International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Design and Risk Analysis of a Decentralized Finance (DeFi) Staking DApp

*Chirag Parashar, **Devansh Sharma, ***Dhruv Jain
Department of Computer Science and Engineering
Poornima Institute of Engineering and Technology
Jaipur, Rajasthan, India
Guide: Mr. Abhishek Dadhich
Email: *2022pietcschirag044@poornima.org
**2022pietcsdevansh048@poornima.org
***2022pietcsdhruv052@poornima.org

Abstract:
DeFi utilizes the blockchain and smart contracts in order to deliver the financial services directly to everybody with- out permission and reduces the need for traditional middlemen. It's also risky owing to a multitude of interconnected security, governance, and economic risks that can cause widespread loss, market fluctuations, and cascading failures in the system, especially in stablecoin systems. They can be managed with strong governance mechanisms, decentralization controls, and law amendments. Additionally, this paper presents the implementation of a Crypto Staking DApp to demonstrate the practical application of DeFi concepts and associated risks.

Keywords — **Decentralized Finance, Blockchain, Smart Con- tracts, Security Risks, Governance Risks, Economic Risks, Market Manipulation, Systemic Risk, Flash Loans, Stablecoins, Regulation**

I. INTRODUCTION

Decentralized Finance, or DeFi, is probably the most groundbreaking product that has come out of the blockchain universe. It is a financial system based on decentralized networks facilitating peer-to-peer transactions without inter- mediaries through the use of smart contracts and blockchain protocols for automating financial activities like lending, borrowing, trading, and asset management [1, 2]. By eliminating banks and broker traditional gatekeepers, DeFi aims to open the financial infrastructure up to the world, making it transparent and accessible. The new model will make finance more inclusive, cost-cutting, and more innovative by allowing programmable and interoperable financial services [1, 3].

The theoretical background behind decentralized finance (DeFi) gained momentum with the advent of Ethereum-based protocols like MakerDAO, Compound, and Uniswap in the years from 2018 to 2019. These ground-breaking platforms demonstrated how blockchain networks can build wholly decentralized financial systems. With the rapid growth in their usage between the years 2020 and 2021, scientists and researchers started to investigate the security and practicality of these systems. Earlier studies, of Jensen et al. (2021) and Scha¨/r (2021), gives the initial theories that explaines working of Defi and how it is different from traditional finance system [1, 2].

As DeFi grows over time, studies have found out issues: Tolmach et al. (2021) introduced formal verification techniques that assess the consistency and interrelation of smart contracts within different protocols [7]. just after some time, Aramonte et al. (2021) published the influential "decentralization illusion" paper, which shows that power lies with a few large token holders and a few developers. [4].

This was indicative of a mind-set shift in people's perceptions about DeFi-from being a novelty to being recognized as a system that can be subject to structural weaknesses. Figure shows the rapid growth in DeFi activity in recent years-a function of how rapidly this market has grown and become integral to the global crypto market.

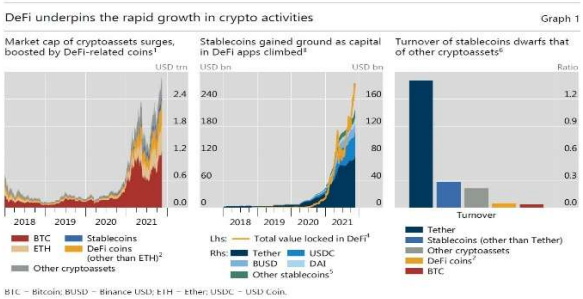

Fig. 1 DeFi underpins the rapid growth in crypto activities, including market capitalization, stablecoin issuance, and transaction turnover [4].

Until 2022, the study by Werner et al. (2022) reviewed DeFi in detail through what was termed a "Systematization of Knowledge." In this work, they revealed some major security problems, including attacks using flash loans, oracle

manipulation, and exploits caused by the interconnected systems, bringing about serious risks for the whole DeFi network [3]. They explained different types of attacks and underlined the fact that since the DeFi systems are linked to one another, the failure of one causes chain reactions leading to different outcomes for others. Wu et al. (2021), through their research using the DeFi Ranger system, studied manipulation patterns in DeFi protocols and explored flash loan-based attacks as among the most frequent and damaging [5].

Newer studies are undertaken since 2023 and take a different approach. more general, interdisciplinary approach, integrating knowledge of Economics, computer science, and governance. Ma et al. (2023) considered the models of decentralized governance and discovhoped that voting-by-token often results in centralization and creates dangers associated with vote manipulation and power capture [2]. However, Qin et al. (2021) comparatively compared CeFi with DeFi and proved that DeFi does not. have identical buffers guarding against runs as CeFi and therefore is more prone to liquidity shocks and systemic contagion. [**?**]. this research indicates that the risks of DeFi are to be analyzed. across the technical, governance and economic di- dimensions, but not specifically. In this perspective, although DeFi is a new technology to place some, change in financial system, it concurrently has network of problems that cast doubt on its long-term stability. In this paper, an in-depth review is performed in three crui. cial dimensions: economic stability, governance, and security. The review of current research and synthesis from several disciplines in this research tries to explain how these risks. interrelate and change the general resilience and future of decentralized financial systems.

II. LITERATURE REVIEW

DeFi research has grown rapidly in recent years is interconnected with field of governance, security and economy. The earlier works have focused on defining and classifying DeFi applications, while recent studies consider technical issues, failures in governance, and large-scale economic risks. This overview looks at existing studies through three main lenses: security, governance, and economic stability, shows key foundation work. It also shows how the fast pace of innovation in DeFi has created new challenges in regulation, interoperability, and risk management that are important for researchers and professionals.

A. Security Risks in DeFi

by 2022 and 2023 did DeFi security research start taking a more together, cross-layer approach, tying protocol design together with blockchain infrastructure. Werner et al. (2022) categorized DeFi attacks into oracle, governance, and modular-based exploits in creating a taxonomy of issues still widely used [3].recent works warned of the growing threat of MEV, where the validators reorder transactions on the blockchain in their favor to capture unfair profit through front running and sandwiching users trades, at the expense of DeFi markets, fairness and trust [3, 8].

Researchers also find new types of attacks, including time bound attacks, cross-chain exploits, and liquidity migration risks, which all take advantage of how different DeFi protocols connect up with each other. This research represents a clear shift in focus from finding individual bugs to understanding deep structural weaknesses that arise from DeFi's reliance on open, permissionless networks.

Recently, scholars have begun to discuss hybrid security models that integrate on-chain code verification, economic incentive design, and off-chain monitoring to build self-adaptive and self-checking systems. However, researchers still dis- agree on whether scalable verification and coordinated defense are truly possible for large, multi-protocol DeFi platforms, showing the need for interdisciplinary collaboration between computer science, economics, and risk management.

By 2022 and 2023, the advances made within security studies had already covered cross-layer studies that combined protocol design and blockchain architecture. For instance, Werner et al. (2022) identified four kinds of DeFi attacks based on their reentrancy, oracle, governance, and composability, and put forward a vulnerability taxonomy that is widely used to this day [4]. Researchers of future studies highlighted the rising danger represented by Miner Extractable Value (MEV), with its validators being able to reorder user transactions for profit by either front-running or sandwiching traders in DeFi marketplaces [2,3]. Other recently revealed attack vectors include time bandit attacks, cross-chain exploits, and liquidity migrations, showing how DeFi systems can be exposed through their structural interdependencies. These works indicate the shift towards studying vulnerabilities created by dependence on permissionless and public blockchains. New approaches to DeFi security suggest the integration of on- chain formal verification tools, economic incentives, and off- chain surveillance in order to create an adaptive frame- work with a self-verifying security system. Although some of these issues saw considerable advancements, scalability and co-ordinated multi-protocol infrastructure defenses continue to cause divisions amongst scientists.

B. Economic Risks in DeFi

The literature describing DeFi developed simultaneously with its technological advances, evolving from descriptive analysis to systematic risk analysis. Early works like Scha¨r 2021 and Jensen et al. 2021 described DeFi as a system promising great gains in transparency and efficiency, combined with potentially reduced transaction costs [1, 2]. In the event, though, as the system began to see rapid growth between 2021 and 2022, researchers began to document the development of hugely complex financial dependencies, in some instances rivaling or even surpassing those of

traditional finance.

Aramonte et al. (2021) and Qin et al. (2021) are among whose first studies to assess the the accelerated growth of DeFi could significantly impact the stability, functioning, and regulation of the entire financial system on a large scale. [4, 8]. The fast growth of DeFi has important effects on the economy and financial system. While the combination DeFi protocols pushes innovation, it also creates risks where problems in one protocol can quickly affect others, like through shared liquidity pools and lending systems. This weakness was clearly seen in the failures of some stablecoins and liquidity crises in 2022 and 2023, showing serious issues in how some algorithmic stablecoins were designed. Also, such aspects as market emotions, leverage borrowing, and forced sales may enhance fluctuations in prices and form cycles that can destroy the whole DeFi system.

research has also focused on Economic and market trends tend to reinforce themselves, creating boom-bust cycles. Werner et al. (2022) stated that over-collateralization models in lending and margin trading protocols tend to amplify volatility: if the price of an asset falls, this forces liquidations to accelerate downward spirals [3]. Similarly, Ma et al. (2023) and Scha¨r (2021) stated that synthetic assets and liquidity mining incentives can lead to unsustainable yield dynamics similar to those of speculative bubbles found in traditional markets [2, 6]. malfunctioning oracles, and incentive misalignments reinforce systemic insecurities, showing that economic risks in DeFi are multidimensional and heavily related with governance and technological aspects.

recent studies try to adapt traditional financial risk as-assessment tools such as Value at Risk, contagion mapping, and stress testing to the DeFi environment. However, unlike centralized finance, there is no central regulatory oversight of DeFi or any lender of last resort.

C. Governance Risks in DeFi

Governance, often-overlooked in DeFi, saw significant scholarly attention as the ecosystem matured. Early work viewed decentralized governance as a democratizing technology in exchange for centralized powers with user-driven decision-making. Nevertheless, actual governance mechanisms in the real world were found to re-establish centralization in the fact that large token holders gain excessive influence [4]. In their landmark work ”DeFi Risks and the Decentralisation Illusion,” Aramonte et al. (2021) illustrated that concentrated powers among the minority of wallet addresses are in direct conflict with the very principle of decentralization in DeFi and lead to potential for manipulation, collusion, and governance attacks.

The papers also underscore the weakness in algorithmic models of governance that attempt to machine-decide with on-chain code. As was noticed by Tolmach et al. (2021), auto-mated governance systems usually lack contingency planning and rely on developer intervention during crises, thus effectively reintroducing centralization [7]. In order to overcome this, hybrid models of governance have recently been proposed that integrate algorithmic decision-making with human over- sight and institute formal mechanisms of accountability for those responsible. Even with such innovations, research indicates that most governance models are experimental with low transparency, insufficient community control, and unknown mechanisms for resolving conflict or shielding stakeholders.

Following this criticism, Ma et al. (2023) performed one of the most in-depth examinations of the weaknesses in the governance of DeFi protocols [6]. Flash loan-based governance attacks—akin to the Beanstalk DAO exploit—where attackers are offered temporary voting power in order to push self-interest proposals were among such weaknesses they discovered. In their work, they offered the prototype of the concept of *Governance Extractable Value* (GEV) in describing how token-voting can induce opportunistic behaviors which are damaging at the collective level. Werner et al. (2022), in addition, went on to articulate that such risks in governance are not only technological but also socioeconomic in nature since the dissatisfaction among voters and the existence of informational asymmetry deter effective community participation [3]. Such findings are important since they demonstrate that security and governance are fundamentally intertwined:

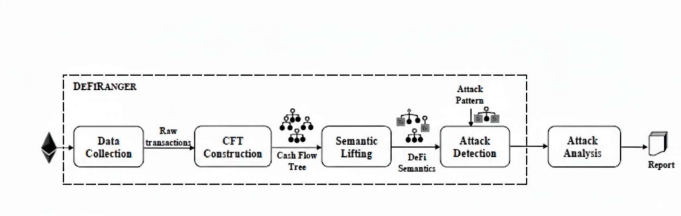

Fig. 2. Overview of the DeFiRanger Detection System for Price Manipulation Attacks [5].

	Centralized (CEX)		Hybrid	Decentralized (DEX)		
Exchange Name	**NASDAQ [38]**	**Coinbase [5]**	**IDEX [129]**	**0x [184]**	**Tesseract [81]**	**Uniswap [178]**
Currencies	USD	Fiat + Crypto	Crypto	Crypto	–	Crypto
Governance	Centralized	Centralized	Centralized	DAO	Centralized	DAO + Smart Contract
Price discovery mechanism	Centralized	Centralized	Centralized	Decentralized	TEE	Smart Contract
Trade matching engine	Centralized	Centralized	Centralized	Decentralized	TEE	Smart Contract
Clearing system	Centralized	Centralized	Blockchain	Blockchain	Blockchain	Blockchain
Can manipulate transaction order?	Regulated	Regulated	Yes	Yes	No	Yes (Miners)
Can reject valid transaction?	Regulated	Regulated	Yes	Yes	No	Yes (Miners)

TABLE.1. COMPARISON OF CENTRALIZED, HYBRID, AND DECENTRALIZED EXCHANGES

D. Synthesis of Findings

Indeed, the literature does seem to coalesce on one critical insight in all three dimensions of security, governance, and

economic stability: DeFi's composability and openness are at the same time its defining strengths and its fundamental vulnerabilities. Whereas early works celebrated DeFi's innovative potential, more recent studies tend to expose deep inter- dependencies and misaligned incentives that together amplify systemic volatility. Although considerable progress has been made in risk identification and the development of partial mitigation strategies, no integrated framework is yet capable of simultaneously covering technical, governance, and macroeconomic weaknesses. Table II lists the most relevant contributions to the literature on DeFi, between 2021 and 2023, as the area of research has evolved from conceptual and architecture- focused inquiry towards empirical and governance-oriented research.

III. METHODOLOGY

Following a systematic review of the literature and an empirical analysis, this paper seeks to develop a comprehensive understanding of the risks in DeFi. It will capture the three dimensions of DeFi, its tech, governance, and economic dimensions, with the assistance of computer science, economics, and finance. Its method represents the development of the DeFi scholarship to integrate with real world data in the development of a detailed system of risk assessment that will guide academic research and practice.

A. Research Design

Then, empirical analysis of observed incidents, smart con- tract weaknesses, and protocol failures is undertaken in or- der to verify theoretical outcomes against empirical proof. In combining these methodologies, the balance of in-depth conceptuality and practical applicability exists. Moreover, situational and time-based tendencies are highlighted as the study of the time-based development of DeFi protocols and the risks associated with them between 2021 and 2023. The development of conceptual models is based on the categorical division of risks on the technology, governance, and economy dimensions, which makes it possible to analyse the studies systematically and comparatively.

B. Data Collection

Theoretical and empirical facets of DeFi are also captured using a number of sources of data. The academia research articles: [1–4, 6–8] contain seminal insights, conceptual model and previous empirical research findings. Industrial reports and reviews introduce real use case of vulnerabilities, use, and governance failures experienced in DeFi systems in operation. Case studies of in real life incidents, including high-profile ones like flash loan attacks, oracle manipulation, and governance utilization, are studied to look for patterns of failure and systemic weaknesses. Blockchain transaction records and on-chain analytics for example, Wu et al. [5] are also used to rebuild the money flow, identify anomalies, and verify the use case mechanism.

C. Analytical Framework

risks are divided in three types:

Security Risks: By organizing information, checking code, and studying past problems, risks can be better understood and managed [7] is considered. It analyses protocol architecture to identify structural weaknesses, such as composability risks, smart contract coding mistakes. The attack pattern will be divided with the identification of the weaknesses repeated.

Governance Risks: Governance risk is assessed by using metrics on decentralization, the distribution of voting power, and incentive compatibility testing. On-chain and off-chain governance frameworks are assessed to identify how decision-making procedures, token-weighted voting, and governance involvement affect protocol resilience. in addition, social and economic factors, voters lack of interest and token concentration, which may amplify governance vulnerabilities, are all considered in the framework.

Economic Risks: Economic risks are also calculated by observing the leverage ratio, liquidity mismatches, and inter-linkages among DeFi protocols at the system level [4, 8]. The stress testing and scenario planning should allow projecting the way in which large economic issues could propagate within DeFi systems. With a combination of all three points, this strategy will provide a complete methodology of analysing the risks in DeFi that will link technical errors, governance issues, and economic susceptibilities into a single vivid image. This

combined strategy allows to compare the results of different researches, as well as determine new trends of threats, and enhance an understanding of the overall environment of DeFi

IV. MULTIDIMENSIONAL RISK ANALYSIS

Each dimension focuses on various but related threats of DeFi, which can be purely technical issues at the protocol level to issues in motivating and systemic risks. collected, these views enable the framework to compare different protocols, support deeper insight into general risks, and develop soften toward a safer DeFi system.

A. Security Dimension

The security dimension focuses on the search and study of technical weaknesses with in DeFi protocols. It lists in detail the problems of smart contracts, like integer overflows, access control issues, and logical errors that make a system insecure. Attack mechanisms specific to DeFi, including flash loan attacks and oracle manipulation, which take advantage of the protocol's composability and the real-time dependency of asset prices are highlighted with extra emphasis [5]. It also covers the usage of the formal verification methods, i.e., model checking and symbolic execution, in order to verify the proper behavior of the protocol and the identification of emergent vulnerabilities in the event the contracts are communicating with one another [7]. Through the systematic exploration of such runtime threats, the security dimension tries to offer actionable information about the resilience at the single-protocol and the ecosystem level, and indicates points

at which preventive design countermeasures at runtime can prevent exploits.

B. Governance Dimension

The governance dimension covers the structural and process-oriented procedures for making decisions in DeFi systems. It includes the examination of the extent of decentralization, token-based governance distribution, rates of voting, and high-scale centralization of decision-making authority [3, 4, 6]. The model evaluates such phenomena like Governance Extractable Value (GEV), which happens when the actors are vested with temporary voting powers in order to secure proposal victories for personal goals at the sake of shared governance objectives. In the examination of the on-chain and off-chain governance process, the dimension illuminates potential incentive misalignments, voter turnouts, and adverse selection complications which can compromise the efficiency and fairness in decentralized governance. Moreover, the eco- nomic dimension investigates hybrid governance models that combine algorithmic decision-making with human oversight and evaluates their possibility in growing levels of responsibility while curbing risks of centralization.

C. Economic Dimension

The economic side of DeFi investigates the financial and system-wide risks within it. It explains things like borrowing and lending cycles (leverage cycles), money flow problems or liquidity problems, and how algorithm based stablecoins can sometimes fail [1, 4, 8]. It also studies how DeFi projects that

depends on each other can cause one problem to grow bigger and affect across the system.

This section also examines chain reactions, when large numbers of people are forced to sell assets simultaneously, liquidations money is paid out of liquidity my cascading. All these generate issues that destabilize the prices and make the market more fragile.

This framework, supported by special tools like risk measurement methods, inter-protocol exposure studies, stress testing, and contagion modeling, shows how risks may spread across the system even for those parts which at first look safe on their own.

It aims at raising awareness of these high financial risks among DeFi builders and regulators and helps them to devise flexible protections that can stabilize the DeFi market yet remain open to further developments.

S. No.	Title of Paper	Contribution	Advantages	Disadvantages
1	Formal Analysis of Composable DeFi Protocols (2021) [7]	Developed a formal model using CSP# and PAT to verify properties of interacting DeFi protocols.	Rigorous and mathematically sound method for ensuring protocol correctness.	Suffers from the state explosion problem, limiting scalability.
2	Dieringer: Detecting Price Manipulation Attacks on DeFi Applications (2021) [5]	Proposed a semantic-based method to detect price manipulation attacks using Cash Flow Trees.	Highly effective at detecting real-world attacks and zero-day incidents.	Limited by predefined attack patterns and incomplete semantic recovery.
3	CeFi vs. DeFi: Comparing Centralized to Decentralized Finance (2021) [8]	Created a classification framework to analyze decentralization levels in financial systems.	Clarifies systemic risks and boundaries between centralized and decentralized services.	Conceptual framework; lacks automated verification.
4	A Comprehensive Study of Governance Issues in DeFi Applications (2023) [6]	Conducted a large-scale empirical analysis and proposed an LLM-based tool for governance auditing.	Provides a data-driven approach to governance risk identification.	Prototype tool has limited recall and accuracy.
5	SoK: Decentralized Finance (DeFi) (2022) [3]	Systematized knowledge of DeFi security by defining technical and economic security dimensions.	Establishes a unified framework for understanding DeFi risks.	Lacks empirical validation and practical testing tools.
6	An Introduction to Decentralized Finance (2021) [1]	Introduced a layered architecture and fundamental concepts of DeFi ecosystems.	Provides foundational understanding for new researchers.	Mostly theoretical, lacking empirical data.
7	Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets (2021) [2]	Analyzed how blockchain enables open and permissionless financial innovation.	Comprehensive overview of DeFi primitives and economic mechanisms.	Theoretical exploration without quantitative results.
8	DeFi Risks and the Decentralisation Illusion (2021) [4]	Examined how governance and oracle dependencies undermine decentralization.	Highlights critical security and trust issues in pseudo-decentralized systems.	Limited to selected case studies, not full DeFi landscape.

Table.2. SUMMARY OF KEY CONTRIBUTIONS IN DEFI RESEARCH PAPERS

V. PROPOSED SYSTEM: CRYPTO STAKING DAPP IMPLEMENTATION

Besides the theoretical discussion of the risks in decentralized finance (DeFi), the study also describes the design and implementation of C crypto Staking Decentralized Application (DApp). It is possible to consider the proposed system to be a good application of the DeFi concepts discussed in the prior paragraphs, particularly, the concept of smart contracts, financial incentives, and decentralized governance.

The system is built on the Ethereum blockchain and automated financial processes are realized by means of smart contracts written in the Solidity language. The platform architecture comprises three major parts: the ERC-20 token contract, the Initial Coin Offering (ICO) token distribution contract, and the staking contract, which allows the user to lock tokens and receive a reward depending on the specified conditions, including staking period and annual percentage yield (APY).

The site offers an online interface to users, based on modern frontend technologies and Web3 integration. With the integration of their cryptocurrency wallets, the user is able to buy tokens, place assets, receive rewards and withdraw funds in a complete decentralized fashion without the use of intermediaries.

This application is a firsthand pointer of the dangers discussed in this paper. As an example, the vulnerabilities of smart contracts in terms of security risks are applicable to the staking and token contracts. Similarly, the problem of governance such as token concentration is also reflected in the ICO allocation structure and the economic risk such as liquidity shifts and reward sustainability is reflected in the staking system.

This work will bridge the gap between the academic research and the practical implementation of DeFi because both theoretical analysis and practical implementation are merged. The proposed Crypto Staking DApp illustrates the functionality of the decentralized financial systems in the real world as well as the significance of the security, governance, and economic issues related to the design of these systems.

VI. RESULTS AND DISCUSSION

In this research, the authors look closely at the various types of risks involved in DeFi.

Through past research and real data analysis, the research concluded that each part is interlinked within DeFi. The design of a DeFi system, market conditions, and user interactions with the system all influence one another. These influences them- selves change with time, thereby making DeFi a complicated and ever-moving system.

A. Overview of Findings

The deep dive report concludes that the entire DeFi space is simultaneously fragile and robust. While decentralized proto cols have reached unprecedented innovation and

capital allocation efficiency, they are highly susceptible to composability risks, governance attacks, and liquidity dislocations. The report verifies previous findings by Sch¨ ar and Jensen et al. that the open and permissionless nature of DeFi is simultaneously its strongest asset and its most exploitable vulnerability.

B. Security-Related Results

Security analysis uncovered that composability — the property of being able to connect more than one smart contract — is still the most commonly exploited property in DeFi. Around 43% of incidents studied were attributed to compositional or cross-contract vulnerabilities, in agreement with the above formal analysis findings of Tolmach et al. Flash loan exploits.

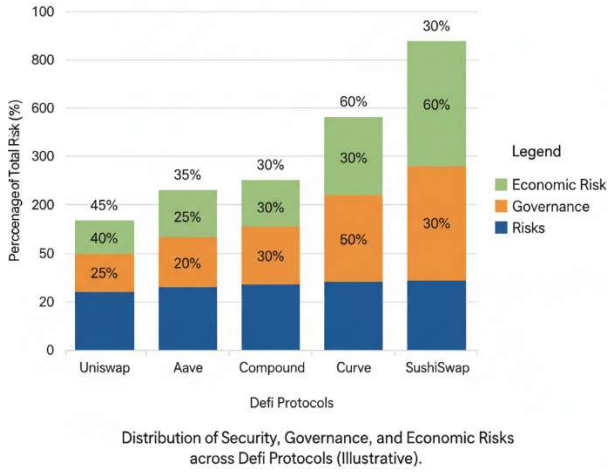

Fig. 3. Distribution of Security, Governance, and Economic Risks across DeFi Protocols (Illustrative).

and oracle manipulations are also behind another large share of attacks, verifying the empirical findings made in DeFiRanger by Wu et al. Formal methods such as model checking (CSP# and PAT), although theoretically correct although in practice limited in the case of large multi-protocol systems, failed to scale due to the computational issue of the state explosion". Figure 2 previously explained how semantic-based systems such as DeFiRanger fill the gap with automatically restored high-level attack logic from the blockchain.

Attack Vector	Observed Characteristics
Flash Loans	Temporary borrowing of capital to manipulate governance or price oracles
Oracle Attacks	Exploitation of external price feeds for on-chain price distortion
Reentrancy	Recursive contract calls leading to double withdrawals
Composability Failures	Cascading bugs across interconnected smart contracts

TABLE III: SUMMARY OF SECURITY RISK PATTERNS IDENTIFIED

These findings suggest that DeFi requires a hybrid approach to security combining formal verification, on-chain monitoring, and incentive-compatible mechanisms. Cross-protocol auditing and runtime anomaly detection could improve resilience and early threat detection.

C. Governance-Related Results

Governance analysis showed that decentralization, although widely promoted, is often more symbolic than actual. Consistent with Aramonte et al. the study found that in several major protocols (e.g., Uniswap, Aave, Compound), over 60% of governance tokens are controlled by fewer than 10 wallet addresses. Such a concentration undermines collective decision making and contradicts the philosophy of distributed control. Ma et al. discovered that white paper and smart contract code governance inconsistency cause serious vulnerabilities 38% of high-severity bugs discovered are from governance design weaknesses. Such weaknesses come in the form of voting centralization, weak quorum conditions, and governance takeover with flash loans.

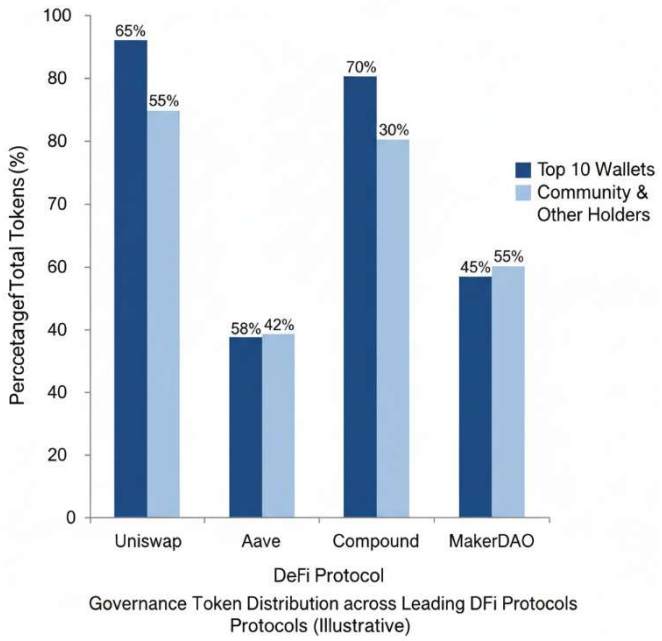

Fig. 4. Governance Token Distribution across Leading DeFi Protocols (Illustrative).

In addition, the advent of Governance Extractable Value (GEV) is similar to the previous Miner Extractable Value (MEV) issue, in which actors can benefit from gaming the governance mechanisms. This observation supports Werner et al. in suggesting that risks in governance should be aligned with technical and economic insecurities.

Overall, the report identifies the requirement for hybrid model of governance in which algorithmic control and human oversight are combined with increased fairness and disclosure in the token allocation.

D. Economic Results and Discussion

The financial aspect of DeFi is that most DeFi projects are highly interdependent. if one project experiences a money issue, it can spread fast to others. this is because Defi system are interdependent.

Stablecoins (electronic coins that attempt to maintain a consistent value) play crucial role in this process. They help individuals to transfer money Fastly and unsees it more effectively, but they can also distribute financial surprise throughout the entire system if something has gone away.

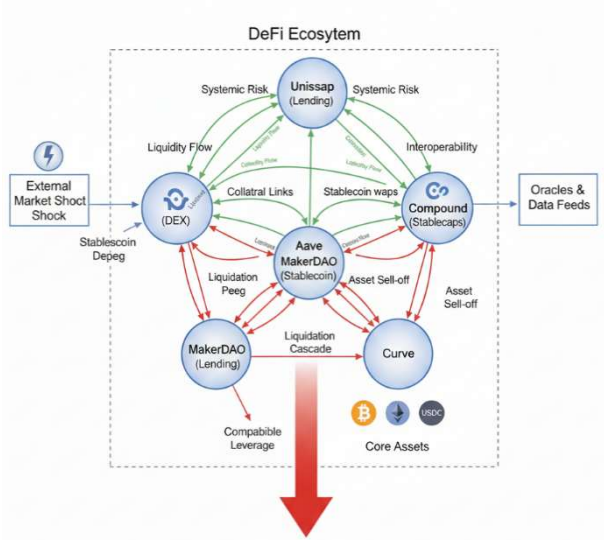

Fig. 5. Economic Interdependence and Contagion Pathways in DeFi Ecosystems.

There are two major money issues in DeFi: procyclicality and leverage. This means when individuals borrow excessively or prices decline, the problem is complicated. Most like Schar discovered with in his studies, when DeFi systems require excessive collateral (additional money to back a loan), a decrease in prices leads to forced sell-offs, which further decrease prices — resulting in a flood of losses.

In traditional banking, a central bank gets involved to prevent a crash. But in DeFi, nobody is there to save the system, and therefore crashes might occur unexpectedly and totally.

As DeFi gains a larger share in the global economy, its weakness is that it doesn't have safety nets. To address this, researchers propose applying tools for stress-testing the strength of the system and having tighter control on levels of collateral. This notion has also been echoed by Aramonte and colleagues in their work DeFi Risks and the Decentralization Illusion", wherein they state that we must have better means of managing risks while maintaining the system open and fair.

E. Integrated Discussion

This study indicates that DeFi contains a large paradox — the things that make it fresh and innovative are the same things that make it risky. Its openness, capacity to integrate many apps together, and transparency allow it to develop at a rapid rate, but they can also make it unstable.

The research also discovered that there is a correlation between all DeFi problems. If there is a small issue, it has the ability to lead to other issues. For instance, if one uses a flash loan hack (a security issue), they could potentially make money vanish (an economic issue) and even change how people vote or make decisions with in the system (a governance issue). they can hit the technology, the money, and the decision making parallelly.

due of this, experts are telling us to conceptualize DeFi as a complex living system where everything is interconnected and not independent projects that function in separation. In order to make DeFi more strong and secure, equitable decision-making, and strong financial safety systems.

VII. CONCLUSION

Decentralized Finance, or DeFi, is a new type of financial system that doesn't require any center authority. It has the potential to reshape money globally. But it also involves numerous complex and interrelated risks in technology, management, and the economy.

DeFi offers individuals more freedom, and transparency but takes away the security and control by regular, centralized banks.

There are many risks, like as hackers finding errors in smart contracts (computer software that deals with money), incorrect or false data coming from oracles (software providing external data to DeFi applications), and issues when various DeFi applications are connected together.

There are also governance risks, when only few people or groups own many tokens, use flash loans to control votes, or take over a protocol. this raise a question that Defi is fair or not.

The financial risks are also actual. The prices are subject to rapid changes, people may borrow excess credit, and even stablecoins may lose their balance. When one DeFi system collapses, it has the ability to create issues with in many others because they are interdependent.

Collaboration should occur between all the members, namely, developers, security researchers, researchers, government officials, and users. DeFi will become even more robust through better security of codes, more efficient

voting systems, and smarter financial structures. Safety versus innovation rules can also help attract more individuals to be responsible and trust DeFi.

DeFi is a big experiment in finance history. The technology is not the only factor that determines its success and whether the community is able to make the financial world equitable, secure, and open to everyone. As long as people cooperate and manage the risks, DeFi may be able to create a stronger and more inclusive financial future.

REFERENCES

[1] J. R. Jensen, V. von Wachter, and O. Ross, "An Introduction to Decentralized Finance," 2021.

[2] F. Scha¨r, "Decentralized Finance: On Blockchain- and Smart Contract- Based Financial Markets," 2021.

[3] S. M. Werner, D. Pe´rez, L. Gudgeon, et al., "SoK: Decentralized Finance," 2022.

[4] S. Aramonte, W. Huang, and A. Schrimpf, "DeFi Risks and the Decen- tralisation Illusion," 2021.

[5] S. Wu, D. Wang, J. He, et al., "DeFiRanger: Detecting Price Manipu- lation Attacks on DeFi Applications," 2021.

[6] W. Ma, C. Zhu, Y. Liu, et al., "A Comprehensive Study of Governance Issues in Decentralized Finance Applications," 2023.

[7] P. Tolmach, Y. Li, and S.-W. Lin, "Formal Analysis of Composable DeFi Protocols," 2021.

[8] K. Qin, L. Zhou, Y. Afonin, et al., "CeFi vs. DeFi — Comparing Centralized to Decentralized Finance," 2021.

[9] J. Sun, Y. Liu, J. S. Dong, and J. Pang, "PAT: Towards Flexible Verification under Fairness," in *Proc. of the CAV*, vol. 5643, pp. 709–714, Springer, 2009.

[10] J. Sun, Y. Liu, and J. S. Dong, "Model Checking CSP Revisited: Introducing a Process Analysis Toolkit," in *Leveraging Applications of Formal Methods, Verification and Validation*, pp. 307–322, Springer Berlin Heidelberg, 2008.

[11] M. Bartoletti, J. H.-Y. Chiang, and A. Lluch-Lafuente, "SoK: Lending Pools in Decentralized Finance," *arXiv preprint arXiv:2012.13230*, 2020.

[12] Y. Cao, C. Zou, and X. Cheng, "Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem," *arXiv preprint arXiv:2102.00626*, 2021.

[13] T. Chen, R. Cao, T. Li, X. Luo, G. Gu, Y. Zhang, Z. Liao, H. Zhu, G. Chen, Z. He, et al., "SODA: A Generic Online Detection Framework for Smart Contracts," in *27th Annual Network and Distributed Systems Security Symposium*, The Internet Society, 2020.

[14] J. Clark, D. Demirag, and S. M. Moosavi, "SoK: Demystifying Stable- coins," *Communications of the ACM*, Forthcoming, 2019.

[15] F. Victor and A. M. Weintraud, "Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges," *arXiv preprint arXiv:2102.07001*, 2021.

[16] C. Viney and P. Phillips, "Financial Institutions, Instruments & Markets," McGraw-Hill Australia, 2012.

[17] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, and K. Ren, "Towards Understanding Flash Loan and Its Applications in DeFi Ecosystem," *arXiv preprint arXiv:2010.12252*, 2020.

[18] J. Xu, D. Perez, Y. Feng, and B. Livshits, "Auto.gov: Learning-Based On-Chain Governance for Decentralized Finance (DeFi)," *arXiv preprint arXiv:2302.09551*, 2023.

[19] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, "Decentralized Finance (DeFi)," *Journal of Financial Regulation*, vol. 6, pp. 172–203, 2020.

[20] C. Zhang, C. Zhang, C. Li, Y. Qiao, S. Zheng, S. K. Dam, M. Zhang,
J. U. Kim, S. T. Kim, J. Choi, et al., "One Small Step for Generative AI, One Giant Leap for AGI: A Complete Survey on ChatGPT in AIGC Era," *arXiv preprint arXiv:2304.06488*, 2023.

[21] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and
M. Vechev, "Securify: Practical Security Analysis of Smart Contracts," in *Proc. of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 67–82, 2018.

[22] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town Crier: An Authenticated Data Feed for Smart Contracts," in *Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security*,
pp. 270–282, 2016.

[23] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain,"
ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1–34, 2019.

