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*
¶ *CSIRO Data61, 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. Lastly, we point out research directions in DeFi, encompassing areas of technological advancements, innovative economics, and privacy optimization.**

***Index Terms*—DeFi, Blockchain, Security, Economics, DApp**

1. Introduction

With the rise of blockchain, 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 centralize most financial functions, coming with defects such as high costs, cumbersome processes, account opening restrictions (e.g., KYC), lack of transparency, and the risk of data manipulation.
- *Non-human-intervention.* DeFi's trading rules are pre-written, making automation and immutability key features [4] while running on the blockchain that reduces counterparty risk and eliminates the risk of a single point of failure.
- *Maximal avaliability.* Most DeFi products have no downtime, enabling 24/7 financial services to everyone without prior identity verification.
- *Permissionless.* Deployed in a decentralized manner across P2P networks, opens new opportunities for flexible 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].

As of August 2023, the total locked value (TLV)[1] in DeFi markets has reached US$40.257 billion, following a peak value of US$253 billion in December 2021 (also claimed in [7]). This substantial investment has sparked numerous innovations, including decentralized exchanges (DEXs, e.g., Uniswap [8], dYdX [9]), lending (e.g., Compound [10], Aave [11]), yield aggregators (e.g., Convex [12], Harvest [13]), liquid staking (e.g., Lido [14], Rocket Pool [15]), and various other developments [1].

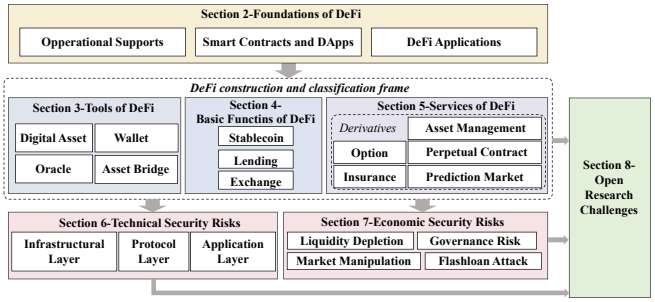

Figure 1: Paper Structure

Previous investigations. We highlight several recent studies that have elegantly reviewed various 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. [16] classified major stablecoin designs, while Zhao et al. [17] specifically explored algorithmic stablecoins. Bartoletti et al. [18] introduced lending protocols using a formal model that describes their transitions as a state machine reflecting user interactions. Xu et al. [19] presented a general business model for a small corpus of DeFi protocols, including protocols for loanable funds, DEXs, and yield aggregators. Cousaer et al. [20] delved into the connotation of yield aggregators, identifying several mainstream yield farming strategies and comparing

1. Data source: https://defillama.com [August 2023].

major 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. [7] 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] [27] [28].

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

- *We purpose a DeFi construction and classification frame based on the complexity of financial services.* The frame (summarized in Table 2) classifies DeFi applications into three categories: tool level (Section 3), basic functionality level (Section 4), and service level (Section 5). We present detailed constructions of DeFi protocols within each category, along with their operational mechanisms.
- *We discuss the security of DeFi applications from two pillars:* technical (Section 6) and economic perspectives (Section 7). 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.
- *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 8) that could lead to enhancements in DeFi.

2. Foundations of DeFi

2.1. Operational Supports

Transactions. The transaction is the smallest unit in the blockchain ledger. It includes sender and receiver addresses, the number of coins involved, a unique hash value (transaction's hash), a timestamp, transaction/gas fee, block information (block ID of the first recording block), and data payloads for execution (cf. Figure 2). 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 2). 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 [29], 2008 [30], and 2014 [31]).

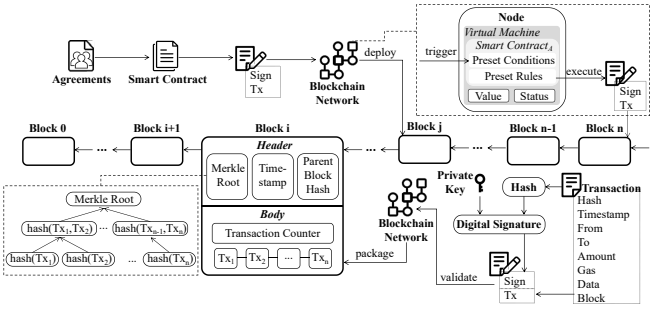

Figure 2: DeFi Foundations

2.2. Smart Contracts and DApps

Smart contracts. Smart contract constitutes a crucial element supporting DeFi protocols. Deployed on-chain, it acts as a computerized transaction protocol that transforms contract terms into executable programs, maintaining logical connections between terms as a flow (see Figure 2). 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 [32]. Smart contracts can be likened to code-based Lego blocks with automatic execution functions [33]. 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.

2.3. DeFi Applications

DeFi applications include *digital assets*, *wallets*, *oracles* and asset *bridges* at the infrastructural level, stablecoins, lending and exchanges at the functional level, and diverse derivatives at the service level. DeFi apps based on the complexity of the financial services are shown in Figure 3, covering all areas of financial services and forming the DeFi ecosystem [1].

3. Tools of DeFi

3.1. Digital Asset

The financial system realizes the flow of funds in monetary and physical forms in traditional finance, which is also

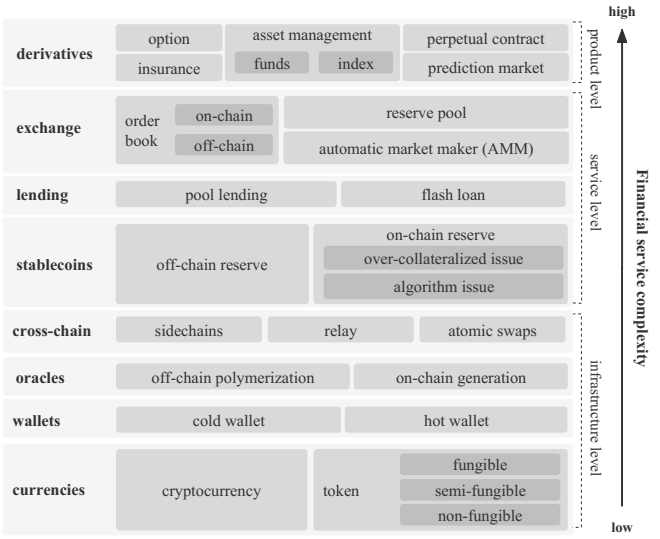

Figure 3: DeFi Ecological Structure

true in DeFi. Digital asset means any form of intangible personal property that can be exclusively possessed from person to person without necessary reliance on an intermediary.

Native cryptocurrency. Native cryptocurrency refers to the primary digital asset of a blockchain, serving various functions within its ecosystem. Being borderless and independent of centralized entities, native cryptocurrencies such as Bitcoin [34] can be stored and transferred with ease. Other prominent examples include Ethereum [35], Litecoin [36], Monero [37] [38] [39], and Zcash [40] [41], all operating on standalone blockchains and incentivized within their respective economies. These cryptocurrencies can be directly transferred on-chain that hosts them and used for paying transaction fees.

Derivative Token. With the most DeFi projects, Ethereum sets diverse token standards [42] (cf. Table 1). These standards are published as Ethereum Improvement Proposals (EIPs), recognized through discussions and voting sessions in Ethereum's open governance. ERC-20 [43] is a widely known token standard, with currencies, voting tokens, and pledge tokens being the primary application scenarios. ERC-20 tokens are fungible, meaning each token is the same, with no difference in value between tokens. They can be infinitely subdivided and interchangeable. Smart contracts can be written to issue ERC-20 tokens with the specified name, symbol, and other features such as transfers.

Various Ethereum token standards have also been designed based on other specific scenarios, such as ERC-721 [44], a non-fungible token standard for artwork, songs, and digital collections, where tokens issued under ERC-721 differ from each other and cannot be subdivided [45]. ERC-1155 [46] is a semi-fungible token standard used in GameFi and copyright to store corroboration and weighting information, where the IDs of each token are non-fungible, but units under the same ID are fungible. ERC-3525 [47] and ERC-3475 [48] support complex financial scenarios, capable of supporting financial assets, instruments, and contracts. To make different standards tokens interoperable, ERC-998 [49], a combined token standard, was designed to map ERC-20 tokens to ERC-721 tokens, achieving compatibility and interoperability between these standards, and providing tools for more complex financial functions.

Beyond Ethereum, several compelling blockchain platforms have introduced their token standards, following similar rules to the ERC standard. Notable examples include BEP-20 and BEP-721 in Binance Smart Chain (BSC), ARC-721 in Avalanche, and BRC-20 in Bitcoin.

Table 1: Comparison between ERC token standard

Standard	Time	Fungibility	Divisibility	Application
ERC-20	2015	Fung.	Divisible	Cryptocurrencies
ERC-721	2017	Non-fung.	Indivisible	Digital collection
ERC-1155	2018	Semi-fung.	Divisible (same ID), indivisible (diff. IDs)	Copyright
ERC-3525	2022	Semi-fung.	Divisible (same ID), divisible (diff. IDs)	Equity
ERC-3475	2022	Semi-fung.	Up to attribute configuration	Equity
BEP-20	2021	Fung.	On BNB Smart Chain, divisible	Cryptocurrencies
BEP-721	2022	Non-fung.	On BNB Smart Chain, indivisible	Digital collection
ARC-721	2022	Non-fung.	On Avalanche, indivisible	Digital collection
BRC-20	2023	Non-fung.	On Bitcoin, indivisible	Digital collection

Native cryptocurrencies and various derivative tokens constitute the money flowing in the DeFi system. Many DeFi applications issue tokens corresponding to the ownership of the assets of the app, which can be traded or held like any other cryptocurrency. Additionally, DeFi app-issued tokens can perform financial functions such as lending [11] [10], staking [14] [15] and insuring [50] [51], and be empowered to participate in governance through voting and other defined conditions. Tokens in physical form represent ownership of real-world assets like real estate, cars, or collectibles.

However, the privacy of these funds is not 100% guaranteed, and as the number of users grows, privacy issues on the blockchain become apparent. Pseudonymity used in public chains can protect users' privacy to a certain extent, but existing analysis techniques can utilize blockchain external information to speculate on the identities of other users, making it difficult to meet privacy needs [52] [53]. Zero-knowledge proof (ZKP) can be applied to enhance blockchain privacy. Initially applied in the ZeroCoin [54], ZKP has been progressively utilized in privacy-preserving for on-chain transactions [38], with zk-SNARK [55] and BulletProofs [56] schemes mostly used in privacy chains [39]. The impact of using ZKP on blockchain speed has been studied, and some researchers have proposed a more plain, simple, and effective scheme, i.e., the mixed-coin scheme. Mixed-coin schemes protect the privacy of users by breaking the linkage between transactions through an intermediary that packages and mixes transactions from multiple users, making it difficult for transaction graph analysis to determine the origin and destination of transfers. Examples of privacy coins built using mixed-coin schemes include CoinJoin [57], TumbleBit [58], Tornado Cash [59], AMR [60], and Mixcoin [61]. For exploring DeFi privacy enhancement technologies, we refer the readers to the relevant SoKs [62].

Due to differences in legal and regulatory frameworks across regions, there is controversy regarding the classification of DeFi tokens as currencies, commodities, or securities. The classification depends on their specific characteristics.

Some DeFi tokens exhibit currency attributes, possessing wide usability and circulation, while others may be classified as securities due to their characteristics of representing ownership, dividends, or investment returns, creating profit expectations among investors. The classification also relies on regulatory standards, which are continuously adjusting given the technical complexity of DeFi.

3.2. Wallet

A wallet is a tool for managing the keys and addresses of blockchain nodes. Wallets serve for interacting with the blockchain instead of storing on-chain assets. Typically, a wallet has three basic functions: recording, receiving, and transferring currencies, and realizing users' basic needs.

In DeFi, a user can manage multiple accounts from a single wallet. Each account has three components: public key, private key, and address, as shown in Figure 4. A cryptographic algorithm generates a pair of one-to-one keys when an account is created on the blockchain. 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.

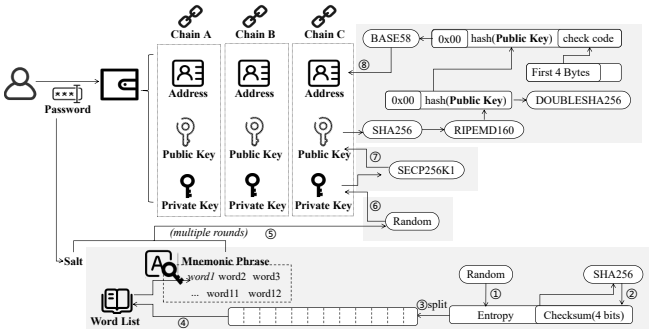

Figure 4: Components of Wallets

A wallet's function to manage assets is the basic need of users. As applications develop, the functions of the wallet are gradually extended to asset custody and other scenarios. Initially, decentralized wallets could only manage a single asset on a single chain and realize a single transfer function. To address the issue of users holding assets on multiple chains and circulating assets on each chain, multi-chain wallets were developed to store and trade multiple digital assets using a single wallet. Multi-chain wallets are more difficult to develop than single-chain wallets since they have to support digital assets on multiple public chains at the same time, as different public chains often adopt different technical solutions. Multi-chain wallets are generally realized by developing interfaces corresponding to different blockchains. Many multi-chain wallets have also developed the "flash exchange" using the "exchange rate" as a medium function to make currency exchange easy and convenient. Software wallets like imToken [63], Bip [64], Wetez [65], TrustWallet [66] and hardware wallets like Ledger [67], Trezor [68] mostly support multiple mainstream ecosystems [28] such as BTC, ETH, EOS.

Security is a crucial factor when using a wallet, covering the procedures of (private-) key preservation and recovery. Cold wallets like paper wallets are physically isolated but have a risk of loss, while hot wallets like MetaMask [69] protect private keys by storing locally and using mnemonics selected from a fixed vocabulary according to the algorithm to help users recover complex private keys. Multi-factor authentication, including biometric [70] [71] [72] [73]and behavioral features [74], can further enhance wallet security during authentication, use and recovery of the wallet. Researchers have studied key recovery based on secret sharing, such as Soltani et al. [75]'s threshold secret sharing cryptography-based backup and recovery protocols which relies on multiple third-party key custodians, Ra et al. [76]'s licensing key recovery systems, Bagherzandi et al. [77]'s secret sharing scheme that stores private keys among multiple servers, Camenisch et al. [78]'s Threshold Password-Authenticated Secret Sharing scheme, Jarecki et al. [79]'s the more efficient PPSS solution and its formalism loosened version [80]. ZenGo [81] wallet implements a recovery solution using both local and server keys. Trusted third-party (TTP) verification is another method for enhancing key recovery security, such as He et al. [82]'s identity-based layered key isolation encryption and Lehto et al. [83]'s wallet recovery method suitable for social networks. Dai et al. [84]'s recovery scheme uses a pre-defined list of assistants, with ZKP to ensure their identity from leaking. Li et al. [85]'s trusted hardware solution provides confidentiality for off-chain wallets. The Argent wallet [86]'s guardian feature uses TTP verification, requiring approval from more than half of the authorized guardians to restore the wallet.

3.3. Oracle

The execution of smart contracts requires meeting conditions specified in the contracts, while also requiring support from external data. Oracle provides external data sources for smart contracts on blockchain, supplying them with data information. The data flow of oracles illustrates in Figure 5. 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.

The accuracy of data is the main concern of oracles [87]. To ensure trustworthy on-chain data, Heiss et al. [88] define key requirements and evaluate existing oracle systems in TLS-based, enclave-based using TEE, and voting-based categories. Williams et al. [89] introduce a design methodology for decentralized oracles that is incentive compatible, while Goel et al. [90] use a peer prediction mechanism to incentivize data providers to provide real data. Cai et al. [91] propose a scoring scheme based on peer-to-peer prediction

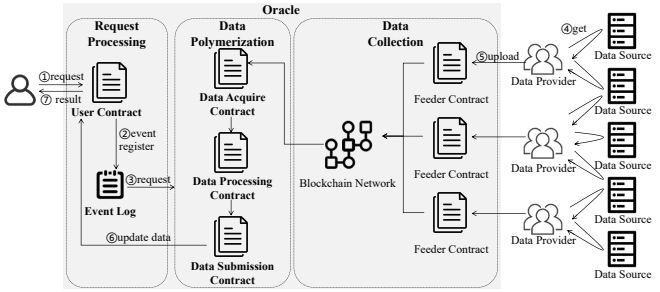

Figure 5: Data Flow of Oracles

and a nonlinear pledge rule for truthful extraction of subjective data. Merlini et al. [92] propose a new pairwise problem oracle that can increase the cost of forcing outcomes and reduce transaction costs. MakerDao [93] proposes a consortium oracle approach, Chainlink [94] introduces a reputation scheme, and NEST [95] [96] implements a game-theoretic approach for price data verification. Taghavi et al. [97] propose a Bayesian Bandit Learning model for Oracles Reliability(BLOR) to identify reliable and cost-effective oracles. These works provide frameworks and approaches for designing and selecting reliable oracles.

3.4. Asset Bridge

Increased heterogeneous blockchains pose a challenge to achieving smooth interoperability in DeFi protocols. Atomic swaps allow the direct exchange of cryptocurrency across blockchains [98]. . In 2012, Ripple introduced the InterLedger protocol (ILP), enabling cross-ledger interactions through third-party notaries. Pegged sidechains were proposed by the Bitcoin Core development team in 2014. Interoperability platforms such as Cosmos [99]and Polkadot [100] 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 [101], a cross-chain solution based on a relay chain, achieved one-way cross-chain connectivity between Ethereum and Bitcoin [102]. Vitalik Buterin [103]'s effort in the same year provided an in-depth analysis of blockchain interoperability issues. Notable cross-chain DeFi projects include Thorswap [104], AnySwap, and Chainswap [105].

4. Basic Functions of DeFi

4.1. Stablecoin

Cryptocurrencies are highly volatile, but stablecoins offer price stability as they are pegged to fiat currencies. The ideal stablecoin possesses low volatility and is widely used in trading, cross-border payments, and lending [106]. 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 (cf. Figure 6).

Off-chain reserved stablecoins, such as USDT [107], USDC [108], and GUSD [109], 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 like Dai [93] and LUSD [110], and algorithmic stablecoins such as AMPL [111], Basis [112], FRAX [113], and UST [114], 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, as demonstrated by Luna-UST collapse in 2022 [115].

To address these challenges, Klages Mundt et al. [116] propose modeling-based approaches to enhance stablecoin design and resilience, ensuring price stability even amidst market shocks and maintaining user confidence. Catalini [117] suggests setting reserve standards for stablecoin issuers, bolstering the security of reserves while fostering financial resilience and encouraging innovation and competition. Fu et al. [118] propose a rational Ponzi model to analyze the sustainability of algorithmic stablecoins.

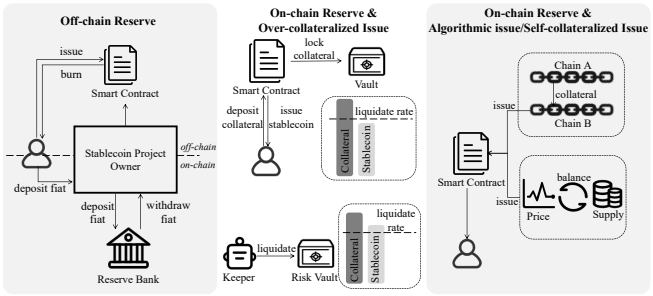

Figure 6: Stablecoins Implementation Models

4.2. Lending

DeFi lending apps abandon the centralized credit assessment framework but rely on recognized collateral for assessment. Additionally, DeFi lending apps pool liquidity, enable low-cost lending and arbitrage, and improve the transferability of debt holdings. Traditional intermediaries are replaced with publicly available smart contracts, reducing intermediation costs and resulting in more efficient use of market liquidity.

Decentralized lending protocols typically involve collateralization, lending, and liquidation (cf. Figure 7). Users provide digital assets as collateral, which are aggregated into a pool that forms a reserve used for redemption [18]. 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 [119]. Liquidation is triggered

when a user's debts exceed the borrowing capacity, and any participant can compete to liquidate debts and earn rewards. Some DeFi lending protocols distribute governance tokens to users to incentivize participation.

Based on such model, projects like Compound [10] and AAVE [11], enable over-collateralized, trust-less DeFi lending. But out of the demand for low/zero collateralization and regulatory requirements for KYC, people have built credit on the blockchain or set the constraints for using the borrowed assets [120] to enable undercollateralized lending. Xie et al. [121] proposed an evaluation model to establish on-chain credit, while Uriawan et al. [122] realized unsecured personal lending based on credit. Hassija et al. [123]'s lending model ensure the safety and reliability of unsecured lending by punishing default. TrueFi [124] combines CeFi and DeFi's on-chain credit rating system into a credit evaluation model managed by its token holders. CreDA [125] can collect data for deep mining across multiple chains, and its Credit Predictor models public history cross-chain data to provide users with a dynamic credit rating.

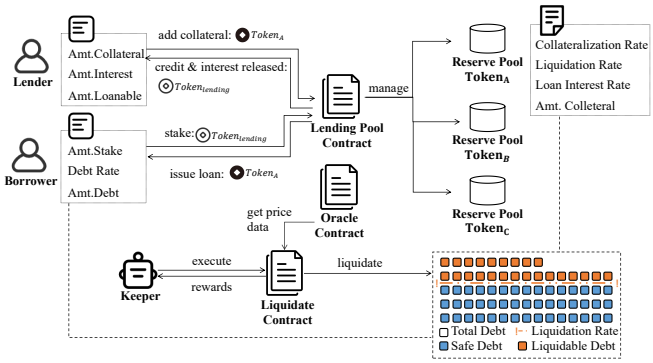

Figure 7: Interaction of Decentralized Lending

Decentralized lending allows borrowers to engage in trading activities such as arbitrage, leverage, and market-making to hedge against volatility, while lenders can earn additional revenue via collateral rates [126]. The primary motivation for users to use DeFi lending protocols is to obtain participation rewards, such as governance tokens. In extreme cases, borrowers can borrow, re-deposit borrowed assets, and re-borrow repeatedly, forming a *borrowing spiral* to maximize rewards available to users [127]. Leveraged trading, common among institutional investors can lead to leverage spirals that maximize the value of appreciating crypto assets [128].

Flash loans are DeFi's innovative non-collateralized lending tool, that leverages the atomicity of blockchain transactions to allow borrowing without collateral, as long as it is repaid in a single transaction. Flash loans have various use cases, such as arbitrage opportunities, collateral swapping, and self-liquidation [6]. Flash swaps provide similar services to flash loans within DEXs, but with the key difference being repayment with either the borrowed or acquired token from the swap. Both flash loans and flash swaps utilize "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 8).

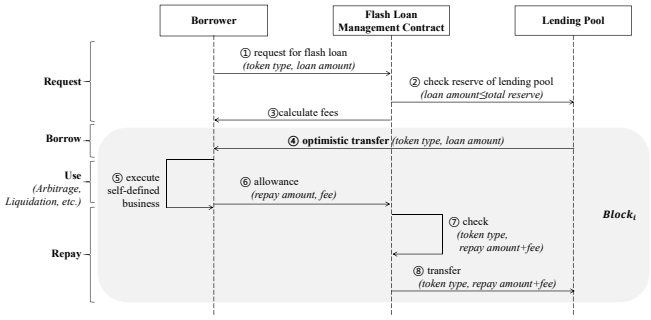

Figure 8: Flash Loan Workflow

4.3. 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 [129] [130].

DEX can be divided into different models based on the implementation of trading pair discovery and order matching [131] (cf. Figure 9). Some DEXs use traditional order book model, where orders are recorded in an order book, and transactions are aggregated using principles of high and low bids and time order. Exchanges 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 of two orders in its own order book and automatically executes the trade. Stellar [132] [133] implements this model. 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 with all orders and matches them off-chain. This model is implemented by projects like 0x [134], AirSwap [135], and IDEX [136]. dYdX [9] uses StarkEx [137] as the trading engine to package, validate, and update trades, supporting leveraged lending and margin trading of the off-chain order book model.

Several DEXs innovate the non-order book model. Two methods are (i) the establishment of a reserve pool, as done by KyberNetwork [138], and (ii) the use of the Automatic Market Maker (AMM) mode, which calculates the exchange rate between two or more assets according to specific algorithms, providing the quotation between assets at any time [22] [139]. 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. Angeris et al. [140] analyzed the advantages and disadvantages of various AMM algorithms. The constant mean algorithm can be summarized as $\prod_{i=1}^{n} x_i^{w_i} = k$, where the product of the quantities (x_i) of all tokens raised

to their respective weights (w_i) is constant. Balancer [141] uses the constant mean algorithm, while Uniswap [8] uses the constant product algorithm for only two assets with the same weight in a constant mean algorithm, shown as $x \times y = k$. Bancor [142] uses the dynamic weighting algorithm which allows for n assets with weights that can be adjusted dynamically. The constant sum algorithm computes price according to the formula $x + y = k$, where the sum of the quantities of two assets is constant. Egorove [143] demonstrated the defects of the constant sum algorithm. The Curve Finance [144] exchange uses a mixed-function algorithm to avoid the drawbacks of both constant mean and constant sum algorithms.

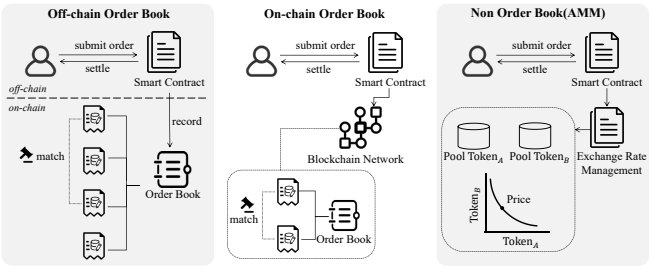

Figure 9: DEX Implementation Models

5. Services of DeFi

DeFi, inspired by traditional derivatives, offers a range of financial services, including on-chain options, asset management, and decentralized insurance. These services are achieved by replacing traditional processes with on-chain automatic executions [3]. Additionally, new financial derivatives have emerged, such as the perpetuity contract and prediction market.

5.1. Option

DeFi options are the buying or selling of an asset at a specific price in the future through a decentralized platform. The two main players are the buyer and the seller, and the process is automated through smart contracts. Compared to traditional options trading, DeFi markets offer higher efficiency and wider liquidity through smart contracts and liquidity pools. Decentralized options protocols meet the needs of investors seeking high-risk, high-leverage, high-return cryptocurrencies for speculation, as well as traders seeking hedging and protection against cryptocurrencies with high volatility.

The workflow of options trading in DeFi typically includes creating a smart contract that defines the conditions and parameters of the option, buying the option contract by paying a certain number of tokens, exercising the option based on market conditions, and settlement. These processes are facilitated by smart contracts to ensure transparency and security of transactions, and liquidity pools and market orders are provided to facilitate options trading.

The off-chain order matching model for options is similar to a decentralized exchange where orders and trades are maintained off-chain and cleared on-chain. Opium [149] is a typical project that adopts this model and proposes a holistic solution for the derivatives market not limited to options. Opyn [150] uses UniSwap's AMM mechanism to build mint smart contracts to generate tokenized options. Options programs implemented with liquid collateral-sharing asset pools are the options programs with the largest market share among current option contracts. Hegic [151] is a representative program that transforms a discrete market maker structure into point pool trading where anyone can pledge assets into the shared pool as collateral for the option seller and become an automated market maker for the option. According to the option execution process, common decentralized option products include standardized European options, some non-standard options, and OTC options. Deribit [157], OKEx [158], and other exchanges have launched standardized options trading services. MatrixPort [159] has launched "watch currency rise" over-the-counter options. Babel Finance [160] has launched a "sharkfin" capital-protected income management product based on barrier options.

5.2. Asset Management

DeFi asset management combines digital assets, oracles, lending, and other functions of DeFi apps to achieve asset management, portfolio management and risk management. DeFi asset management allows investors to delegate investment decisions to external third parties without having to give up trustless functionality. The smart contract of these apps invests, trades, and automatically adjusts the portfolio according to the investor's requirements. It has the advantage of low start-up costs and short start-up times, and it allows anyone to become a fund manager and investor.

Decentralized asset management involves user registration, asset deposition into the smart contract addresses, allocation to different portfolios, automatic execution by smart contracts, risk management through tools like stop-loss orders and alerts, and asset withdrawal at any time.

Decentralized asset management can be active or passive. Active asset management involves a professional team or algorithm making investment decisions and trades, such as Enzyme [152] managed by managers or DAO members, and Babylon Finance [161] focused on community governance, while passive asset management creates smart contracts based on individual projects, allowing users to create their own indices, structured products, spot-based portfolios, leveraged products, and more, such as Set [153] and Index Coop [162].

Integrated platforms offer both active and passive asset management to provide more flexible services, combining quantitative analysis with machine learning. Comprehensive DeFi asset management platforms such as SW DAO [163], Kava DeFi Platform [164], and DAOventures [165] offer robo-advisory services which automatically account for and evaluate the funds of DeFi products in the background, combining the skills of quantitative analysts with machine-learning artificial intelligence.

Table 2: DeFi Construction and Classification

	Project	Type	Feature: *Trust Model*	*Connected Chains*	*Centralization*	*Anonymous*	*Tokenization*	*Technique*	Property: *Stability*	*Scalability*	*Complexity*
Digital Assets	Bitcoin [30]	Native Crypocurrency	-	One	-	M.	-	BC	-	-	-
	Ethereum [35]		-	One	-	M.	-	BC	-	-	-
	Litecoin		-	One	-	M.	-	BC	-	-	-
	Monero [145]		-	One	-	H.	-	Ring-sig, Stealth Address	-	-	-
	Zcash [146]		-	One	-	H.	-	zk-Snark, Multi-sig	-	-	-
	ERC-20 [43]	Token Standard	-	One	Up to Apps	M.	-	SC	-	-	-
Wallets	Ledger [67]	Cold Wallet	-	Multiple	-	M.	-	TEE	-	-	-
	Trezor [68]		-	Multiple	-	H.	-	Multi-sig, 2FA	-	-	-
	Metamask [69]	Hot Wallet	-	Multiple	-	H.	-	Offline Storage	-	-	-
	Zengo [81]		TTP	Multiple	-	M.	-	MPC-TSS, 3FA	-	-	-
	Argent [86]		TTP	Multiple	-	H.	-	Multi-sig, 2FA	-	-	-
Oracle	MakerDao [93]	Alliance Oracle, Stablecoin	TTP	One	DAO	M.	Dai, MKR	Allowlist	H.	M.	L.
	Chainlink [94]	Off-chain Input	-	Multiple	-	M.	LINK	Reputation, Staking	H.	H.	M.
	NEST [96]	Fact Generation	-	One	-	M.	QP Token	Game Theory	H.	M.	H.
Bridges	Cosmos [99]	BC Engine	TTP	Multiple	Hub	H.	ATOM	IBC	-	H.	L.
	Polkadot [100]		TTP	Multiple	Validator	M.	DOT	Parachain	-	H.	L.
	BTC-relay [101]	Relay	TTP	Two	Mainchain	M.	ETH-BTC	SPV	-	M.	M.
	Polygon Bridge [147]	DApps Based	-	Multiple	-	M.	POL	Lock&Mint	-	-	-
	ThorSwap [104]		-	Multiple(Cosmos)	-	M.	RUNE	Third Party Chains, LP	-	-	-
Stablecoins	Tether [107]	Off-chain Reserve	-	Multiple	Issuer	L.	USDT	-	H.	H.	L.
	Liquity [110]	Over-collateral	-	One	-	M.	LQTY, LUSD	-	M.	M.	M.
	Ampleforth [111]	Algorithmic	-	Multiple	-	M.	AMPL	QTM-based Algorithmic	L.	L.	H.
	Frax Finance [113]		-	One	-	M.	FRAX, FXS	Algorithmic Seigniorage	L.	L.	H.
	Basis [112]		-	One	-	M.	BAC, BAS, BAB	Algorithmic Seigniorage	L.	L.	H.
	Terra [114]		-	One	-	M.	UST, LUNA	Parachain	L.	M.	H.
Lendings	AAVE [11]	Over-collateral	-	Multiple	No	M.	Aave	-	-	-	-
	Compound [10]		-	Multiple	No	M.	COMP	-	-	-	-
	TrueFi [124]	Under-collateral	TTP	One	Staker	M.	TRU	-	-	-	-
	Maple Finance [148]		TTP	One	Pool Delegates	L.	MPL	-	-	-	-
Exchanges	Stellar [132]	On-chain Orderbook	-	Multiple	-	M.	XLM	Manual Matching	-	L.	-
	0x [134]	Off-chain Orderbook	-	Multiple	Orderbook	M.	ZRX	Manual Matching	-	M.	-
	dYdX [9]		-	Multiple(Cosmos)	Orderbook	M.	DYDX	Manual Matching	-	M.	-
	KyberNetwork [138]	Non-orderbook	-	One	-	M.	KNC	Reserve Pool	-	H.	-
	Bancor [142]		-	One	-	M.	BNT	Constant product	-	H.	-
	Uniswap [8]		-	Multiple	-	M.	UNI	Constant mean	-	H.	-
	Balancer [141]		-	One	-	M.	BAL	Dynamic weight	-	H.	-
	Curve Finance [144]		-	One	-	M.	CRV	Hybrid function	-	H.	-
Derivatives	Opium [149]	Option	TTP	One	Orderbook	M.	OPIUM	Off-chain Orderbook	-	-	-
	Opyn [150]		-	One	-	M.	Squeeth	AMM	-	-	-
	Hegic [151]		-	One	-	M.	HEGIC	Peer-to-Pool	-	-	-
	Enzyme [152]	Asset Management	TTP	One	DAO/Manager	M.	MLN	Active Asset Management	-	-	-
	Set [153]		-	One	-	M.	-	Passive Strategy, Social Trading	-	-	-
	Nexus Manual [50]	Insurance	-	One	-	M.	-	Risk Sharing Pool	-	H.	-
	VouchForMe [154]		TTP	One	-	M.	-	Social Network Proof	-	H.	-
	Augur [155]		-	One	-	M.	REP	Prediction Market	-	H.	-
	CDx [51]		-	One	-	M.	CDX, Cred	Tokenized CDS	-	L.	-
	oTokens [150]		-	One	-	M.	oToken	Put Option	-	L.	-
	Augur [155]	Prediction Market	-	One	Staker	M.	REP	Voting	-	-	-
	Omen [156]		-	One	-	M.	OWL	Conditional Tokens	-	-	-

− = Does not provide property; N/A = Not known due to the absence of supporting documents.
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.

5.3. Insurance

DeFi insurance has the same working aspects as traditional insurance, including the creation of insurance, the purchase of insurance, and insurance claims. However, DeFi insurance replaces traditional insurance intermediaries with the joint work of blockchain nodes, enables all users to create their insurance and turns the decision on insurance claims into an open, transparent, and verifiable process.

Platforms like Etherisc [166] offer common infrastructure, product templates, and insurance licenses. Nexus Mutual [50] adopts a shared capital pool model with community voting on claims. VouchForMe [154] provides social proof endorsement insurance, where guarantees are collected from social network connections. DeFi insurance can leverage prediction markets and financial derivatives for multiple payout sources. Augur [155] enables users to build prediction markets for risk hedging, while oTokens [150] allows the

purchase of put options for asset protection.

Considering efficiency, Sayegh et al. [167] presented several applications of blockchain to simplify the insurance claim process. Raikwar et al. [168] proposed a blockchain framework for the entire insurance process. Lamberti et al. [169] discussed the potential of using blockchain and sensors for implementing claims. Lepoint et al. [170] introduced BlockCIS, a network insurance system based on blockchain. In terms of publicly verifiable properties, Singer et al. [171] demonstrated the risks of combining blockchain with insurance. Zhang et al. [172] proposed a scheme based on blockchain and deep learning to identify fraudulent claims. Chen et al. [173] proposed a traceable on-chain insurance claim system.

5.4. Perpetual Contract

Decentralized perpetual contracts are derivative contracts executed on a decentralized network. They allow participants to speculate or hedge against the price movements of an underlying asset, similar to leveraged spot trades. Perpetual contracts have no expiration date and use a fund fee mechanism to track the price index of the underlying asset. To complete a contract, four processes are required: contract creation where the contract creator writes and deploys smart contracts with the parameters, rules and conditions, trading through decentralized exchanges or other trading platforms on the blockchain, settlement automatically done based on rules, and funding by calculating the participant's profit or loss based on the market price at settlement. Perpetual holding is a unique feature, allowing participants to hold positions without an expiration date. Participants can be incentivized by providing liquidity and receiving rewards.

5.5. Prediction Market

A decentralized prediction market is a financial application that uses smart contracts to predict and trade outcomes of real-world events. Users can create prediction contracts anonymously. The operational process of a prediction market includes creating a market that predicts the outcome of a specific event, entering the terms, including the predicted outcome, time frame, market size, and cost into contracts, buying or selling predicting trades, and settling the results with the smart contract executing the settlement based on the actual result. In the market creation phase, any user can create a new market which can be a share or scalar market. The outcome of an event directly affects the revenue of users in a prediction market, making it a key motivator.

There are several ways to determine the outcome of an event. Reward and punishment mechanism that encourages users to report accurately is one of them. Augur [155], for example, incentivizes accurate reporting through a dispute mechanism where users stake tokens to challenge reports and the winner receives the loser's tokens. Another approach is to create an oracle that feeds back any data in the real world. The Omen Prediction Market [156] project created Reality.eth, a decentralized oracle that challenges the results of previous users to get closer to the truth. Users participating in a prediction market are incentivized by both profit-sharing and liquidity rewards. Correct predictions are rewarded, motivating users to actively participate and provide accurate predictions. Users also provide liquidity, increasing the market's liquidity and earning income from transaction fees.

6. Technical Security Risks

According to the architecture layer, three types of technical security risks faced by DeFi applications are identified: infrastructure layer risk, protocol layer risk, and application layer attack. We list in Table 3 known historical attacks against DeFi applications and literature on their solutions.

6.1. DeFi Infrastructural Layer

The blockchain architecture consists of layers: application, contract, incentive and consensus, and network and data [31] [35]. DeFi applications reside at application layer, while the layers below contract layer serve as the infrastructural layers, providing technical support for DeFi [174].

6.1.1. Risks in Network Communication. DeFi is network-based. Users interact with DeFi through communication protocols such as TCP/IP, while nodes in the network connect with others through blockchain network protocols. The security of network protocols directly affects the security of blockchain networks. Attackers may exploit multiple links including controlling the network service provider, manipulating incoming messages to trick nodes into perceiving the current state and censoring or delaying message transmission. Sheyner et al. [175] proposed an algorithm that generates attack graphs and analyzes network security, while Wang et al. [176] developed a framework for measuring network security metrics based on attack graphs. Khan et al. [177] proposed a mathematical model for cybersecurity that quantifies parameters such as risk, vulnerability and threat. Amin et al. [178] used a structural Bayesian network to capture the relationship between financial loss, cyber risk, and resilience and developed a scorecard-based approach to assess the level of cyber risk.

DoS Attack. A Denial of Service (DoS) attack overloads or disrupts the normal operation of a target system, preventing it from providing services to legitimate users. DApps, as decentralized applications, still communicate with users through traditional web servers, making them vulnerable to DoS attacks [179]. Congested network environments or attacks on blockchain nodes can affect the functionality and performance of DApps. Attackers may also use transactions to achieve DoS attacks on DeFi, taking advantage of network congestion by sending a large number of invalid transactions or taking up a large amount of bandwidth and computing resources, resulting in transaction delays and the blocking of legitimate users.

Node Transparency. Node transparency risks refer to the opacity or non-transparency of information and operations in blockchain, which can affect trust, security, and stability.

The ability of nodes to hide their true identity and location information makes it impossible for participants to accurately assess the trustworthiness and intentions of the nodes [180], as shown in Eclipse attacks [181] which involve an attacker controlling the entry node of a blockchain network and isolating the target node from the network. Attackers may use names, IP addresses, or other identifiers similar to real nodes to spoof legitimate DApp nodes and gain access to users' data or funds, like in Sybil attacks [182] in which an attacker forging multiple fake nodes to control the network and perform malicious operations. Dishonest nodes may exist in the network, providing false information or performing dishonest operations. Untrustworthy or easily manipulated data provided by nodes can affect the correctness of the DApp and the accuracy of its decisions [183]. Centralized control by a single entity or a small number of entities can lead to potential manipulation, censorship, or abuse of power, typical in 51% attacks [184] where an attacker compromises the security of a DeFi application by controlling more than 51% of the arithmetic power of the blockchain network and executing attacks such as double-flowering attacks, denial-of-service attacks, and malicious transaction injections.

6.1.2. Risks in Consensus Algorithm. Consensus algorithms in blockchains facilitate agreement among nodes, governing tasks like transaction ordering, block generation, and data validation. Nodes receive block rewards and transaction fees as incentives. However, this decision-making power also enables attackers to exploit Miner Extractable Value (MEV) [24]. While MEV is not always a bad thing, for example, it can be used in lending protocols to ensure timely liquidation of on-chain assets, or arbitraging in DEX to facilitate the formation of more accurate and consistent prices. MEVs do cause a lot of problems for users. MEV may lead to advantageous forks over the main chain [185] [186]. Attackers use MEV to engage in front-running [187] [188] or sandwich attacks [27], compromising fairness [189] and potentially colluding with nodes for profit.

Forks. A fork occurs when the main chain splits into two separate chains at a certain node. The original and forked chains may have differing security and stability, making the forked chain susceptible to new vulnerabilities and attacks. Smart contracts on both chains may not be compatible, disrupting contract functions and requiring redevelopment and migration. In DeFi, chain forks can lead to market fragmentation and reduced liquidity. Users may make mistakes and lose funds by operating on the wrong chain. Attackers may exploit forks to catch up and overwrite the main chain, gaining undeserved rewards.

Front-running. A front-running attack is when an attacker predicts or listens to a user's transaction activity and quickly submits priority transactions before their execution [190], resulting in blocking other users' transactions, changing the outcome of transactions, and gaining additional revenue. To implement a front-running attack, attackers monitor the memory pool to find profitable opportunities and quickly submit their own transactions with higher gas fees or replace the target transaction [26] once identify target transactions (cf. Figure 10). The bZx decentralized lending platform suffered a front-running attack in February 2020, wherein attackers managed to borrow a large amount of assets and then sell them at a higher price when the platform price was manipulated, thus reaping huge profits. Solutions to reduce the risk of front-running attacks include lightning networks that conduct transactions off-chain to reduce transaction latency and the chance of a front-running attack, batch order processing that combines multiple transactions into one block to narrow the batch window and cost attackers of faster submit speed, sealed transactions to avoid attackers listen for details, and improving the efficiency and competitiveness of the miners' fee market to reduce the profit margin of MEV and front-running attacks [191] [192]. FaaS (e.g. Flashbots [193]) allows traders to send transactions directly to miners. It aims to reduce the risk of front-running attacks and provide users with more control over transactions, regulating front-running to improve fairness. But a study by Weintraub et al. [194] found that more than 80% of MEV in Ethereum happens through Flashbots. Thus the feasibility of the goal of Flashbots-like FaaS services is questioned, and FaaS may put more competitive pressure on other participants and raise new competitive issues.

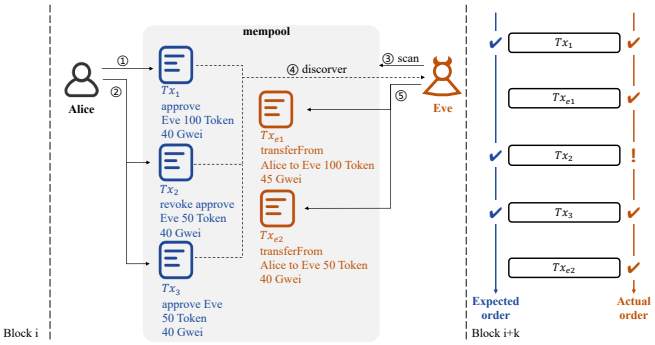

Figure 10: Front-running Attack

Sandwich Attack. Sandwich attack [27] (cf. Figure 11) is when an attacker executes counterparty trades before and after a target trade to exploit price discrepancies and illiquidity for profit, squeezing the low-cost trade between the target trade and pushing the price of the target trade up or down [195]. This is similar to a front-running attack, with attackers monitoring the order book and trading activity of DEXs to identify profitable opportunities and determine the execution time and price range of the target trade. The attacker then quickly submits counterparty trades to gain additional revenue. The main difference between sandwich attacks and front-running attacks is the timing of the target transaction execution and the targets of the attacks. Sandwich attacks affect prices by executing counterparty trades at the same time, pushing the price of the target trade up or down and causing the target trader to experience unfair trading losses. In contrast, front-running attacks gain an advantage by submitting trades before they are executed,

preventing other traders from getting the expected results or incurring unfair trading costs. Although specific sandwich attacks can be difficult to confirm, there are reports of many instances of DeFi sandwich attacks, with attackers taking advantage of illiquidity, price slippage, and execution delays on DEX to pad trades for additional profit.

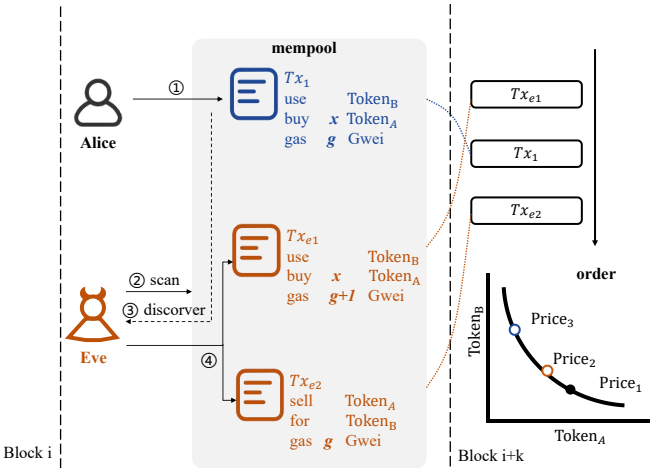

Figure 11: Sandwich Attack

6.2. DeFi Protocol Layer

The smart contract is crucial for the proper implementation and security of DeFi functions. However, smart contract vulnerabilities are the most common threat to DeFi security. Praitheeshan et al. [196] investigated how common vulnerabilities are in smart contracts layers. Atzei et al. [197] categorized common programming traps and studied security vulnerabilities in the smart contract of Ethereum. Samree et al. [198] identified eight application-level security vulnerabilities in smart contracts, analyzed past attacks, and categorized detection tools. Wan et al. [199] conducted surveys and interviews to investigate practitioners' perceptions and practices of smart contract security. Improper design of the protocols may also pose security risks.

6.2.1. 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 [174] [197].

Reentry. A reentry attack is an important threat to the security of smart contracts, which allows attackers to execute a specific contract function multiple times and re-invoke malicious contracts during each execution [200]. To implement a reentry attack, the attacker creates and deploys a malicious contract with callable functions into the target contract, and re-invokes it by calling a function of the target contract, repeating the attack logic many times. With a reentry attack, an attacker can gain access to funds in a contract, modify the status of the contract, or perform other unauthorized actions. The DAO, designed for investment and fund allocation based on community decisions, suffered a reentry attack in 2016. The attacker exploited a vulnerability in its contract by repeatedly calling the withdrawal function through a malicious contract, withdrawing funds from the contract multiple times successfully, leading to the theft of millions of Ether. Since then, the Ethereum community has made a series of improvements and fixes to prevent reentry attacks. These include "backward transfer" mode to avoid re-calling the attacker's contract, modifiers to limit calls to key functions by external contracts, locking mechanisms or status markers to prevent repeated function execution, and state variables or lock flags to track function execution state and prohibit re-calls.

Overflow. Overflow vulnerability is a common smart contract vulnerability that can cause unexpected money transfers, contract lockouts, or denial of service. Overflow includes integer overflow, array overflow, and memory overflow. An attacker can exploit integer overflow to change the state of a contract or transfer funds. Array overreach can also be exploited by attackers to access other data in a contract's memory leading to data leakage or tampering. Memory overflow can be exploited to make the contract fail to execute properly or deny service. If a contract uses loops to process a large amount of data, an attacker can send transactions with a large amount of input data to cause the contract to run out of memory. BeautyChain is an Ethereum-based platform that suffered an integer overflow vulnerability in its contract code in 2018. Attackers exploited this vulnerability to steal approximately $3 million in cryptocurrency by causing the funds in the contract to overflow. Meerkat Finance, a BSC-based lending protocol, also lost $31 million in user funds in March 2021 due to an overflow vulnerability. To prevent such vulnerabilities, coders should pay attention to boundary checking during coding and code review before deployment.

Random Numbers Misuse. The misuse of random numbers in smart contracts can be exploited to predict or manipulate the random number results of a contract, leading to security and fairness issues [201] [202]. This can result in attackers gaining unfair advantages in contracts such as gambling or voting. In 2018, hackers exploited a flaw in the random number generator of the EOSPlay gambling contract on the EOS blockchain, successfully predicting outcomes and receiving significant rewards. The use of insecure random numbers in contracts of secure functions, such as key generation, can also lead to security vulnerabilities and the cracking of encryption algorithms. To prevent such vulnerabilities, developers should avoid using predictable or manipulable random number generation algorithms and leverage external sources such as block hashes or timestamps.

6.2.2. Risks in Updating Smart Contracts. When updating smart contracts, there may be potential issues and security risks that can result in contractual misbehavior, loss of funds, unavailability of contracts, or reduced contract security. Upgraded contracts may not be compatible with previous versions, introducing new vulnerabilities or security concerns, or causing issues with data migration or contract dependencies. Incorrect configuration parameters or tampered configuration files may also cause contracts to fail to function properly or produce unexpected results [203]. Additionally, new permission mechanisms or access control

rules introduced in contract upgrades may result in incorrect or too loose permission configurations, allowing unauthorized actions. Mismanagement of multiple contract versions can also lead to unexpected results or inconsistent data. In April 2021, the Uranium Finance Project on BSC forgot to change parameters during a contract upgrade, leading to an attack during the liquidity migration process. To prevent such issues, contract developers and deployers should plan, test, and audit upgrades and deployments and establish monitoring and rollback mechanisms to detect and mitigate problems in a timely manner.

6.2.3. Risks in Design of Protocols. The design of DeFi protocols is a highly technical and complex process. In addition to vulnerabilities in codes, improper design of the protocols including logical vulnerabilities, faulty economic models, insufficient risk management and inappropriate authorization may also pose security risks. When protocols rely on complex algorithms or models, there may be unconsidered situations leading to logical vulnerabilities that prevent the protocol from functioning properly. The design of their economic model may have inflationary, deflationary, or unreasonable revenue sharing that results in users losing the expected revenue or prevents the protocol from remaining stable. The protocol may lack the necessary risk management measures preventing the protocol from responding to adverse events or limiting risks. These issues caused crises for Iron Finance on June 16, 2021, when the price of its governing token TITAN collapsed. At a time when both TITAN and its stablecoin IRON were sold off in large quantities, its issuance mechanism minted more TITAN as the IRON's price dropped and further lowered TITAN's price, which in turn sent TITAN into a death spiral. In addition to this, the design of the protocol may have authorization that allows administrators to tamper with the protocol to gain undue benefit or perform Rug Pull. The team of the DeFi project Compounder.Finance had used administrator privileges to replace audited contracts with malicious strategy contracts containing backdoors thereby stealing user funds.

6.3. DeFi Application Layer

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

6.3.1. Risks in Cross-chain. Cross-chain attacks involve attackers using the mechanism of cross-chain transactions to carry out malicious actions. These attacks can result in asset loss, transaction delays, and information tampering, impacting the security and stability of cross-chain DeFi applications. Cross-chain attacks can be divided into two types: native-chain attacks and inter-chain attacks. Native-chain attacks aim to affect the security of the specific blockchain, whereas inter-chain attacks disrupt communications and interactions between different chains. Various types of native chain attacks exist, such as double-spend attacks, false proof attacks as seen in the attack case on BSC Token Hub in October 2022, vulnerability exploits, reverse transaction attacks and replay attacks [226]. Relay blocking and inter-chain route hijacking [229] are common types of inter-chain attacks. Payment channels may also be vulnerable to wormhole attacks [231], where fees of the intermediate node can be stolen.

DeFi cross-chain applications face unique security risks compared to traditional ones due to their complex financial logic and asset management. Cross-chain smart contracts in DeFi apps face risks not only from their own vulnerabilities but also from the calling relationship between contracts. Price manipulation attacks, repeated borrowing and lending attacks are some of the unique types of cross-chain attacks faced by DeFi applications, as seen in the case of the attack on PancakeSwap's contract in April 2021.

6.3.2. Risks in Auxiliary Tools. Auxiliary services are entities that promote efficiency but are external of the system.

Oracle Manipulate. Hackers can manipulate or provide false, inaccurate, or beneficial data to oracle smart contracts [235], leading to improper benefits or interference with normal operation [1]. Oracles manipulation can lead to negative consequences such as stablecoin unanchoring, malicious carry trades, forced liquidation, and protocol liquidity drying up. Implementation processes of oracle manipulation vary. An attacker may attempt to take control of the data sources for example by attacking or tampering with the data source's API interface or supply chain. Attackers provide false or inaccurate data to oracles, such as modifying price data or providing incorrect market information. To prevent oracle manipulation, developers must ensure the security, tamper resistance, and incentives of the oracle, as well as the quality of the markets that the oracle connects to.

6.3.3. Risks of Being Phished. Users may not understand the smart contracts or assess their security and risk before making assets available, which can lead to unforeseen circumstances [240]. Users' lack of security awareness makes them vulnerable to phishing attacks, leading to personal information leakage and fund theft [241]. Phishing attacks in DeFi involve an attacker impersonating a legitimate entity or creating a deceptive false environment to gain access to a user's sensitive information, private keys, or login credentials in order to further acquire their digital assets or conduct other malicious activities. Attackers commonly create fake DeFi platforms or send fake notifications to trick users. In December 2021, Badger DAO suffered a $120 million loss due to a phishing attack where attackers inserted malicious wallet requests into the user interface. In 2021, attackers stole assets by posting fraudulent links on social media to a fake Uniswap website.

7. Economic Security Risks

DeFi economic risks pertain to vulnerabilities beyond traditional system vulnerabilities, such as design flaws or

Table 3: Overview of Technical Attacks against DeFi Applications and Their Solutions

Affected Layers		Attacks	Incidents			Solutions
			Time	Application	Loss	
Infrastructural Layer	Network Communication	Dos (DDoS) [179] [204]	*2020/05*	*Youbi*	*N/A*	[204] [205]
		Eclipse Attack [181] [206]	-	-	-	[207]
		Sybil Attack [182]	*Various*	*Arbitrum*	*253M ARB*	[208]
		51% Attack [184] [209]	*2020/04*	*PegNet*	*0.6M USD*	[210]
	Consensus Algorithm	Fork [211] [187] [27]	-	-	-	[211]
		MEV: Front-running Attack [26] [190]	*2021/03*	*DODO*	*0.7M USD*	[191] [192]
		MEV: Sandwich Attack [195] [27]	*2021/10*	*Alpha Homora V2*	*40.93 ETH*	[212] [213]
		MEV: Arbitrage Attack [214]	*2021/01*	*Saddle Finance*	*8 BTC*	[215]
Protocol Layer	Smart Contract	Reentry [216] [200]	*2016/06*	*The DAO*	*3.6M ETH*	[200]
		Overflow [217] [218]	*2018/07*	*Bancor*	*1.2M USD*	[219] [220]
		Misuse of Random Number [201] [202]	*2021/07*	*AnySwap*	*8M USD*	[220]
	Protocol	Rug Pull [221]	*2021/03*	*Meerkat Finance*	*20M USD*	[222]
Application Layer	Bridge	Double Spend Attack [223]	*2020/02*	*DForce*	*2.5M USD*	[224]
		False Proof Attack [223] [225]	*2022/02*	*Wormhole*	*1.2M ETH*	[225]
		Replay Attack [226]	*2022/09*	*OmniBridge*	*2M ETHW*	[227] [228]
		Inter-Chain Route Hijacking [229]	-	-	-	[230] [228]
		Wormhole Attack [231]	-	-	-	[232]
		Cross-chain Price Manipulation [233]	*2023/08*	*Neutra Finance*	*23.5 ETH*	[233] [234]
	Auxiliary Tools	Oracle Manipulation [235] [1] [87]	*2023/06*	*Themis Protocol*	*0.37M USD*	[236]
	Usage Method	Phishing Attack [231] [237]	*2022/12*	*Bitkeep*	*8M USD*	[238] [239]

insecure dependencies. Instead, they arise from the instability caused by rational players' actions within the ecosystem.

7.1. Liquidity Depletion

DeFi liquidity depletion risk occurs when there is a shortage of liquidity supply in the market, leading to transaction delays, price fluctuations and instability of the entire market. Liquidity in the DeFi market is dependent on speculators, and adverse market conditions or increased risk sentiment can cause users to withdraw funds quickly, resulting in insufficient liquidity. Wild market fluctuations, falling collateral prices, or market manipulation can also lead to insufficient liquidity. The Black Thursday event of MakerDAO in March 2020 [242] led to users' collateral being liquidated and liquidity drying up.

DeFi platforms should attract a diverse pool of liquidity providers and reduce reliance on specific liquidity sources. Projects can design incentives to attract and retain liquidity providers [131] [243]. In addition, DeFi projects should develop risk management strategies and contingency plans to deal with liquidity depletion scenarios.

7.2. Governance Risk

In DeFi systems, flexible governance and cash flow incentives can drive choices that benefit the project. However, inadequate incentives may lead token holders to prioritize external gains, potentially harming the system. Immediate updates in governance designs can be vulnerable to attacks if malicious contract code is executed using acquired governance tokens. For instance, the Beanstalk protocol encountered governance risks when an attacker accumulated tokens and proposed a malicious governance proposal to divert funds. In Ethereum2.0 (after the Merge), validators face censorship pressure due to the US OFAC's sanctions against Tornado Cash [244] [245].

7.3. Market Manipulation

Market manipulation artificially manipulates asset prices to profit from other traders. Illiquid assets are more prone to market manipulation and pose a greater risk to underlying financial products. Market manipulation strategies include spoofing [246], ramping [247], bear raids, cross-market manipulation, and oracle manipulation [236], which can manipulate a small segment or the entire market.

Market manipulation has caused DeFi to lose value in various ways. Lending agreements that do not liquidate low mortgages timely may lead to bad debts or dry up liquidity. Clearing must be triggered efficiently in the options market to remain liquid. In synthetic assets, paying out positions based on false prices can result in capital losses for liquidity providers. Automated trading algorithms based on erroneous prices can result in investment losses. For the algorithm stablecoins, if their incentive mechanism for stability is destroyed, the stablecoin may depeg from the anchor [118].

7.4. Flashloan Attack

Flash loan security risk is the vulnerability, contract, or attack risk when borrowing and repaying funds in a single blockchain transaction [187] [248]. Flash loan attacks can

cause capital losses, liquidity risks, and system instability. Vulnerabilities in codes of smart contracts can lead to malicious operations and attacks. Flash loan attacks happen frequently, some cases are shown in Table 4. Flash loans can be used as a means for attackers to manipulate if the transaction execution order is improper. Defending against flash loan attacks requires platforms to manage the security of flash loan agreements, fix potential vulnerabilities, limit the execution order of transactions, and introduce delay mechanisms or time windows to limit transaction execution.

Table 4: Flashloan Attack Cases

Date	Target Protocol	Flashloan Protocol	Attack Type
2020/2/15	bZx	dYdX	Bid arbitrage
2020/2/18	bZx	bZx	Price manipulation
2020/10/26	Harvest	Uniswap V2	Price manipulation
2020/11/6	Cheese Bank	dYdX	Price manipulation
2020/11/12	Akropolis	dYdX	Code vulnerability
2020/12/18	Warp Finance	Uniswap V2/dYdX	Price manipulation
2021/2/4	Yearn.Finance	dYdX/Aave	Bid arbitrage
2021/2/13	Alpha.Finance	Aave	Code vulnerability
2021/5/2	Spartan	PancakeSwap	Bid arbitrage
2021/5/8	Value.DeFi	Value.DeFi	Code vulnerability
2021/5/20	PancakeBunny	PancakeSwap	Price manipulation
2021/5/22	Bogged Finance	PancakeSwap	Code vulnerability
2021/5/25	AutoShark	PancakeSwap	Code vulnerability
2021/5/28	JulSwap	JulSwap	Price manipulation
2021/6/10	EvoDeFi	PancakeSwap	Code vulnerability
2021/6/25	xWin Finance	PancakeSwap	Price manipulation
2021/7/2	XDXSwap	XDXSwap	Code vulnerability
2021/7/14	ApeRocket	AAVE	Code vulnerability
2021/7/18	Array.Finance	AAVE	Code vulnerability
2021/8/4	Popsicle Finance	AAVE	Code vulnerability
2021/8/25	Dot.Finance	PancakeSwap	Code vulnerability
2022/3/15	Deus Finance	SpiritSwap	Price manipulation
2022/10/15	Earning.Farm	AAVE	Code vulnerability
2022/10/25	ULME	Uniswap V2	Price manipulation
2022/11/11	DFXFinance	Uniswap V3	Code vulnerability
2023/3/13	Euler Finance	AAVE	Code vulnerability
2023/4/13	Yearn Finance	AAVE	Code vulnerability
2023/7/24	Palmswap	AAVE	Code vulnerability

8. Open Research Challenges

While DeFi is growing fast and numerous excellent projects have emerged, there is still room for further development, expansion and exploration. Based on the existing literature, observations of recent trends in the field, and the main issues that need to be addressed, the directions and challenges of future research from the perspectives of information and communications technology (ICT) construction, economics construction, and sociology construction are discussed in this section. Figure 12 graphically illustrates the relationship between future research avenues and DeFi architecture.

8.1. DeFi ICT Construction

8.1.1. Functionality. DeFi function integration platforms offer unified access to various DeFi protocols and functions like lending, trading, and liquidity provision. Their goals include user-friendly interfaces, protocol integration, security, and interoperability for seamless asset and data transfers. However, the dynamic nature of the DeFi market poses risk management challenges, necessitating better risk management practices. Security vulnerabilities in DeFi protocols and smart contracts call for strengthened security audits and vulnerability repair mechanisms. Integration of multiple protocols can affect their stability and availability, potentially triggering a system crash.

8.1.2. Security. DeFi security involves analyzing various attack and threat models at the network, protocol, and application layers. Some research has been conducted on network communication security [175] [176] [177] [178] [249]. However, there is still a lack of in-depth research specifically focused on DeFi network communication security, standardized evaluation and auditing methods, and corresponding security mechanisms and defense strategies.

To enhance DeFi security, researchers can analyze the network topology and communication methods among nodes to identify attack paths and vulnerabilities. DeFi protocols including consensus mechanisms, identity verification, access control, encryption algorithms, privacy protection, and secure smart contracts can also be considered.

In particular, contract security auditing is crucial in DeFi security. Zhou et al. [7] found that security audits reduce the average probability of exploitation by one-fourth. Smart contract auditing primarily relies on a combination of manual review and automated tools currently, with the latter statically analyzing contract code to detect common vulnerability patterns. Existing audit tools may have limitations, and advanced vulnerability types require further research. Researchers should improve smart contract audit tools, explore machine learning and artificial intelligence techniques, and develop methods to track contract changes and conduct timely audits. Establishing standards and best practices is also a promising research area in DeFi security.

8.1.3. Incident Detection and Emergency response. Incident discovery and post-processing are vital for safeguarding users' assets and ensuring the healthy development of DeFi. Timely detection and handling of DeFi events can reduce the risk of asset loss for users and build trust in DeFi projects. Future research should focus on effective monitoring and detection of DeFi events. This involves developing intelligent monitoring systems, analyzing data and traffic patterns, and using machine learning to identify unusual activity and risk events. Post-event processing and risk management are equally important, requiring the establishment of incident response mechanisms, cooperation and collaboration mechanisms, and asset recovery mechanisms.

8.2. DeFi Sociology Construction

8.2.1. Privacy. Privacy protection in DeFi aims to safeguard users' personal information, transaction data, and financial flows from tracking, monitoring, and unauthorized access. Ideally, in the DeFi ecosystem, transaction data should be protected from unauthorized access and analysis, and personal information and money flow data should be safeguarded against data leakage and abuse. Anonymity in DeFi can be achieved through privacy techniques such as ZKPs [59], ring signatures [38], and trusted hardware (e.g., TEE).

Transaction privacy can be protected through encryption technologies and privacy protocols such as coin mixing [54], while data privacy can be realized through confidential smart contracts [21] [250]. However, balancing anonymity and traceability to meet regulatory and compliance needs is a challenge. Existing privacy protection technologies often require significant computing and storage resources, leading to performance degradation and scalability issues. Researchers need to focus on more efficient privacy protection schemes.

8.2.2. Compliance. Compliance of DeFi applications is a growing concern as it plays a vital role in protecting users' rights and the security of their funds, reducing fraud and risk, and maintaining the stability of the financial system. In addition, ensuring compliance and preventing illegal activities such as money laundering and terrorist financing is of paramount importance for regulators. However, DeFi's core concepts of decentralization and permissionless financial innovation are in conflict with compliance and regulation. For example, Tornado.Cash was sanctioned by US OFAC for providing anonymous transfers that were used for illegal activities such as money laundering. Balancing the two is a challenge for future research. The rapid growth of DeFi also poses a challenge in bridging the gap between research and practice. The uniqueness of DeFi requires the development of an appropriate compliance framework, which involves facilitating cross-border regulatory cooperation and information sharing, as well as utilizing technology to increase the automation and efficiency of the compliance process.

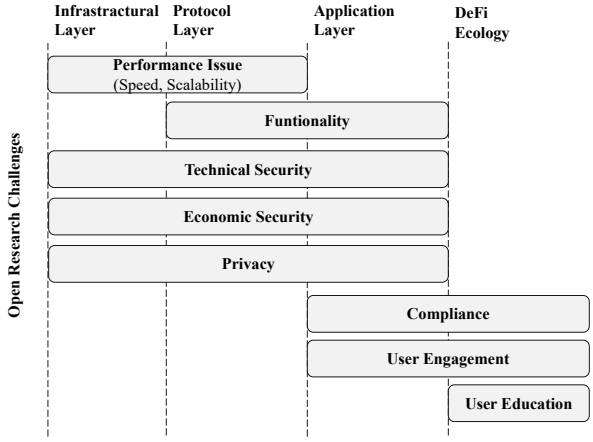

Figure 12: Open Research Challenges

8.3. DeFi Ecology Construction

8.3.1. User Engagement. Increasing user engagement is crucial for the growth of the DeFi ecosystem. Low user engagement can lead to issues like reduced liquidity, higher transaction costs, shallow market depth, and increased price volatility. Moreover, it may create an environment where market and price manipulation become easier for a few influential players. To address this, improving ease of use is paramount. Researchers should focus on designing user-friendly interfaces, streamlining operational processes, and offering personalized services to attract more users. Additionally, implementing effective incentive mechanisms, such as reward systems and token economic models, can encourage user participation and contributions, presenting promising research opportunities.

8.3.2. User Education. User education is important in increasing users' awareness of the opportunities and risks of DeFi. With the deepening of cognition of DeFi, users' participation in DeFi will increase, making the DeFi market more dynamic. To promote sustainable development, rich, systematic, and easy-to-understand DeFi education resources are needed. This includes teaching materials, online courses, guides, and tools. Building a positive community education and support system can further promote user education. Researchers can also examine how collaboration and knowledge sharing in the DeFi community can be fostered to help users learn from and support each other.

9. Conclusion

In this paper, we present a comprehensive overview of DeFi applications. We purpose a DeFi construction and classification frame based on the complexity of financial services and present details of DeFi protocols within each category. We also discuss the security of DeFi applications of our frame from technical and economic perspectives by referring to relevant DeFi academic papers and real-world incidents, highlighting the risks, attack implementations, and possible defenses. We provide research directions including functional integrity, security enhancement, compliance, and eco-construction, addressing the gap between existing DeFi realizations and the ideal state.

References

[1] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, "SoK: Decentralized finance (DeFi)," in *ACM Conference on Advances in Financial Technologies (AFT)*, 2022, pp. 30–46.

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

[3] P. Schueffel, "DeFi: Decentralized finance-an introduction and overview," *Journal of Innovation Management*, vol. 9, no. 3, pp. I–XI, 2021.

[4] R. Li, Q. Wang, Q. Wang, and D. Galindo, "How do smart contracts benefit security protocols?" *arXiv preprint arXiv:2202.08699*, 2022.

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

[6] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, and K. Ren, "Towards understanding flash loan and its applications in DeFi ecosystem," *International Workshop on Security in Blockchain and Cloud Computing (SBC@AsiaCCS)*, 2021.

[7] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "SoK: Decentralized finance (DeFi) attacks," *IEEE Symposium on Security and Privacy (SP)*, 2023.

[8] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, "Uniswap v3 core," *Tech. rep., Uniswap, Tech. Rep.*, 2021.

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

[10] C. Labs, "Compound finance," Retrieved from https://compound.finance/, 2019.

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

[12] C. Finance, "Convex," Retrieved from https://www.convexfinance.com/, 2023.

[13] H. Finance, "Harvest finance document," Retrieved from https://docs.harvest.finance/, 2023.

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

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

[16] A. Moin, K. Sekniqi, and E. G. Sirer, "SoK: A classification framework for stablecoin designs," in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2020, pp. 174–197.

[17] W. Zhao, H. Li, and Y. Yuan, "Understand volatility of algorithmic stablecoin: Modeling, verification and empirical analysis," in *International Conference on Financial Cryptography and Data Security Workshop on Decentralized Finance (DeFi@FC)*. Springer, 2021, pp. 97–108.

[18] M. Bartoletti, J. H.-y. Chiang, and A. L. Lafuente, "SoK: Lending pools in decentralized finance," in *International Conference on Financial Cryptography and Data Security Workshop on Decentralized Finance (DeFi@FC)*. Springer, 2021, pp. 553–578.

[19] T. A. Xu and J. Xu, "A short survey on business models of decentralized finance (defi) protocols," *International Conference on Financial Cryptography and Data Security Workshop on Decentralized Finance (DeFi@FC)*, 2022.

[20] S. Cousaert, J. Xu, and T. Matsui, "SoK: Yield aggregators in DeFi," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2022, pp. 1–14.

[21] R. Li *et al.*, "SoK: TEE-assisted confidential smart contract," *Proceedings on Privacy Enhancing Technologies (PETs)*, vol. 3, pp. 1–21, 2022.

[22] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols," *ACM Computing Surveys (CSUR)*, vol. 55, no. 11, pp. 1–50, 2023.

[23] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu, "SoK: Design, vulnerabilities and defense of cryptocurrency wallets," *arXiv preprint arXiv:2307.12874*, 2023.

[24] K. Qin, L. Zhou, and A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?" in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 198–214.

[25] S. Yang, F. Zhang, K. Huang, X. Chen, Y. Yang, and F. Zhu, "SoK: Mev countermeasures: Theory and practice," *arXiv preprint arXiv:2212.05111*, 2022.

[26] S. Eskandari, S. Moosavi, and J. Clark, "SoK: Transparent dishonesty: Front-running attacks on blockchain," in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2020, pp. 170–189.

[27] L. Zhou, K. Qin, A. Cully, B. Livshits, and A. Gervais, "On the just-in-time discovery of profit-generating transactions in DeFi protocols," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 919–936.

[28] Q. Wang, R. Li, Q. Wang, S. Chen, and Y. Xiang, "Exploring unfairness on proof of authority: Order manipulation attacks and remedies," in *ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2022, pp. 123–137.

[29] S. Haber and W. S. Stornetta, *How to time-stamp a digital document*. Springer, 1991.

[30] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin. https://bitcoin.org/bitcoin.pdf*, vol. 4, no. 2, p. 15, 2008.

[31] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[32] A.-D. Popescu, "Decentralized finance (DeFi)–the lego of finance," *Social Sciences and Education Research Review*, vol. 7, no. 1, pp. 321–349, 2020.

[33] T. Katona, "Decentralized finance: The possibilities of a blockchain "money lego" system," *Financial and Economic Review*, vol. 20, no. 1, pp. 74–102, 2021.

[34] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.

[35] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[36] L. W. contributors, "Main page — litecoin wiki," Retrieved from https://litecoin.info/index.php/Main_Page, 2019.

[37] K. M. Alonso *et al.*, "Zero to monero," 2020.

[38] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. 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)*. Springer, 2017, pp. 456–474.

[39] A. Hinteregger and B. Haslhofer, "An empirical analysis of monero cross-chain traceability," *International Conference on Financial Cryptography and Data Security (FC)*, 2019.

[40] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," *GitHub: San Francisco, CA, USA*, vol. 4, p. 220, 2016.

[41] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in Zcash," in *USENIX security symposium (USENIX Sec)*, 2018, pp. 463–477.

[42] M. Shirole, M. Darisi, and S. Bhirud, "Cryptocurrency token: An overview," in *International Conference on Blockchain Technology (ICBCT)*. Springer, 2020, pp. 133–140.

[43] F. Vogelsteller and V. Buterin, "Erc-20: Token standard," Retrieved from https://eips.ethereum.org/EIPS/eip-20, 2015.

[44] W. Entriken, D. Shirley, J. Evans, and N. Sachs, "Erc-721: Non-fungible token standard," Retrieved from https://eips.ethereum.org/EIPS/eip-721, 2018.

[45] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*, 2021.

[46] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and R. Sandford, "Erc-1155: Multi-token standard," Retrieved from https://eips.ethereum.org/EIPS/eip-1155, 2018.

[47] M. Wang, Willand Meng, Y. Cai, R. Chow, Z. Wu, and AlvisDu, "Erc-3525: Semi-fungible token," Retrieved from https://eips.ethereum.org/EIPS/eip-3525, 2020.

[48] Y. Liu, V. Deshpande, C. Ngakam, D. Malik, S. Samuel Gwlanold Edoumou, and T. Batrice, "Erc-3475: Abstract storage bonds," Retrieved from https://eips.ethereum.org/EIPS/eip-3475, 2021.

[49] M. Lockyer, N. Mudge, J. Schalm, s. echeverry, Z. Zhou, and Victor, "Erc-998: Composable non-fungible token," Retrieved from https://eips.ethereum.org/EIPS/eip-998, 2018.

[50] N. Mutual, "The nexus mutual protocol," Retrieved from https://docs.nexusmutual.io/protocol/, 2020.

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

[52] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*, 2013, pp. 127–140.

[53] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *International Conference on Financial Cryptography and Data Security*, Springer. Berlin, Heidelberg: Springer Science & Business Media, 2013, pp. 34–51.

[54] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from Bitcoin," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2013, pp. 397–411.

[55] J. Groth, "On the size of pairing-based non-interactive arguments," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2016, pp. 305–326.

[56] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 315–334.

[57] A. Hayes, "Coinjoin: What it is, how it works, privacy considerations," Retrieved from https://www.investopedia.com/terms/c/coinjoin.asp, 2021.

[58] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "Tumblebit: An untrusted Bitcoin-compatible anonymous payment hub," in *Network and Distributed System Security Symposium*, 2017.

[59] Z. Wang, S. Chaliasos, K. Qin, L. Zhou, L. Gao, P. Berrang, B. Livshits, and A. Gervais, "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy," in *Proceedings of the ACM Web Conference (WWW)*, 2023, pp. 2022–2032.

[60] D. V. Le and A. Gervais, "Amr: Autonomous coin mixer with privacy preserving reward distribution," in *Proceedings of the ACM Conference on Advances in Financial Technologies (AFT)*, 2021, pp. 142–155.

[61] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with accountable mixes," in *Interantional Conference on Financial Cryptography and Data Security (FC)*. Springer, 2014, pp. 486–504.

[62] C. Baum, J. H.-y. Chiang, B. David, and T. K. Frederiksen, "Sok: Privacy-enhancing technologies in finance," *Cryptology ePrint Archive*, 2023.

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

[64] M. Team, "Bip wallet," Retrieved from https://github.com/MinterTeam/bip-wallet-web, 2023.

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

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

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

[68] T. company, "Trezor hardware wallet (official)," Retrieved from https://trezor.io/, 2013.

[69] MetaMask, "The crypto wallet for defi, web3 dapps and nfts," Retrieved from https://metamask.io/, 2016.

[70] S. Şahan, A. F. Ekici, and Ş. Bahtiyar, "A multi-factor authentication framework for secure access to blockchain," in *International Conference on Computer and Technology Applications (CCAT)*, 2019, pp. 160–164.

[71] E. Benli, I. Engin, C. Giousouf, M. Ulak, and Ş. Bahtiyar, "Biowallet: a biometric digital wallet," *ICONS 2017*, p. 45, 2017.

[72] 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.

[73] M. Aydar, S. C. Cetin, S. Ayvaz, and B. Aygun, "Private key encryption and recovery in blockchain," *arXiv preprint arXiv:1907.04156*, 2019.

[74] T. Hu, X. Liu, W. Niu, K. Ding, Y. Wang, and X. Zhang, "Securing the private key in your blockchain wallet: a continuous authentication approach based on behavioral biometric," in *Journal of Physics: Conference Series*, vol. 1631. IOP Publishing, 2020, p. 012104.

[75] R. Soltani, U. T. Nguyen, and A. 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)*. IEEE, 2019, pp. 320–325.

[76] G.-J. Ra, C.-H. Roh, and I.-Y. Lee, "A key recovery system based on password-protected secret sharing in a permissioned blockchain," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 153–170, 2020.

[77] A. Bagherzandi, S. Jarecki, N. Saxena, and Y. Lu, "Password-protected secret sharing," in *ACM conference on Computer and Communications Security (CCS)*, 2011, pp. 433–444.

[78] J. Camenisch, A. Lehmann, A. Lysyanskaya, and G. Neven, "Memento: How to reconstruct your secrets from a single password in a hostile environment," in *Annual Cryptology Conference (CRYPTO)*. Springer, 2014, pp. 256–275.

[79] S. Jarecki, A. Kiayias, and H. Krawczyk, "Round-optimal password-protected secret sharing and t-pake in the password-only model," in *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer, 2014, pp. 233–253.

[80] S. Jarecki, A. Kiayias, H. Krawczyk, and J. Xu, "Highly-efficient and composable password-protected secret sharing (or: How to protect your Bitcoin wallet online)," in *IEEE European Symposium on Security and Privacy (EuroSP)*. IEEE, 2016, pp. 276–291.

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

[82] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, and Y. Li, "A social-network-based cryptocurrency wallet-management scheme," *IEEE Access*, vol. 6, pp. 7654–7663, 2018.

[83] N. Lehto, K. Halunen, O.-M. Latvala, A. Karinsalo, and J. Salonen, "Cryptovault-a secure hardware wallet for decentralized key management," in *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*. IEEE, 2021, pp. 1–4.

[84] W. Dai, Y. Lv, K.-K. R. Choo, Z. Liu, D. Zou, and H. Jin, "Crsa: A cryptocurrency recovery scheme based on hidden assistance relationships," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4291–4305, 2021.

[85] R. Li *et al.*, "An offline delegatable cryptocurrency system," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021, pp. 1–9.

[86] argentlabs, "Argent smart wallet specification," Retrieved from https://github.com/argentlabs/argent-contracts/blob/develop/specifications/specifications.pdf, 2021.

[87] T. Mackinga, T. Nadahalli, and R. Wattenhofer, "Twap oracle attacks: Easier done than said?" in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2022, pp. 1–8.

[88] J. Heiss, J. Eberhardt, and S. Tai, "From oracles to trustworthy data on-chaining systems," in *IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 496–503.

[89] A. K. Williams and J. Peterson, "Decentralized common knowledge oracles," *arXiv preprint arXiv:1912.01215*, 2019.

[90] N. Goel, A. Filos-Ratsikas, and B. Faltings, "Decentralized oracles via peer-prediction in the presence of lying incentives," 2019.

[91] Y. Cai, N. Irtija, E. E. Tsiropoulou, and A. Veneris, "Truthful decentralized blockchain oracles," *International Journal of Network Management*, vol. 32, no. 2, p. e2179, 2022.

[92] M. Merlini, N. Veira, R. Berryhill, and A. Veneris, "On public decentralized ledger oracles via a paired-question protocol," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 337–344.

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

[94] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz *et al.*, "Chainlink 2.0: Next steps in the evolution of decentralized oracle networks," *Chainlink Labs*, vol. 1, 2021.

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

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

[97] M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "A reinforcement learning model for the reliability of blockchain oracles," *Expert Systems with Applications*, vol. 214, p. 119160, 2023.

[98] G. Wang *et al.*, "Exploring blockchains interoperability: A systematic survey," *ACM Computing Surveys (CSUR)*, 2023.

[99] J. Kwon and E. Buchman, "Cosmos whitepaper," *A Netw. Distrib. Ledgers*, vol. 27, 2019.

[100] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White paper*, vol. 21, no. 2327, p. 4662, 2016.

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

[102] B. Relay, "Frequently asked questions—btc relay 1.0 documentation. retrieved april 7, 2019," 2016.

[103] V. Buterin, "Chain interoperability," *R3 research paper*, vol. 9, pp. 1–25, 2016.

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

[105] B. Wang, X. Yuan, L. Duan, H. Ma, C. Su, and W. Wang, "Defiscanner: Spotting DeFi attacks exploiting logic vulnerabilities on blockchain," *IEEE Transactions on Computational Social Systems (TCSS)*, pp. 1–12, 2022.

[106] C. Catalini, A. de Gortari, and N. Shah, "Some simple economics of stablecoins," *Annual Review of Financial Economics*, vol. 14, 2022.

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

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

[109] G. T. Company, "Gemini," Retrieved from https://www.gemini.com/dollar, 2023.

[110] Liquity, "Official liquity documentation," Retrieved from https://docs.liquity.org/, 2023.

[111] E. Kuo, B. Iles, and M. R. Cruz, "Ampleforth: A new synthetic commodity," *Ampleforth White Paper*, 2019.

[112] N. Al-Naji, J. Chen, and L. Diao, "Basis: a price-stable cryptocurrency with an algorithmic central bank," Retrieved from https://basis.io/basis_whitepaper_en.pdf, 2017.

[113] S. Kazemian, J. Huan, J. Shomroni, and K. Iyer, "Frax: A fractional-algorithmic stablecoin protocol," in *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2022, pp. 406–411.

[114] E. Kereiakes, M. D. M. Do Kwon, and N. Platias, "Terra money: Stability and adoption," *White Paper, Apr*, 2019.

[115] A. Briola, D. Vidal-Tomás, Y. Wang, and T. Aste, "Anatomy of a stablecoin's failure: The terra-luna case," *Finance Research Letters*, vol. 51, p. 103358, 2023.

[116] A. Klages-Mundt and A. Minca, "(in) stability for the blockchain: Deleveraging spirals and stablecoin attacks," 2021.

[117] C. Catalini and N. Shah, "Setting standards for stablecoin reserves," *Available at SSRN 3970885*, 2021.

[118] S. Fu *et al.*, "Rational ponzi game in algorithmic stablecoin," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2023, pp. 1–6.

[119] S. Kim, "New crypto-secured lending system with a two-way collateral function," *Ledger*, vol. 6, 2021.

[120] Z. Wang, K. Qin, D. V. Minh, and A. Gervais, "Speculative multipliers on DeFi: Quantifying on-chain leverage risks," in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2022, pp. 38–56.

[121] Y. Xie, X. Kang, T. Li, C.-K. Chu, and H. Wang, "Towards secure and trustworthy flash loans: A blockchain-based trust management approach," in *International Conference on Network and System Security (NSS)*. Springer, 2022, pp. 499–513.

[122] W. Uriawan, O. Hasan, Y. Badr, and L. Brunie, "Collateral-free trustworthiness-based personal lending on a decentralized application (DApp)." in *SECRYPT*, 2021, pp. 839–844.

[123] V. Hassija, G. Bansal, V. Chamola, N. Kumar, and M. Guizani, "Secure lending: Blockchain and prospect theory-based decentralized credit scoring model," *IEEE Transactions on Network Science and Engineering (TNSE)*, vol. 7, no. 4, pp. 2566–2575, 2020.

[124] TrueFi, "Truefi docs," Retrieved from https://docs.truefi.io/faq/, 2023.

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

[126] M. Black, T. Liu, and T. Cai, "Atomic loans: Cryptocurrency debt instruments," *arXiv preprint arXiv:1901.05117*, 2019.

[127] V.-B. Pham and T.-D. Trinh, "Analysis model for decentralized lending protocols," in *International Symposium on Information and Communication Technology (SOICT)*, 2022, pp. 405–412.

[128] K. Saengchote, "Decentralized lending and its users: Insights from compound," *arXiv preprint arXiv:2212.05734*, 2022.

[129] A. Barbon and A. Ranaldo, "On the quality of cryptocurrency markets: Centralized versus decentralized exchanges," *arXiv preprint arXiv:2112.07386*, 2021.

[130] J. A. Berg, R. Fritsch, L. Heimbach, and R. Wattenhofer, "An empirical study of market inefficiencies in Uniswap and SushiSwap," *arXiv preprint arXiv:2203.07774*, 2022.

[131] L. Heimbach, Y. Wang, and R. Wattenhofer, "Behavior of liquidity providers in decentralized exchanges," *arXiv preprint arXiv:2105.13822*, 2021.

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

[133] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, vol. 32, pp. 1–45, 2015.

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

[135] M. Oved and D. Mosites, "Swap: A peer-to-peer protocol for trading ethereum tokens," *Whitepaper Database*, vol. 21, 2017.

[136] A. 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.

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

[138] Y. V. L. Luu and Y. Velner, "Kybernetwork: A trustless decentralized exchange and payment service," Retrieved from https://home.kyber.network/assets/KyberNetworkWhitepaper.pdf, 2017.

[139] V. Mohan, "Automated market makers and decentralized exchanges: a DeFi primer," *Financial Innovation*, vol. 8, no. 1, p. 20, 2022.

[140] G. Angeris and T. Chitra, "Improved price oracles: Constant function market makers," in *ACM Conference on Advances in Financial Technologies (AFT)*, 2020, pp. 80–91.

[141] F. Martinelli and N. Mushegian, "A non-custodial portfolio manager, liquidity provider, and price sensor," Retrieved from https://balancer.finance/whitepaper, 2019.

[142] E. Hertzog, G. Benartzi, and G. 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(accessedon6June2020)*, 2017.

[143] M. Egorov, "Stableswap-efficient mechanism for stablecoin liquidity," *Retrieved Feb*, vol. 24, p. 2021, 2019.

[144] M. Egorov and C. Finance, "Automatic market-making with dynamic peg," 2021.

[145] T. M. Project, "Moneropedia," Retrived from https://www.getmonero.org/resources/moneropedia/, 2014.

[146] E. C. Company, "Zcash," Retrieved from https://z.cash/learn/, 2016.

[147] P. Bridge, "Matic whitepaper," Retrieved from https://github.com/maticnetwork/whitepaper/, 2020.

[148] M. Labs, "Maple finance," Retrieved from https://maplefinance.gitbook.io/maple/, 2023.

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

[150] Z. Koticha, "Building a generalized liquid options protocol in DeFi," *Opyn*, 2019.

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

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

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

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

[155] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, and S. Alexander, "Augur: a decentralized oracle and prediction market platform," *arXiv preprint arXiv:1501.01042*, 2015.

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

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

[158] O. Team, "Okx exchange," Retrieved from https://wp.whitepaper.io/okx/, 2022.

[159] M. Technologies, "Matrixport: All-in-one crypto financial services platform," Retrieved from https://matrixport.com/, 2021.

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

[161] ——, "Babylon litepaper," Retrieved from https://docs.babylon.finance/protocol/litepaper, 2022.

[162] I. Coop, "The definitive guide to earning yield on digital assets," Retrieved from https://indexcoop.com/whitepapers/the-definitive-guide-to-earning-yield-on-digital-assets, 2020.

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

[164] 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.

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

[166] S. Cousaert, N. Vadgama, and J. Xu, "Token-based insurance solutions on blockchain," in *Blockchains and the Token Economy: Theory and Practice*. Springer, 2022, pp. 237–260.

[167] K. Sayegh and M. Desoky, "Blockchain application in insurance and reinsurance. france: Skema business school," *Work in Progress papers*, 2019.

[168] M. Raikwar, S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay, and K.-Y. Lam, "A blockchain framework for insurance processes," in *IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2018, pp. 1–4.

[169] F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gomez, and V. Santamaria, "Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 72–81, 2018.

[170] T. Lepoint, G. Ciocarlie, and K. Eldefrawy, "Blockcis—a blockchain-based cyber insurance system," in *IEEE International Conference on Cloud Engineering (IC2E)*. IEEE, 2018, pp. 378–384.

[171] A. W. Singer, "Can blockchain improve insurance?" *Risk Management*, vol. 66, no. 1, pp. 20–25, 2019.

[172] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," *Future Generation Computer Systems*, vol. 130, pp. 140–154, 2022.

[173] C.-L. Chen, Y.-Y. Deng, W.-J. Tsaur, C.-T. Li, C.-C. Lee, and C.-M. Wu, "A traceable online insurance claims system based on blockchain and smart contract technology," *Sustainability*, vol. 13, no. 16, p. 9386, 2021.

[174] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on Ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.

[175] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2002, pp. 273–284.

[176] L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs," in *ACM workshop on Quality of Protection (QoP@CCS)*, 2007, pp. 49–54.

[177] M. A. Khan and M. Hussain, "Cyber security quantification model," in *International Conference on Security of Information and Networks (SIN)*, 2010, pp. 142–148.

[178] Z. Amin, "A practical road map for assessing cyber risk," *Journal of Risk Research*, vol. 22, no. 1, pp. 32–43, 2019.

[179] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels, "Bdos: Blockchain denial-of-service," in *ACM SIGSAC conference on Computer and Communications Security (CCS)*, 2020, pp. 601–619.

[180] S. K. Kim, Z. Ma, S. Murali, J. Mason, A. Miller, and M. Bailey, "Measuring Ethereum network peers," in *ACM Internet Measurement Conference (IMC))*, 2018, pp. 91–104.

[181] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on {Bitcoin's}{peer-to-peer} network," in *24th USENIX security symposium (USENIX security 15)*, 2015, pp. 129–144.

[182] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260.

[183] L. T. Nguyen, L. D. Nguyen, T. Hoang, D. Bandara, Q. Wang, Q. Lu, X. Xu, L. Zhu, P. Popovski, and S. Chen, "Blockchain-empowered trustworthy data sharing: Fundamentals, applications, and challenges," *arXiv preprint arXiv:2303.06546*, 2023.

[184] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials (COMST)*, vol. 22, no. 3, pp. 1977–2008, 2020.

[185] D. Perez and B. Livshits, "Smart contract vulnerabilities: Vulnerable does not imply exploited." in *USENIX Security Symposium (USENIX Sec)*, 2021, pp. 1325–1341.

[186] X. Zhang, R. Li *et al.*, "Time-manipulation attack: Breaking fairness against proof of authority aura," in *Proceedings of the ACM Web Conference (WWWW)*, 2023, pp. 2076–2086.

[187] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 910–927.

[188] Y. Wang, Y. Chen, H. Wu, L. Zhou, S. Deng, and R. Wattenhofer, "Cyclic arbitrage in decentralized exchanges," in *Companion Proceedings of the Web Conference (WWW)*, 2022, pp. 12–19.

[189] R. Li, X. Hu *et al.*, "Transaction fairness in blockchains, revisited," *Cryptology ePrint Archive*, 2023.

[190] C. F. Torres, R. 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)*, 2021, pp. 1343–1359.

[191] P. Momeni, S. Gorbunov, and B. Zhang, "Fairblock: Preventing blockchain front-running with minimal overheads," in *International Conference on Security and Privacy in Communication Systems (SecureComm)*. Springer, 2022, pp. 250–271.

[192] X. Zhang *et al.*, "Frontrunning block attack in PoA Clique: A case study," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2022, pp. 1–3.

[193] Flashbots, "Flashbots blocks api," Retrieved from https://blocks.flashbots.net/, 2023.

[194] B. Weintraub, C. F. Torres, C. Nita-Rotaru, and R. State, "A flash (bot) in the pan: measuring maximal extractable value in private pools," in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 458–471.

[195] Y. Wang, P. Zuest, Y. Yao, Z. Lu, and R. 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)*, 2022, pp. 1–15.

[196] P. Praitheeshan, L. Pan, J. Yu, J. Liu, and R. Doss, "Security analysis methods on Ethereum smart contract vulnerabilities: a survey," *arXiv preprint arXiv:1908.08605*, 2019.

[197] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *International Conference on Principles of Security and Trust (POST)*. Springer, 2017, pp. 164–186.

[198] N. F. Samreen and M. H. Alalfi, "A survey of security vulnerabilities in Ethereum smart contracts," *arXiv preprint arXiv:2105.06974*, 2021.

[199] Z. Wan, X. Xia, D. Lo, J. Chen, X. Luo, and X. Yang, "Smart contract security: A practitioners' perspective," in *IEEE/ACM International Conference on Software Engineering (ICSE)*. IEEE, 2021, pp. 1410–1422.

[200] Z. Wang, B. Wen, Z. Luo, and S. Liu, "MAR: A dynamic symbol execution detection method for smart contract reentry vulnerability," in *International Conference on Blockchain and Trustworthy Systems (BlockSys)*. Springer, 2021, pp. 418–429.

[201] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng, and N. Guizani, "Smart contract vulnerability analysis and security audit," *IEEE Network*, vol. 34, no. 5, pp. 276–282, 2020.

[202] S. So, S. Hong, and H. Oh, "Smartest: Effectively hunting vulnerable transaction sequences in smart contracts through language model-guided symbolic execution." in *USENIX Security Symposium (USENIX Sec)*, 2021, pp. 1361–1378.

[203] M. Zhang, X. Zhang, Y. Zhang, and Z. Lin, "Txspector: Uncovering attacks in Ethereum from transactions," in *USENIX Security Symposium (USENIX Sec)*, 2020.

[204] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, E. Lee, and I. Ashraf, "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges," *IEEE Access*, vol. 10, pp. 96 538–96 555, 2022.

[205] M. Raikwar and D. Gligoroski, "Dos attacks on blockchain ecosystem," in *Euro-Par 2021: Parallel Processing Workshops*, R. Chaves, D. B. Heras, A. Ilic, D. Unat, R. M. Badia, A. Bracciali, P. Diehl, A. Dubey, O. Sangyoon, S. L. Scott, and L. Ricci, Eds. Springer International Publishing, 2022, pp. 230–242.

[206] K. Wüst and A. Gervais, "Ethereum eclipse attacks," ETH Zurich, Tech. Rep., 2016.

[207] Y. Marcus, E. Heilman, and S. Goldberg, "Low-resource eclipse attacks on Ethereum's peer-to-peer network," *Cryptology ePrint Archive*, 2018.

[208] B. Nasrulin, G. Ishmaev, and J. Pouwelse, "Meritrank: Sybil tolerant reputation for merit-based tokenomics," in *Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2022, pp. 95–102.

[209] D. J. Moroz, D. J. Aronoff, N. Narula, and D. C. Parkes, "Double-spend counterattacks: Threat of retaliation in proof-of-work systems," *arXiv preprint arXiv:2002.10736*, 2020.

[210] M. 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.

[211] K. Qin, L. Zhou, and A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?" in *IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 198–214.

[212] P. Züst, T. Nadahalli, and Y. W. R. Wattenhofer, "Analyzing and preventing sandwich attacks in Ethereum," *ETH Zürich*, 2021.

[213] L. Heimbach and R. Wattenhofer, "Eliminating sandwich attacks with the help of game theory," in *ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, 2022, pp. 153–167.

[214] Y. Wang, J. Li, Z. Su, and Y. Wang, "Arbitrage attack: Miners of the world, unite!" in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2022, pp. 464–487.

[215] K. Babel, P. Daian, M. Kelkar, and A. Juels, "Clockwork finance: Automated analysis of economic security in smart contracts," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 2499–2516.

[216] B. Pretre, "Attacks on peer-to-peer networks," *Dept. of Computer Science Swiss Federal Institute of Technology (ETH) Zurich Autumn*, 2005.

[217] W. Li, J. Bu, X. Li, H. Peng, Y. Niu, and Y. Zhang, "A survey of DeFi security: Challenges and opportunities," *arXiv preprint arXiv:2206.11821*, 2022.

[218] K. Oosthoek, "Flash crash for cash: Cyber threats in decentralized finance," *arXiv preprint arXiv:2106.10740*, 2021.

[219] J. Huang, S. Han, W. You, W. Shi, B. Liang, J. Wu, and Y. Wu, "Hunting vulnerable smart contracts via graph embedding based bytecode matching," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2144–2156, 2021.

[220] Z. Gao, V. Jayasundara, L. Jiang, X. Xia, D. Lo, and J. 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)*. IEEE, 2019, pp. 394–397.

[221] S. Dos Santos, J. Singh, R. K. Thulasiram, S. Kamali, L. Sirico, and L. Loud, "A new era of blockchain-powered decentralized finance (DeFi)-a review," in *IEEE Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2022, pp. 1286–1292.

[222] B. Mazorra, V. Adan, and V. Daza, "Do not rug on me: Leveraging machine learning techniques for automated scam detection," *Mathematics*, vol. 10, no. 6, p. 949, 2022.

[223] S.-S. Lee, A. Murashkin, M. Derka, and J. Gorzny, "SoK: Not quite water under the bridge: Review of cross-chain bridge hacks," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2023, pp. 1–14.

[224] K. Sai and D. 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)*. IEEE, 2019, pp. 36–45.

[225] M. Herlihy, B. Liskov, and L. Shrira, "Cross-chain deals and adversarial commerce," *arXiv preprint arXiv:1905.09743*, 2019.

[226] A. Sonnino, S. Bano, M. Al-Bassam, and G. Danezis, "Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers," in *IEEE European Symposium on Security and Privacy (EuroSP)*. IEEE, 2020, pp. 294–308.

[227] P. Han, Z. Yan, W. Ding, S. Fei, and Z. Wan, "A survey on cross-chain technologies," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 2, pp. 1–30, 2023.

[228] L. Duan, Y. Sun, W. Ni, W. Ding, J. Liu, and W. Wang, "Attacks against cross-chain systems and defense approaches: A contemporary survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 8, pp. 1647–1667, 2023.

[229] M. A. A. Careem and A. Dutta, "Reputation based routing in manet using blockchain," in *International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2020, pp. 1–6.

[230] Z. Lv, D. Wu, W. Yang, and L. Duan, "Attack and protection schemes on fabric isomorphic crosschain systems," *International Journal of Distributed Sensor Networks*, vol. 18, no. 1, p. 15501477211059945, 2022.

[231] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability," *Cryptology ePrint Archive*, 2018.

[232] Y. Sun, L. Yi, L. Duan, and W. Wang, "A decentralized cross-chain service protocol based on notary schemes and hash-locking," in *IEEE International Conference on Services Computing (SCC)*. IEEE, 2022, pp. 152–157.

[233] C. G. Harris, "Cross-chain technologies: Challenges and opportunities for blockchain interoperability," in *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*. IEEE, 2023, pp. 1–6.

[234] S. Wu, D. Wang, J. He, Y. Zhou, L. Wu, X. Yuan, Q. He, and K. Ren, "Defiranger: Detecting price manipulation attacks on DeFi applications," *arXiv preprint arXiv:2104.15068*, 2021.

[235] L. Su, X. Shen, X. Du, X. Liao, X. Wang, L. Xing, and B. Liu, "Evil under the sun: Understanding and discovering attacks on Ethereum decentralized applications." in *USENIX Security Symposium (USENIX Sec)*, 2021, pp. 1307–1324.

[236] S. Eskandari, M. Salehi, W. C. Gu, and J. Clark, "Sok: Oracles from the ground truth to market manipulation," in *ACM Conference on Advances in Financial Technologies (AFT)*, 2021, pp. 127–141.

[237] P. Winter, A. H. Lorimer, P. Snyder, and B. Livshits, "What's in your wallet? privacy and security issues in web 3.0," *arXiv preprint arXiv:2109.06836*, 2021.

[238] S. Li, F. Xu, R. Wang, and S. Zhong, "Self-supervised incremental deep graph learning for Ethereum phishing scam detection," *arXiv preprint arXiv:2106.10176*, 2021.

[239] J. Wang, P. Chen, X. Xu, J. Wu, M. Shen, Q. Xuan, and X. Yang, "Tsgn: Transaction subgraph networks assisting phishing detection in Ethereum," *arXiv preprint arXiv:2208.12938*, 2022.

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

[241] F. Schär, "Decentralized finance: On blockchain-and smart contract-based financial markets," *FRB of St. Louis Review*, 2021.

[242] Q. Wang, G. Yu, Y. Sai, C. Sun, L. D. Nguyen, S. Xu, and S. Chen, "An empirical study on Snapshot DAOs," *arXiv preprint arXiv:2211.15993*, 2022.

[243] L. Heimbach, E. Schertenleib, and R. Wattenhofer, "Risks and returns of Uniswap v3 liquidity providers," *ACM Conference on Advances in Financial Technologies (AFT)*, 2022.

[244] Z. Wang, X. Xiong, and W. J. Knottenbelt, "Blockchain transaction censorship:(in) secure and (in) efficient?" *Cryptology ePrint Archive*, 2023.

[245] A. Wahrstätter, J. Ernstberger, A. Yaish, L. Zhou, K. Qin, T. Tsuchiya, S. Steinhorst, D. Svetinovic, N. Christin, M. Barczentewicz *et al.*, "Blockchain censorship," *arXiv preprint arXiv:2305.18545*, 2023.

[246] F. Cernera, M. La Morgia, A. Mei, and F. 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.

[247] J. Xu and B. Livshits, "The anatomy of a cryptocurrency Pump-and-Dump scheme," in *USENIX Security Symposium (USENIX Sec)*, 2019, pp. 1609–1625.

[248] K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the DeFi ecosystem with flash loans for fun and profit," in *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2021, pp. 3–32.

[249] D. W. Woods and R. Böhme, "SoK: Quantifying cyber risk," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 211–228.

[250] R. Li *et al.*, "An accountable decryption system based on privacy-preserving smart contracts," in *International Conference on Information Security (ISC)*. Springer, 2020, pp. 372–390.