Migration Letters

Volume: 21, No: 7 (2024), pp. 235-250

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

How To Identify Spam Blockchain Projects

Faisal M. Alshehri [1], Turki I. Alshamrani [1], Meteb R. Alqahtani [1], Suliman O. Alanazi [1], and Adel R. Alharbi [1], *

Abstract

Decentralized Finance (Defi) is an ecosystem that operates peer-to-peer without the need for an intermediary such as banks. Defi relies on blockchain technology to manage financial transactions such as transfers, withdrawals, and deposits. It is an open-source system that anyone can follow, unlike banks. Defi is rapidly advancing and reshaping the financial industry by providing pio-neering, transparent, and environmentally sustainable cash solutions. In our previous study, we noticed that the world of Defi is large and complex in terms of the projects presented, and the worrying thing is that some of these proposed projects are not safe enough t[1]o work on. In this work we comprehensively examine and perform a comparative evaluation of each toolkit, evaluating their advantages and disadvantages. In addition, coding techniques are used to evaluate the advantages and disadvantages of Defi projects about their security. 100 smart contracts were analyzed using 10 tools, the top five high-risk tokens were analyzed, five risk-free tokens were analyzed, and Defi platforms were analyzed using Scam Detector.

Keywords: *(DeFi) decentralized finance, fraud, blockchain, token, defi tools.*

Introduction

Decentralized Finance (DeFi) refers to a wide range of monetary goods and utilities that are distributed in a decentralized and unlimited manner via smart agreements on the blockchain, the Ethereum platform. Their promoters declare that smart contracts are programs stored on the blockchain that automatically perform specific actions when certain conditions are met. A blockchain is a secure, decentralized database consisting of entries called blocks, which are cryptographically linked to each other through a hash of the previous block, thus ensuring its security and fraud-resistance [1]. Many find entering the world of DeFi exciting but also confusing. After waiting for a while, it is natural to think about ways to maximize gains from your investment portfolio. However, there are a large number of aspects that need to be analyzed when it comes to decentralized finance. DeFi DApps and projects can become powerful tools. However, if one gets involved prematurely, it is very easy to be overcome and make unwise choices regarding investments. The best course of action is to gain knowledge about the potential risks and ensure activities are appropriate for your personal condition. DeFi seeks to create a publicly available, unrestricted and transparent financial services environment. One accessible to all individu-als and functions without any central power. Users will retain full control of their proper-ties and communicate with this environment through peer-to-peer (P2P) and decentral-ized applications (DApps). The primary advantage of DeFi is its ability to facilitate con-venient entry into financial services, especially for individuals who find themselves dis-connected from the existing financial framework. Another advantage of DeFi is the mod-ular framework built with interoperable DeFi applications on public blockchains. It has the potential to create entirely new markets, products, and financial services [2]. Smart contracts are transactions that occur automatically if the conditions stipulated in the con-

[1] College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia.
* Correspondence: Adel R. Alharbi

tract are met. These contracts are flexible in terms of being programmed as the user desires. To clarify, for example Ahmed bought a mobile phone through a website, and he required that payment be made immediately after he received the device and signed a receipt from the postal company. It then explains that the smart contract condition has been met, and that both parties are in agreement. The mobile phone will not be received until the amount is paid, and in the event of non-payment it will not be received. This is a sim-ple example of a smart contract mechanism. For businesses and financial institutions, smart contracts are large, complex, fine-grained, and run around the clock, and Defi takes care of those things.

1.1. What are the main advantages of DeFi?

Traditional finance relies on institutions such as banks to act as intermediaries and courts to provide arbitration. DeFi applications eliminate the necessity of intermediaries or arbitrators. The resolution of every conceivable dispute is clearly outlined in the blog, and users retain full control of their funds at all times. This mechanism reduces the expenses associated with providing and using these products and facilitates the creation of a sim-pler financial system. Built on blockchain technology, these new financial services elimi-nate any point of failure. Data is saved on the blockchain and distributed across many nodes, making any attempts at censorship or potential shutdown of service a complex endeavor. Another notable benefit of this open ecosystem is the accessibility it provides to individuals who may be deprived of any financial services. Because the traditional finan-cial system relies on intermediaries to generate profits, their services are typically absent in areas populated by low-income communities. However, in the field of decentralized fi-nance (DeFi), there is a significant reduction in costs, thus enabling individuals from low-income backgrounds to benefit from a more comprehensive range of financial services [2]. Most current and potential applications of decentralized finance involve creating and executing smart contracts. Smart Contract Unlike a traditional contract, smart contracts exhibit a unique ability to enforce their terms in an automated manner, since these terms are expressed in a programming language. Thus, this enables reliable execution and automation of many work processes that currently require manual supervision. The use of smart contracts provides a faster and more convenient approach, while simultaneously mitigating risks for both parties involved. Smart contracts also bring new forms of risk. Given that computer code is vulnerable to errors and vulnerabilities, assets and confidential information contained in smart contracts are at risk [2].

1.2. What challenges does DeFi face?

Bad performance: blockchains have the inherent property of being relatively less fast than their centralized counterparts, which affects the functionality of applications built on them. Developers of decentralized finance (DeFi) applications are required to duly acknowledge these limitations and then improve their products accordingly.

High risk of user error: defi applications shift the burden of responsibility from intermedi-aries to the user, which many individuals may consider a disadvantage. Developing products that mitigate the possibility of user errors is a huge hurdle, especially in the con-text of deploying these products on immutable blockchains [2]. DeFi utilities refer to tools that DeFi (decentralized finance) investors and traders can leverage to augment their DeFi encounters. DeFi utilities include a variety of applications, including DeFi analytics, trad-ing tools, screening tools, tracking tools, insights, liquidity analysis, portfolio tracking, and statistics [2].

Table 1. Overview of DeFi products.

Decentralized exchanges	These services enable users to trade cryptocurrencies by utilizing the liquidity offered by other users, typically through Automated Market Makers that employ algorithms to establish prices. Users have the option to contribute liquidity to liquidity pools for specific pairs of cryptocurrencies, and in return, they receive a Liquidity Provider token. This token can be "staked," meaning it is locked into the system and cannot be withdrawn for a designated period, allowing users to earn interest on it. The interest is usually paid in the form of the decentralized exchange's governance token, a concept referred to as "yield farming." These yield farms can yield returns on investment in the range of hundreds or even thousands of percent. Additionally, participants can stake governance tokens in "pools" and receive additional rewards. This incentivizes users to contribute liquidity in order to ensure the smooth operation of the exchanges [1].
Defi lending	Loans are distributed through smart contracts in lieu of intermediaries while utilizing cryptocurrencies as collateral. Loans are frequently disbursed in stablecoins, which are crypto assets with a value that is tethered to fiat currencies issued by governments, and interest rates are typically determined algorithmically. Users have the opportunity to accrue interest by providing liquidity for loans and obtaining fees from said loans. A significant development in the realm of Decentralized Finance (DeFi) lending that merits attention is the emergence of flash loans, an innovative financial instrument that facilitates the provision and settlement of loans all within the confines of a solitary transaction. As they are completed within a single transaction, collateral is not necessary for these loans [1]
Prediction markets	These enable individuals to wager on real-world consequences—such as athletic competitions or electoral contests—via intelligent agreements. Forecasting markets depend on blockchain oracles, which are external origins of data that ascertain the result of the prognostication market. Deriving from this data regarding the consequence, the intelligent agreement disburses the suitable funds to the victors [1].
Defi insurance	The individuals within the DeFi insurance community fulfill the role of underwriters and participate in the distribution of premiums received by the protocol. The project's governance token holders exercise their voting rights in determining the disbursement of claims. Although the field of DeFi insurance is still at an early stage of development, certain companies are endeavoring to manage claims through smart contracts. Presently, DeFi insurance primarily focuses on insuring other DeFi protocols [1].
Other financial products	A variety of additional financial instruments, encompassing those typically inaccessible to individual investors, can be integrated into the realm of Decentralized Finance (DeFi). Such instruments encompass the trading of derivatives, engaging in margin trading, as well as involvement with other forms of securities [1].

1.3. The most popular tools used to scan smart contracts and verify security are as follows:

1.3.1. Defi Score Solidity Scanner

The DeFi smart contract scanner can be used to conduct comprehensive, high-speed analyses of more than 10 supported blockchains. Its interaction plan is secure, without having to rely on misleading audits, which often lack adequate coverage [3]. The scanner is fully automated and high quality, and it can be used on precise smart contracts by anyone interested in investing. The DeFi smart contract scanner can analyze any smart contract published on the Ethereum– Binance Smart Chain or on Polygon, providing users with a comprehensive analysis of a contract. The process can be cleared within 15 sec-onds, depending on the complexity of the contract. It works iteratively and uses different databases and tools, including DeFi smart contracts. Users only need to enter a smart contract's address, and the contract is analyzed and the user notified of the present and associated risks to their DeFi investments [4].

1.3.2. Token Sniffer

Token Sniffer offers a platform for users to validate and verify the legitimacy of vari-ous tokens. It is more than just a token scanner; it is an essential token scam checker. Its primary role revolves around "sniffing out" potentially malicious contracts or tokens that could pose risks to unsuspecting investors. In a domain riddled with a history of hacks and scams, Token Sniffer acts as a proactive crypto contract scanner, helping users dis-tinguish the genuine from the fraudulent [5].

1.3.3. GoPlus Token security detection

Go Plus functions as the "security infrastructure" for Web3 through its provision of open, permissionless, and user-driven security services. It is currently being used in the construction of a safer Web3 ecosystem by leveraging the security data infrastructure and security service platform. At present, Go Plus has successfully developed a dynamic and real-time automated security detection platform, which includes the Token Security, NFT Security, Malicious Address, Approval Security, dApp Security Info, and Signature Data Decode APIs. These APIs receive approximately 5 million data requests per day. Furthermore, in 2023, Go Plus introduced the Security Ecosystem [6].

1.3.4. HAPI Labs

HAPI Labs offers a powerful address checking tool that allows for the identification and risk-logging of any address in already integrated blockchains.

Data are checked for their degree of risk. The risk score is calculated based on several factors, including interactions with high-risk addresses, and incidents of theft, penalties, exploits, or breaches are also reported in the risk category, as well as other categories un-der which they fall. The data check includes:

- Signs of risk, as well as their types and movements.
- A breakdown of the equilibrium and interactions;
- Determination of whether all transactions took place at the respective address [7].

1.3.5. Cyberscope

Cyberscope possesses a notable assortment of advantageous commodities that sup-port investors in their pursuit of well-informed decisions. Among them, Cyberscan, a con-tract address scanning tool, stands out. Given the inclination of investors toward new and promising ventures, this tool addresses the specific concern of smart contract security. By providing all pertinent metrics within one reliable repository, Cyberscan obviates the necessity of multiple verifications and queries across disparate sources. [8].

Mechanism of Action:

Smart contract audits involve a thorough analysis of the code and transactions re-lated with a project to identify potential vulnerabilities and ensure the integrity of the con-tract. Auditors typically work closely with the developers of a smart contract to address any

potential vulnerabilities and ensure that all aspects of the contract are properly re-viewed. The final analysis report is made public to investors, allowing them to make in-formed decisions about investing in the project. Auditors use various tools, such as the Slither, Security, SmartCheck, Oyente, Mythril, MythX, and Remix plugins, to aid in the auditing process. Defining the scope of an audit is crucial, as it helps in creating a test plan and strategy for the smart contract audit, which includes checking the business logic, analyzing transaction costs, conducting a performance review, and performing a vulner-ability assessment [9].

1.3.6. BSc Check

BSc Check is an online tool that is accessible at no cost to users. Its purpose is to facil-itate the scanning of tokens from various blockchains, including the Binance Smart Chain (BSC), Ethereum (ETH), Polygon (POLY), Fantom (FTM), and Dogechain (DC). The tool is specifically designed to offer users comprehensive insight into the potential risks associ-ated with trading these tokens. By utilizing BSc Check, users can acquire pertinent infor-mation about a given token, such as its available liquidity, the viability of trading it (i.e., honeypot detectors), the primary holders of said token, the quantity of tokens held by the creator, and details concerning the smart contract code (including the owner and any ma-licious functions, among other relevant information) [10].

1.3.7. Quick Intel

Quick Intel (QUICKI) is a collection of safety and security instruments that facilitate the prompt and real-time evaluation of tokens. QUICKI Scan is a unique and first-of-its-kind scanner that scans tokens and NFTs down to the contract level. It alerts users when known scams and malicious code are detected directly in a contract, elimi-nating the guessing game and providing individuals with more confidence in a project [11].

1.3.8. Solidity Scan Quick Scan

Solidity Scan offers a cloud-based smart-contract vulnerability scanner built to dis-cover vulnerabilities and help publish audit reports after vulnerability mitigations. It scans all of a user's smart contract codes to detect potential security vulnerabilities and anti-patterns. The product is designed to sit in a user's development pipeline, where it runs a scan on a contract's code and flags known vulnerabilities. The end output of the product is an audit report of the code, which contains information on which parts may lead to potential security vulnerabilities [12].

1.3.9. Honeypot Detector

A honeypot detector simulates a buy-and-sell transaction to determine whether the token is a honeypot. To prevent being tricked, the honeypot detector performs many extra checks to minimize false results. Detect Honeypot on the BSC Chain provides crypto's most advanced tool for detecting honeypots, with the highest accuracy [13].

1.3.10. Check

Ave.ai is a platform that provides tools and information to help users navigate the world of crypto currency. Ave.ai strives to empower users to make informed decisions and protect their assets, including through the provision of information on topics such as trading, portfolio, and cryptocurrency analysis. It also offers an interesting feature called "Check", which allows users to check a cryptocurrency contract address and whether it is a scam [14].

1.3.11. Scam Detector

Scam Detector provides original information, reporting, research, reviews, and anal-ysis of websites, domain names, and e-commerce platforms, advising readers if these are legitimate, safe, and trustworthy [15].

1.3.12. Smart contract scanning speed statistics of five tools

Score Solidity Scanner: It takes an average of 9 seconds to scan a smart contract.

BSC Check: It takes an average of one and a half minutes to scan a smart contract.

HAPI Labs: It takes an average of 10 seconds to scan a smart contract.

Cyberscope : It takes an average of 6 seconds to scan a smart contract.

Check: The duration of a smart contract scan is, on average, 2 seconds.

1.2. Problem Statement

One problem associated with decentralized finance (DeFi), which poses a major challenge for its users, is related to knowledge of the legitimacy of a platform. In addition, DeFi faces various obstacles, namely, scalability, security, and user experience. An influx of users leads to network congestion which, subsequently, causes slow transaction times and high fees. Moreover, despite the generally secure nature of blockchain technology, DeFi is a case in point, with abuse and manipulation having been recorded. In addition, the complexity of the user experience on DeFi platforms may hinder beginners getting started in this field.

1.3. Research Objectives

The goal of this endeavor is to eliminate a significant portion of the deception. The next steps for decentralized finance will be interesting, and it is expected that in the com-ing period tangible assets will be integrated with blockchain technology via decentralized finance. In the coming years, we are convinced that many national economies will adopt this approach and build their own individual decentralized economies for the betterment of society. This would facilitate the enhancement of national resources and end corruption across various fields.

1.4. Rationale for Solving the Problem

Defi aims to help individuals who do not have access or who have limited access to banking services. This financial system was created to be transparent, as well as more comprehensive and accessible to everyone. Defi often uses smart contracts, and this en-hances the security of transactions and reduces vulnerability to fraudulent activities. The main research question of this project: how can one determine whether DEFI is a scam?

1.5. Structure of the Report

The rest of the paper is organized as follows: Section 2 we discuss the most im-portant studies on this topic and review the advantages and disadvantages of each tool. In Section 3, we explain the work methodology used in this scientific paper, data collection and analysis, and then in Section 4 we review the results, and finally we conclude the pa-per with suggested recommendations for future work.

Literature Review

This section reviews the most important studies related to DeFi and security screen-ing tools for Defi users.

Previous studies analyze the ratings of 30 specific DeFi protocols and their relation-ship to performance metrics, such as total value locked (TVL), protocol revenue, total rev-enue, total merchandise volume, and inflation factor. Correlation analysis shows that there is a statistically significant positive relationship between DeFi protocols' ratings and their TVLs. However, it is necessary to acknowledge that this examination is based on a temporal sequence of information, which may show lower reliability in contrast to cross-sectional information. Panel regression analysis revealed that TVL, total revenue, and total merchandise volume had a positive impact on the evaluations of DeFi protocols. On the other hand, protocol revenues and inflation factors showed a negative correlation with valuations. TVL was found to be the most influential variable. The Granger causality test indicates that future DeFi protocol valuations can be predicted by TVL and total mer-chandise volume. However, confirming the causal relationship between variables remains

unproven in some cases. The study also compares the relationship between valuations and TVL for different categories of DeFi protocols, showing that TVL is relatively more important for asset management protocols [16]. Attention to the potential and risks of the DeFi ecosystem, focusing on its qualities in terms of efficiency, openness, availability and ability to combine. The research suggests that DeFi remains a niche market with specific risks, but it also has the potential to contribute to a stronger and more transparent finan-cial framework. A comprehensive survey and introduction to the topic of DeFi, aimed at individuals from organizations with an economic or legal background. It characterizes potential prospects and risks and should be considered as a basis for subsequent investi-gations [17]. A comprehensive and diverse analysis of decentralized finance (DeFi) is pro-vided through a comprehensive literature review. This review aims to clarify the current state of research in this particular area, identify gaps in the literature and point out future directions for research in DeFi. Several drawbacks of DeFi that have emerged without widespread adoption have been highlighted. The review compiled a final set of 79 items from the relevant DeFi literature for polyphonic analysis [18]. Most of the current works focused on classifying the blockchain. Oracle classified these works according to data sources, transfer methods, and transmission routing. Data sources are mainly classified into Oracle, software, and hardware data sources, in addition to human sources, accord-ing to data transfer trends. Outgoing and incoming information is classified. Incoming data transfers data from the off-chain side to the on-chain side and vice versa for outgoing data. These classifications describe Oracle in detail, mostly inbound data transfer-based software, and present extensive classification criteria to provide an effective analysis of the trustworthiness of Oracle Defi. Some research works have classified Oracle according to data validation mechanism, for example classification of statements, user opinions and reputation, classification of prediction markets. One method of validating data is hearing majority vote, weighted vote, self-verification, etc. The accuracy, integrity, confidentiality and availability of the data must be ensured. Businesses currently neglect the reliability and provenance of data and it is important to take action Lots of studies and research on the study of data feeding and validation [19]. The manuscript presents a blueprint for an Intrusion Detection System (IDS) built on the innovative method of cryptographic indica-tors based on honeycomb tokens to disrupt cyber attacks on critical infrastructure net-works, specifically zero-day risks. IDS uses different amounts of honey tokens per frame for different groups of entities within the network, with varying levels of protection measures and encryption schemes. The effectiveness of the IDS is evaluated in terms of accurate false positive and negative warnings, and undergoes network penetration testing (NPT) in real-life conditions. The IDS system not only detects hacks but also recovers the entire zero-day attack using a reverse engineering method. The results show that the IDS effectively identifies and recovers from previously unidentified cyberattacks while dis-playing a negligible percentage of false negative alerts, which is less than 2% for high-capacity arithmetic (Pool-A) architectures and about 12% for low-capacity arithmetic systems. (Pool-D). The various configurations use multiple encryption methodologies, such as AES-128, AES-192, and AES-256. An evaluation was conducted comparing the IDS with a traditional signature-based IDS, which showed the former outperforming the latter in terms of its effectiveness in identifying zero-day attacks. IDS screening results show detection of cyberattacks on specific entities [20]. Evaluated five advanced automat-ed security tools and found that they could have prevented only 8% of high-impact attacks in their data set, amounting to $149 million worth of Out of $2.3 billion in losses. All pre-ventable attacks were associated with reentry vulnerabilities. The study highlights that logic-related errors and vulnerabilities in the protocol layer represent significant threats that are not adequately addressed by current security tools. The need for specialized tools that meet the distinct requirements and expectations of developers and auditors is em-phasized. Continued advances in security tools are essential to effectively address evolv-ing challenges in the decentralized finance (DeFi) ecosystem [21] He mentioned 27 tools for analyzing Ethereum smart contracts, including academic tools, enterprise tools, and community tools in open repositories. Most of the tools focus on security issues, and 18 of

them revealed the presence of vulnerabilities, while 4 of them revealed their absence. There are four tools capable of creating vulnerabilities, and two of them are multi-transaction tools. The paper provides a guide for those who want to develop secure smart contracts or who plan to teach on a related topic. The functions and characteristics of the tools are compared to each other in a concise and structured way [22]. There are many target-based cryptocurrency pump-and-dump schemes with an emphasis on successful target pumps over long periods of time. Nearly half of Target Pumps reached at least one of their sale goals, often reaching peak price in days, minutes, or seconds. The study found that groups promoting coins try a variety of distinct methods, and that the most successful groups promote many coins. In addition, many pumps are issued but not in the same currencies, and target pump price fluctuations operate over longer time periods, with price jumps measured in hours and days rather than seconds and minutes. Successful pumps are unlikely to reach their stop targets quickly, while unsuccessful pumps reach their stop loss targets much faster. The analysis determined success by taking only the first cycle after the pump signal [23]. In addition to smart contract technologies, analyzing vulnerabilities in decentralized finance and evaluating their effectiveness in complex analyzes is crucial. For DeFi protocols, traditional methods are used to detect smart contract vulnerabilities, and DeFi analysis methods achieve results with higher accuracy and F1 scores compared to traditional methods. The RECHECKER method, which is based on deep learning, is a fast tool that takes an average of only 8.02 seconds to analyze a DeFi protocol. However, execution time does not provide a complete picture of the tool's performance. Traditional methods for detecting smart contract errors, as applied to DeFi protocols, are delayed by difficulties in understanding the logical semantics of DeFi protocols. Existing DeFi analysis methods are still unable to handle multiple types of attacks and detect high-level logical vulnerabilities [24].

Table 2. Advantages and disadvantages of the tools.

Tools	Advantages	Disadvantages
DeFi Score Solidity Scanner	- Smart contract development [25] - Privacy - Complex data structures [25]	- Limited information [26] - Lack of legal framework [26]
Token Sniffer	-Faster and more effective token search [27] - Provides complete information [27]	-Set up and use can take a long time [28] - Accurate information [28]
Token security detection	- Security [29] - Efficiency [29] - Accuracy [29]	- Needs additional infrastructure [29]
HAPI Labs	- Comprehensive site security assessment [30] - Real-time data update [30]	- Complexity [30] - Single point of failure [30]
Cyberscope	- Comprehensive site security assessment [31] - Protection of sensitive data [31]	- Complexity [31]
BSC check	- Easy to use [10] - Free token analyzer [10]	- Not 100% guaranteed [10]
Quick Intel	- Security [32] - Lower transaction fees [32]	- Lack of regulation [32] - Limited acceptance [32]
SolidityScan QuickScan	- Accessibility [33] - Ease of use [33] - Speed [33]	- False positives [33] - Limited scope [33]
Honeypot Detector	- Straightforward and low maintenance [13]	- False positives [13] - Limited accuracy [13]
Check	-Real-time data update [14] -Comprehensive security system [14]	- Complexity [14]

Methodology

Currently, the domain of decentralized finance, commonly referred to as DeFi, finds itself in the early stages of its development. This emerging sector is rapidly progressing and transforming the financial industry through the introduction of innovative and groundbreaking solutions. However, the DeFi realm has encountered numerous challenges, encompassing various concerns pertaining to security, regulatory compliance, and the need to streamline processes. With our undivided attention directed toward the matter of secu-rity, we embark upon a comprehensive exploration of the potential risks associated with this novel financial landscape. Our primary objective revolves around the thorough investigation of methodologies that can effectively be employed to assess the legitimacy of a DeFi project, specifically focusing on its potential involvement in fraudulent activities.

In this scholarly article, we present a collection of ten widely recognized tools that can be utilized to examine DeFi projects. To ensure the robustness of our study, we carefully gathered a sample of one hundred prominent tokens, employing a random selection process. Subsequently, we conducted a comprehensive evaluation and comparative analysis of each set of tools, diligently assessing their respective advantages and disadvantages. Additionally, we incorporated an additional tool that enables the external examination of DeFi websites, aiming to verify their authenticity and determine whether they are legitimate or potential scam sites. By including this tool, we aim to enhance the reliability and comprehensiveness of our research.

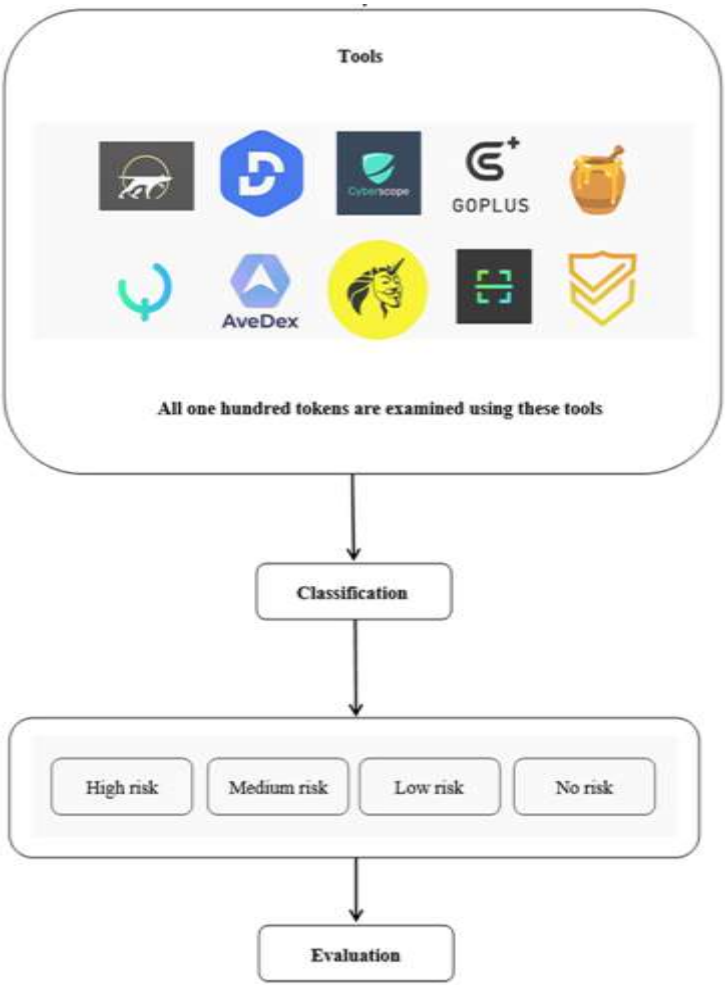

Figure 1. Method for detecting securities violations with a DeFi token smart contract code.

In order to determine which DeFi websites and tools would be included in our study, we meticulously prepared by compiling an extensive list of potential candidates. A com-prehensive evaluation was carried out by thoroughly examining all of the DeFi

websites listed within the “Smart Contracts” category, as well the tools’ websites. The selection process prioritized those DeFi websites that boasted a substantial database, acknowledg-ing the possibility that these platforms might inadvertently attract scammers or even serve as a conduit for their promotion. Consequently, it was imperative that each chosen web-site underwent meticulous scrutiny to ascertain its safety and security credentials. With regard to the selection criteria, reliance was placed on four key factors: (1) DeFi websites that possessed a considerable database; (2) preference for platforms that exhibited a cer-tain level of popularity, allowing users to access them with ease, thereby increasing the likelihood of promoters or scammers utilizing them; (3) our sole reliance on token exami-nation; and (4) random selection of the tokens.

3.1. Data Collection

The selection of the aforementioned platforms (Rugdoc, Ether scan, de.fi, BSc Scan, SolidityScan, Dap Radar, Gecko terminal, Dex screener, and Dex tools) [34, 35, 26, 36, 37, 38, 39, 40, 41] for the current project was based on a number of factors that were taken into consideration. Firstly, one pivotal aspect in the determination of which plat-forms to include was their ease of access. This consideration was of the utmost im-portance, as this project is aimed at catering to individuals who may possess limited ex-perience in the domain of decentralized finance (DeFi) and, as a result, require an interface that is both readily usable and comprehensible. Additionally, the input received from in-dividuals on various communication platforms played a crucial role in the selection pro-cess. It was observed that certain DeFi platforms have gained significant attention and promotion on the Internet. The intensity of this promotion raised suspicions concerning potential scams [42, 23], which prompted the implementation of a scam detector tool as an integral part of our research methodology. This tool allowed us to thoroughly scan the DeFi platforms and associated websites, providing a comprehensive analysis of their le-gitimacy and trustworthiness [15].

These tools, which included DeFi Scanner, Token Sniffer, Token Security Detection, HAPI Labs, Cyberscope, Bscheck, Quick Intel, SolidityScan QuickScan, Honeypot Detector, and Check, were procured from various platforms in order to facilitate user accessibility. The purpose of sourcing these tools from multiple platforms was to ensure that users can easily access them without inconvenience. By having these tools readily available, users can easily perform tasks, such as scan for DeFi vulnerabilities, detect potential token secu-rity breaches, conduct HAPI Labs experiments, analyze cyber threats using Cyberscope, perform quick scans with Quick Intel Scan, verify the solidity of smart contracts using So-liditScan QuickScan, detect potential honeypots with Honeypot Detector, and generate comprehensive reports with the Check feature. The inclusion of these tools sourced from different platforms enhances the overall efficiency and effectiveness of the user experience [26, 28, 29, 30, 31, 32, 13, 14, 10, 12]. Furthermore, the utilization of a diverse range of plat-forms for sourcing these tools exemplifies a comprehensive approach toward providing users with a wide array of options. This methodology guarantees that individuals have the capacity to select the instruments that correspond most effectively with their particular requirements and inclinations. Moreover, the accessibility of these instruments via several platforms bolsters vigorous competition, as each platform endeavors to present the utmost inventive and user-friendly instruments. This competition, ultimately, benefits the users, as they have access to cutting-edge technology and solutions.

In conclusion, the sourcing of these tools from multiple platforms was a strategic decision aimed at enhancing user convenience and promoting healthy competition. The accessibil-ity of these instruments through diverse platforms guarantees that individuals possess an extensive array of alternatives to select from while concurrently fostering ingenuity and progress in the domain. It is of the utmost significance to take into consideration that we did not discriminate between commendable and objectionable tokens

throughout the cu-ration procedure, as randomness was an indispensable facet of our approach to the selec-tion.

3.2. Analysis of smart contracts

For the analysis of the smart contracts, we proposed the following classification scheme: from 0 to 4, high risk; from 5 to 7, medium risk; from 8 to 9, low risk; and 10 safe.

Results and Discussion

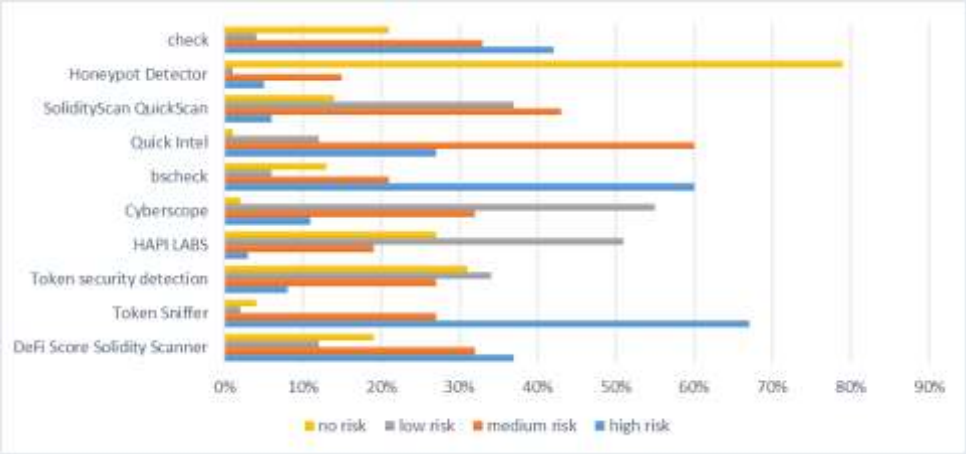

Figure 2. Results of the evaluation of 100 smart contracts using ten tools.

Risk	DeFi Score Solidity Scanner	Token Sniffer	Token security detection	HAPI LABS	Cyberscope	bscheck	Quick Intel	SolidityScan QuickScan	Honeypot Detector	goplusla bs.io
high risk	37%	67%	8%	3%	11%	60%	27%	6%	5%	42%
medium risk	32%	27%	27%	19%	32%	21%	60%	43%	15%	13%
low risk	12%	2%	34%	51%	55%	6%	12%	37%	1%	4%
no risk	19%	4%	31%	27%	2%	13%	1%	14%	79%	21%

Figure 3. Evaluation results.

Figures 2 and 3 show the final results of the evaluation of the tools at detecting secu-rities violations in DeFi projects based on smart contract tokenization. After applying the 10 tools to the 100 tokens used, we found that the best tool for detecting high-risk smart contracts is Token Sniffer, which had a rate of 67%, whereas the BsCheck tool came in second at detecting high-risk contracts. The Honeypot Detector tool had the highest per-centage of protected smart contracts at 79%, and the Quick Intel tool had an average risk of 60%. We noted a discrepancy in the ratios among the tools. Many vulnerabilities were discovered in the tokens, and we focused on spam tokens, also referred to as rug pulls and honeypots, which have a high-risk rating. The tools are insufficient for the detection of spam tokens in a guaranteed manner, as some tools specialize in discovering certain types of vulnerabilities; therefore, we chose ten tools to increase the overall security in DeFi systems.

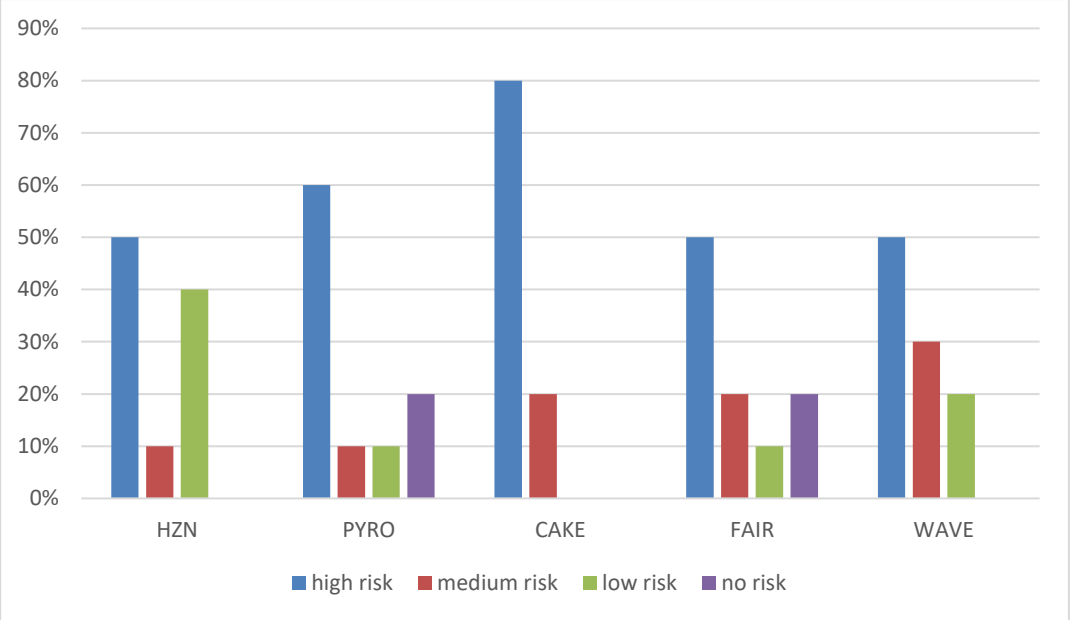

Figure 4. Top five high-risk tokens that were checked or detected using the tools.

The top 5 high-risk tokens out of the 100 tokens were identified, showing that they were detected by all 10 high-risk tools. If we take the CAKE token as an example, the results show that all 10 tools identified it as high-risk, except for the HAPI Labs and Honeypot Detector tools, for which the token was evaluated as having an average medium risk.

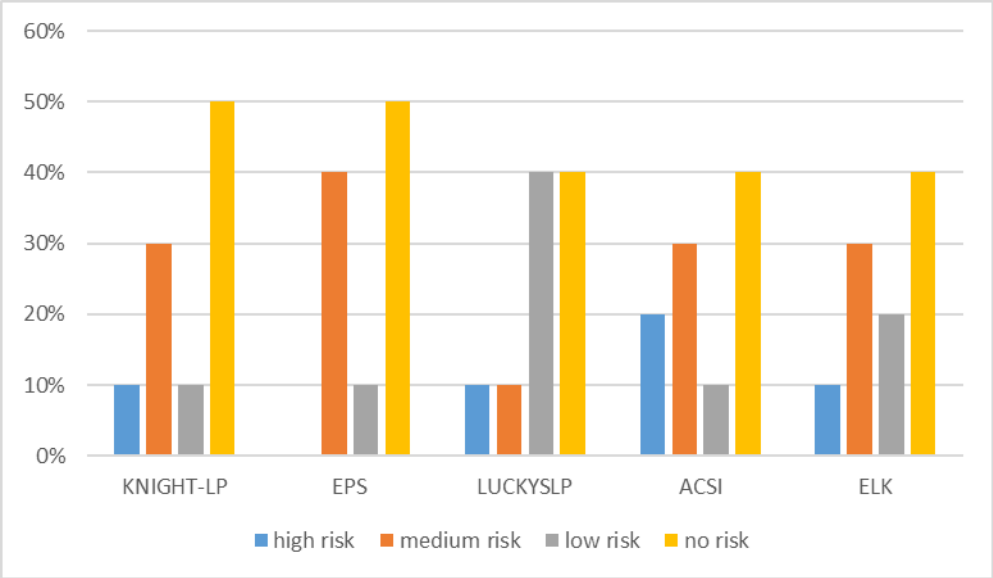

Figure 5. Top five no-risk tokens that were checked or detected using the tools.

The top five no-risk tokens out of the 100 tokens were determined, identified by their high per-centage of being ranked as nondangerous by the 10 tools. If we take the EPS token as an example, 5 out of 10 tools determined it to have a high level of protection, and the rest of the tools catego-rized it as a low risk or medium risk.

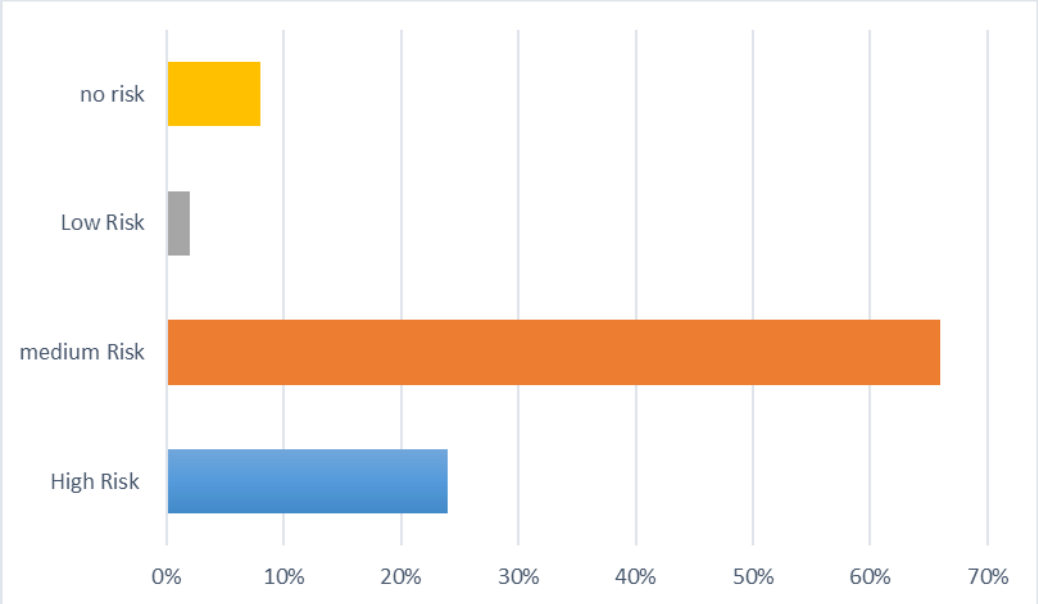

Figure 6. Analysis of DeFi platforms using Scam Detector.

The results show that upon examining approximately 50 DeFi platforms, 66% had a medium risk. We also discovered fraudulent DeFi websites through which fraud and deception were also being carried; these sites were designed to defraud others by promising them a tremendous rate of profit. Users must be careful when entering the world of DeFi, especially those who are new to it, as 24% of the sites were scam sites We also noticed that some tokens were not active with the tools, because they were not available in some databases and could not be verified. It is recommended that users use a token that is able to perform security checks and provide a comprehensive analysis of its advantages and disadvantages. Some tools, such as Bscheck, required a significant amount of time to complete the security check, causing users to feel overwhelmed and turn to alternative tools. The Token Sniffer tool is the best scanning tool for the detection of vulnerabilities that provides ac-curate, reliable, and comprehensive results, as well as detailed analytical reports. In addition, the interface is easy to use for new users and beginners. Finally, on the on our previous investigations, we identified cases of fraudulent activities within the DEFI project. To get started and experiment, individuals must gain knowledge, engage in practical exercises, understand the operating mechanism, and thoroughly verify smart contracts using various methods. These methods include applying the “Know Your Customer” principle when examining smart contracts, as well as con-sidering the opinions of previous users, among other measures.

4.1. Recommendation

When entering the field of decentralized finance (Defi), it is necessary to ensure there exists a reliable team that can assist in all aspects. The following are some of the roles that may need to be filled.

4.1.1. Smart Contracts Developer

Look for developers with sufficient experience in blockchain programming languages, such as Solidity. In addition, their previous projects should be checked to ensure that they have a good understanding of smart contract security best practices.

4.1.2. Blockchain developer

It is necessary to recruit skilled developers in a blockchain ecosystem to handle tasks, such as setting up smart contracts.

4.1.3. Security auditor

A professional security auditor or a company that specializes in smart contract security is required to conduct a comprehensive audit of smart contracts, helping identify weak points and address them before deployment.

4.1.4. User Interface Designer

The backend is essential for handling the logic and data processing of a defi application. Developers with experience building secure and scalable back-end systems should be chosen.

4.1.5. Blockchain consultant

It is advisable to appoint a consultant with experience in the field of decentralized finance. They can provide guidance on industry best practices, regulatory compliance, and help with navigating the complexities of a decentralized ecosystem.

4.1.6. Project Manager

Having a project manager to coordinate and supervise the development process is crucial.

4.1.7. Legal advisor

A legal professional specializing in blockchain and cryptocurrencies should be consulted to ensure that a project complies with the relevant regulations.

4.1.8. Community Manager

Because Defi often includes a community of users, having a community manager to interact with the public, address concerns, and gather feedback is important to the success of a project.

Careful research should be conducted and appropriate caution exercised before investing. With any cryptocurrency endeavor, it is essential to evaluate its validity and legitimacy. It is advisable to be careful when dealing with projects that employ official and financial inducements to imitate legitimate projects, especially during the initial advertising stage. Stay up to date, as knowledge about scams and cryptocurrencies is crucial for the protection of investments. Be aware of the common methods used by individuals seeking to defraud. It is necessary to adopt a skeptical approach to projects that make extravagant promises, such as significant returns, or that implement aggressive marketing strategies to attract potential investors. To ensure the credibility of the project developers and team members, it is necessary to check their professional and personal qualifications and Backgrounds. Seek guidance from trusted sources, such as experienced investors or reputable communities that specialize in cryptocurrencies, before finalizing the investment. Resolutions are highly recommended. In the case of encountering suspicious activities or fraud, it is important to immediately report such incidents to the appropriate authorities or regulatory bodies to protect the interests of fellow investors [43]. The effectiveness of detection and labeling mechanisms for fraudulent tokens can be enhanced through the use of techniques such as inference of guilt by association and machine learning algorithms. User awareness of the risks associated with fraud should be increased by providing educational resources to help identify signs of fraud. Moreover, the promotion of a culture of reporting such activity and suspicious smart contract codes and addresses facilitates the identification and removal of fraudulent codes from a platform. Token listing patterns and liquidity pool creation should be continuously monitored and analyzed to identify any irregular or suspicious activities that may serve as potential indicators of fraud [44].

Conclusions

This paper discusses various aspects of decentralized finance (DeFi) and cryptocurrencies, as well as the use of token scanners for validation and verification. One hundred tokens were identified, randomly collected, screened and evaluated, and nearly 50 DeFi platforms were examined. This has led to a comprehensive study of DeFi and its role in assessing trustworthiness during data transfer. This paper also points out the need for a legal

framework and highlights the limitations and risks associated with privacy, limited information, and single points of failure in DeFi systems. Overall, this paper contributes to the understanding of DeFi and its potential implications for the financial industry. The optimal course of action includes gaining knowledge regarding potential risks and ensuring that activities are compatible with the individual's particular circumstances. Get-ting involved in decentralized finance (DeFi) is lucrative but complex. Before entering the world of Defi, it is necessary to conduct due diligence to verify the legitimacy and security of projects. Among the takeaways regarding DeFi innovation and potential: Decentralized Finance (DeFi) represents a groundbreaking transformation of the traditional financial landscape, providing increased access, transparency, and financial inclusion. Risks and Challenges: Despite its potential, the DeFi space is not without risks. Smart contract vulnerabilities, market volatility, and regulatory uncertainties are among the challenges participants must overcome. Diverse opportunities: DeFi includes a wide range of financial services, including lending, borrowing, decentralized exchanges, and yield farming. Community-centric: Decentralized finance (DeFi) projects often thrive through community engagement and governance. Interacting with the community, understanding the project goals, and assessing community sentiment can provide valuable insights. As mentioned earlier, to ensure the health of projects, methods should be followed that include, for example, code audits, team transparency, community feedback, regulatory compliance, transparency, and documentation. In summary, although DeFi offers exciting opportunities, thorough research and verification is crucial. The combination of technical assessments, community feedback, and legal considerations can help investors and participants make sound decisions in the rapidly evolving DeFi landscape.

Author Contributions: The authors contributed equally to this work.

Funding: This research received no external funding.

References

1. A. B. K. a. T. D. Trozze, "Detecting DeFi Securities Violations from Token Smart Contract Code," 2021. [Online]. Available: https://arxiv.org/abs/2112.02731. [Accessed 15 10 2023].
2. "Binance Academy," [Online]. Available: https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi. [Accessed 10 10 2023].
3. "DocsDe.Fi," [Online]. Available: https://docs.de.fi/security-toolkit/scanner.
4. de.fi, "Whitepaper de.fi," 8 March 2023. [Online]. Available: https://de.fi/whitepaper.pdf. [Accessed 2020].
5. "BlogTokenSniffer," [Online]. Available: https://de.fi/blog/token-sniffer-alternative-defi-scanner.
6. "MediumGoPlusSecurity," 2023. [Online]. Available: https://goplussecurity.medium.com/about.
7. "Medium HAPI LABS," [Online]. Available: https://medium.com/i-am-hapi/hapi-terminal-open-beta-a66693936649. [Accessed 16 Aug 2022].
8. "CyberScope," [Online]. Available: https://www.cyberscope.io/.
9. "cyberscope whitpaper," [Online]. Available: https://www.cyberscope.io/.
10. "bscheck," [Online]. Available: https://bscheck.eu/bsc.
11. "Quick Intel Documentation," [Online]. Available: https://docs.quickintel.io/quicki-scan/introduction.
12. "SolidityScan Docs," [Online]. Available: https://docs.solidityscan.com/.
13. "honeypot Detector," [Online]. Available: https://honeypot.is/.
14. "check," [Online]. Available: https://avedex.cc/check.
15. "Scam Detector," [Online]. Available: https://www.scam-detector.com/.
16. J. S. Dominik Metelski, "Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations," MDPI, vol. 10, no. 4, 2022.
17. F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," p. 22, 2021.
18. T. G. M. P. B. S. N. U. Vincent Gramlich, "A multivocal literature review of decentralized finance: Current knowledge and future research avenues," vol. 33, no. 1, 2023.
19. X. K. T. L. e. a. YINJIE ZHAO, "Toward Trustworthy DeFi Oracles: Past, Present, and Future," IEEE Access, 2022.

20. Y. A.-H. Muhammad Kamran Asif, "ntrusion Detection System using Honey Token based Encrypted Pointers to Mitigate Cyber Threats for Critical Infrastructure Networks," IEEE International Conference on Systems, 2014.
21. M. A. C. L. Z. R. G. A. G. D. M. B. L. Stefanos Chaliasos, "Smart Contract and DeFi Security: Insights from Tool Evaluations and Practitioner Surveys," arXiv, vol. abs/2304.02981, 2023.
22. G. S. e. a. Monika di Angelo, "A Survey of Tools for Analyzing Ethereum Smart Contracts," IEEE , 2019.
23. F. R. A. M. M. V. T. M. N. G. J T Hamrick, "Analyzing Target-Based Cryptocurrency Pump and Dump Schemes," Proceedings of the 2021 ACM CCS Workshop on Decentralized Finance and Security, vol. https://dl.acm.org/doi/abs/10.1145/3464967.3488591, pp. 21-27, 2021.
24. R. C. Z. L. e. a. Peng Qian, "Empirical Review of Smart Contract and DeFi Security: Vulnerability Detection and Automated Repair," arxiv, 2023.
25. "cellularnews.com," [Online]. Available: https://cellularnews.com/definitions/what-is-solidity-features-pros-cons-examples/. [Accessed 6 10 2023].
26. "de.fi," [Online]. Available: https://de.fi/scanner.
27. "academy," [Online]. Available: https://indodax.com/academy/en/advantages-of-the-token-sniffer/. [Accessed 10 11 2023].
28. "Token Sniffer," [Online]. Available: https://tokensniffer.com/.
29. "Token security detection," GoPlus Labs, [Online]. Available: https://gopluslabs.io/token-security. [Accessed 2023].
30. "HAPI LABS terminal," [Online]. Available: https://terminal.hapilabs.one/guest-address-check.
31. "CyberScope tool," [Online]. Available: https://www.cyberscope.io/cyberscan.
32. "Quick intel," [Online]. Available: https://app.quickintel.io/scanner.
33. "solidityscan," [Online]. Available: https://solidityscan.com/. [Accessed 10 11 2023].
34. "RugDoc," [Online]. Available: https://rugdoc.io/project-type/token/.
35. "Etherscan," [Online]. Available: https://etherscan.io/.
36. "BscScan," [Online]. Available: https://bscscan.com/.
37. "solidityscan quickscan," [Online]. Available: https://solidityscan.com/quickscan.
38. "DappRadar," [Online]. Available: https://dappradar.com/rankings/tokens.
39. "GeckoTerminal," [Online]. Available: https://www.geckoterminal.com/.
40. "DexScreener," [Online]. Available: https://dexscreener.com/.
41. "DexTools," [Online]. Available: https://www.dextools.io/app/ar/pairs.
42. T. D. B. K. Arianna Trozze, "Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering," Forensic Science International: Digital Investigation, vol. 46, no. 301575, p. 301575, 2023.
43. S. e. a. Agarwal, "DeFi Deception - Uncovering the prevalence of rugpulls in cryptocurrency projects," Stichting Financial Cryptography/International Financial Cryptography Association, 2023.
44. P. e. a. Xia, "Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange," Proceedings of the ACM on Measurement and Analysis of Computing Systems 5.3, 2021.