to users to incentivize participation.

**Flash Loan.** The workflow of flash loans or flash swaps is illustrated in Figure 3.

**Exchange.** DEX can be divided into different models based on the implementation of trading pair discovery and order matching (cf. Figure 4). Some DEXs use order book, where orders are recorded in an order book, and transactions are aggregated using principles of high and low bids and time order. DEXs using on-chain order books maintain order books at each node, with orders submitted to smart contracts and broadcasted to the network. When receiving the order, the node records and matches the prices and automatically executes the trade. The discovery of transactions in this model is limited by network performance. The off-chain order book model is similar to traditional exchanges, where the exchange maintains an order book and matches them off-chain. Several DEXs innovate the non-order book model. Two methods are (i) the establishment of a reserve pool, and (ii) the use of the AMM mode, which calculates the exchange rate between two or more assets according to specific algorithms, providing the quotation between assets at any time. Both sides of AMM trades interact with on-chain liquidity pools that allow users to seamlessly switch between tokens. Liquidity providers earn income based on the percentage of their contribution to the pool. The core of AMM lies in various exchange rate algorithms, including constant mean, constant product, dynamic weighting, and constant sum.