A Systematic Review of Security Innovations in Decentralized Finance (DeFi) Using Blockchain Technology

Chnar Mohammed Kareem, Ahmed Chalack Shakir
College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq
E-mail: stcm23002@uokirkuk.edu.iq, and ahmedchalak@uokirkuk.edu.iq

Review paper

Keywords: decentralized finance (DeFi), blockchain, security, smart contracts

Received: January 7, 2025

Decentralized Finance (DeFi) represents the new generation of blockchain financial services by developing an open-access financial model without banking or lending institution intermediaries. However, DeFi's open feature threatens its security, making it vulnerable and a target for different attack types. In this systematic review, we present the security of DeFi by selecting fifteen studies from 2020 to 2024 to determine and display the security solutions' effectiveness in identifying the attacks, focusing on various DeFi components such as smart contracts, DEX, AMM, governance, AMM-based DEX, and smart contracts with (DEX, Oracle); detecting different kinds of attacks (e.g., price manipulation, Oracle manipulation, flash loan) using detection tools (e.g., DeFort, CRPWarner, FORAY); we find out that 40% of the selected studies focus on Oracle manipulation attack, 33.33% for price manipulation and flash loan attacks separately, followed by 13.33% for (MEV, rug pull, front-running, Token Leakage, and deep logical bugs), 6.67% for (EEV, reentrancy, sandwich, access control, and state derailment defects). We compare the studies based on the attack type that they detected using four state-of-the-art types of research, such as DeFiScope, FlashSyn, SecPLF, and DeFiGuard; this indicates the concentration of the trend studies is on accuracy and combining AI in DeFi security, or aggregating the existing tools with it, giving an overview of DeFi components' security, underlining the gaps in the attack types that future research can address to build more robust, trustworthy, and secure DeFi systems.

Povzetek: Narejen je sistematičen pregled varnostne rešitve v DeFi z analiziro 15 študij (2020–2024). Identificirani so glavni napadi (Oracle, cenovne manipulacije, flash posojila), poudarjena je vloga AI.

1 Introduction

DeFi (Decentralized Finance) operates on-chain financial services through lending, investing, and borrowing methods that eliminate dependence on central authority management[1]. As is known, regular economic systems restrict individual data access and transmission time to central authorities or financial institutions, creating problems like chargeback scams, costly fees, counterfeiting currencies, and limited system transparency. DeFi represents a monetary system built on blockchain, which has recently experienced strong interest because it operates without permission while maintaining absolute openness and strong participant interaction through innovative contract platforms based on the Ethereum blockchain [2], [3]. The DeFi-oriented lending processes encompass agent borrowing agreements, decentralized peer-to-peer transactions, and leveraged fund management systems that enable users to obtain crypto assets by paying interest [4]. In addition, governance tokens, which are commercial units used in DeFi, represent user participation in decision-making through changes or new functions by using the power of voting in most systems of the vote [4], [5], as an open system remains exposed to attacks, it represents security risks for participant-held assets [6]. The attacks on vulnerable smart contracts led to monetary losses of 6.45 billion dollars despite researchers' attempts to establish secure Decentralized Applications (DApps) [7]. DeFi challenges that prevent it from reaching its full potential are volatility, usability, fraud, and regulatory uncertainty [2]. DeFi protocols run on Ethereum platforms; these protocol contract codes may have vulnerabilities or bugs, and hackers can utilize them to exhaust the providers' funds from the contracts [6].

Another problem is that the rise in liquidity and popularity of DeFi increases the vulnerability risks for consumers due to its natural openness, leading to potential security threats [8] For instance, many DeFi platform vulnerabilities are subject to attacks. In March 2022, 624 million USD by attackers utilizing a backdoor attack to get the signatures of a third-parity validator and four local verifier signatures were stolen on the Ronin Bridge, as the attacks through the Flash loan in 2021 that targeted PancakeBunny and Cream Finance suffered the loss of 200 and 130 million USD respectively, other incidents on

the GREM FINANCE and DEFORCE platforms via reentrancy cause a loss of 54 USD million [9] and other attacks that continue and increase day by day as a result of the DeFi growing technology with these challenges in DeFi as a new modern technology, enhancing it concurrently by forecasting research and exploring these challenges, depending on blockchain technology to provide innovative solutions in decentralization, tracking, security, and transparency without intermediaries. In this study, we try to determine and show the evaluation of the security solutions in DeFi using blockchain technology through various studies, focusing on how these solutions detect vulnerabilities and attacks and maintain security within different focusses for DeFi elements, like Automated Market Makers (AMMs), Decentralized Exchanges (DEXs), smart contracts, and governance, systematically examining and comparing the security methods utilized in each study that enhance DeFi security in various domain and possibility of leveraging those security methods to other DeFi field such as donation, or combining them for better security approach on DeFi; the review structure follows: Section 2, Background; Section 3, Research Methodology; Section 4, Results; Section 5, Discussion; and Section 6, Conclusion.

2 Background

2.1 Blockchain

The central construct of blockchain technology works via its cryptocurrency systems. Bitcoin stands as the leading standard offered by Satoshi Nakamoto in 2009, performing as a distributed ledger that saves transactions in an open, secure, and irrevocable log through a network of computers [10]. It is a distributed database that executes and follows transactions with allocated nodes. Transactions are stored in connected blocks like a chain in an unchangeable manner, maintaining data privacy, integrity, and confidentiality [11], and it achieves security through decentralization, transparency, and permanent data characteristics, which gives network participants trust in the system [12]. Each block contains a block header in addition to its body, which makes up the minimum components of a blockchain system. Furthermore, the block header has: Nonce, Hash value, Hash value from the preceding blocks, Merkel root, A version number, and Timestamp; the block body contains a binary tree familiar as the Merkel tree, with its root constructed by the transaction hashes [13], as demonstrated in Figure 1. Hashing employs a precise algorithm to generate and change input data of any length into a fixed-length string [14], functions through a consensus mechanism for verifying and processing transactions via nodes and agreement decisions; the most popular consensus algorithms are proof-of-stake (PoS), proof-of-work (PoW), and Practical Byzantine Fault Tolerance (PBFT) [15].

Generally, there are two categories of blockchain: private and public; a private blockchain authorizes companies and organizations to operate blockchain without disclosing their data publicly. Additionally, a public blockchain, on the other hand, is an open and well-known network from which anyone can download the rules through reading, contributing, or posting on the network, resulting in its dispersed and decentralized nature. Ethereum is a decentralized public blockchain framework, not constrained by anyone, which means it is independent [16], [17]; multiple fields apply blockchains, such as health, education, and finance [18], supply chain, voting, real estate, and other domains, this technology provides benefits like robust security, cost-effectiveness, fast transactions, and keeping records transparently, assuring data is tamper-proof through cryptographic hashing, where each block contains the previous block hash and the transaction is validated through network participants and implemented before adding it to the blockchain, ensuring decentralization, protecting data privacy and security, removing intermediaries, and supporting transaction ability [19].

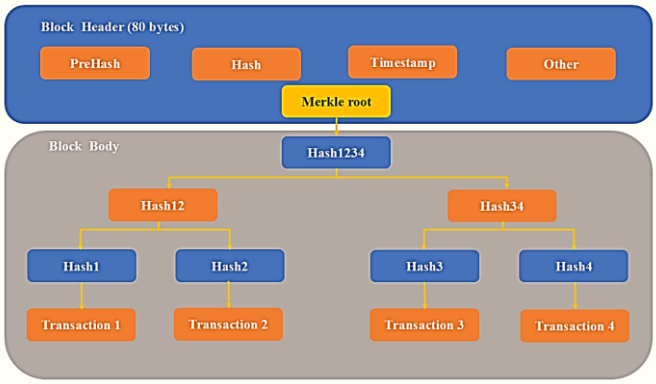


Figure 1: The blockchain Merkle tree content [75].

2.2 Blockchain platform for DeFi

DeFi finds wide applications through innovations like crypto loans, decentralized exchange, P2P lending, etc.; these applications are accessible on different blockchain platforms used for DeFi applications and provide unique advantages, such as:

Ethereum is a protected, public, decentralized blockchain technology for smart contract performance. Through its mechanism, developers create arbitrary applications that standardize operations, basing their designs on consensus features that enable interoperability at scale and streamline development processes. It also implements the blockchain paradigm, which is cryptographically secure and has processes that everyone can access.

Binance Smart Chain (BSC) is a sovereign blockchain that provides users and developers with safety and security; as a native dual-chain interoperability, it facilitates cross-chain communication and scales up the performance of DApps built on 21 validators that confirm transactions, offering decentralization and enabling smooth community involvement through validation.

Solana is a model of blockchain that relies on proof-of-history (PoH) to prove the rank and the transit of periods within events; the leader functions and arranges communications to boost throughput, and the node is handled as a leader to generate a PoH sequence, which gives verifiable passage of time and read consistency. The system also uses a cryptographic hash function whose outcomes are impossible to predict without running the function, which ensures the PoH sequence's integrity. However, relying on a leader node may introduce risks if the leader is compromised.

Cardano is a blockchain project that launched in 2015 to alter the manner of cryptocurrency evolution and construction. Some principal designs of Cardano include the separation of computation and accounting into different layers implemented in a highly modular function of core components, relies fundamentally on capitalizing on these findings to improve the current state of cryptocurrencies using a proof-of-stake consensus mechanism, which ensures security by requiring validators to hold and stake the native cryptocurrency, reducing the risk of malicious behavior.

Avalanche is a high-performance, customizable, secure, and scalable blockchain platform that targets highly scalable and distributed applications and provides security to the blockchain system by withstanding more than 51% of attacks (51% of the miners are attackers), where one subnet validates each blockchain offering many advantages, including compliance, trusted validations, and reduced network traffic.

Polygon is a structured framework for joining networks to establish an appropriate Ethereum blockchain network. By combining networks, Polygon employs security as a service; the security layer is an optional and specialized layer offering a set of validators to verify periodically that Polygon blockchains are legitimate.

Fantom is a directed acyclic graph (DAG) built on a smart contracts platform that aims to address the scalability issues of existing publicly distributed ledgers and takes the Lachesis protocol as a new protocol known to maintain consensus; employing DAG technology helps to provide high reliability for transactions; furthermore, it breaks the sequential processing of transactions; the Lachesis protocol uses asynchronous Byzantine Fault Tolerance (aBFT) to ensure security and enable networks to achieve consensus even with malicious nodes present [20].

While multiple blockchains support DeFi, Ethereum remains the most common platform for DeFi due to its smart contract functionality, proven security, and ability to supply decentralization, interoperability, and scalability; the Ethereum frameworks are the most significant platforms facilitating application establishment in specific fields. In addition, since the Ethereum blockchain integrated with finance more effectively, the appearance of Ethereum and blockchains within smart contracts capabilities led to the evolution of decentralized applications (DApps), opening new opportunities for innovation [7]. Any individual in the Ethereum chain can propagate their DApps and contact others; DeFi technology in the finance field is gaining more interest [18], becoming the most common application in the financial area and supplying a broad financial service [9] Table 1 below shows a summary of the key features of different blockchain platforms [20]. However, within Ethereum 2.0, the risk of Miner Extractable Value (MEV) presents the biggest threat to decentralization, as validators may gain by changing the order of transactions; MEV can result in validator centralization as it advantages well-resourced validators over standard ones; collecting MEV includes significant funds, computational resources, and intelligence that ordinary validators may not have [21].

2.3 Smart contract

It was a term coined by Nick Szabo in the mid-1990s; its features are automated, immutable, and self-enforcing; smart contracts offer security in a way that traditional contract agreements cannot provide [22]. It is simply an agreement between the various parties involved in the application, who have closed the smart contract code; they activate automatically if certain conditions are met in the agreement [23]. In general, smart contracts have several properties that enable them to be known to each peer in the blockchain, implement themselves, not be stopped, and fit various requirements, as illustrated in Figure 2 [24].

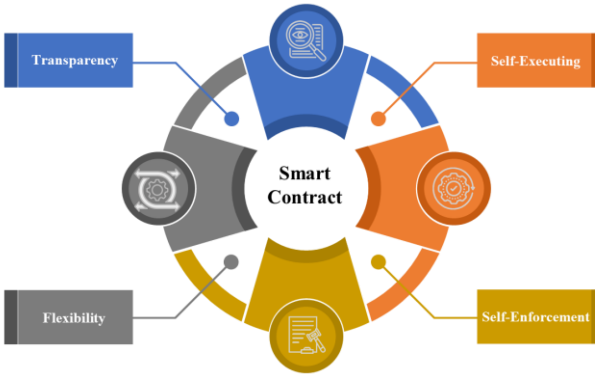


Figure 2: Properties of smart contracts [24].

2.4 Decentralized finance (DeFi)

Financial services developed on Ethereum blockchain smart contracts are referred to as Decentralized Finance (DeFi) [25], [26], stating all terms in financial services and products without relying on intermediaries or institutions; it generally depends on decentralized applications and public protocols [27], [28]. It's also the most common application used in the financial industry to provide various services. DeFi presents a variety of types of applications, such as buying assets linked to the United States dollar (USD), known as stablecoins, on a decentralized exchange, transferring these assets to a decentralized lending platform to collect interest and apply them to a decentralized liquidity pool, or depositing money directly on the chain. In addition, the core of all DeFi applications and protocols are smart contracts that describe a small application stored in a blockchain [2],

representing a monetary system established on public blockchains. The features of available finance services are decentralized applications (DApps), digital assets, smart contracts, and protocols constructed on the blockchain, as shown in Figure 3 [29]. When the DeFi applications start running on the blockchain, the smart contract modifies the transaction state that attackers may exploit, which would cause irreversible harm to DeFi, so making the contracts more secure is critical [7].

Figure 3: Decentralized Finance components [29].

Financing: In the financing sector, DeFi sustains separate models: prepayment financing, receivable financing, and inventory financing. Newly, many requests for small-to-medium enterprises (SMEs) have been made in financial operations worldwide, and they face a serious challenge in funding due to poor creditworthiness and unreliable company information. Blockchain technology proposes a solution with DeFi features, ensuring data transparency and security, enhancing trust between financing parties using smart contracts on Ethereum, facilitating real-time monitoring and accurate data collection, improving SME information's credibility, and simplifying investor financing access [30].

Supply Chain DeFi can strengthen the supply chain systems based on DeFi properties on the blockchain, which is robust for traceability. Such a system contains planning, services, distribution, acquisition, and storage, where the data is saved in a block, indicating that each supply chain link is tamper-proof [30]. Supply chain finance (SCF) also reduces costs and enhances employed capital by allowing sellers and buyers to optimize their working capital in trade transactions. Combining DeFi with the SCF introduces a range of attractive opportunities that can transform how businesses interact and work within the supply chain ecosystem.

Table 1: Comparison of blockchain platforms' security for DeFi applications [20].

Platform	Features	Security Mechanisms	Advantages of DeFi Applications
Ethereum	Decentralized, smart contract, and secure	Cryptographically secured and single-instance machine.	Developer-friendly and expandable
BSC	Sovereign blockchain and dual-chain.	A total of twenty-one validators	Cross-chain with decentralized governance
Solana	PoH and high throughput.	PoH sequence and a cryptographic hash function.	Large capacity and quick execution
Cardano	Modular and separation accounting.	PoS, the validators hold and stake cryptocurrency.	Improves the design and energy performance
Avalanche	It is Adjustable and scalable.	Subnet-based validation 51% attacks.	Expandable and reduces the network bandwidth.
Polygon	Ethereum-compatible framework.	Security layer with the validator.	Scalable for Ethereum DApps.
Fantom	DAG and Lachesis protocol.	aBFT for malicious node tolerance.	The transaction is reliable and efficient.

2.5 DeFi applications in Ethereum

In this section, we present some of the DeFi applications on the Ethereum blockchain to help the reader understand many DeFi applications by explaining them so they can understand them, such as:

Thanks to smart contracts, decentralized platforms, and the use of the blockchain system, DeFi can address issues that traditional SCFs, those oriented toward providing access to finance, traceability, transparency, improved efficiency, and process automation, can face

challenges when they include restricted financing, inefficient operations, and a lack of transparency [31].

Loan DeFi has significantly lowered the barriers to financial services, and one of the many DeFi trends in Aave 2020 is the launch of flash loans; these loans permit borrowers to acquire any amount of equity without collateral and for a fee of only 0.09%, unlike conventional loans, which need collateral to secure the borrower, flash loans feature instant borrowing and disbursement in one transaction; if some conditions are not satisfied, the deal will regenerate, and the borrower funds will not be at risk. Flash loan security depends on smart contracts and blockchain technology, which are irreversible and immutable; this modification offers mortgage loans and increases access to credit institutions. However, Flash Loan as a DeFi application employs loan services: The borrowers repay and borrow the funds with the same transaction, which implies that after getting funds, the borrower must use them immediately to pay back and turn a profit on the loan. In this manner, if the borrower defaults on the loan or any conditions in the smart contract are not met, the transaction will roll back, and all things will go back to the situation before borrowing without collateral, and the lender does not have to worry about lending risks; because of the blockchain and smart contracts' characteristics of non-repudiation and tamper-proof, Flash loans enable security and feasibility. Neither lender nor borrower can cheat or change the terms; as a DeFi application, Flash Loan gives new services of loans using blockchain technology, even without collateral, with a low fee and without worry of risks by borrowing funds through Flash Loan DeFi increases the number of customers and significantly lowers the bar on loan services [30].

Stablecoins are one type of digital currency that maintains stability for fiat currency and crypto assets, which differs from Ethereum and Bitcoin, except that they have minimal price fluctuations, with their resilience correlated to traditional currencies such as fiat and gold [30]. There are four properties for stablecoins: tokenized, meaning that a smart contract manages cryptocurrency tokens; convertible, which allows conversion to another currency or the pegged asset; tradable, which enables direct trading between parties; and fungible, meaning units of financial value with a bit of pricing volatility regarding their pigged assets or index. They use most of the stablecoin applications, and they can develop with different characteristics [32].

Charity Projects Describing the utilization of DeFi in various Ethereum applications, such as supply chain, banking, and finance, with the leverage of the Ethereum blockchain and smart contracts in the donation field, taking advantage of transparency, which earns donors' trust and simplifies the use of money [33]. DeFi can integrate two methods: the variable, non-linear process of the UniSwap decentralized exchange (DEX) coin system for secure offerings [34].

2.6 Real-world operation of the DeFi application

DeFi applications concentrate on financial services. DeFi covers a wide range of application sectors [35], such as:

Decentralized Exchanges (DEXs) enable users to exchange digital assets using their wallets through a supervision-resistant platform in parallel without any custody for exchanging tokens, as UniSwap allows users to trade tokens without any middleman involvement because DEXs provide users with lower fees, asset control, and privacy, attracting more users and higher volumes than centralized exchanges [36], enabling cryptocurrency users to offer exchange liquidity and earn transaction fees using AMM algorithms. A DEX does not require centralized management because it handles liquidity through AMM algorithms. In contrast, the different decentralized liquidity pools present opportunities for investment and profit but expose shareholders to risks that must be analyzed and managed [37]. DEX with AMM protocols is the most familiar DeFi application, which provides benefits like continuous liquidity, decentralization, and automation, where the word AMM refers to the algorithm of a protocol, while DEX refers to the application or protocol use case; as for blockchain-based DeFi, there are order books-based DEX, such as dYdX and Gnosis, which do not depend on AMM algorithms, with the use of AMM-based DEX, one must consider security and privacy into account; being a distributed, complex system with different hardware and software elements communicating together; AMM-based DEX is particularly susceptible to interface attacks [38].

Automated Market Makers (AMMs) are essential in DeFi for liquidity and DEXs by implementing protocols such as Balancer and UniSwap to ease liquidity pool trading and determine asset costs, improve DeFi market expansion and liquidity by boosting price detection, trading, and liquidity [36], supplying liquidity algorithm by determining users' funds and setting prices using a conservation function, in this liquidity, two base actors consist of the general mechanisms of the AMM: the first is called liquidity providers, who contribute funds to the assets pool, and the second is known as traders, who interchange assets for another, and the exchange rate between structured assets depends on the amount desired for trading. The most vital AMMs enclose Bancor, Balancer, Curve, and UniSwap [39].

Decentralized (Lending and Borrowing) DeFi services, such as borrowing and lending, allow organizations and individuals to earn interest by borrowing digital assets, giving cryptocurrency loans to consumers, and acquiring stakes; meanwhile, the borrowers ensure their valuables on these platforms, replacing traditional banking because of their quick accessibility and sensible cash interest rates [36].

Synthetic Assets and Derivatives establishing fiat currencies, evolution, trading, duplicating equities, and switching commodities formed the protocols of synthesizing assets in the Synthetix, which reduced the need for intermediaries, enabling hedgers and DeFi

investors to access different assets through mirrors and Synthetix protocols despite intermediaries, people can look for traditional financial market exposition to choose synthetic assets for availability, liquidity, and flexibility possible in controlling their transactions and financial services. This application democratizes monetary services and enables considerable financial participation throughout a wide range, as it continues developing and growing [36].

Yield Farming and Liquidity Mining are practices where intensive users share their tokens to supply passive liquidity to DeFi platforms. Yearn and Curve Finance reward consumers who deposit assets into liquidity mining and stake tokens into governance systems or contribute to the liquidity pools. Yield farming is users' most common strategy to increase profits and earnings from passive income [36].

Governance Tokens and Decentralized Autonomous Organizations (DAOs) emerge as member-owned communities without central management, governed via the principle of democracy, and individuals determining decisions together, whereas in DAOs, voting power tends to be expressed by held tokens, and the proposal implementation follows the voting process. Most DeFi projects have an associated governance token where people can vote based on the level of activity in the service. Tokens have to be classified by regulatory authorities. To decentralize governance partly, token holders can offer limited voting rights, and the developers may not be required to make changes if they hold many tokens on the platforms related to ideas and policies. The governance often incorporates communication in both formal and informal forums. Moreover, DeFi protocols persist on the Ethereum blockchain and have a form of participation where individuals can vote on issues affecting the blockchain. A quorum is needed to pass votes, which can cancel the proposal, as the decentralized governance in blockchain and DeFi applications introduces significant risks. It's even feasible to attack a protocol that enables users to borrow many governance tokens permanently, but just enough to vote against other users. The DeFi protocol's pseudo-decentralized governance operates by a few users having governance tokens, which causes concern about the token concentration, where the governance token holders may not be the only factor considered in DeFi applications or blockchain protocols, as some organizations with voting authority may affect the decisions [40].

2.7 DeFi challenges

Besides the benefits of DeFi, it faces various challenges as a new technology. This section lists some of these challenges, explains them for clarification, and helps future researchers address them and find solutions to improve the use of DeFi. The challenges are:

2.7.1 Regulatory

It provides financial system stability and security, as the DeFi platform's decentralized nature and the lack of central authority present challenges and make it hard to apply Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations, allowing criminals to utilize DeFi for their illegal activities, and it contains DeFi services that present significant risks as they do not require identity verification or creating an account [41]; utilizing Zero-Knowledge Proofs (ZKPs) could overcome regulatory challenges, enabling people to execute transactions and keeping privacy for sensitive details to improve security in DeFi ecosystems, the ability to maintain confidentiality and verify the information is crucial, whereas, in peer-to-peer transactions, trust and protection are essential by combining blockchain and ZKPs, DeFi platforms can follow regulatory requirements like AML and KYC without exposing user privacy, for instance, ZKPs can qualify the user to confirm their residency or age without revealing their address and birth date, observing General Data Protection Regulation (GDPR) that imposes lowering data demands [42].

2.7.2 Scalability

Blockchain networks determine the scale of diverse DeFi outlets, so platform creators lean on layer two scaling to handle expanding volumes efficiently, as the network's transaction allocation system faces difficulties when users conduct multiple transactions due to the fee costs that can delay the network procedure. Recently, the asset platforms of DeFi processes were separated, which restricted communication among them, as enhancing interoperability and scalability is critical to improving user experience and making DeFi development [43]. The speed and durability of transactions on blockchain infrastructure depend on its network bandwidth and growth rate because AMM-based DEXs exist on this platform. All DEX transactions depend on time to be verified on the blockchain network before they become activated. The verification operation relies on the validators or miners instead of DEX; unlike Centralized Exchange (CEX), which executes transactions immediately, DEX incurs a process delay in transactions from seconds to hours. Various blockchain networks with velocity requirements were created (e.g., EOSIO, Tezos, XRPL).

On the other hand, the blocks utilized for storing data on DEX transactions limit the total number of transactions that DEX can approve per patch, and their throughput is still far behind CEX. Several multi-layer blockchains, such as layer-2 blockchains, were presented to fix the throughput problem [38]. The blockchain network Ethereum, which hosts the most DeFi applications, finds difficulty with the requests growing due to the rise of the DeFi platform's usability and popularity, especially for users whose price is out by excess gas fees; DeFi platforms may become inefficient during intervals of network congestion, it limits the ability and lowers the efficiency of DeFi to challenge regular financial systems that can process transactions with minimum costs and much faster; several solutions, such as alternative blockchain networks like Solana and Polkadot and layer-2 scaling technologies, handle these limitations, but the adoption and development are still early, as DeFi platforms will struggle to reach their potential until the scalability issue is solved.

Zk-Rollups and Optimistic Rollups are layer-2 protocols that ensure the final arrangement on the main blockchain by processing off-chain transactions, reducing fees, and expanding transaction throughput, making DeFi serviceable for everyday transactions and its application availability.

A ZKP solution creates transaction assurance through privacy enhancement methods that do not require disclosure of full details. The global adoption of DeFi involves applying those technologies to manage existing limitations [44].

2.7.3 Security

DeFi security is related to three characteristics: infrastructure risks, failure in interdependence, and smart contract vulnerabilities. All services and applications that DeFi offers are built on smart contracts to handle users' finances, indicating that more funds are associated with these contracts, making them more targeted by the attackers, as their code is composed by any person who can find a bug in it and steal the funds inside it, thus, contract developers should concentrate on designing such a contract, testing it, and auditing its security before deploying it on the blockchain, another security issue is the infrastructure, which needs to be considered through the design of DeFi applications, checking that no congestions exist on the network because loaded networks could miss out on members' queues, leading to not storing valid transactions by honest members. Therefore, the main feature of consensus affects the attributes of the application's security [45]. A critical part of DeFi security is exploring vulnerabilities as they happen or before they occur (i.e., preventative), and common vulnerabilities include these parts:

- Deployment of malicious.
- Attack execution.
- Fund extraction.

Hackers used private pools to withdraw $197 million from Euler Finance. Yet, they established the malicious smart contract a few blocks before the attack transaction began, giving them a critical opportunity for prevention and intervention; another example is the attack on the Rubic exchange incident, resulting in a $1.4 million loss, the attackers released a malicious contract and immediately executed the attack transaction after deploying it with private pools [46], another example of attacks, in February 2020, DeFi protocol bZx suffered from two sequential attacks; the attackers utilized the logic flaws in bZx to accomplish arbitrage at a low cost (i.e., robbing over $8 million ETH at that time), this is not an isolated event, in April 2020, another DeFi protocol, UniSwapV1, was compromised by cybercriminals, stealing 1,278 ETH through exploiting a reentrancy vulnerability attack that arises on DeFi protocols approximately every few months. More than $130 million was also lost when Cream Finance experienced an external attack [47].

2.7.4 Oracles

Different DeFi products depend on external information, such as exchange prices that Oracle supplies. These data in Oracle affect the user and the contract's behavior, and the challenge appears when transforming that exterior data from outside into the chain, on which DeFi product security relies on the precision, credibility, and validity of information from Oracles. Thus, an Oracle is valued based on its liability, transparency, and required trust levels [48]. However, Many DeFi activities, including tampering with Oracles and delivering faulty information to smart contracts for personal benefits; an instance of an Oracle attack that includes modifying the token price denoted by the Oracle from an attack on the Venus Protocol, where hackers used 900,000 XVS tokens to extend the price referenced from the Venus Oracle by (US$80 to US$145) via a hack on the Venus protocol, taking (US$77) of the system [49]. In addition, on February 2nd, 2022, a wormhole, which is a multiple-purpose cross-chain that supports about 35 blockchains, hacked Solana by leveraging a bug in the wormhole smart contract on Solana, letting the attacker make an arbitrary verification payload, execute one transaction, and mint 120,000 wETH, worth around $350 million on Solana [50]. Also, the NFT game Ronin and DeFi cross-chain Wormhole Network hackers attacked them with $611 million, and $622 million serially disappeared. According to the REKT database, the DeFi protocol lost $77.1 billion due to hacks, scams, and vulnerabilities, and only $6.5 billion has been returned [47]. Oracle also presents a danger to the investor's funds in DeFi to keep the liquidity available for the user to trade, making them independent of counterparties and minimizing the risk of market manipulation, a solution called the function Oracle and the AMM, which is an entity programmed to serve as an intermediary between the AMM and Oracle it maintains the pool that returns and collects a user-wrapped premium; function Oracle provides a dynamic discovering price mechanism that modifies user evaluation, enabling price flexibility even when the counterparties are absent [51]. Therefore, Oracles serve as a critical component for properly functioning DeFi protocols. Price Oracles provide crucial information that impacts the execution of smart contracts and their results; for example, the DeFi protocol Compound gets the Oracle price from many resources, like the centralized Oracle service suppliers Chainlink, and the price of trading assets from UniSwap as a decentralized protocol.

On the other hand, the values of those resources may differ from the actual data; when the price of a digital asset varies, determining the asset price can be difficult [52]. There are multiple types of Oracles: a decentralized Oracle gets the data on-chain, e.g., from other DeFi protocols, and the centralized Oracle depends on a reliable third party, which violates the DeFi concept; for instance, a decentralized Oracle may obtain the swap rates between tokens from an AMM-based DEX. However, this method is vulnerable to manipulation attacks that alter the price of DeFi protocols called Oracle attacks [53], or on-chain Oracle manipulation, which emphasizes the importance of

automatic tools like DeFiPoser and DeFiRanger, which are tools with the capability of addressing the vulnerabilities of Oracle manipulation [54]. Other studies suggest Over, an automated approach for assessing Oracle variance and its effects on DeFi smart contracts, and provide a smart contract protocol source code and the scope of certain Oracle variables in the contracts by automatically examining its source code to get the protocol summary for a secure requirement to the protocol, identify the best way to set essential control parameters in the contract, this will ascertain that the produced contract continues to meet the need of constraints, even when Oracle deviations arise [52].

2.7.5 Liquidity

It is well known that DeFi produces market volatility through its speculative platforms and exposure to market volatility. The price of assets changes on DeFi platforms because the platforms depend on the liquidity pools as their transaction facilitation method. Users may face difficulties executing transactions and accessing their funds because of the changing liquidity levels in DeFi systems. Communication within traditional finance and DeFi may increase these issues. The Liquidity Constructions of DeFi impact the change of regularity in financial markets, mainly if a link exists among financial sectors [55]. That results a temporary loss that appears due to AMM, which only affects the Liquidity Providers (LPs) to AMM DEX and consumer services to the protocol of yield farming that utilized liquidity provisions AMM, DEX in their approaches, and gets worse because of the cryptocurrency volatility and prevented by giving equal or similar values to token pairs liquidity, such as synthetic tokens targeting the same value (e.g., a pair of USD stablecoin) or synthetic tokens and their target tokens (e.g., native tokens), another attack targeted liquidity the Just In Time Liquidity (JIT) which is one of the Miner Extractable Value (MEV) attacks appears at the Concentrated Liquidity AMM (CLAMM), which refers to the improvement to AMM that increases the efficiency of the capital in the liquidity pool, introduced by UniSwap V3, letting the LPs define the price domain, for instance, in UniSwap V3, one of the transactions implemented the JIT attack, that will withdraw liquidity within the pool by splitting the transaction into smaller units, it is secure against MEV attacks [53].

2.7.6 Transparency

The blockchain implements and saves transactions redundantly, fostering transparency and trust in executing transactions, presenting significant constraints for individuals and institutions, as the visibility of publicly recorded transactions affects the institution and users, which increases when critical information is transparently stored, such as Centralized Exchanges (CEXs) from KYC processes can use metadata, patterns of transactions, and business information to remove anonymous users. Despite many blockchains ensuring pseudonymity, which increases risks of violating data protection regulations, such as antitrust laws or the GDPR, when working on DeFi platforms, for example, a competitor who can observe the competitor's financial transactions of an institution raises a risk. Also, the economic challenges due to the transparent implementation of transactions, known as Extractable Value (EV), are some of the well-known examples of front-running attacks; one of the EV examples occurs when block arbitrageurs or producers exploit volatile prices in the mempool from publicly visible transaction data, for instance, an arbitrageur buys a token before a large DEX transaction request and sells it when the price rises, gaining profit from the margin; presenting solutions like ZKP's Privacy-Enhancing Technologies (PETs) and gradual decryption to reduce these challenges in cryptocurrencies, combining transparency with economic exploitation and information protection [35].

3 Methodology

We used a systematic review on "security innovations in Decentralized Finance (DeFi)" guided by the methodology specified by Okoli and Schabram [56]. The sections below describe the methods applied throughout the review. The study aims to review research studies related to security in DeFi and identify research gaps consistent with the study objective of determining and evaluating security solutions to identify attacks in DeFi using blockchain technology.

3.1 Research questions

We define our research questions to be answered through the review based on the study objective as follows:

Q1: What type of attacks affect DeFi security?

Q2: What solutions do the studies offer to address those attacks?

Q3: How can those security solutions enhance the security of DeFi platforms?

3.2 Search technique

In this study, we used a scientific database with established reputations, such as Google Scholar, ACM digital library, and IEEE Xplore, typing relevant keywords to the subject, such as "DeFi security", "DEX security", "DeFi security on the blockchain", "AMM security", "DeFi smart contracts security", and "Governance token security" or "DeFi and Governance token security", gathering studies about DeFi security. The study contained primary publications from 2020 to 2024 to provide the most up-to-date and accurate research findings for evaluation.

3.3 Inclusion and exclusion

This section includes papers handling questions, with the review concentrating on the security solutions they utilized in DeFi via blockchain technology. It employs and evaluates the criteria for the exclusion and inclusion of the selected studies for applicability and quality, retaining

them based on their titles, abstracts, and relevance to the review subject, as illustrated in Table 2.

Table 2: Inclusion and exclusion criteria of related studies.

Inclusion	Exclusion
Studies published from 2020 to 2024.	Studies publicized before 2020.
Open access.	Duplicated records or not fully available text.
Written in English.	Not in English.
Studies related to DeFi security, like AMM, DEX, AMM-based DEX, governance tokens, and smart contracts	Studies are irrelevant to DeFi security in blockchain or do not include DeFi-based blockchain.
Journal, conference, and preprints	White paper with books and editorial comments.

3.4 Data extraction

The review selected appropriate and relevant data with a focus on DeFi security by selecting studies and including them based on inclusion criteria that analyzed and processed different data from the studies to the security of DeFi components like DEX, smart contracts, AMM, governance tokens, and encompassing fifteen studies referenced in [8], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], and [70].

3.5 Data analysis

By employing a data extraction model, we abstract information from the studies and construct a form based on five components for examining and evaluating throughout the review. The selected papers have already determined three key themes via research questions, including the types of security attacks, proposed solutions, and their effectiveness in improving security in DeFi, as displayed below the five elements of the form in Table 3.

Table 3: Data extraction elements from the form.

Items of Data	Definition
Title	Papers title
Year	Publication year
Authors	Name of the authors
Country	Country of the researchers
Type	Conference, Journal, and Preprints

4 Results

This section outlines the results from 15 studies that we found in the systematic review, demonstrating the DeFi components (AMM, DEX, AMM-based DEX, and smart contracts), the vulnerabilities they handled, mitigation approaches, and evaluation procedures, followed by Table 4, which provides a contrast between the studies for better understanding. Figure 4 below shows the process of including the studies, eliminating 15 of 225 studies because of duplication, 210 records remained for screening then 115 were incompatible via their title and abstract, 60 studies were already analyzed at that time, removing another 45 studies since they did not include enough information for the review, in the end, we choose fifteen studies for to the review incorporated into the data extraction phase, as displayed in Figure 4.

4.1 Graphical distribution and publication years

Various studies analyzed the security challenges they handled in DeFi through blockchain technology, including 15 relevant studies, as demonstrated by the publication years in Figure 6. Seven were published in 2024, four in 2023, one in 2022, one in 2021, and one in 2020, as illustrated in Figure 5, indicating that adopting blockchain technology for the security of DeFi remains in its earlier phases and is evolving. On the other hand, Figure 6 shows the appearance of China (46.7%), the United States (26.7%), the United Kingdom (13.3%), and India and Singapore each produce (6.7%).

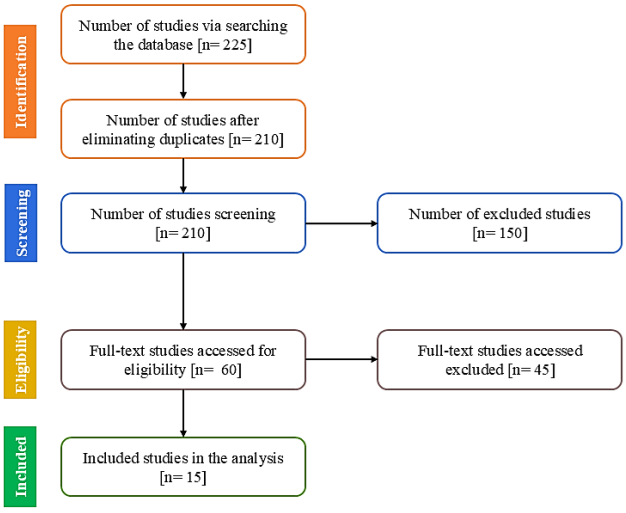


Figure 4: Review process flowchart.

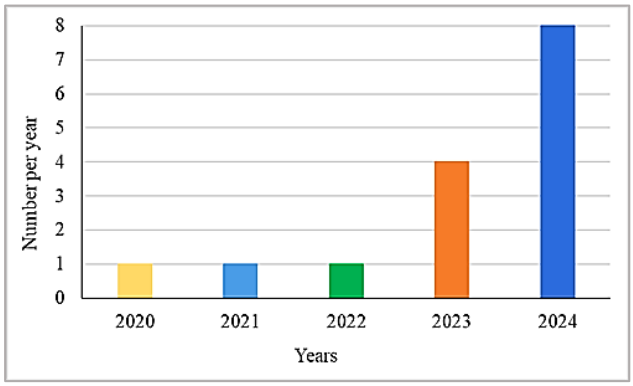
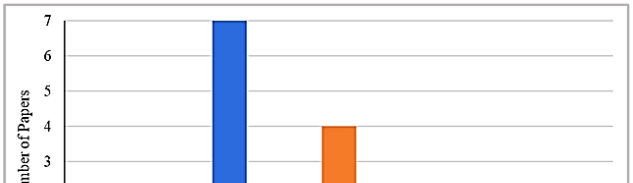


Figure 5: Publication year for the selected studies.



4.2 Publication source

The research publications distributed themselves across seven conference venues, four journal publications, and four preprints, as shown in Figure 7.

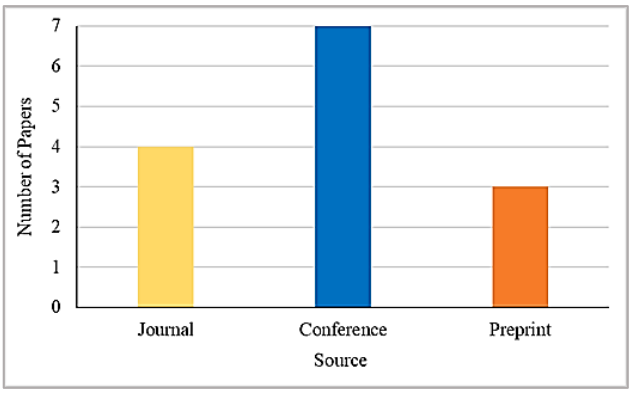


Figure 7: Review distribution by publication source.

4.3 Summary of the studies

• Amit Kumar et al. [8]. Explained in their study how to detect vulnerabilities in DeFi by using BLOCKEYE, due to the lack of existing tools to determine the vulnerabilities related to Oracle dependency like Codefi, by focusing on protocols that are processing on the Ethereum platform, such as Synthetix, Kyber, and UniSwap, via static analysis and dynamic monitoring transactions at runtime, combining SERAPH symbolic analyzer reasoning about Oracle asset feed, the examination of eight real-world DeFi protocols does not show any false positives or false negatives compared to Codefi. Yet, it does not address the scalability challenges to employ it across different blockchain platforms (e.g., BSC, Solana, Avalanche, etc.) and its possibilities to utilize it with other DeFi models such as AMM, DEX, governance tokens, etc.

• Zecheng Li et al. [57]. The authors introduced SolSaviour, which executes voting mechanisms and a Trusted Execution Environment (TEE) cluster to protect DeFi protocols and deploy smart contracts from attacks and vulnerabilities. The study manages the vulnerability issues in deployed DeFi and smart contracts employing a Trusted Execution Environment (TEE) cluster and voting mechanisms by examining 12 real-world vulnerable smart contracts, such as Fei protocol, DAO, and POWH coin, and mitigating the attacks to 2.3% for Fei protocol, 6.5 for DAO contracts, and PoWH coin to 0%, as d=for latency around 6.7%. However, it possessed restrictions like TEE dependency risks and manual patching requirements, with the study focusing on its two core VoteDestruct and TEE cluster, implementing more research to address how to protect the framework from possible attacks that may arise from the core contents, like a failure of one point in the TEE cluster and the manipulation or governance attack.

• Siwei Wu et al. [58]. Proposed an independent platform called DeFiRanger to determine price manipulation attacks by developing Cash Flow Trees (CFTs) and applying low-level semantics to advance DeFi's actions, such as deposits, withdrawals, and transactions through crossbreed approaches, identifying a pair of attacks: manipulated prices for the DEX pool, and attacks targeting weak DeFi applications that rely on manipulated price Oracles, examining 41 real-world, actual incidents, reaching 0.996 precision and 0.962 True Positive across 15.272 transactions; but it detects the attack types depending on external data, the possibility of false positive and negative which restricting the analytical scope, as the complex nature of the DeFi environment when new attack type rises.

• Conor McMenamin et al. [59]. Present FairTraDEX, a decentralized exchange protocol that uses Frequent Batch Auctions (FBAs) to supply formal game-theoretic assurances against extractable value, addressing the Expected Extractable Value (EEV) where players inject order or censor to obtain profits that UniSwap DEX suffered with, by duplicating key characteristics of an FBA with a various set of zero-knowledge protocols and escrow-enforced commit-reveal mechanism, protecting against EEV and execution costs, guaranteeing a fixed fee model independent of order sizes for large retail users seeking to avoid prohibitive execution costs. However, it does not fully address how the protocol will operate in irrational behavior of market manipulation, which is common in many trading environments.

• Zewei Lin et al. [60]. Proposed an automated analysis method that assesses the risk of contract-related rug pulls called CRPWarner, which decompiles the Ethereum Virtual Machine (EVM) bytecode, builds a Control Flow Graph (CFG) and operates a domain-specific datalog analysis, employing three types of contract-related rug pulls: hidden mint function, limiting sell order, and leaking token, by establishing a border classification of rug pull behavior through manually analyzing 103 real-world rugs pull events, addressing rug pulls in contracts, and transactions-related rug pulls as primary types. As a result, CRPWarner achieved 91.8% precision, 85.9% recall, and an 88.7% F1 score, exploring a broad dataset of 13,484 real-token contracts on Ethereum; still, as the method shows, it just offers static detection for contract-related rug pulls; it can't provide real-time monitoring, limiting its capabilities to inform users after the contract deployment.

• Wenkai Li et al. [61]. Present DeFiTail, a technical DeFi check framework that learns the invocation patterns in data paths using Deep Learning (DL) to solve invocation pattern learning, external and internal path unification, and data path feasibility validation via rows and graph learning technology transforming data paths

into opcode sequences and constructing a heterogeneous graph to extract sequential execution process characteristics, also studies the exterior transactions in Ethereum Virtual Machine (EVM), combining external and internal paths with function segmentation and Control Flow Graph (CFG) structure; as stated by the authors, DeFiTail overcomes 98.39% of access control and 97.43% flash loan threats. Yet, the study lacks the evaluation of executing latency impact, which reduces its effectiveness for detecting threats and responding in real time.

• Liyi Zhou et al. [62]. Introduce Automated Arbitrage Market Maker (A2MM) service, which creates atomic swap routing mechanisms that automatically perform two-point arbitrage between UniSwap and SushiSwap AMMs to secure blockchain protocols from Miner Extractable Value attacks. The study reduces block-space consumption by 32.8% and transaction fees by 90% while mitigating 88.8% of back-running arbitrage transactions associated with back-run flooding (BRF). Yet, it has drawbacks, like requiring more smart contract logic, which increases gas costs and fails to identify the issue when interacting with multiple AMMs, problems related to scalability and assumptions about the security of smart contracts, and frequent vulnerabilities, such as reentrancy and Oracle manipulation, are also not addressed.

• Jiahua Xu et al. [63]. Introduce (Auto.giv) to operate as a framework to protect DeFi platforms by decreasing security risks through Deep Q-Network (DQN) reinforcement learning, which analyzes AAVE-like DeFi model changes by altering protocol parameters to sustain security and operational excellence over traditional methods, documenting that the agent can create robust, profitable decisions in just 20 minutes of training, showing a reactive, efficient, and objective solution compared to traditional procedures. Yet, the evaluation process does not examine how Auto.gov would perform in different protocols and chains.

• Maoyi Xie et al. [64]. Propose a framework called DeFort to determine and study the price manipulation attacks via price pattern models and multiple token examination tools for dataset evaluations in D1 and D2. It functions automatically to detect transactions that cause abnormal price fluctuations and recognizes attackers and victims by comprising three elements: an on-chain monitor, a model-driven detector, and a model-driven analyzer. The study reached a recall rate of 96.3% and attained zero False Positives (FP) on D2. However, the study focuses on transaction execution, not the source code level, and it does not explain the speed of the detection process or the gas or computational costs.

• Yongge Wang et al. [65]. Introduce an AMM CoinSwap-based-constant ellipse cost function for AMMs and compare it with the existing AMM mathematical models, such as the Logarithmic Market Scoring Rule (LMSR), Liquidity Sensitive LSMR (LS-LMSR), and mean/constant product/sum, which aims to lower slippage-based front-running attacks, by examining the gas price corresponding to UniSwap V2 and UniSwap V3, which reduced the gas cost to 44.99% for UniSwap V2 and 184.29% for UniSwap V3; but, it does not overlook other potential exposures that AMMs face, such as liquidity or market manipulation attacks; further research could offer more about the threats concerned in AMMs.

• Zongwei Li et al. [66]. Introduce StateGuard, a deep learning-based platform for assessing and discovering state defects in DEX projects, and locate a new kind of state derailment fault in DEX smart contracts as its structure from Abstract Syntax Tree (AST) includes five dependent elements: data dependencies, declaration dependencies, expression dependencies, function dependencies, and control dependencies, it also applies a Graph Convolution Network (GCN) to determine state derailment defects, matching the StateGuard efficiency within Confuzzius, Conkas, Oyente, Securify, and Mythril utilizing 2,000 contracts through the SmartBugs dataset, it revealed that StateGuard overcame other tools in each of five key performance metrics, with 22.31% accuracy and 7.39% in F1-score; despite graph optimization methods providing benefits. The study has a complexity issue in many AST traversals for comprehensive analysis, and it does not assess its effectiveness in non-DEX DeFi protocols, which restricts its adaptability for applications throughout the broader DeFi domain.

• Bing Wang et al. [67]. Propose DeFiScanner, a deep-learning-based attack detection system on DeFi, detecting attacks that utilized logic flaws conducted by integrating multiple protocols consisting of price manipulation and flash loan attacks that regular tools fail to identify, gathering 50-910 real-world DeFi transactions on Ethereum seven models used comparative procedure: K-means, autoencoder, Support Vector Machine (SVM), Convolution neural networks (CNN), deep autoencoder, LSTM-CNN and long short-term memory (LSTM), it explaining that it can solves gaps within the literature by detecting key components to improve the implementation of DeFi attack detection. However, it fails to examine its performance within multiple types of DeFi applications and unpredictable market situations, as the broad application scope of the system becomes difficult to predict because of potential limitations that affect its effectiveness in real-world deployments.

• Viraaji Mothukuri et al. [68]. Present TrustScore, an AI-based framework developed to score and analyze DeFi projects for their possible risks and reliability, smart contract code, transaction records, social media activity, and project metadata data sources for identification of DeFi rug pull and flash loan attacks, using models such as FinBERT, XGBoost, Prophet, GPT4, and Slither to execute static analysis of smart contracts to detect vulnerabilities, as the smart contracts audit models provide quantitative data true negative = 30%, false negative = 0.00%, accurate positive = 23.75%, false positive = 46.25%, the model considerably enhances trust score competitive efficiency and prediction within some evaluation metrics. Yet, while the paper estimates current security weaknesses and assesses AI detection methods, it fails to consider forthcoming threats that may develop with evolving DeFi technological developments.

• Hongbo Wen et al. [69]. Introduce FORAY, an attack synthesis framework against deep logical bugs in DeFi protocols, as current vulnerability methods mainly

analyze specific contracts using brute-force approaches for DeFi protocols. FORAY synthesizes attacks through different DeFi protocols using attack sketch generation, synthesizing 27 attacks out of 34 benchmarks of DeFi logical flaws, and completion with Counterexample-Guided Inductive Synthesis (CEGIS) and Abstract Financial language labeled Domain-Specific Language (DSL) that runs within FORAY to prove and enhance the synthesized attacks. However, the system exists to handle fundamental logical vulnerabilities within DeFi protocols, leaving FORAY's operation scope limited by its ability to detect existing vulnerabilities, as it may not update to detect new problems when they appear frequently with the changes in the DeFi domain.

Table 4: Key differences and study comparisons (TP= True Positive, TPR= True Positive Rate, FP= False Positive, FPR= False Positive Rate, TN= True Negative, FN= False Negative; s= seconds; MVE= Miner Extractable Value, EEV= Expected Extractable Value).

Ref.	DeFi Component	Vulnerability Addressed	Mitigation Strategy	Evaluation Method	Reported Results
[8]	Smart contract (Oracle)	Oracle dependency vulnerabilities	BLOCKEYE	Tested on eight DeFi platforms and compared with Codefi.	Enhanced vulnerability detection and exposed unknown vulnerabilities.
[57]	Smart contracts	Reentrancy, integer Underflow	SolSaviour	Collect DAO contracts, Fei protocols, and PoWH coin.	Decreased attack risk and maintained patchability and state migration.
[58]	DEX	Front-running and cross-market manipulation	DeFiRanger	Established 15,272 transactions and 92 million transactions backtest	Enhanced exposure of price manipulation attacks
[59]	DEX	MEV, EEV	FairTraDEX	Conceptual proposal	Prevent extractable value, fixed trading cost.
[60]	Smart contracts	Hidden mint function, limiting sell-order, Leaking Token, dumping the cryptocurrency, withdrawing liquidity, and abandoning the project after funding	CRPWarner	Evaluate 69 open-source smart contracts and 13,484 real-world ERC tokens	Improve detection of contract-related rug pulls

• Jianzhong Su et al. [70]. Present DeFiWarder to check on-chain transactions and prevent DeFi applications from Token Leakage vulnerabilities that occur when an authorized user can implement token leaking behavior, maintain the smart contracts execution logs, and put them into a Call Flow Tree (CFT), performing role/ relation mining and token flow generation, and employ WETH for calculating the value of tokens based on UniSwap V2 token exchanges; the study focused on practical detection outcomes, discovered seven False Positive (FP), and determined the causes such as price variation, Liquidity Provider (LP) token transfers over applications. However, it does not consider the nature of DeFi applications with their smart contracts when new vulnerabilities and attacks arise.

Ref.	DeFi Component	Vulnerability Addressed	Mitigation Strategy	Evaluation Method	Reported Results
[61]	Smart contracts	Access control exploits and flash loan exploits	DeFiTail	Using REKT and CVE datasets and comparing with Mythril, SPCon, and AChecker	Improved detection of access control and flash loan exploits
[62]	AMM	MEV, sandwich	A2MM	Evaluated against Ethereum real-world data and compared with UniSwap and SushiSwap	Enhance consensus security and reduce transaction costs.
[63]	On-chain governance	Price Oracle attacks, malicious market manipulation	Auto.giv	Simulate an AAVE-like lending protocol	Improved system stability and governance decision-making
[64]	AMM-DEX	Price manipulation attacks (front-running, pump and dump, Oracle, flash loan)	DeFort	Experienced in 441 real-world DeFi projects	Increase price manipulation attack recognition
[65]	AMM	Slippage-based front-running	CoinSwap (constant ellipse-based cost function)	Evaluated via a prototype deployment, and compared the gas costs of UniSwap V2 and V3	Reduce slippage-based front-running and gas cost
[66]	Smart contract (DEX)	State derailment defects (incomplete, incorrect, or unauthorized changes to the system)	StateGuard	Evaluate 46 DEX projects, test 5,671 contracts from DAppSCAN and SmartBugs datasets.	Optimize the recognition of state derailment defects.
[67]	Smart contract	Logic vulnerabilities in the blockchain, flash loans, and price manipulation	DeFiScanner	Using a dataset of 50,910 real-world DeFi transactions	Improved detection logic based on DeFi attacks
[68]	Smart contract	Scams, rug pulls, flash loan attacks, and malicious behaviors	TrustScore	Test DeFi's real-world data	Enhances malicious behavior detection and scams
[69]	Smart contract,	Deep logical bugs and logical	FORAY	Estimate 34 DeFi logical bugs, benchmarks, and	Improved the discovery of deep

After this comparison, we found that the main attacks from the selected studies, about 40% of them focus on Oracle manipulation attacks, 33.33% on price manipulation and flash loan attacks separately, followed by 13.33% on (MEV, rug pull, front-running, Token Leakage, and deep logical bugs), 6.67% on (EEV, reentrancy, sandwich, access control, and state derailment defects).

5 Discussion

As illustrated in Figure 8, 40% of the selected studies focus on the smart contract, 13% for each component DEX, AMM, smart contract DEX, and smart contract Oracle, AMM-DEX, and on-chain governance each present 7% respectively, as is illustrated in Figure 8. This section presents the answers to the review research questions (Q1, Q2, and Q3), compares the assigned fifteen studies with the SOTA, and explains their restrictions.

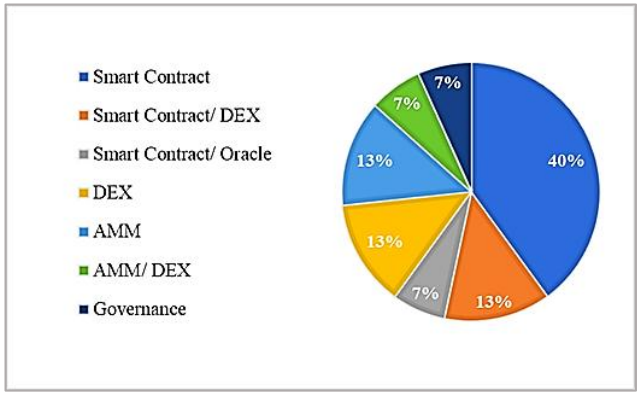


Figure 8: The percentage of DeFi components addressed through the review.

5.1 Q1: What type of attacks affect DeFi security?

Based on the summary explanation from Section 4 (Results) and Table 4, various attacks affect the security of DeFi; we summarize the identification of each attack as follows:

Price manipulation attacks happen when attackers increase cryptocurrency prices through deceptive means to get additional financial gain [64]. They alter the token prices inside DEX using flash loans to gain funds by causing abnormal variations in token prices and benefiting from the abnormal pricing [58].

Oracle price manipulation attacks involve manipulating Oracles that incorporate third-party elements to supply abnormal prices, and the attackers misuse the abnormal prices to conduct transactions and gain profit [64]. Attackers may leverage the use of bZx Oracle with other DeFi projects to affect the exchange rate of profit and crypto assets [67], and includes three stages: ***Hoard*** the attacker purchases some token (x), Pump due to the victim contract relies on the token (x) price in DEX, the attacker utilizes a large number of funds to manipulate the DEX pool, ***Dump*** the attacker sells all hoarded token (x) to the target contract or employed it as collateral at a higher price than the market [58].

Miner Extractable Value (MEV) defines the entire quantity of returns miners can acquire using transaction order manipulation, which aims to incentivize miners to fork the chain. For instance, a rational miner with only 5% hash power will split the Ethereum when an MEV possibility yields 4x the block incentive [62].

Expected Extractable Value (EEV) refers to any profits a player predicts and extracts from other players who communicate with the blockchain by injecting, changing, or censoring transactions in prospective blocks[59].

Flash loan attackers generally exploit them to increase profit due to the simplicity of flash loans, showing significant financial security concerns for the evolution of the DeFi ecosystem. Flash loan attacks are usually associated with Oracle (price) manipulation, an arbitrageur using a strategy to increase or decrease a specific asset [67]. Using lending tools like flash loans, attackers can borrow many tokens and manipulate their value to gain profit [64].

A reentrancy attack is well-known for enabling attackers to call back to the contracts to steal funds recursively; additionally, some attackers deploy parameter injection attacks with unauthorized parameters to call the vulnerable contracts to obtain illicit advantages [70]. One of the most notable occurrences was the DAO hack, in which the attackers used the reentrancy flaw to steal funds without authorization. Different reentrancy attacks happened in April 2022 on the Fei protocol, in which the attacker discovered a vulnerability in Fei collateral mechanisms to leave assets locked in the Fei contract, causing a loss of about 28,380 ETH [57].

Rug pull attack is a specific type of cryptocurrency scam that exists when the developer of a token project purposely gives up the project and escapes with the consumers' funds, making it difficult for the consumers to earn back their investment by selling their cryptocurrencies, as they become worthless [60]. ***Soft rug pulls*** are less noticeable and more subtle scamming strategies in this category. On the other hand, Hard Rug Pulls are abrupt and significantly affect the project, reducing consumers' assets extensively. On the other hand, ***Hard Rug Pulls*** are abrupt and significantly affect the project, reducing consumers' assets extensively. Another type, the ***Sell Rug Pulls Scam***, includes fooling consumers with promises of project excitement and great returns, allowing the scammers to disappear after the sale [68].

Front-running attacks appear when the attacker conducts the same or equivalent transactions for profit despite realizing the price movements and what other users are about to execute. Both require transaction mechanisms, directly or indirectly changing prices and using abnormal prices to gain profits [64]. If a DeFi contract's public interfaces that connect to DEX pools are not sufficiently secured, an attacker may execute front-running to attack the contract [58]. ***Slippage*** is an alteration to the price of an asset within a transaction; anticipated price slippage is an expected decrease or increase in the cost based on the available liquidity and the value to be traded [62]. At the same time, ***Slippage-based front-running*** remains possible if the tangent line for a slope of the cost function curve is unstable. When the tangent line slope changes within a current market circumstance, the more effective the benefit the frontrunner may earn [65].

A sandwich attack is a malicious trading method that benefits from delayed trades that remain unexecuted under the assumption that asset value shifts due to pending trades, and when the deal expires, a designated frontrunner executes a trade by buying or selling the asset before finalizing the transaction, followed by buying or selling the precise asset once the transaction has been validated [62].

A Token Leaking attack on a DeFi application has a Token Leaking flaw if any unauthorized person can perform Token Leaking behavior, such as withdrawing funds far over their deposits (i.e., abnormal return rate) [70]. Or when token contracts don't perform authentication of users on crucial interfaces like transform and burn, particularly on LUME, VOOP, CB3, TRM, Zenon, CollectCoin, IVM, ARFI, BWHALE, B, LACK07MIGE, SFM, and BSCAnt3 that don't succeed in ensuring a caller's identification before allowing it to burn tokens, letting the attackers burn any of the mentioned tokens simply [60].

Access control attacks are a security issue that is a problem within standard programs and smart contracts. Security holes in access control systems allow attackers to modify critical variables within the DeFi application and steal all funds through essential functions [70]. The main issue arises through unauthorized access to crucial interfaces, which lack proper user authentication on LUME, VOOP, CB3, TRM, Zenon, CollectCoin, IVM, ARFI, BWHALE, B, LACK07MIGE, SFM, and BSCAnt3. These contracts fail to verify a caller's identification before enabling the caller to burn tokens, allowing the attackers to burn any of the mentioned tokens [58].

Deep logical vulnerabilities are flaws that employ public functions on different smart contracts in DeFi protocols to raise an attacker's profits. Detecting these weaknesses is extremely difficult due to the condition for a deep understanding of the business logic, the semantics of DeFi protocols, and the architecture of transaction sequences. The attacker aims to execute a transaction sequence that combines logical vulnerabilities in the target DeFi protocol to increase profit [69].

State derailment defects result when system state modifications become invalid or fail due to resource limits, code-related design flaws, or other unexpected code issues, as the safeTransferFrom function is vital in transmitting tokens that will be accessible. Still, it lacks adequate verification mechanisms, so anyone can use it, possibly triggering a state derailment defect [66].

5.2 Q2: What solutions do the studies offer to address those attacks?

Different security solutions are introduced in the studies to fight DeFi attacks through artificial intelligence models as well as deep learning and symbolic execution and real-time detection and governance systems. ***BLOCKEYE*** [8] tracks external network transactions alongside its symbolic logic system to resolve vulnerabilities affecting smart contracts or Oracle manipulations, and ***DeFiWarder*** [70] determines real-time token Leakage on-chain by keeping track of smart contracts and examining the transaction flaws. ***CRPWarner*** [60] addresses the rug pulls associated with the smart contracts, such as (Token Leakage, hidden mint functions), using static analysis of Ethereum Virtual Machine (EVM) bytecode, ***DeFiTail*** [61] expose access control and flash loan flaws within the smart contracts via symbolic execution and heterogeneous graph learning, and ***DeFiRanger*** [58] expose access control and flash loan flaws within the smart contracts via symbolic execution, which utilizes symbolic reasoning to attack through various smart contracts and domain-specific languages, deterring 10 zero-day flaws and 27 vulnerabilities. ***FairTraDEX*** [59] proposes a decentralized exchange protocol based on frequent batch auctions (FBAs) replicating the characteristics of an FBA using a multiple set of zero-knowledge protocols and an escrow-enforced commit-reveal mechanism, while ***StateGuard*** [66] applies Graph Convolutional Networks (GCNs), AST DEX smart contracts, and pattern dependency to discover the state derailment defects, ***DeFiScanner*** [67] detect attack transactions using LSTM-CNN, such as logic flaws, price manipulation, and flash loans, and ***DeFort*** [64] utilizes on-chain monitoring and a general behavior model to determine price manipulation attacks, and ***TrustScore*** [68] Integrates AI models such as GPT models (GPT3.5, GPT4), FinBERT, and XGBoost to assess risks in DeFi projects, social data, flash loans, and rug pulls. ***Auto.giv*** [63] Handel's governance parameters in AAVE include a system to defend against governance and price manipulation attacks using reinforcement learning (DQN). In contrast, ***SolSaviour*** [57] improves and removes vulnerable contracts such as DAO and Fei protocol during the deployment, utilizing TEEs' voting mechanisms (VoteDestruct), ***A^2MM*** [62] avoid sandwich attacks and MEV by allowing atomic routing swap over UniSwap, SushiSwap, and ***CoinSwap*** [65] constant ellipse-based cost function, and AMM pricing for mitigating slippage-based front-running attacks.

As the solutions from the selected studies perform well in detecting the attack type, formal verification reduces uncertainty and inconsistency in smart contracts

by transforming logic, concepts, and judgments into a formal model, using rigorous proofs to verify the security functions and correctness, where deductive verification and model checking are two frequent approaches to formal verifications. Deductive verification utilizes logical formulas to describe [1system verification. Then, it proves whether the system has particular security properties through specified rules. Model checking provides all possible states of smart contracts employing state-space scanning and then evaluates if the contract has the corresponding security features. It suggests a formal paradigm and indicates the formal semantics of contracts to authenticate smart contracts' security properties [47].

5.3 Q3: How can those security solutions enhance the security of DeFi platforms?

The studies proposed different solutions and applied them to improve the security of DeFi platforms, each of them successfully addressing vulnerabilities and protecting them from attacks as intended by their design. Some solutions even discovered a new type of Token Leakage on DeFi, such as ***DeFiWarder***, and the detection of state derailment defects with ***StateGuard***, and the runtime operations of ***BLOCKEYE*** protect against abnormal transactions by utilizing Oracle manipulation methods, smart contracts analysis, and abnormal transaction detection tools. ***FORAY*** improves the security by discovering 10 zero-day vulnerabilities that led to the protection of the security of deployed smart contracts and other solutions such as ***DeFiRanger***, ***DeFort***, and ***DeFiScanner*** detected price manipulation attacks (e.g., Oracle manipulation, flash loans), which is the most frequent incident attacks that appear on DeFi platform that traditional security tools could not provide, they lowered the false positive rate or the gas cost. Other solutions enhance DeFi security by determining scam projects, flash loans based on social data, and the project metadata using many models such as GPT, FinBERT, and XGBoost. ***Auto.giv*** governance security tools can modify their governance parameters to react to security threats. At the same time, ***SolSaviour*** effectively detects reentrancy attacks and logic bugs by using the TEE and VoteDestruct supply post-deployment and fixing the DAO contracts by securely removing malicious contracts. Additionally, the ***A^2MM*** and ***CoinSwap*** with constant ellipse-based cost function provide a security solution of DeFi based on the AMM, where ***A^2MM*** minimizes the front-running attacks and MEV by applying atomic cross routing; CoinSwap lowers the slippage-based front-running attack by presenting a price model and stops manipulation, preventing extractable value and fixed trading costs within ***FairTraDEX***. In general, all of the security solution tools introduced through the studies for DeFi minimized the influence of detected attacks, which raises the security of each DeFi component and the users' confidence, and is vital to the security of DeFi projects.

5.4 Study comparison with SOTA

In this section, we present a comparison between the findings from the fifteen studies and advanced SOTA research studies in the security of DeFi, including four studies, ***DeFiScope*** [71], ***FlashSyn*** [72], ***SecPLF*** [73], and ***DeFiGuard*** [74]. These are not part of the selected ones in the systematic review. The selection of the studies made based on their new techniques for DeFi security; as their publication is from (2024-2025), we draw a comparative table to align the differences between them based on the attack type that they determine to asses' researchers what are the recent attacks that identified and concentrated on in the security field of DeFi.

As stated in Table 5, the selected studies covered a wide range of attacks on DeFi, including price manipulation, oracle manipulation, flash loan, and governance. On the other hand, the SOTA studies focus on a specific kind of attack employing advanced techniques, like ***DeFiScope,*** that addresses Oracle and price manipulation. ***FlashSyn*** identifies different flash loan scenarios, as ***SecPLF*** presents a loanable protocol based on Oracle, and ***DeFiGuard*** applies a Graph Neural Network (GNN) to detect price manipulation. Current research adopts accurate solutions based on deep learning methods or by integrating existing tools. It also evaluates the value of the selected studies on detecting multiple types of attacks while the SOTA discovers new strategies. The collection of work creates an extensive security overview of Defi while identifying necessary research to achieve security scalability and advanced attack defense.

5.5 Contribution of the review

In this systematic review, we present the security solutions that are applied to DeFi to protect it from attacks by focusing on the recent and advanced studies in the field: three studies selected from the years 2020, 2021, and 2022, respectively, the most studies (twelve of fifteen) was from years (2023-2024) which it reflects the most newly attacks and security methods used, as most research focuses on the security of the DeFi smart contracts, in this review we present the security of DeFi based on their components such as AMM, DEX, AMM based DEX, governance, and smart contracts in general or the smart contracts with (Oracle, DEX), providing border view of the attacks in new DeFi platforms. Furthermore, the concentrate of the review results conducted based on three questions, compare the studies with SOTA to evaluate their effectiveness, modesty, and its practical implications by highlight the missing gaps, such as, formal verification security approaches, and updatability, which are critical characteristics to border and develop DeFi for any new incident or attacks.

Table 5: Comparison of selected studies towards SOTA based on attack type.

Ref.	Tools	Price manipulation	Oracle manipulation	MEV	EEV	Flash Loan	Reentrancy	Rug Pulls	Front-Running	Sandwich	Token Leakage	Access Control	Deep logical Bugs	State Derailment defects
[8]	BLOCKEYE	✓	✓	×	×	×	×	×	×	×	×	×	×	×
[57]	SolSaviour	×	×	×	×	×	✓	×	×	×	×	×	×	×
[58]	DeFiRanger	×	✓	×	×	×	×	×	×	×	×	×	×	×
[59]	FairTraDEX	×	×	✓	✓	×	×	×	×	×	×	×	×	×
[60]	CRPWarner	×	×	×	×	×	×	✓	×	×	×	×	×	×
[61]	DeFiTail	×	×	×	×	✓	×	×	×	×	×	✓	×	×
[62]	A^2MM	×	×	✓	×	×	×	×	×	✓	×	×	×	×
[63]	Auto.giv	✓	✓	×	×	×	×	×	×	×	✓	×	×	×
[64]	DeFort	✓	✓	×	×	✓	×	×	✓	×	×	×	×	×
[65]	CoinSwap	×	×	×	×	×	×	×	✓	×	×	×	×	×
[66]	StateGuard	×	×	×	×	×	×	×	×	×	×	×	×	✓
[67]	DeFiScanner	✓	✓	×	×	✓	×	×	×	×	×	×	✓	×
[68]	TrustScore	×	×	×	×	✓	×	✓	×	×	×	×	×	×
[69]	FORAY	✓	✓	×	×	✓	×	×	×	×	×	×	✓	×
[70]	DeFiWarder	×	×	×	×	×	×	×	×	×	✓	×	×	×
[71]	DeFiScope (SOTA)	✓	✓	×	×	✓	×	×	×	×	×	×	×	×
[72]	FlashSyn (SOTA)	×	×	×	×	✓	×	×	×	×	×	×	×	×
[73]	SecPLF (SOTA)	×	✓	×	×	✓	×	×	×	×	×	×	×	×
[74]	DeFiGuard (SOTA)	✓	×	×	×	×	×	×	×	×	×	×	×	×

5.6 Limitations

Despite the review explaining various studies that focus on the security of DeFi and how they defend against attacks and vulnerabilities, there are still some limitations: one limitation is the inconsistency in how the selected studies present their outcomes. In contrast, some studies explain it in a comprehensive explanation, others introduce them descriptively, and others concentrate on one or two specific attacks through particular DeFi components (e.g., smart contracts, DEX, AMM-based DEX) such as price manipulation, Oracle manipulation; which limited scope restricted our ability to review a wide range of attacks types that threaten DeFi security, and the absence of formal verification approaches in many studies prevented us from proposing a more consistent comparison process; if the evaluation criteria were consistent across the studies, it would have enabled more accurate comparison and synthesis. However, they present recent trends in research directions and do not impact the reviews' effectiveness in showing flaws and improvements in the research of DeFi in the security field.

6 Conclusion

We discuss in this systematic review the security of DeFi using blockchain technology by presenting fifteen selected studies from 2020 to 2024 in different fields of DeFi smart contracts, governance, AMM, DEX, and AMM-based DEX, determining the attack types that affect DeFi security, including (price manipulations, Oracle manipulations, flash loan attack, reentrancy, and Token Leakage,...etc.) utilizing tools (e.g., BLOCKEYE, SolSaviour, DeFiScanner, DeFiTail, DeFiWarder, FORAY), evaluating them based on attacks type, vulnerabilities, techniques, models, then provide a comparison between them and advanced SOTA studies (e.g., DeFiScope, SecPLF) according to the attack detecting, and demonstrating how trend researches focuses on new approaches, the accuracy, and integrating AI models with them. This review helps to draw a map for DeFi security and show the direction of the current research in this field, highlighting the gaps in covering attacks on the areas that need more research by understanding different threats and how to handle them

through blockchain technology, to ensuring the immunity of DeFi platform against advanced attacks type and offering a summary for developers and researcher to construct trustable, and secure DeFi systems.

References

[1] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese, and F. Victor, "The Technology of Decentralized Finance (DeFi)," 2023. [Online]. Available: www.bis.org

[2] F. Schär, "Decentralized finance: on blockchain- and smart contract-based financial markets," *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021, doi: 10.20955/r.103.153-74.

[3] V. Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM."

[4] J. R. Jensen, V. von Wachter, and O. Ross, "An Introduction to Decentralized Finance (DeFi)," *Complex Systems Informatics and Modeling Quarterly*, vol. 2021, no. 26, pp. 46–54, 2021, doi: 10.7250/csimq.2021-26.03.

[5] J. R. Jensen and O. Ross, "HOW DECENTRALIZED IS THE GOVERNANCE OF BLOCKCHAIN-BASED FINANCE?" [Online]. Available: https://www.balancer.finance

[6] 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 *Proceedings - 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1286–1292. doi: 10.1109/COMPSAC54236.2022.00203.

[7] S. Chaliasos *et al.*, "Smart Contract and DeFi Security Tools: Do They Meet the Needs of Practitioners?," in *Proceedings - International Conference on Software Engineering*, IEEE Computer Society, Feb. 2024. doi: 10.1145/3597503.3623302.

[8] A. Kumar, N. Sharma, S. Malhotra, S. Devliyal, and B. V. Kumar, "Smart Contract Security: A Review with a Focus on Decentralized Finance," in *2024 3rd International Conference for Innovation in Technology, INOCON 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/INOCON60754.2024.10511387.

[9] W. Li, J. Bu, X. Li, and X. Chen, "Security Analysis of DeFi: Vulnerabilities, Attacks and Advances," May 2022, [Online]. Available: http://arxiv.org/abs/2205.09524

[10] M. Saleem and C. Chawla, "Blockchain-Powered Decentralized Finance (DeFi): Transforming Financial Inclusion & Investment Landscapes," in *Proceedings of the 2023 12th International Conference on System Modeling and Advancement in Research Trends, SMART 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 342–346. doi: 10.1109/SMART59791.2023.10428666.

[11] A. Djeddai and R. Khemaissia, "PrivyKG: Security and Privacy Preservation of Knowledge Graphs Using BlockChain Technology," *Informatica (Slovenia)*, vol. 47, no. 5, pp. 137–152, Jan. 2023, doi: 10.31449/inf.v47i5.4698.

[12] O. Ali, M. Ally, P. Clutterbuck, and Y. K. Dwivedi, "The State of Play of Blockchain Technology in the Financial Services Sector: A Systematic Literature Review."

[13] Y. Long, Y. Gong, W. Huang, J. Cai, N. Xu, and K. ching Li, "Cryptography of Blockchain," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Science and Business Media Deutschland GmbH, 2023, pp. 340–349. doi: 10.1007/978-3-031-28124-2_32.

[14] Q. Razi, A. Devrani, H. Abhyankar, G. S. S. Chalapathi, V. Hassija, and M. Guizani, "Non-Fungible Tokens (NFTs) - Survey of Current Applications, Evolution, and Future Directions," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2765–2791, 2024, doi: 10.1109/OJCOMS.2023.3343926.

[15] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," 2020.

[16] N. Yadav and V. Sarasvathi, "Venturing crowdfunding using smart contracts in Blockchain," in *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 192–197. doi: 10.1109/ICSSIT48917.2020.9214295.

[17] D. Vujičić, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in *2018 17th International Symposium on INFOTEH-JAHORINA, INFOTEH 2018 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Apr. 2018, pp. 1–6. doi: 10.1109/INFOTEH.2018.8345547.

[18] W. Li, J. Bu, X. Li, H. Peng, Y. Niu, and Y. Zhang, "A survey of DeFi security: Challenges and opportunities," Nov. 01, 2022, *King Saud bin Abdulaziz University*. doi: 10.1016/j.jksuci.2022.10.028.

[19] R. K. Sharma and R. S. Pippal, "Blockchain-based Efficient and Secure Peer-to-Peer Distributed IoT Network for Non-Trusting Device-to-Device Communication," *Informatica (Slovenia)*, vol. 47, no. 4, pp. 515–522, Dec. 2023, doi: 10.31449/inf.v47i4.3494.

[20] G. Kaur, A. Habibi, L. Iman, S. Ziba, and H. Lashkari, "Understanding Cybersecurity Management in Decentralized Finance

Challenges, Strategies, and Trends Financial Innovation and Technology."

[21] S. Yang, K. Nayak, and F. Zhang, "Decentralization of Ethereum's Builder Market," May 2024, [Online]. Available: http://arxiv.org/abs/2405.01329

[22] M. H. Jumaa and A. C. Shakir, "Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology," *Informatica (Slovenia)*, vol. 46, no. 6, pp. 87–94, 2022, doi: 10.31449/inf.v46i6.4241.

[23] J. Swati, P. Nitin, P. Saurabh, D. Parikshit, P. Gitesh, and S. Rahul, "Blockchain based Trusted Secure Philanthropy Platform: Crypto-GoCharity," in *2022 6th International Conference on Computing, Communication, Control and Automation, ICCUBEA 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICCUBEA54992.2022.10011026.

[24] Z. Wang, H. Jin, W. Dai, K. K. R. Choo, and D. Zou, "Ethereum smart contract security research: survey and future research opportunities," Apr. 01, 2021, *Higher Education Press Limited Company*. doi: 10.1007/s11704-020-9284-9.

[25] A. Trozze, T. Davies, and B. Kleinberg, "Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering," *Forensic Science International: Digital Investigation*, vol. 46, Sep. 2023, doi: 10.1016/j.fsidi.2023.301575.

[26] J. Collins *et al.*, "Crypto, crime and control in writing from the Global Initiative. Cover: © Da-kuk/iStock via Getty Images Plus Please direct inquiries to: The Global Initiative Against Transnational Organized Crime," 2022. [Online]. Available: www.globalinitiative.net

[27] T. Barbereau and B. Bodó, "Beyond financial regulation of crypto-asset wallet software: In search of secondary liability," *Computer Law and Security Review*, vol. 49, Jul. 2023, doi: 10.1016/j.clsr.2023.105829.

[28] T. Katona, "Decentralized Finance : The Possibilities of a Blockchain 'Money Lego' System," *Financial and Economic Review*, vol. 20, no. 1, pp. 74–102, 2021, doi: 10.33893/fer.20.1.74102.

[29] M. Salah and S. Gonzalez, "Decentralized Finance (DeFi) on Blockchain: Current Landscape and Future Trends," 2023.

[30] H. Teng, W. Tian, H. Wang, and Z. Yang, "Applications of the Decentralized Finance (DeFi) on the Ethereum," in *2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers, IPEC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 573–578. doi: 10.1109/IPEC54454.2022.9777543.

[31] O. S. Owolabi, P. C. Uche, N. T. Adeniken, E. Hinneh, and S. Attakorah, "Integration of Decentralized Finance (DeFi) in the U.S. Supply Chain Finance: Opportunities, Challenges, and Future Prospects," *International Journal of Computer Science and Information Technology*, vol. 16, no. 3, pp. 121–141, Jun. 2024, doi: 10.5121/ijcsit.2024.16310.

[32] P. Mell and D. Yaga, "Understanding stablecoin technology and related security considerations," Sep. 2023. doi: 10.6028/NIST.IR.8408.

[33] M. Lathkar, P. Deshmukh, A. Patil, and P. Shelke, "Increasing Donation Transparency in Disaster Relief: A Blockchain-based Solution," in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1527–1532. doi: 10.1109/ICETSIS61505.2024.10459402.

[34] I. Segeda, V. Kotsiuba, O. Shushura, V. Bokovets, N. Koval, and A. Kalizhanova, "DECENTRALIZED PLATFORM FOR FINANCING CHARITY PROJECTS," *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*, vol. 14, no. 3, pp. 129–134, 2024, doi: 10.35784/iapgos.6140.

[35] V. Gramlich *et al.*, "Decentralized Finance (DeFi): Foundations, Applications, Potentials, and Challenges," *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4535868.

[36] A. A. A. Ahmed, "The Rise of DeFi: Transforming Traditional Finance with Blockchain Innovation," Feb. 13, 2024. doi: 10.20944/preprints202402.0738.v1.

[37] E. Bayraktar, A. Cohen, and A. Nellis, "DEX Specs: A Mean Field Approach to DeFi Currency Exchanges," Apr. 2024, [Online]. Available: http://arxiv.org/abs/2404.09090

[38] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols," Mar. 2021, doi: 10.1145/3570639.

[39] S. Cousaert, J. Xu, and T. Matsui, "SoK: Yield Aggregators in DeFi," May 2021, doi: 10.1109/ICBC54727.2022.9805523.

[40] T. Surve, A. Tyagi, and G. Kaur, "Article ID: IJARET_14_07_003 Review of The Literature." [Online]. Available: https://iaeme.com/Home/journal/IJARET48editor@iaeme.com

[41] V. Benson, U. Turksen, and B. Adamyk, "Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities," *Journal of Financial Regulation and Compliance*, vol. 32, no. 1, pp. 80–97, Jan. 2024, doi: 10.1108/JFRC-04-2023-0065.

[42] A. Soyele, O. J. Enyejo, A. A. Ajayi, I. Emmanuel, A. D. Soyele, and J. O. Enyejo, "Enhancing Digital Identity and Financial Security in Decentralized Finance (Defi) through Zero-Knowledge Proofs (ZKPs) and Blockchain Solutions for Regulatory Compliance and Privac... Enhancing Digital Identity and Financial Security in Decentralized Finance (Defi) through Zero-Knowledge Proofs (ZKPs) and Blockchain

Solutions for Regulatory Compliance and Privacy," 2024. [Online]. Available: https://www.researchgate.net/publication/385686688

[43] Gailan Ismael Abdullah, "Unraveling the Potential of Decentralized Finance: A Comprehensive Analysis of Opportunities, Risks, and Future Trends," *American Journal of Economics and Business Management*, vol. 7, no. 8, pp. 370–387, Aug. 2024, doi: 10.31150/ajebm.v7i8.2891.

[44] C. Johnson, "Decentralized Finance (DeFi): Opportunities and Risks in the Global Financial Ecosystem," 2024.

[45] S. Borisov, "DeFi-Potential, Advantages and Challenges DEFI-POTENTIAL, ADVANTAGES AND CHALLENGES 2." [Online]. Available: https://www.researchgate.net/publication/361890666

[46] "Timely Identification of Victim Addresses in DeFi Attacks."

[47] P. Qian *et al.*, "Empirical Review of Smart Contract and DeFi Security: Vulnerability Detection and Automated Repair," Sep. 2023, [Online]. Available: http://arxiv.org/abs/2309.02391

[48] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner, and B. Schlosser, "DeFi-ning DeFi: Challenges & Pathway," Jan. 2021, [Online]. Available: http://arxiv.org/abs/2101.05589

[49] S. M. Bhambhwani and A. H. Huang, "Auditing decentralized finance," *British Accounting Review*, vol. 56, no. 2, Mar. 2024, doi: 10.1016/j.bar.2023.101270.

[50] E. Liu *et al.*, "Count of Monte Crypto: Accounting-based Defenses for Cross-Chain Bridges," Oct. 2024, [Online]. Available: http://arxiv.org/abs/2410.01107

[51] L. Zhang, "Function Oracle Automated Market Makers: A Peer-to-Pool System for Decentralized Premium Token."

[52] S. Haque, Z. Eberhart, A. Bansal, and C. McMillan, "Semantic Similarity Metrics for Evaluating Source Code Summarization," in *IEEE International Conference on Program Comprehension*, IEEE Computer Society, 2022, pp. 36–47. doi: 10.1145/nnnnnnn.nnnnnnn.

[53] K. Gogol, C. Killer, M. Schlosser, T. Bocek, B. Stiller, and C. Tessone, "SoK: Decentralized Finance (DeFi) -- Fundamentals, Taxonomy and Risks," Apr. 2024, [Online]. Available: http://arxiv.org/abs/2404.11281

[54] L. Zhou *et al.*, "SoK: Decentralized Finance (DeFi) Attacks," Aug. 2022, [Online]. Available: http://arxiv.org/abs/2208.13035

[55] L. Judijanto, I. Ketut Kusuma Wijaya, I. Jayanto, and S. P. Anantadjaya, "THE INFLUENCE OF DECENTRALIZED FINANCE (DEFI) ON GLOBAL FINANCIAL STABILITY: AN EMERGING CHALLENGE PENGARUH KEUANGAN TERDESENTRALISASI (DEFI) TERHADAP STABILITAS KEUANGAN GLOBAL: TANTANGAN YANG MUNCUL."

[56] C. Okoli and K. Schabram, "A Guide to Conducting a Systematic Literature Review of Information Systems Research," 2015. [Online]. Available: http://ssrn.com/abstract=1954824910.http://aisel.aisnet.org/cais/vol37/iss1/43Electroniccopyavailableat:https://ssrn.com/abstract=1954824Electroniccopyavailableat:https://ssrn.com/abstract=1954824

[57] Z. Li, B. Xiao, S. Guo, and Y. Yang, "Securing Deployed Smart Contracts and DeFi With Distributed TEE Cluster," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 3, pp. 828–842, Mar. 2023, doi: 10.1109/TPDS.2022.3232548.

[58] S. Wu *et al.*, "DeFiRanger: Detecting DeFi Price Manipulation Attacks," *IEEE Trans Dependable Secure Comput*, vol. 21, no. 4, pp. 4147–4161, 2024, doi: 10.1109/TDSC.2023.3346888.

[59] C. McMenamin, V. Daza, M. Fitzi, and P. O'Donoghue, "FairTraDEX: A Decentralised Exchange Preventing Value Extraction," in *DeFi 2022 - Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security, co-located with CCS 2022*, Association for Computing Machinery, Inc, Nov. 2022, pp. 39–46. doi: 10.1145/3560832.3563439.

[60] Z. Lin, J. Chen, Z. Zheng, J. Wu, W. Zhang, and Y. Wang, "CRPWarner: Warning the Risk of Contract-related Rug Pull in DeFi Smart Contracts," Mar. 2024, [Online]. Available: http://arxiv.org/abs/2403.01425

[61] W. Li, X. Li, Y. Zhang, and Z. Li, "DeFiTail: DeFi Protocol Inspection through Cross-Contract Execution Analysis," in *WWW 2024 Companion - Companion Proceedings of the ACM Web Conference*, Association for Computing Machinery, Inc, May 2024, pp. 786–789. doi: 10.1145/3589335.3651488.

[62] L. Zhou, K. Qin, and A. Gervais, "A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges," Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.07371

[63] J. Xu, D. Perez, Y. Feng, and B. Livshits, "Auto.gov: Learning-based On-chain Governance for Decentralized Finance (DeFi)," Feb. 2023, [Online]. Available: http://arxiv.org/abs/2302.09551

[64] M. Xie *et al.*, "DeFort: Automatic Detection and Analysis of Price Manipulation Attacks in DeFi Applications," in *ISSTA 2024 - Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis*, Association for Computing Machinery, Inc, Sep. 2024, pp. 402–414. doi: 10.1145/3650212.3652137.

[65] Y. Wang, "Automated Market Makers for Decentralized Finance (DeFi)," Sep. 2020,

[Online]. Available: http://arxiv.org/abs/2009.01676

[66] Z. Li, W. Li, X. Li, and Y. Zhang, "StateGuard: Detecting State Derailment Defects in Decentralized Exchange Smart Contract," in *WWW 2024 Companion - Companion Proceedings of the ACM Web Conference*, Association for Computing Machinery, Inc, May 2024, pp. 810–813. doi: 10.1145/3589335.3651562.

[67] B. Wang *et al.*, "DeFiScanner: Spotting DeFi Attacks Exploiting Logic Vulnerabilities on Blockchain," *IEEE Trans Comput Soc Syst*, vol. 11, no. 2, pp. 1577–1588, Apr. 2024, doi: 10.1109/TCSS.2022.3228122.

[68] V. Mothukuri, R. M. Parizi, J. L. Massa, and A. Yazdinejad, "An AI Multi-Model Approach to DeFi Project Trust Scoring and Security," in *Proceedings - 2024 IEEE International Conference on Blockchain, Blockchain 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 19–28. doi: 10.1109/Blockchain62396.2024.00013.

[69] H. Wen, H. Liu, J. Song, Y. Chen, W. Guo, and Y. Feng, "FORAY: Towards Effective Attack Synthesis against Deep Logical Vulnerabilities in DeFi Protocols," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Dec. 2024, pp. 1001–1015. doi: 10.1145/3658644.3690293.

[70] J. Su *et al.*, "DeFiWarder: Protecting DeFi Apps from Token Leaking Vulnerabilities," in *Proceedings - 2023 38th IEEE/ACM International Conference on Automated Software Engineering, ASE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1664–1675. doi: 10.1109/ASE56229.2023.00110.

[71] J. Zhong *et al.*, "DeFiScope: Detecting Various DeFi Price Manipulations with LLM Reasoning," Feb. 2025, [Online]. Available: http://arxiv.org/abs/2502.11521

[72] Z. Chen, S. M. Beillahi, and F. Long, "FlashSyn: Flash Loan Attack Synthesis via Counter Example Driven Approximation," in *Proceedings - International Conference on Software Engineering*, IEEE Computer Society, 2024, pp. 1749–1761. doi: 10.1145/3597503.3639190.

[73] S. Arora, Y. Li, Y. Feng, and J. Xu, "SecPLF: Secure Protocols for Loanable Funds against Oracle Manipulation Attacks," in *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, Association for Computing Machinery, Inc, Jul. 2024, pp. 1394–1405. doi: 10.1145/3634737.3637681.

[74] D. Wang, B. Wu, X. Yuan, L. Wu, Y. Zhou, and H. Cui, "DeFiGuard: A Price Manipulation Detection Service in DeFi using Graph Neural Networks," Jun. 2024, [Online]. Available: http://arxiv.org/abs/2406.11157

[75] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. K. Raymond Choo, "Blockchain-based identity management systems: A review," Sep. 15, 2020, *Academic Press*. doi: 10.1016/j.jnca.2020.102731.