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 revenues, 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 prewritten, 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-

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

cal methods (Section 2), we obtain more than 10,000 DeFi-related research articles and conduct qualitative and quantitative analyses.

- We propose a DeFi classification framework based on the complexity of financial services. The framework (summarized in Table 1) classifies DeFi applications into three categories (Section 3): 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).

Figure 1: Paper Structure

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 levels, 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.

Figure 2: DeFi Ecological Structure

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.

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.

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

The digital asset research eld within DeFi emerged early and has a wealth of literature. Quantitative and predictive research, speci cally focused on the cryptocurrency market, is a signi cant 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 eld.

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 " ash 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, which has led to the development of hot and non-custodial wallets. Multi-factor authentication, such as biometrics and behavioral features, has been implemented to enhance security. Secret sharing and Trusted Third Party (TTP) veri cation have also been employed to strengthen security of key recovery.

Oracle. The execution of smart contracts requires meeting conditions speci ed 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 (DeFi Llama).

To ensure trustworthy on-chain data, the accuracy of data is the main concern [44]. We have observed that review articles in this eld 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 speci c implementation methods such as setting whitelists/blacklists, incorporating identity veri cation 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 veri cation [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 veri cation, which restricts them to publicly accessible information. These oracles also face challenges like data latency and high veri cation 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. 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 $1.232b (DeFi Llama), re ecting 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 at currencies, which is exactly why stablecoins were born. As a foundational currency, stablecoins support liquidity pools, lending, insurance, and other nancial activities [60], mitigating the risks associated with market uctuations. As of Oct. 2023, the stablecoin market contains a total market capitalization of over $120b and over 100 projects (# Llama).

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 identi ed in stablecoin research is the lack of widely accepted de nitions for stablecoins. Existing literature often lacks clarity in de ning what precisely constitutes a stablecoin. While some review articles discuss various implementation approaches, they do not provide a de nitive core de nition. Many papers focus on highlighting the desired characteristics and advantages of an ideal stablecoin, without delving into a concrete de nition. Only a few studies examine stablecoin de nitions from a legislative perspective or attempt to model speci c 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 (# De Llama). 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 bene t.

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 ash loans within DEXs. Both ash loans and ash 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 (# De Llama).

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 speci c 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 nancial 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 (# De Llama), research on DeFi derivatives is limited, with only a few available papers. Empirical research in this eld is almost non-existent, and most review articles focus on discussing the feasibility of DeFi derivatives. They emphasize the bene ts compared

Table 1: DeFi Construction and Classi cation

	Project	Type	Feature: Trust Model	Connected Chains	Centralization	Anonymous	Tokenization	Technique	Property: Stability	Scalability	Complexity
Digital Assets	Bitcoin [29]	Native Crypocurrency	-	One	-	M.	-	BC	-	-	-
	Ethereum [30]		-	One	-	M.	-	BC	-	-	-
	Litecoin		-	One	-	M.	-	BC	-	-	-
	Monero [96]		-	One	-	H.	-	Ring-sig, Stealth Address	-	-	-
	Zcash [97]		-	One	-	H.	-	zk-Snark, Multi-sig	-	-	-
	ERC-20 [98]	Token Standard	-	One	Up to Apps	M.	-	SC	-	-	-
Wallets	Ledger [42]	Cold Wallet	-	Multiple	-	M.	-	TEE	-	-	-
	Trezor [43]		-	Multiple	-	H.	-	Multi-sig, 2FA	-	-	-
	Metamask [99]	Hot Wallet	-	Multiple	-	H.	-	Of ine Storage	-	-	-
	Zengo [100]		TTP	Multiple	-	M.	-	MPC-TSS, 3FA	-	-	-
	Argent [101]		TTP	Multiple	-	H.	-	Multi-sig, 2FA	-	-	-
Oracle	MakerDao [46]	Alliance Oracle, Stablecoin	TTP	One	DAO	M.	Dai, MKR	Allowlist	H.	M.	L.
	Chainlink [49]	Off-chain Input	-	Multiple	-	M.	LINK	Reputation, Staking	H.	H.	M.
	NEST [51]	Fact Generation	-	One	-	M.	QP Token	Game Theory	H.	M.	H.
Bridges	Cosmos [53]	BC Engine	TTP	Multiple	Hub	H.	ATOM	IBC	-	H.	L.
	Polkadot [54]		TTP	Multiple	Validator	M.	DOT	Parachain	-	H.	L.
	BTC-relay [55]	Relay	TTP	Two	Mainchain	M.	ETH-BTC	SPV	-	M.	M.
	Polygon Bridge [102]	DApps Based	-	Multiple	-	M.	POL	Lock&Mint	-	-	-
	ThorSwap [58]		-	Multiple(Cosmos)	-	M.	RUNE	Third Party Chains, LP	-	-	-
Stablecoins	Tether [61]	Off-chain Reserve	-	Multiple	Issuer	L.	USDT	-	H.	H.	L.
	Liquity [64]	Over-collateral	-	One	-	M.	LQTY, LUSD	-	M.	M.	M.
	Ampleforth [65]	Algorithmic	-	Multiple	-	M.	AMPL	QTM-based Algorithmic	L.	L.	H.
	Frax Finance [67]		-	One	-	M.	FRAX, FXS	Algorithmic Seigniorage	L.	L.	H.
	Basis [66]		-	One	-	M.	BAC, BAS, BAB	Algorithmic Seigniorage	L.	L.	H.
	Terra [68]		-	One	-	M.	UST, LUNA	Parachain	L.	M.	H.
Lendings	AAVE [12]	Over-collateral	-	Multiple	No	M.	Aave	-	-	-	-
	Compound [11]		-	Multiple	No	M.	COMP	-	-	-	-
	TrueFi [79]	Under-collateral	TTP	One	Staker	M.	TRU	-	-	-	-
	Maple Finance [103]		TTP	One	Pool Delegates	L.	MPL	-	-	-	-
Exchanges	Stellar [104]	On-chain Orderbook	-	Multiple	-	M.	XLM	Manual Matching	-	L.	-
	0x [85]	Off-chain Orderbook	-	Multiple	Orderbook	M.	ZRX	Manual Matching	-	M.	-
	dYdX [10]		-	Multiple(Cosmos)	Orderbook	M.	DYDX	Manual Matching	-	M.	-
	KyberNetwork [89]	Non-orderbook	-	One	-	M.	KNC	Reserve Pool	-	H.	-
	Bancor [91]		-	One	-	M.	BNT	Constant product	-	H.	-
	Uniswap [9]		-	Multiple	-	M.	UNI	Constant mean	-	H.	-
	Balancer [90]		-	One	-	M.	BAL	Dynamic weight	-	H.	-
	Curve Finance [92]		-	One	-	M.	CRV	Hybrid function	-	H.	-
Derivatives	Opium [105]	Option	TTP	One	Orderbook	M.	OPIUM	Off-chain Orderbook	-	-	-
	Opyn [106]		-	One	-	M.	Squeeth	AMM	-	-	-
	Hegic [107]		-	One	-	M.	HEGIC	Peer-to-Pool	-	-	-
	Enzyme [108]	Asset Management	TTP	One	DAO/Manager	M.	MLN	Active Asset Management	-	-	-
	Set [109]		-	One	-	M.	-	Passive Strategy, Social Trading	-	-	-
	Nexus Manual [37]	Insurance	-	One	-	M.	-	Risk Sharing Pool	-	H.	-
	VouchForMe [110]		TTP	One	-	M.	-	Social Network Proof	-	H.	-
	Augur [111]		-	One	-	M.	REP	Prediction Market	-	H.	-
	CDx [112]		-	One	-	M.	CDX, Cred	Tokenized CDS	-	L.	-
	Tokens [106]		-	One	-	M.	oToken	Put Option	-	L.	-
	Augur [111]	Prediction Market	-	One	Staker	M.	REP	Voting	-	-	-
	Omen [113]		-	One	-	M.	OWL	Conditional Tokens	-	-	-

= Does not provide property;
Abbr. : BC = Blockchain; Tx = Transaction; SC = Smart Contracts; QTM = Quantity Theory of Money;
LP = Liquity Pool; IBC = Inter-Blockchain Protocol; CDS = Credit Default Swap; H./M./L. = High/Medium/Low.

to traditional solutions but lack evaluations of implemented solutions. This may be related to the novelty of the eld.

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 signi cant concerns about the security of funds. Insurance is seen as a signi cant 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-

tively scarce. This may be because insurance is a traditional nancial instrument with well-established concepts and applications, while other derivatives such as perpetual contracts are still in relatively early stages of development, involving more technical and compliance challenges.

Option. DeFi options enable the buying or selling of an asset at a predetermined price in the future through decentralized platforms. The process is automated by smart contracts and involves two main participants: the buyer and the seller. DeFi markets offer higher ef ciency and liquidity compared to traditional options trading. These decentralized options protocols cater to investors seeking high-risk, high-leverage cryptocurrencies for speculation, as well as traders looking for hedging and protection against volatile cryptocurrencies.

The work ow of DeFi options trading is similar to traditional options, with two main players facilitated by smart contracts. Various solutions exist based on the matching process, including off-chain order matching models like Opium [105], where orders are handled off-chain and settled on-chain. AMM mechanisms are implemented by Opyn [106], while Hegic adopts liquid sharing pools [107]. DeFi options encompass standardized European options, some non-standard options, and over-the-counter (OTC) options. Deribit [114], OKEx [115], and other exchanges have launched standardized options trading services. MatrixPort [116] offers "watch currency rise" OTC options, while Babel Finance [117] provides a “shark n” capital-protected income management product based on barrier options.

Asset ManagementDeFi asset management combines functions of digital assets, oracles, lending, and more DeFi apps to achieve asset management, portfolio management, and risk management. It allows investors to delegate investment decisions to third parties while maintaining trustless functionality. Smart contracts handle investments, trades, and portfolio adjustments based on investor requirements. DeFi asset management offers low start-up costs, and quick set-up times, and enables anyone to become a fund manager or investor.

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].

Insurance. 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 veri able 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 nancial 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 ef ciency [128], veri ability [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 pro t-sharing for accurate predictions and liquidity rewards. The revenue in prediction markets is directly impacted by event outcomes, making it a signi cant 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 identi ed 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 ood 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 threat [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 pro t.

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 pro t [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 signi cant pro ts. 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 ef ciency improvement to reduce MEV and front-running pro tability [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 pro t 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 pro table opportunities and swiftly submit

(a) Front-running Attack

(b) Sandwich Attack

Figure 5: Front-running and Sandwich Attack

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 con rming speci c 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 pro t.

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 signi cant threat to smart contract security. Attackers exploit this vulnerability by repeatedly executing a speci c contract function and invoking malicious contracts during each execution [151]. The attacker deploys a malicious contract with callable functions into the

target contract and re-invokes it multiple times by calling a function of the target contract. This attack allows unauthorized access to contract funds, modi es 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, modi ers to restrict external contract calls, locking mechanisms, status markers, state variables, and lock ags to track and prevent re-calls of functions.

Over ow. Over ow is common in smart contracts and can result in unexpected money transfers, contract lockouts, or DoS. These vulnerabilities include integer over ow, array over ow, and memory over ow. Attackers exploit integer over ow to alter contract states or transfer funds. Array over ow allows attackers to access other data in a contract's memory, leading to data tampering. Memory over ow can cause contract execution failure. In 2018, attackers exploited an integer over ow 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 over ow 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 signi - cant rewards. Insecure random numbers in functions like key generation compromise encryption algorithms. To prevent misuse, developers should carefully assess the need for random numbers. Veri able 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 con guration 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 con gurations, 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, awed economic models, insuf cient risk management, and inappropriate authorization. Complex algorithms or models may overlook speci c scenarios, impeding proper functionality. Economic models with in ationary, de ationary, or unfair revenue sharing may lead to revenue loss or instability. Insuf cient 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, awed 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 ef ciency but are external to the system.

Oracle Manipulate.Oracle manipulation by hackers involves providing false data to smart contracts, leading to improper bene ts or disruption of normal operations [187]. This manipulation can result in negative consequences, including stablecoin unanchoring, malicious carry trades, forced liquidation,

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

	Affected Layers			Attacks	Incidents: Time	Application	Loss	Solutions	Research Perspective: Technology	Sociology	Economy	Ecology
Technical Security Risk	Infrastructural Layer	Network Communication		Dos (DDoS) [155] [156]	2020/05	Youbi	N/A	[156] [157]	3			
				Eclipse Attack [131] [158]	-	-	-	[159]	3			
				Sybil Attack [132]	Various	Arbitrum	253M ARB	[160]	3			
				51% Attack [133] [161]	2020/04	PegNet	0.6M USD	[162]	3			
		Consensus Algorithm		Fork [163] [139] [27]	-	-	-	[163]	3		3	
			MEV	Front-running Attack [26] [142]	2021/03	DODO	0.7M USD	[143] [144]	3		3	
			MEV	Sandwich Attack [146] [27]	2021/10	Alpha Homora V2	40.93 ETH	[164] [165]	3		3	
			MEV	Arbitrage Attack [166]	2021/01	Saddle Finance	8 BTC	[167]	3		3	
	Protocol Layer	Smart Contract		Reentry [168] [151]	2016/06	The DAO	3.6M ETH	[151]	3			
				Over ow [169] [170]	2018/07	Bancor	1.2M USD	[171] [172]	3			
				Misuse of Random Number [152] [153]	2021/07	AnySwap	8M USD	[172]	3			
		Protocol		Rug Pull [173]	2021/03	Meerkat Finance	20M USD	[174]	3	3		
	Application Layer	Bridge		Double Spend Attack [175]	2020/02	DForce	2.5M USD	[176]	3			
				False Proof Attack [175] [177]	2022/02	Wormhole	1.2M ETH	[177]	3			
				Replay Attack [178]	2022/09	OmniBridge	2M ETHW	[179] [180]	3			
				Inter-Chain Route Hijacking [181]	-	-	-	[182] [180]	3			
				Wormhole Attack [183]	-	-	-	[184]	3			
				Cross-chain Price Manipulation [185]	2023/08	Neutra Finance	23.5 ETH	[185] [186]	3		3	
		Auxiliary Tools		Oracle Manipulation [187] [1] [44]	2023/06	Themis Protocol	0.37M USD	[188]	3		3	
		Usage Method		Phishing Attack [183] [189]	2022/12	Bitkeep	8M USD	[190] [191]	3	3		3
					Real Collapse/Incidents							
Economic Risk	Infrastructural + Protocol + Applicatoin Layers			Liquidity Depletion	2019/09	Compound	-	[192] [193]			3	
				Governance Risk	2022/04	Beanstalk	77M USD	[194] [195]	3	3	3	3
				Market Manipulation	2022/10	Mango	114M USD	[196] [197]	3	3	3	3
				Flashloan	various	various	various	[139] [7]	3		3	
				Death Spiral	2022/05	Luna-UST Collapse	60B USD	[198] [71]			3	
				Ponzi and Fraud	2022/11	FTX Collapse	32B USD	[199]		3	3	3
				CeFi Impact	2023/03	SVB Collapse	23B USD	[200] [201]			3	

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 noti cations 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 uctuations, and market instability. Insuf cient liquidity can result from adverse market conditions, increased risk sentiment, or rapid fund withdrawals. Factors like market uctuations, falling collateral prices, or manipulation can also contribute to liquidity depletion. The Black Thursday event in Mar. 2020, involving MakerDAO, exempli es the consequences of liquidity depletion [204]. To mitigate this risk, DeFi platforms should attract diverse liquidity providers and reduce dependency on speci c 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 ash loans [7, 139]. We observed that such attacks occur frequently and can be categorized into code vulnerabilities, bid arbitrage, and price manipulation. Attackers exploit ash 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 ash loan funds for large-scale trading, in uencing prices. Defending against ash loan attacks requires managing protocol security, auditing contracts, and implementing measures like transaction order restrictions, delays, or time windows.

Market Manipulation. Market manipulation arti cially in uences asset prices to pro t. Illiquid assets pose higher risks to underlying nancial products. Manipulative strategies include spoo ng [206], ramping [207], bear raids, cross-market

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 deppeg 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, ef ciency, 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 eld 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 insuf cient 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. Speci cally, these talents need to possess expertise in areas such as blockchain, network security, code analysis, nancial markets, investment analysis, risk management, and nancial 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 speci c 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

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

6.1 DeFi Technology Construction

Functionality. There are numerous protocols and functionalities in DeFi. Function integration platforms can provide uni ed 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 xes, 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 [134136], 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 ampli er for information security issues and risks, making disaster recovery and emergency response more urgent. Currently, this is a relatively unexplored research eld. 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 traf c 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 nancial ows 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 con dential 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 ef cient privacy coin schemes, including mixing schemes, have also been proposed. These technologies offer improved privacy protection, data security, anonymous transactions, and smart contract veri cation in DeFi. However, how these technologies can adapt to the speci c 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 signi cant 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 nancing for regulators. However, the decentralized and permissionless nature of DeFi con icts with compliance and regulation. For instance, Tornado Cash faced sanctions by the US OFAC for enabling anonymous transfers used in illicit activities. Balancing these con icting 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 ef cient 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 bene ts 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 nd 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.

Figure 6: Open Research Challenges

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 insuf cient 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 classi cation 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

[1] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. SoK: Decentralized nance (DeFi). InACM Conference on Advances in Financial Technologies (AFT), pages 30–46, 2022.

[2] Kaihua Qin, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti, and Arthur Gervais. CeFi vs. DeFi–comparing centralized to decentralized nance. arXiv preprint arXiv:2106.08157, 2021.

[3] Patrick Schueffel. DeFi: Decentralized nance-an introduction and overview. Journal of Innovation Management, 9(3):I–XI, 2021.

[4] Rujia Li, Qin Wang, Qi Wang, and David Galindo. How do smart contracts bene t security protocols? arXiv preprint arXiv:2202.08699, 2022.

[5] Guangsheng Yu et al. Leveraging architectural approaches in Web3 applications-a DAO perspective focused. InIEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 1–6. IEEE, 2023.

[6] Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. Towards understanding ash loan and its applications in DeFi ecosystem. International Workshop on Security in Blockchain and Cloud Computing (SBC@AsiaCCS) 2021.

[7] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. Attacking the DeFi ecosystem with ash loans for fun and pro t. InInternational Conference on Financial Cryptography and Data Security (FC), pages 3–32. Springer, 2021.

[8] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. SoK: Decentralized nance (DeFi) attacks. IEEE Symposium on Security and Privacy (SP), 2023.

[9] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. Tech. rep., Uniswap, Tech. Rep, 2021.

[10] Antonio Juliano. dydx: A standard for decentralized margin trading and derivatives. Retrieved from https://whitepaper.dydx.exchange, 2018.

[11] Compound Labs. Compound nance. Retrieved from https://compound.finance/, 2019.

[12] AAVE. Aave protocol whitepaper v1.0. Retrieved from https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf, 2020.

[13] Convex Finance. Convex. Retrieved from https://www.convexfinance.com/, 2023.

[14] Harvest Finance. Harvest nance document. Retrieved from https://docs.harvest.finance/, 2023.

[15] Lido. Lido docs. Retrieved from https://docs.lido.fi/, 2023.

[16] Rocket Pool. Rocket pool documentation. Retrieved from https://docs.rocketpool.net/guides/, 2023.

[17] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. SoK: A classi cation framework for stablecoin designs. In International Conference on Financial Cryptography and Data Security (FC), pages 174–197. Springer, 2020.

[18] Wenqi Zhao, Hui Li, and Yuming Yuan. Understand volatility of algorithmic stablecoin: Modeling, veri - cation and empirical analysis. International Conference on Financial Cryptography and Data Security Workshop on Decentralized Finance (DeFi@FC), pages 97–108. Springer, 2021.

[19] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente. SoK: Lending pools in decentralized nance. InInternational Conference on Financial Cryptography and Data Security Workshop on Decentralized Finance (DeFi@FC), pages 553–578. Springer, 2021.

[20] Teng Andrea Xu and Jiahua Xu. A short survey on business models of decentralized nance (de) protocols. International Conference on Financial Cryptography and Data Security Workshop on Decentralized Finance (DeFi@FC), 2022.

[21] Rujia Li et al. SoK: TEE-assisted con dential smart contract. Proceedings on Privacy Enhancing Technologies (PETs), 3:1–21, 2022.

[22] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. ACM Computing Surveys (CSUR), 55(11):1–50, 2023.

[23] Yimika Erinle, Yathin Kethepalli, Yebo Feng, and Jiahua Xu. SoK: Design, vulnerabilities and defense of cryptocurrency wallets. arXiv preprint arXiv:2307.12874, 2023.

[24] Kaihua Qin, Liyi Zhou, and Arthur Gervais. Quantifying blockchain extractable value: How dark is the forest? In IEEE Symposium on Security and Privacy (SP), pages 198–214. IEEE, 2022.

[25] Sen Yang, Fan Zhang, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu. SoK: Mev countermeasures: Theory and practice. arXiv preprint arXiv:2212.05111, 2022.

[26] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. SoK: Transparent dishonesty: Front-running attacks on blockchain. In International Conference on Financial Cryptography and Data Security (FC), pages 170–189. Springer, 2020.

[27] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. On the just-in-time discovery of pro t-generating transactions in DeFi protocols. In IEEE Symposium on Security and Privacy (SP), pages 919–936. IEEE, 2021.

[28] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, and Yang Xiang. Exploring unfairness on proof of authority: Order manipulation attacks and remedies. ACM on Asia Conference on Computer and Communications Security (AsiaCCS), pages 123–137, 2022.

[29] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 2008.

[30] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 3(37):2–1, 2014.

[31] Litecoin Wiki contributors. Main page — litecoin wiki. Retrieved from https://litecoin.info/index.php/Main_Page, 2019.

[32] Kurt M Alonso et al. Zero to monero, 2020.

[33] Shi-Feng Sun, Man Ho Au, Joseph K Liu, and Tsz Hon Yuen. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In European Symposium on Research in Computer Security (ESORICS), pages 456–474. Springer, 2017.

[34] Abraham Hinteregger and Bernhard Haslhofer. An empirical analysis of monero cross-chain traceability. International Conference on Financial Cryptography and Data Security (FC), 2019.

[35] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol speci cation. GitHub: San Francisco, CA, USA, 4:220, 2016.

[36] George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. An empirical analysis of anonymity in Zcash. In USENIX security symposium (USENIX Sec), pages 463–477, 2018.

[37] Nexus Mutual. The nexus mutual protocol. Retrieved from https://docs.nexusmutual.io/protocol/, 2020.

[38] ConsenLabs. imtoken. Retrieved from https://github.com/consenlabs, 2023.

[39] Minter Team. Bip wallet. Retrieved from https://github.com/MinterTeam/bip-wallet-web, 2023.

[40] Wetez. Wetez. Retrieved from https://docs.wetez.io/wetez/, 2023.

[41] Trust Wallet. Trust wallet developer documentation. Retrieved from https://developer.trustwallet.com/developer/, 2023.

[42] Ledger. Ledger developer portal. Retrieved from https://developers.ledger.com/, 2023.

[43] Trezor company. Trezor hardware wallet (of cial). Retrieved from https://trezor.io/, 2013.

[44] Torgin Mackinga, Tejaswi Nadahalli, and Roger Wattenhofer. Twap oracle attacks: Easier done than said? In IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 1–8. IEEE, 2022.

[45] Mona Taghavi, Jamal Bentahar, Hadi Otrok, and Kaveh Bakhtiyari. A reinforcement learning model for the reliability of blockchain oracles. Expert Systems with Applications, 214:119160, 2023.

[46] Maker Foundation. The maker protocol: Makerdao's multi-collateral dai (mcd) system. Retrieved from https://makerdao.com/en/whitepaper/, 2023.

[47] Yuxi Cai, Na s Irtija, Eirini Eleni Tsiropoulou, and Andreas Veneris. Truthful decentralized blockchain oracles. International Journal of Network Management, 32(2):e2179, 2022.

[48] Naman Goel, Aris Filos-Ratsikas, and Boi Faltings. Decentralized oracles via peer-prediction in the presence of lying incentives, 2019.

[49] Lorenz Breidenbach, Christian Cachin, Benedict Chan, Alex Coventry, Steve Ellis, Ari Juels, Farinaz Koushanfar, Andrew Miller, Brendan Magauran, Daniel Moroz, et al. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. Chainlink Labs, 1, 2021.

[50] nestprotocol.org. Nest: Decentralized martingale network. Retrieved from https://www.nestprotocol.org/doc/ennestwhitepaper.pdf, 2023.

[51] nestprotocol.org. Nest: Decentralized martingale network. Retrieved from https://www.nestprotocol.org/doc/ennestwhitepaper.pdf, 2023.

[52] Gang Wang et al. Exploring blockchains interoperability: A systematic survey. ACM Computing Surveys (CSUR), 2023.

[53] Jae Kwon and Ethan Buchman. Cosmos whitepaper. A Netw. Distrib. Ledgers, p. 27, 2019.

[54] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. White paper, 21(2327):4662, 2016.

[55] Ethereum and Consensys. Btc-relay. Retrieved from http://btcrelay.org/, 2016.

[56] BTC Relay. Frequently asked questions—btc relay 1.0 documentation. retrieved april 7, 2019, 2016.

[57] Vitalik Buterin. Chain interoperability. R3 research paper, 9:1–25, 2016.

[58] Thorchain. Thorchain whitepapers. Retrieved from https://github.com/thorchain/Resources/tree/master/Whitepapers, 2021.

[59] Bin Wang, Xiaohan Yuan, Li Duan, Hongliang Ma, Chunhua Su, and Wei Wang. De scanner: Spotting DeFi attacks exploiting logic vulnerabilities on blockchain. IEEE Transactions on Computational Social Systems (TCSS), pages 1–12, 2022.

[60] Christian Catalini, Alonso de Gortari, and Nihar Shah. Some simple economics of stablecoins. Annual Review of Financial Economics, p. 14, 2022.

[61] Tether. Tether: Fiat currencies on the Bitcoin blockchain. Retrieved from https://assets.ctfassets.net/vyse88cgwfbl/5UWgHMvz071t2Cq5yTw5vi/c9798ea8db99311bf90ebe0810938b01/TetherWhitePaper.pdf, 2023.

[62] Coinbase. Usdc: The dollar for the digital age. Retrieved from https://www.coinbase.com/usdc, 2023.

[63] Gemini Trust Company. Gemini. Retrieved from https://www.gemini.com/dollar, 2023.

[64] Liquity. Of cial liquity documentation. Retrieved from https://docs.liquity.org/, 2023.

[65] Evan Kuo, Brandon Iles, and Manny Rincon Cruz. Ampleforth: A new synthetic commodity. Ampleforth White Paper, 2019.

[66] Nader Al-Naji, Josh Chen, and Lawrence Diao. Basis: a price-stable cryptocurrency with an algorithmic central bank. Retrieved from https://basis.io/basis_whitepaper_en.pdf, 2017.

[67] Sam Kazemian, Jason Huan, Jonathan Shomroni, and Kedar Iyer. Frax: A fractional-algorithmic stablecoin protocol. In 2022 IEEE International Conference on Blockchain (Blockchain), pages 406–411. IEEE, 2022.

[68] Evan Kereiakes, Marco Di Maggio Do Kwon, and Nicholas Platias. Terra money: Stability and adoption. White Paper, Apr, 2019.

[69] Antonio Briola, David Vidal-Tomás, Yuanrong Wang, and Tomaso Aste. Anatomy of a stablecoin's failure: The terra-luna case. Finance Research Letters, 51:103358, 2023.

[70] Ariah Klages-Mundt and Andreea Minca. (in) stability for the blockchain: Deleveraging spirals and stablecoin attacks, 2021.

[71] Shange Fu et al. Rational ponzi game in algorithmic stablecoin. In IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 1–6. IEEE, 2023.

[72] Matthew Black, Tingwei Liu, and Tony Cai. Atomic loans: Cryptocurrency debt instruments. arXiv preprint arXiv:1901.05117, 2019.

[73] Viet-Bang Pham and Tuan-Dat Trinh. Analysis model for decentralized lending protocols. In International Symposium on Information and Communication Technology (SOICT), pages 405–412, 2022.

[74] Kanis Saengchote. Decentralized lending and its users: Insights from compound. arXiv preprint arXiv:2212.05734, 2022.

[75] Zhipeng Wang, Kaihua Qin, Duc Vu Minh, and Arthur Gervais. Speculative multipliers on DeFi: Quantifying on-chain leverage risks. In International Conference on Financial Cryptography and Data Security (FC), pages 38–56. Springer, 2022.

[76] Wisnu Uriawan, Omar Hasan, Youakim Badr, and Lionel Brunie. Collateral-free trustworthiness-based personal lending on a decentralized application (DApp). In SECRYPT, pages 839–844, 2021.

[77] Yining Xie, Xin Kang, Tieyan Li, Cheng-Kang Chu, and Haiguang Wang. Towards secure and trustworthy ash loans: A blockchain-based trust management approach. In International Conference on Network and System Security (NSS), pages 499–513. Springer, 2022.

[78] Vikas Hassija, Gaurang Bansal, Vinay Chamola, Neeraj Kumar, and Mohsen Guizani. Secure lending: Blockchain and prospect theory-based decentralized credit scoring model. IEEE Transactions on Network Science and Engineering (TNSE), 7(4):2566–2575, 2020.

[79] TrueFi. True docs. Retrieved from https://docs.truefi.io/faq/, 2023.

[80] Michael Elisha. Introducing arcx sapphire (v3). Retrieved from https://arcx.substack.com/p/introducing-arcx-sapphire-v3, 2021.

[81] CreDA. Creda whitepaper: Turn data into wealth. Retrieved from https://creda-app.gitbook.io/creda-protocol/introduction/creda-protocol-whitepaper, 2022.

[82] Andrea Barbon and Angelo Ranaldo. On the quality of cryptocurrency markets: Centralized versus decentralized exchanges. arXiv preprint arXiv:2112.07386, 2021.

[83] Jan Arvid Berg, Robin Fritsch, Lioba Heimbach, and Roger Wattenhofer. An empirical study of market inefficiencies in Uniswap and SushiSwap. arXiv preprint arXiv:2203.07774, 2022.

[84] Lioba Heimbach, Ye Wang, and Roger Wattenhofer. Behavior of liquidity providers in decentralized exchanges. arXiv preprint arXiv:2105.13822, 2021.

[85] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the Ethereum blockchain. Retrieved from https://github.com/0xProject/whitepaper, 2017.

[86] Michael Oved and Don Mosites. Swap: A peer-to-peer protocol for trading Ethereum tokens. Whitepaper Database, 21, 2017.

[87] Aurora Labs. Idex: A real-time and high-throughput Ethereum smart contract exchange. Retrieved from https://static1.squarespace.com/static/5d641c0fc8f92f0001cd9358/t/5d691f20eb666000012a45a7/1567170337906/IDEX-Whitepaper-V0.7.6.pdf, 2019.

[88] StarkEx. Starkex documentation. Retrieved from https://docs.starkware.co/starkex/index.html, 2023.

[89] Yaron Velner Loi Luu and Y Velner. Kybernetwork: A trustless decentralized exchange and payment service. Retrieved from https://home.kyber.network/assets/KyberNetworkWhitepaper.pdf, 2017.

[90] Fernando Martinelli and Nikolai Mushegian. A non-custodial portfolio manager, liquidity provider, and price sensor. Retrieved from https://balancer.finance/whitepaper, 2019.

[91] Eyal Hertzog, Guy Benartzi, and Galia Benartzi. Bancor protocol: Continuous liquidity for cryptographic tokens through their smart contracts. Available online: https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf, 2017.

[92] Michael Egorov and Curve Finance. Automatic market-making with dynamic peg, 2021.

[93] Vijay Mohan. Automated market makers and decentralized exchanges: a DeFi primer. Financial Innovation, 8(1):20, 2022.

[94] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. ACM Conference on Advances in Financial Technologies (AFT), pages 80–91, 2020.

[95] Michael Egorov. Stableswap-ef cient mechanism for stablecoin liquidity. Retrieved Feb, 24:2021, 2019.

[96] The Monero Project. Moneropedia. Retrived from https://www.getmonero.org/resources/moneropedia/, 2014.

[97] Electric Coin Company. Zcash. Retrieved from https://z.cash/learn/, 2016.

[98] Fabian Vogelsteller and Vitalik Buterin. Erc-20: Token standard. Retrieved from https://eips.ethereum.org/EIPS/eip-20, 2015.

[99] MetaMask. The crypto wallet for de , Web3 dapps and nfts. Retrieved from https://metamask.io/, 2016.

[100] Ouriel Ohayon. Zengo: What is zengo recovery kit? Retrieved from https://help.zengo.com/en/articles/2603673-what-is-zengo-recovery-kit, 2018.

[101] argentlabs. Argent smart wallet speci cation. Retrieved from https://github.com/argentlabs/argent-contracts/blob/develop/specifications/specifications.pdf, 2021.

[102] Polygon Bridge. Matic whitepaper. Retrieved from https://github.com/maticnetwork/whitepaper/, 2020.

[103] Maple Labs. Maple nance. Retrieved from https://maplefinance.gitbook.io/maple/, 2023.

[104] Stellar. Liquidity on stellar: Sdex and liquidity pools. Retrieved from https://developers.stellar.org/docs/encyclopedia/liquidity-on-stellar-sdex-liquidity-pools#sdex , 2023.

[105] Opium Team. Opium protocol whitepaper. Retrieved from https://github.com/OpiumProtocol/opium-contracts/blob/master/docs/opium_whitepaper.pdf , 2020.

[106] Zubin Koticha. Building a generalized liquid options protocol in DeFi.Opyn, 2019.

[107] Molly Wintermute. Hegic: On-chain options trading protocol on Ethereum powered by hedge contracts and liquidity pools. Technical report, Tech. Rep., 2020.[Online]. Available: https://github.com/hegic/whitepaper~âÆe, 2020.

[108] Enzyme Finance. Enzyme user docs(v4). Retrieved from https://docs.enzyme.finance/ , 2023.

[109] F Feng and B Weickmann. Set: A protocol for baskets of tokenized assets, 2019.

[110] Insurepal. Vouvhforme(insurepal) whitepaper. Retrieved from http://vouchforme.co/VouchForMe_whitepaper_2018.pdf , 2018.

[111] Jack Peterson, Joseph Krug, Micah Zoltu, Austin K Williams, and Stephanie Alexander. Augur: a decentralized oracle and prediction market platform. arXiv preprint arXiv:1501.01042, 2015.

[112] CDx. Cdx whitepaper. Retrieved from https://cdxproject.com/assets/resources/whitepaper.pdf , 2018.

[113] Omen. Omen. Retrieved from https://omen.eth.link/ , 2020.

[114] Deribit Insights. The best information for crypto derivatives trading. Retrieved from https://insights.deribit.com/ , 2021.

[115] OKX Team. Okx exchange. Retrieved from https://wp.whitepaper.io/okx/ , 2022.

[116] Matrixport Technologies. Matrixport: All-in-one crypto nancial services platform. Retrieved from https://matrixport.com/ , 2021.

[117] Babel Finance. Babel business and solutions. Retrieved from https://babel.finance/solutions.html , 2021.

[118] Babylon Finance. Babylon litepaper. Retrieved from https://docs.babylon.finance/protocol/litepaper , 2022.

[119] Index Coop. The de nitive guide to earning yield on digital assets. Retrieved from https://indexcoop.com/whitepapers/the-definitive-guide-to-earning-yield-on-digital-assets , 2020.

[120] Sunlabs. Sw dao. Retrieved from https://www.suninvest.com/ , 2020.

[121] Kava. DeFi for crypto: Leverage assets with kava's cross-chain cdp platform. Retrieved from https://api-new.whitepaper.io/documents/pdf?id=Sk_Ny2S9v, 2022.

[122] Daoventures. Daoventures whitepaper. Retrieved from https://daoventures.gitbook.io/daoventures/ , 2022.

[123] Simon Cousaert, Nikhil Vadgama, and Jiahua Xu. Token-based insurance solutions on blockchain. In Blockchains and the Token Economy: Theory and Practice, pages 237–260. Springer, 2022.

[124] Fabrizio Lamberti, Valentina Gatteschi, Claudio Demartini, Matteo Pelissier, Alfonso Gomez, and Victor Santamaria. Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage. IEEE Consumer Electronics Magazine, 7(4):72–81, 2018.

[125] Andrew W Singer. Can blockchain improve insurance? Risk Management, 66(1):20–25, 2019.

[126] Mayank Raikwar, Subhra Mazumdar, Sushmita Ruj, Sourav Sen Gupta, Anupam Chattopadhyay, and Kwok-Yan Lam. A blockchain framework for insurance processes. In IFIP International Conference on New Technologies, Mobility and Security (NTMS), pages 1–4. IEEE, 2018.

[127] Tancrede Lepoint, Gabriela Ciocarlie, and Karim Eldefrawy. Blockcis—a blockchain-based cyber insurance system. In IEEE International Conference on Cloud Engineering (IC2E), pages 378–384. IEEE, 2018.

[128] K Sayegh and M Desoky. Blockchain application in insurance and reinsurance. france: Skema business school. Work in Progress paper, 2019.

[129] Guoming Zhang, Xuyun Zhang, Muhammad Bilal, Wanchun Dou, Xiaolong Xu, and Joel JPC Rodrigues. Identifying fraud in medical insurance based on blockchain and deep learning. Future Generation Computer Systems (FGCS), 130:140–154, 2022.

[130] Chin-Ling Chen, Yong-Yuan Deng, Woei-Jiunn Tsaur, Chun-Ta Li, Cheng-Chi Lee, and Chih-Ming Wu. A traceable online insurance claims system based on blockchain and smart contract technology. Sustainability, 13(16):9386, 2021.

[131] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on Bitcoin's peer-to-peer network. In 24th USENIX security symposium (USENIX Sec), pages 129–144, 2015.

[132] John R. Douceur. The sybil attack. In Peer-to-Peer Systems, pages 251–260, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[133] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and David Mohaisen. Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials (COMST), 22(3):1977–2008, 2020.

[134] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M Wing. Automated generation and analysis of attack graphs. In IEEE Symposium on Security and Privacy (SP), pages 273–284. IEEE, 2002.

[135] Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Toward measuring network security using attack graphs. In ACM workshop on Quality of Protection (QoP@CCS), pages 49–54, 2007.

[136] M Asif Khan and Mureed Hussain. Cyber security quanti cation model. In International Conference on Security of Information and Networks (SIN), pages 142–148, 2010.

[137] Daniel Perez and Benjamin Livshits. Smart contract vulnerabilities: Vulnerable does not imply exploited. In USENIX Security Symposium (USENIX Sec), pages 1325–1341, 2021.

[138] Xinrui Zhang, Rujia Li, et al. Time-manipulation attack: Breaking fairness against proof of authority aura. In Proceedings of the ACM Web Conference (WWW), pages 2076–2086, 2023.

[139] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In IEEE Symposium on Security and Privacy (SP), pages 910–927. IEEE, 2020.

[140] Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng, and Roger Wattenhofer. Cyclic arbitrage in decentralized exchanges. In Companion Proceedings of the Web Conference (WWW), pages 12–19, 2022.

[141] Rujia Li, Xuanwei Hu, et al. Transaction fairness in blockchains, revisited. Cryptology ePrint Archive, 2023.

[142] Christof Ferreira Torres, Ramiro Camino, et al. Frontrunner jones and the raiders of the dark forest: An empirical study of frontrunning on the Ethereum blockchain. In USENIX Security Symposium (USENIX Sec), pages 1343–1359, 2021.

[143] Peyman Momeni, Sergey Gorbunov, and Bohan Zhang. Fairblock: Preventing blockchain front-running with minimal overheads. In International Conference on Security and Privacy in Communication Systems (SecureComm), pages 250–271. Springer, 2022.

[144] Xinrui Zhang et al. Frontrunning block attack in PoA Clique: A case study. In IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 1–3. IEEE, 2022.

[145] Ben Weintraub, Christof Ferreira Torres, Cristina Nita-Rotaru, and Radu State. A flash (bot) in the pan: measuring maximal extractable value in private pools. In Proceedings of the 22nd ACM Internet Measurement Conference, pages 458–471, 2022.

[146] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. Impact and user perception of sandwich attacks in the DeFi ecosystem. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI), pages 1–15, 2022.

[147] Purathani Praitheeshan, Lei Pan, Jiangshan Yu, Joseph Liu, and Robin Doss. Security analysis methods on Ethereum smart contract vulnerabilities: a survey. arXiv preprint arXiv:1908.08605, 2019.

[148] Zhiyuan Wan, Xin Xia, David Lo, Jiachi Chen, Xiapu Luo, and Xiaohu Yang. Smart contract security: A practitioners' perspective. In IEEE/ACM International Conference on Software Engineering (ICSE), pages 1410–1422. IEEE, 2021.

[149] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. A survey on Ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys (CSUR), 53(3):1–43, 2020.

[150] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on Ethereum smart contracts (SoK). In International Conference on Principles of Security and Trust (POST), pages 164–186. Springer, 2017.

[151] Zexu Wang, Bin Wen, Ziqiang Luo, and Shaojie Liu. MAR: A dynamic symbol execution detection method for smart contract reentry vulnerability. In International Conference on Blockchain and Trustworthy Systems (BlockSys), pages 418–429. Springer, 2021.

[152] Daojing He, Zhi Deng, Yuxing Zhang, Sammy Chan, Yao Cheng, and Nadra Guizani. Smart contract vulnerability analysis and security audit. IEEE Network, 34(5):276–282, 2020.

[153] Sunbeom So, Seongjoon Hong, and Hakjoo Oh. Smartest: Effectively hunting vulnerable transaction sequences in smart contracts through language model-guided symbolic execution. In USENIX Security Symposium (USENIX Sec), pages 1361–1378, 2021.

[154] Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. Txspector: Uncovering attacks in Ethereum from transactions. In USENIX Security Symposium (USENIX Sec), 2020.

[155] Michael Mirkin, Yan Ji, Jonathan Pang, Ariah Klages-Mundt, Ittay Eyal, and Ari Juels. Bdos: Blockchain denial-of-service. In ACM SIGSAC conference on Computer and Communications Security (CCS), pages 601–619, 2020.

[156] Rajasekhar Chaganti, Rajendra V. Boppana, Vinayakumar Ravi, Kashif Munir, Mubarak Almutairi, Furqan Rustam, Ernesto Lee, and Imran Ashraf. A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. IEEE Access, 10:96538–96555, 2022.

[157] Mayank Raikwar and Danilo Gligoroski. Dos attacks on blockchain ecosystem. In Euro-Par 2021: Parallel Processing Workshops, pages 230–242. Springer International Publishing, 2022.

[158] Karl Wüst and Arthur Gervais. Ethereum eclipse attacks. Technical report, ETH Zurich, 2016.

[159] Yuval Marcus, Ethan Heilman, and Sharon Goldberg. Low-resource eclipse attacks on Ethereum's peer-to-peer network. Cryptology ePrint Archive, 2018.

[160] Bulat Nasrulin, Georgy Ishmaev, and Johan Pouwelse. Meritrank: Sybil tolerant reputation for merit-based tokenomics. In Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pages 95–102. IEEE, 2022.

[161] Daniel J Moroz, Daniel J Aronoff, Neha Narula, and David C Parkes. Double-spend counterattacks: Threat of retaliation in proof-of-work systems. arXiv preprint arXiv:2002.10736, 2020.

[162] Martijn Bastiaan. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in Bitcoin. In Availab le at https://fmt.ewi.utwente.nl /media/175.pdf , 2015.

[163] Kaihua Qin, Liyi Zhou, and Arthur Gervais. Quantifying blockchain extractable value: How dark is the forest? In IEEE Symposium on Security and Privacy (SP), pages 198–214, 2022.

[164] Patrick Züst, Tejaswi Nadahalli, and Ye Wang Roger Wattenhofer. Analyzing and preventing sandwich attacks in Ethereum. ETH Zürich, 2021.

[165] Lioba Heimbach and Roger Wattenhofer. Eliminating sandwich attacks with the help of game theory. ACM on Asia Conference on Computer and Communications Security (AsiaCCS), pages 153–167, 2022.

[166] Yuheng Wang, Jiliang Li, Zhou Su, and Yuyi Wang. Arbitrage attack: Miners of the world, unite! In International Conference on Financial Cryptography and Data Security (FC), pages 464–487. Springer, 2022.

[167] Kushal Babel, Philip Daian, Mahimna Kelkar, and Ari Juels. Clockwork nance: Automated analysis of economic security in smart contracts. In IEEE Symposium on Security and Privacy (SP), pages 2499–2516. IEEE, 2023.

[168] Baptiste Pretre. Attacks on peer-to-peer networks. Dept. of Computer Science Swiss Federal Institute of Technology (ETH) Zurich Autum, 2005.

[169] Wenkai Li, Jiuyang Bu, Xiaoqi Li, Hongli Peng, Yuanzheng Niu, and Yuqing Zhang. A survey of DeFi security: Challenges and opportunities. arXiv preprint arXiv:2206.11821, 2022.

[170] Kris Oosthoek. Flash crash for cash: Cyber threats in decentralized nance. arXiv preprint arXiv:2106.10740, 2021.

[171] Jianjun Huang, Songming Han, Wei You, Wenchang Shi, Bin Liang, Jingzheng Wu, and Yanjun Wu. Hunting vulnerable smart contracts via graph embedding based bytecode matching. IEEE Transactions on Information Forensics and Security (TIFS), 16:2144–2156, 2021.

[172] Zhipeng Gao, Vinoj Jayasundara, Lingxiao Jiang, Xin Xia, David Lo, and John Grundy. Smartembed: A tool for clone and bug detection in smart contracts through structural code embedding. In IEEE International Conference on Software Maintenance and Evolution (ICSME), pages 394–397. IEEE, 2019.

[173] Saulo Dos Santos, Japjeet Singh, Ruppa K Thulasiram, Shahin Kamali, Louis Sirico, and Lisa Loud. A new era of blockchain-powered decentralized nance (DeFi)-a review. In IEEE Annual Computers, Software, and Applications Conference (COMPSAC), pages 1286–1292. IEEE, 2022.

[174] Bruno Mazorra, Victor Adan, and Vanesa Daza. Do not rug on me: Leveraging machine learning techniques for automated scam detection. Mathematics, 10(6):949, 2022.

[175] Sung-Shine Lee, Alexandr Murashkin, Martin Derka, and Jan Gorzny. SoK: Not quite water under the bridge: Review of cross-chain bridge hacks. In IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 1–14. IEEE, 2023.

[176] Kuheli Sai and David Tipper. Disincentivizing double spend attacks across interoperable blockchains. In First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pages 36–45. IEEE, 2019.

[177] Maurice Herlihy, Barbara Liskov, and Liuba Shrira. Cross-chain deals and adversarial commerce. arXiv preprint arXiv:1905.09743, 2019.

[178] Alberto Sonnino, Shehar Bano, Mustafa Al-Bassam, and George Danezis. Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers. In IEEE European Symposium on Security and Privacy (EuroSP), pages 294–308. IEEE, 2020.

[179] Panpan Han, Zheng Yan, Wenxiu Ding, Shufan Fei, and Zhiguo Wan. A survey on cross-chain technologies. Distributed Ledger Technologies: Research and Practice, 2(2):1–30, 2023.

[180] Li Duan, Yangyang Sun, Wei Ni, Weiping Ding, Jiqiang Liu, and Wei Wang. Attacks against cross-chain systems and defense approaches: A contemporary survey. IEEE/CAA Journal of Automatica Sinica, 10(8):1647–1667, 2023.

[181] Maqsood Ahamed Abdul Careem and Aveek Dutta. Reputation based routing in manet using blockchain. In International Conference on COMmunication Systems & NETworkS (COMSNETS), pages 1–6. IEEE, 2020.

[182] Zhuo Lv, Di Wu, Wen Yang, and Li Duan. Attack and protection schemes on fabric isomorphic crosschain systems. International Journal of Distributed Sensor Networks, 18(1):15501477211059945, 2022.

[183] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability. Cryptology ePrint Archive, 2018.

[184] Yangyang Sun, Longyang Yi, Li Duan, and Wei Wang. A decentralized cross-chain service protocol based on notary schemes and hash-locking. In IEEE International Conference on Services Computing (SCC), pages 152–157. IEEE, 2022.

[185] Christopher G Harris. Cross-chain technologies: Challenges and opportunities for blockchain interoperability. In 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), pages 1–6. IEEE, 2023.

[186] Siwei Wu, Dabao Wang, Jianting He, Yajin Zhou, Lei Wu, Xingliang Yuan, Qinming He, and Kui Ren. De - Ranger: Detecting price manipulation attacks on DeFi applications. arXiv preprint arXiv:2104.15068, 2021.

[187] Liya Su, Xinyue Shen, Xiangyu Du, Xiaojing Liao, XiaoFeng Wang, Luyi Xing, and Baoxu Liu. Evil under the sun: Understanding and discovering attacks on Ethereum decentralized applications. In USENIX Security Symposium (USENIX Sec), pages 1307–1324, 2021.

[188] Shayan Eskandari, Mehdi Salehi, Wanyun Catherine Gu, and Jeremy Clark. SoK: Oracles from the ground truth to market manipulation. In ACM Conference on Advances in Financial Technologies (AFT), pages 127–141, 2021.

[189] Philipp Winter, Anna Harbluk Lorimer, Peter Snyder, and Benjamin Livshits. What's in your wallet? privacy and security issues in web 3. arXiv preprint arXiv:2109.06836, 2021.

[190] Shucheng Li, Fengyuan Xu, Runchuan Wang, and Sheng Zhong. Self-supervised incremental deep graph learning for Ethereum phishing scam detection. arXiv preprint arXiv:2106.10176, 2021.

[191] Jinhuan Wang, Pengtao Chen, Xinyao Xu, Jiajing Wu, Meng Shen, Qi Xuan, and Xiaoniu Yang. Tsgn: Transaction subgraph networks assisting phishing detection in Ethereum. arXiv preprint arXiv:2208.12938, 2022.

[192] alethio. Illiquidity and bank run risk in de . Retrieved from https://medium.com/alethio/overlooked-risk-illiquidity-and-bank-runs-on-compound-finance-5d6fc3922d0d , 2019.

[193] Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf. De risks and the decentralisation illusion. BIS Quarterly Review, 2021.

[194] Beanstalk Farms. Beanstalk governance exploit. Retrieved from https://bean.money/blog/beanstalk-governance-exploit , 2022.

[195] Brian Sanya Mondoh, Sara M Johnson, Matthew Green, and Aris Georgopoulos. Decentralised autonomous organisations: The future of corporate governance or an illusion? Aris (Aristeidis), Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion, 2022.

[196] Nathan Reiff. Cryptocurrency spoofing: How it works, protecting yourself. Retrieved from https://www.investopedia.com/tech/what-cryptocurrency-spoofing/, 2021.

[197] Raphael Auer, Jon Frost, and Jose María Vidal Pastor. Miners as intermediaries: extractable value and market manipulation in crypto and defi. Technical report, Bank for International Settlements, 2022.

[198] David S Kerr, Karen A Loveland, Katherine Taken Smith, and Lawrence Murphy Smith. Cryptocurrency risks, fraud cases, and financial performance. Risks, 11(3):51, 2023.

[199] Shange Fu, Qin Wang, Jiangshan Yu, and Shiping Chen. FTX collapse: a Ponzi story. arXiv preprint arXiv:2212.09436, 2022.

[200] Imran Yousaf, Yasir Riaz, and John W Goodell. The impact of the SVB collapse on global financial markets: Substantial but narrow. Finance Research Letters, page 103948, 2023.

[201] Qin Wang, Guangsheng Yu, and Shiping Chen. Cryptocurrency in the aftermath: Unveiling the impact of the SVB collapse. HAL-04216338, 2023.

[202] CoinGeco. Coingecko yield farming survey 2020. Retrieved from https://www.coingecko.com/, 2020.

[203] Fabian Schär. Decentralized finance: On blockchain- and smart contract-based financial markets. FRB of St. Louis Review, 2021.

[204] Qin Wang, Guangsheng Yu, Yilin Sai, Caijun Sun, Lam Duc Nguyen, Sherry Xu, and Shiping Chen. An empirical study on Snapshot DAOs. arXiv preprint arXiv:2211.15993, 2022.

[205] Lioba Heimbach, Eric Schertenleib, and Roger Wattenhofer. Risks and returns of Uniswap v3 liquidity providers. ACM Conference on Advances in Financial Technologies (AFT), 2022.

[206] Federico Cernera, Massimo La Morgia, Alessandro Mei, and Francesco Sassi. Token spammers, rug pulls, and sniperbots: An analysis of the ecosystem of tokens in Ethereum and the Binance smart chain (BNB). USENIX Security Symposium (USENIX Sec), 2023.

[207] Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency Pump-and-Dump scheme. USENIX Security Symposium (USENIX Sec), pages 1609–1625, 2019.

[208] Zhipeng Wang, Xihan Xiong, and William J Knottenbelt. Blockchain transaction censorship: (in) secure and (in) efficient? Cryptology ePrint Archive, 2023.

[209] Anton Wahrstätter, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz, et al. Blockchain censorship. arXiv preprint arXiv:2305.18545, 2023.

[210] Bogdan Florin Cornea, Julien Bourgeois, The Tung Nguyen, and Didier El-Baz. Scalable performance predictions of distributed peer-to-peer applications. In IEEE International Conference on High Performance Computing and Communication & IEEE International Conference on Embedded Software and Systems, pages 193–201, 2012.

[211] Shuai Yang and Wei Cui. An evaluation system for defi lending protocols. In 2023 42nd Chinese Control Conference (CCC), pages 8888–8893, 2023.

[212] Mengqi Hao and Jingzhi Ding. Decision-making and impact of blockchain on accounts receivable financing. In LISS 2021, pages 465–477, Singapore, 2022. Springer Nature Singapore.

[213] Lohith J. J, Anusree Manoj K, Guru Nanma P, and Pooja Srinivasan. Tp-detect: trigram-pixel based vulnerability detection for ethereum smart contracts. Multimedia Tools and Applications, 82(23):36379–36393, 2023.

[214] Lejun Zhang, Yuan Li, Ran Guo, Guopeng Wang, Jing Qiu, Shen Su, Yuan Liu, Guangxia Xu, Huiling Chen, and Zhihong Tian. A novel smart contract reentrancy vulnerability detection model based on bigan. Journal of Signal Processing Systems, 2023.

[215] Chuang Ma, Shuaiwu Liu, and Guangxia Xu. Hgat: smart contract vulnerability detection method based on hierarchical graph attention network. Journal of Cloud Computing, 12(1):93, 2023.

[216] Ke Ye, Meng Shen, Zhenbo Gao, and Liehuang Zhu. Real-time detection of cryptocurrency mining behavior. In Blockchain and Trustworthy Systems, pages 278–291, Singapore, 2022. Springer Nature Singapore.

[217] P. Mercy Praise, S. Basil Xavier, Anoop Jose, G. Jaspher W. Kathrine, and J. Andrew. Variants of cryptojacking attacks and their detection techniques. Applications and Techniques in Information Security, pages 71–87, Singapore, 2023. Springer Nature Singapore.

[218] 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

detection. In Algorithms and Architectures for Parallel Processing, pages 494–508, Cham, 2022. Springer International Publishing.

[219] Oleksandr Letychevskyi, Volodymyr Peschanenko, Maksym Poltoratskyi, and Yuliia Tarasich. Our approach to formal veri cation of token economy models. In Information and Communication Technologies in Education, Research, and Industrial Applications, pages 348–363, Cham, 2020. Springer International Publishing.

[220] Li Zhihong and Zhang Jie. Online knowledge community governance based on blockchain token incentives. In Knowledge and Systems Sciences, pages 64–72, Singapore, 2019. Springer Singapore.

[221] Philipp Lesche, Philipp Sandner, and Horst Treiblmaier. Implications of the Token Economy: A Taxonomy and Research Agenda, pages 1–30. Springer International Publishing, Cham, 2022.

[222] Liu B., Zhou J., and Z. Lim Y. Being accountable never cheats: An incentive protocol for DeFi oracles. In IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), pages 1–10, 2022.

[223] Chenquan Gan, Akanksha Saini, Qingyi Zhu, Yong Xiang, and Zufan Zhang. Blockchain-based access control scheme with incentive mechanism for ehealth systems: patient as supervisor. Multimedia Tools and Applications, 80(20):30605–30621, 2021.

[224] Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Ga i, Sarah Meiklejohn, and Edgar Weippl. Sok: Algorithmic incentive manipulation attacks on permissionless PoW cryptocurrencies. In Financial Cryptography and Data Security Workshops, pages 507–532, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg.

[225] Zhiyu Xu, Minfeng Qi, Ziyuan Wang, Sheng Wen, Shiping Chen, and Yang Xiang. Ib2p: An image-based privacy-preserving blockchain model for nancial services. In 2021 IEEE International Conference on Blockchain (Blockchain), pages 552–558, 2021.

[226] Janka Hartmann and Omar Hasan. Privacy considerations for a decentralized nance (de) loans platform. Cluster Computing, 26(4):2147–2161, 2023.

[227] Stéphane Blemus. The compatibility of cbdcs with "de " protocols: A governance rather than a technological issue to comply with nancial crime regulations. In Financial Cryptography and Data Security Workshops, pages 97–105, Cham, 2023. Springer International Publishing.

[228] Ryosuke Ushida and James Angel. Regulatory considerations on centralized aspects of de managed by daos. In Financial Cryptography and Data Security Workshops, pages 21–36, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg.

[229] José Carlos Laguna De Paz. Some implications of the new global digital economy for nancial regulation and supervision. Journal of Banking Regulation, 24(2):146–155, 2023.

[230] Dieter Reichert. How customer communications and interactions become digital assets and critical resources in customer engagement — an interview with dieter reichert, co-founder of censhare ag. Journal of Digital Asset Management, 6(4):232–242, 2010.

[231] Chetan Saiya. Dam in marketing operations and the emergence of customer engagement objects – an interview with chetan saiya, ceo of assetlink. Journal of Digital Asset Management, 6(2):124–129, 2010.

[232] Paul Medeiros and Leonidas Deligiannidis. An educational guide to creating your own cryptocurrency. In Advances in Software Engineering, Education, and e-Learning, pages 163–177, Cham, 2021. Springer International Publishing.

[233] Shi Y., Shahriar H., Lo D., and Chi H. Enhancing blockchain technology education with innovative active learning. In 2022 IEEE 2nd International Conference on Advanced Learning Technologies on Education & Research (ICALTER), pages 1–4, 2022.

[234] Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Buenzli, and Martin Vechev. Securify: Practical security analysis of smart contracts. In Proceedings of the ACM SIGSAC conference on Computer and Communications Security (CCS), pages 67–82, 2018.

[235] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. SoK: Consensus in the age of blockchains. In Proceedings of the ACM Conference on Advances in Financial Technologies (AFT), pages 183–198, 2019.

[236] Zeinab Amin. A practical road map for assessing cyber risk. Journal of Risk Research, 22(1):32–43, 2019.

[237] Daniel W Woods and Rainer Böhme. SoK: Quantifying cyber risk. In IEEE Symposium on Security and Privacy (SP), pages 211–228. IEEE, 2021.

[238] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A stful of bitcoins: characterizing

payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference, pages 127–140, 2013.

[239] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in bitcoin. In International Conference on Financial Cryptography and Data Security, pages 34–51, Berlin, Heidelberg, 2013. Springer, Springer Science & Business Media.

[240] Zhipeng Wang, Stefanos Chaliasos, Kaihua Qin, Liyi Zhou, Lifeng Gao, Pascal Berrang, Benjamin Livshits, and Arthur Gervais. On how zero-knowledge proof blockchain mixers improve, and worsen user privacy. In Proceedings of the ACM Web Conference (WWW) pages 2022–2032, 2023.

[241] Rujia Li et al. An accountable decryption system based on privacy-preserving smart contracts. In International Conference on Information Security (ISC), pages 372–390. Springer, 2020.

[242] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin. In IEEE Symposium on Security and Privacy (SP), pages 397–411. IEEE, 2013.

[243] Jens Groth. On the size of pairing-based non-interactive arguments. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 305–326. Springer, 2016.

[244] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for con dential transactions and more. In IEEE Symposium on Security and Privacy (SP), pages 315–334. IEEE, 2018.

[245] Carsten Baum, James Hsin-yu Chiang, Bernardo David, and Tore Kasper Frederiksen. SoK: Privacy-enhancing technologies in nance. Cryptology ePrint Archive, 2023.

[246] Stuart Haber and W Scott Stornetta. How to time-stamp a digital document. Springer, 1991.

[247] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014):1–32, 2014.

[248] Andrei-Dragoş Popescu. Decentralized nance (DeFi)–the lego of nance. Social Sciences and Education Research Review, 7(1):321–349, 2020.

[249] Tamás Katona. Decentralized nance: The possibilities of a blockchain “money lego” system. Financial and Economic Review, 20(1):74–102, 2021.

[250] Reza Soltani, Uyen Trang Nguyen, and Aijun An. Practical key recovery model for self-sovereign identity based digital wallets. In IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pages 320–325. IEEE, 2019.

[251] Gyeong-Jin Ra, Chang-Hyun Roh, and Im-Yeong Lee. A key recovery system based on password-protected secret sharing in a permissioned blockchain. Computers, Materials & Continua, 65(1):153–170, 2020.

[252] Ali Bagherzandi, Stanislaw Jarecki, Nitesh Saxena, and Yanbin Lu. Password-protected secret sharing. In ACM conference on Computer and Communications Security (CCS), pages 433–444, 2011.

[253] Jan Camenisch, Anja Lehmann, Anna Lysyanskaya, and Gregory Neven. Memento: How to reconstruct your secrets from a single password in a hostile environment. In Annual Cryptology Conference (CRYPTO), pages 256–275. Springer, 2014.

[254] Shuangyu He, Qianhong Wu, Xizhao Luo, Zhi Liang, Dawei Li, Hanwen Feng, Haibin Zheng, and Yanan Li. A social-network-based cryptocurrency wallet-management scheme. IEEE Access, 6:7654–7663, 2018.

[255] Niko Lehto, Kimmo Halunen, Outi-Marja Latvala, Anni Karinsalo, and Jarno Salonen. Cryptovault-a secure hardware wallet for decentralized key management. In 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS), pages 1–4. IEEE, 2021.

[256] Weiqi Dai, Yan Lv, Kim-Kwang Raymond Choo, Zhongze Liu, Deqing Zou, and Hai Jin. Crsa: A cryptocurrency recovery scheme based on hidden assistance relationships. IEEE Transactions on Information Forensics and Security (TIFS), 16:4291–4305, 2021.

[257] Sercan Şahan, Adil Furkan Ekici, and Şerif Bahtiyar. A multi-factor authentication framework for secure access to blockchain. In International Conference on Computer and Technology Applications (ICCTA), pages 160–164, 2019.

[258] E Benli, I Engin, C Giousouf, MA Ulak, and Ş Bahtiyar. Biowallet: a biometric digital wallet. ICONS 2017, page 45, 2017.

[259] Mehmet Aydar, Salih Cemil Cetin, Serkan Ayvaz, and Betul Aygun. Private key encryption and recovery in blockchain. arXiv preprint arXiv:1907.04156, 2019.

[260] A Jagadeesan and K Duraiswamy. Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris. *arXiv preprint arXiv:1003.1458*, 2010.

[261] Teng Hu, Xiaolei Liu, Weina Niu, Kangyi Ding, Yanping Wang, and Xiaosong Zhang. Securing the private key in your blockchain wallet: a continuous authentication approach based on behavioral biometric. In *Journal of Physics: Conference Series*, volume 1631, page 012104. IOP Publishing, 2020.

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 Merkel 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]).

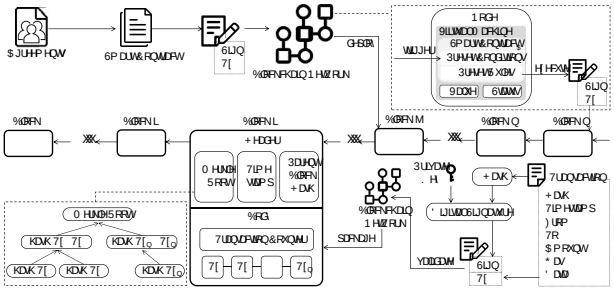

Figure 1: DeFi Foundations

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.

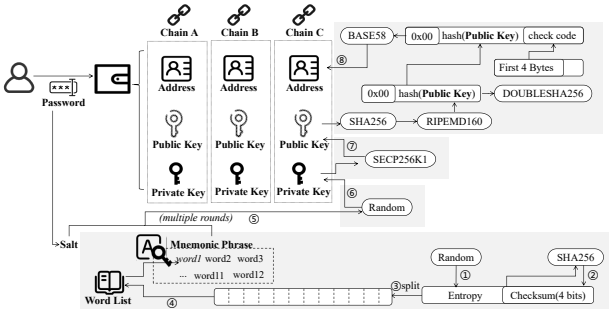

Figure 2: Components of Wallets

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.

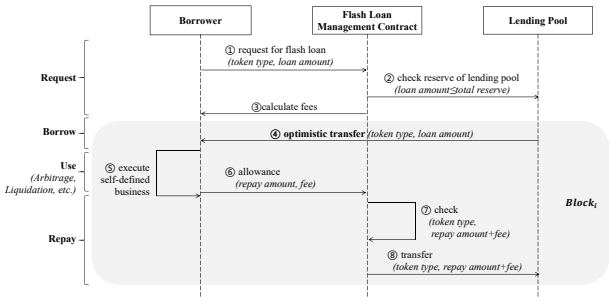

Figure 3: Flash Loan Workflow

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

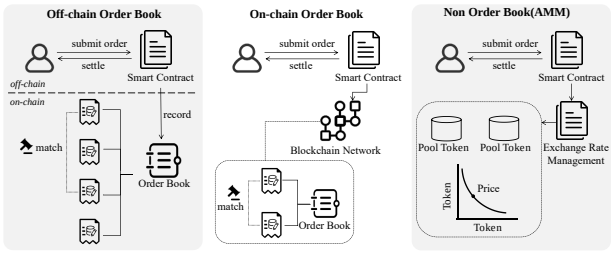

Figure 4: DEX Implementation Models

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.