Overview of Decentralized Finance and Theoretical Analysis of Existing Protocols

1st Vincent DiPerna
Virginia Tech
Blacksburg, United States
dipernavz@vt.edu

2nd Gautham Gali
Virginia Tech
Blacksburg, United States
ggali14@vt.edu

3rd Alexander Marrero
Virginia Tech
Blacksburg, United States
alexmarrero10@vt.edu

4th Xinbei Zhu
Virginia Tech
Blacksburg, United States
helen19@vt.edu

***Abstract*—[TEMP] The following paper will be covering the topic of decentralized finance in blockcahin.**

***Index Terms*—Decentralized Finance, DeFi, Blockchain, Smart Contracts, Cryptocurrencies, Protocols, Ethereum, Uniswap, SushiSwap, Curve Finance, Balancer**

I. Introduction

A. CeFi vs DeFi

There are several financial services people around the world use to help manage their money. These services include (but are not limited to) loans, insurance, savings, and stock exchange. Together, these various services which are built around money management help create our financial system. The current system of centralized finance is completely reliant on intermediaries to help manage money such as governments and banks. However, this system is oftentimes inefficient as it is time-consuming to move money around as it has to move using intermediaries such as companies and people. Additionally, these financial services also operate with a charge and are also susceptible to fraud and corruption. This raises the question of how we can design a system to avoid these pitfalls, and if so, will it be effective and can we trust it? The solution to this issue is decentralized finance, or DeFi for short.

While DeFi offers a plethora of opportunities for innovation, its quick rise in popularity has also raised several questions regarding its security, scalability, regulatory uncertainty, and user understanding. Smart contracts are the main building block behind decentralized finance as they can automatically execute code based on specific conditions and criteria. Security is currently the biggest concern in DeFi as smart contracts have been known to contain vulnerabilities that make them prone to hackers such as through reentrancy attacks. Additionally, the scalability of DeFi is an issue as well since a high number of users on the Ethereum network can lead to high gas prices and slow transaction times. Because DeFi is a new and growing field, many regulatory bodies and policy-makers are also trying to determine how to regulate DeFi protocols to help mitigate market manipulation. The novelty of the field has also caused uncertainty among users since many lack understanding of specific applications since they don't understand the technical side.

Although there are several concerns around DeFi, there are also many advantages. Firstly, DeFi is transparent which means that anyone can view the code for applications which helps build a layer of trust. Secondly, DeFi also supports interoperability, which means that different systems can communicate with each other using the Ethereum network. Additionally, DeFi is also free to use which removes traditional monetary barriers to entry such as in CeFi. There are also a wide variety of DeFi applications out there for users and each has its strengths and weaknesses which makes DeFi flexible. Users and companies can also combine platforms to create one protocol with multiple functionalities. This idea has been coined as "Money Legos" which further emphasizes the interoperability of DeFi.

B. Objective

In this paper, we will conduct a theoretical analysis and comparison of existing DeFi protocols and platforms to address these advantages and concerns. Additionally, we'll be analyzing the performance of these protocols and explaining how they work in depth, to help the users compare them. Our team has two main goals for this research paper:

- Develop a clear understanding of DeFi and the various technologies/applications used in it.
- Explore various popular Protocols to help readers gain a deeper understanding of them.

By addressing these two goals, we hope to help uncover the potential of DeFi and provide useful insights for anyone interested in exploring DeFi. We ultimately hope to improve the readers' understanding of DeFi as a whole, and how various protocols work to make decentralized finance efficient and secure.

mds
May 05, 2024

II. Related Work

Decentralized Finance (DeFi) represents a transformative approach in the financial sector, leveraging blockchain technology to operate financial services without traditional intermediaries like banks. This section reviews several papers and research efforts that have significantly contributed to the understanding and development of DeFi systems, focusing on their technological foundations, security challenges, regulatory implications, and operational intricacies.

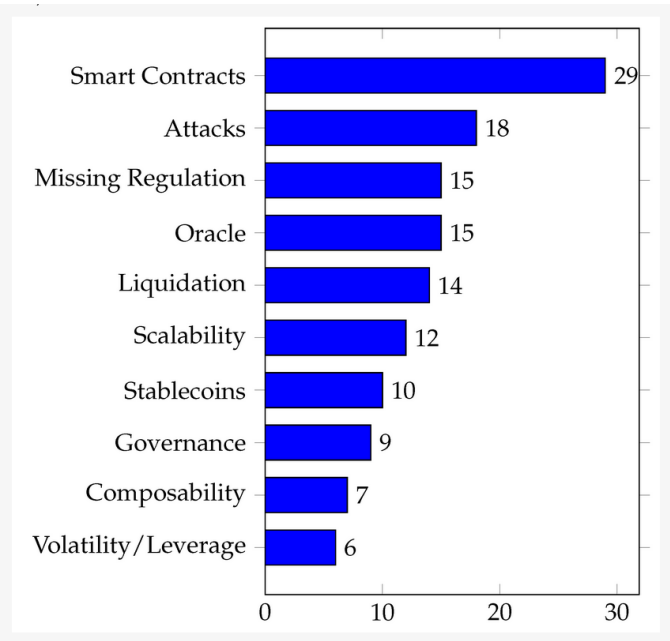

Fig. 1. The ten most-mentioned DeFi risks in the literature

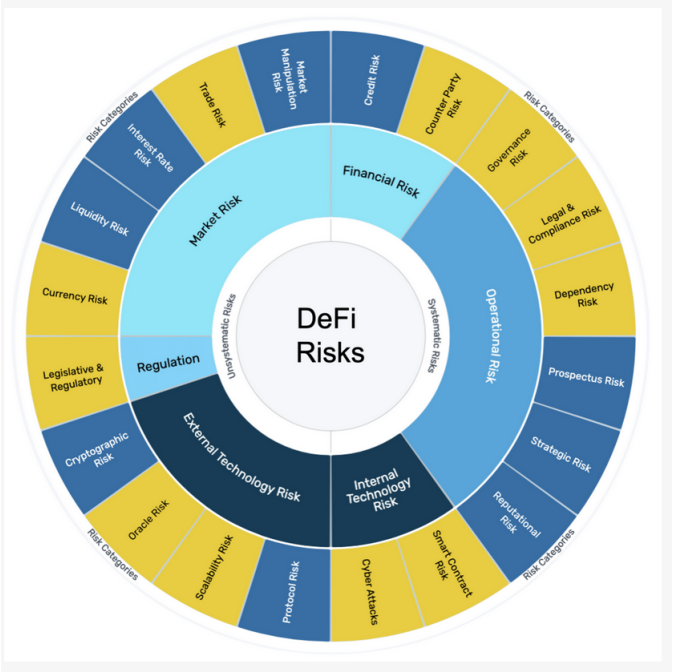

Fig. 2. Suggested risk categories for DeFi. Yellow indicates the top ten risks from the literature, The colors within the inner circle differentiate the DeFi risk categories

A. Blockchain Platforms and DeFi Operations

Extensive research has been conducted on major blockchain platforms like Ethereum, Polkadot, Cardano, and Lukso, with a particular emphasis on their transition to more energy-efficient consensus mechanisms such as proof-of-stake (PoS). These studies highlight the platforms' responses to the environmental challenges posed by the traditional proof-of-work (PoW) systems, illustrating their strategies to reduce carbon footprints while enhancing transaction processing capabilities. For instance, Ethereum's shift to Ethereum 2.0 signifies a major step towards reducing energy consumption by approximately 99 percent, leveraging PoS to maintain network security and consensus. This evolution is pivotal for the broader adoption of blockchain technologies in sectors that prioritize sustainability alongside technological advancement.

B. Data Storage Models in Blockchain

This review also covers in-depth analyses of the contrasting data storage models used in blockchains: UTxO, EUTxO, and account-based systems. Each model offers different advantages and constraints impacting DeFi's operational aspects. For example, Ethereum's account-based model allows for more straightforward execution of stateful applications but at the cost of potential security risks like reentrancy attacks. On the other hand, Cardano's EUTxO model provides enhanced security by avoiding shared states, yet it introduces complexity in designing applications that require multiple steps or interactions. Studies illustrate how these architectural decisions influence the scalability, security, and development flexibility of blockchain platforms, fundamentally shaping the nature and efficiency of DeFi applications built upon them.

C. Security Aspects of DeFi

A groundbreaking tool in this realm is DeFiScanner, a deep-learning-based system designed to identify and mitigate attacks within DeFi platforms. This system's architecture incorporates a comprehensive neural network model that synthesizes global transaction data, local transaction features, and integrated threat intelligence to proactively detect vulnerabilities. Research shows that DeFiScanner effectively enhances security protocols by learning from historical attack patterns, such as those in flash loan schemes, and adapting its detection mechanisms to prevent future exploits. The implementation of such advanced technologies demonstrates the ongoing efforts to secure DeFi environments against increasingly sophisticated attack vectors.

D. Vulnerabilities and Attacks

The discussion extends to specific security challenges in DEXs, particularly focusing on Uniswap and the emerging risks posed by Maximal Extractable Value (MEV) attacks. Research detailed transaction-level analyses on Uniswap, uncovering how MEV attacks exploit transaction ordering within blocks to extract value from users unknowingly. These findings are critical for understanding the security landscape of DEXs and have prompted the development of countermeasures, such as decentralized transaction ordering and enhanced monitoring systems, to safeguard user transactions against such vulnerabilities.

E. DeFi Applications and Their Implications

Significant advancements have been noted in the automation of governmental and trading processes through DeFi applications. Research exploring the automation of Goods and Services Tax (GST) and Letters of Credit (LC) via blockchain showcases how smart contracts can revolutionize traditional bureaucracies. This work proposes a DApp model that automates these processes, ensuring compliance and transparency while significantly reducing administrative overhead. Such applications not only demonstrate the financial capabilities of DeFi but also its potential to impact non-financial sectors by streamlining and securing complex processes.

F. Hamilton Transaction Processor for CBDCs

The Hamilton project represents a significant innovation in DeFi, specifically tailored for the operational needs of Central Bank Digital Currencies (CBDCs). The processor's design is optimized for high throughput and low latency, critical for the demands of modern digital economies. Hamilton's minimalistic approach to data storage on the transaction processor itself allows for scalability and flexibility, paving the way for future adaptations as digital currencies continue to evolve.

G. Ethical and Regulatory Considerations

A study concerning the privacy implications of Web3 technologies sheds light on the paradox between the theoretical privacy assurances provided by blockchain technology and the practical vulnerabilities due to its reliance on existing web technologies. This research is crucial as it highlights the gaps between the intended and actual security outcomes of blockchain applications, urging developers and regulators to address these discrepancies to fully realize the potential of DeFi and Web3 in enhancing user privacy.

H. Using Data from Bitcoin Mixing Services

The ethical considerations of using data from Bitcoin mixing services present a complex scenario, blending legal, moral, and technological issues. This paper discusses the implications of anonymizing transactions and the challenges this poses for both transparency and legality. The analysis underscores a crucial aspect of DeFi's promise versus practice, navigating the thin line between privacy advocacy and potential misuse, which remains a contentious issue within the cryptocurrency community and beyond.

III. Preliminaries

This section of the paper provides a foundational understanding of the technologies and concepts critical to the studies of decentralized finance (DeFi) within blockchain technology. It is imperative to establish a firm grasp of these preliminaries to appreciate the advancements and challenges discussed in the subsequent sections of this paper.

A. DeFi Overview

Decentralized financial services are those that operate without a central authority in charge such as a government or bank. Additionally, these decentralized services use decentralized currencies such as cryptocurrencies like Ether or Dai. Cryptocurrencies can be programmed to automate activities so decentralized exchange services, money markets, and insurance companies can be created. It's also important to note that these services aren't controlled by anyone due to their decentralized nature. These decentralized applications, known as DApps for short, also need to be developed on a decentralized platform, which is where applications such as Ethereum come in.

Ethereum is an open-source blockchain platform that can be used to write automated code known as smart contracts that can be used to build and manage DApps in a decentralized way. Once these DApps are built and deployed on the Ethereum network, the creators no longer have control over it and users can view the code since it is open source. These DApps need a form of currency to run, and an ideal choice to run on the Ethereum network is Ether since it is highly programmable [17]. However, Ether is highly volatile which means that we should use a more stable currency in this system such as Dai, which is pegged against the value of the United States Dollar. Several different cryptocurrencies can be used in the DeFi space, however, Dai and Ether are the most popular. Given these currencies, we can now create applications for our decentralized financial system.

While blockchain, smart contracts, and cryptocurrencies are the backbone of DeFi, applications and software built on top of these act as the engine for this decentralized financial system. These services can even work together with each other to create new kinds of applications similarly to how you can use Lego pieces to build different types of structures. This coined the term "Money Legos" as users can use their creativity to build different applications using existing applications to help meet their specific needs. This has lead to strategies such as yield farming, where users deposit tokens into DeFi applications to earn rewards based on the smart contract to help them earn passive income.

The following sections below cover critical blockchain technology and DeFi technology/concepts in more depth to help the reader gain an understanding of them.

B. Data Storage Models

Two primary data storage models dominate blockchain architectures: the Unspent Transaction Output (UTxO) model and the account-based model. The UTxO model, used by Bitcoin and extended by Cardano (EUTxO), treats each transaction as an output from a previous transaction, ensuring high levels of security and parallelizability. In contrast, the account-based model, employed by Ethereum, views the blockchain as a state machine with accounts holding balances, simplifying direct interactions but introducing complexities in transaction dependencies and potential security risks.

C. Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code. They run on blockchain networks, where they operate in a decentralized manner without the need for intermediaries. Smart contracts are pivotal in automating and enforcing agreement terms, playing a crucial role in the functionality of DeFi applications.

D. Consensus Mechanisms

Blockchain platforms rely on consensus mechanisms to agree on the validity of transactions. These mechanisms include Proof of Work (PoW) and Proof of Stake (PoS), among others. Ethereum's transition from PoW to PoS, for example, marks a significant shift towards more energy-efficient and scalable consensus mechanisms, which is critical for supporting the growth of DeFi applications.

E. Security in DeFi

The security of DeFi platforms is paramount, given the financial and personal data they handle. Studies such as the introduction of DeFiScanner highlight the ongoing need to address vulnerabilities, including smart contract exploits and other attack vectors like those associated with flash loans.

IV. Model

In the following sections, we will be discussing the DeFi model, as well as a threat model and security model. We will also address assumptions associated with the system and security.

A. System Model

Decentralized exchange aggregators, exchange platforms, money markets, and insurance ultimately work together to create the DeFi model. Exchange aggregators such as DEX.AG, Bancor, or Dolomite, are used to find the best prices for trading cryptocurrencies across various platforms. These applications compare prices and provide users with the best trading options across decentralized exchange platforms. Decentralized Exchange Platforms, or DEXes for short, operate similarly to decentralized exchange aggregators as they use smart contracts to allow users to buy or trade cryptocurrencies. While decentralized exchange aggregators give users the best prices for trading cryptocurrencies, DEXes allow users to conduct the exchange between currencies and require no withdrawal fees, identity verification, or exchange operators, which makes them cheaper, safer, and quicker. Examples of these kinds applications include Uniswap, Sushiswap, Balancer, Curve Finance, and PancakeSwap.

Now that we have ways to compare the price of cryptocurrencies and exchange currencies, we need a way to connect borrowers with lenders. Decentralized money markets allow users to this this and even let users lend out cryptocurrencies which they can earn interest on. They also allow users to deposit cryptocurrencies as collateral when borrowing money. Decentralized money market applications also use smart contracts to ensure that loans and interest are distributed properly. This has led to the rise of DeFi lending protocols such as Aave and Compound [15]. While the various kinds of DeFi products on the market help make it efficient, they do come with some level of risk. An example of this would be from vulnerabilities in smart contracts that allow for reentrancy attacks as discussed in the introduction. For this reason, decentralized platforms that focus on insurance have become very popular. [20] Many users on the platform are currently willing to pay high rates for insurance due to the novelty of the field of DeFi which makes it a very profitable market. Examples of insurance applications include Nexus Mutual and Bridge Mutual. These tools work together to help make DeFi a resilient financial system with plenty of potential, which is why the model is appealing to users.

B. Threat Model

While DeFi does have the potential to become very popular and efficient, it does contain several risks that need to be considered when building our threat model. The first risk that needs to be considered is smart contract vulnerabilities. The main technologies that allow for DeFi to exist are blockchain and smart contracts. Everything on the DeFi network is executed using smart contracts, which ultimately eliminates the need for human review to help make it more cost-effective and efficient. However, these smart contracts are developed by humans who are prone to making mistakes due to bugs and inefficiencies in code which creates vulnerabilities. These vulnerabilities allow hackers to exploit logic flaws in a code to steal money. One of the more popular types of attacks is a reentrancy attack, which allows users to reenter code before other code executes which allows them to steal money [19]. An example would be withdrawing money, and then executing the code to withdraw money again before the code to update the account balance executes.

Another common type of attack on DeFi is oracle manipulation, which makes up roughly 15% of attacks [16]. Oracles are software that connect blockchain applications to external systems. Examples of oracles include Chainlink and Band protocol, which both have different strengths and weaknesses when assessing their data trustworthiness [14]. Oracle manipulation occurs when data provided to smart contracts is compromised and manipulated, which leads to DeFi applications being fed inaccurate data. These types of attacks can cause the liquidation of assets and fraudulent transactions to take place which has a significant impact on users. Similarly to other software applications, DeFi users may also be prone to more tradiaional attacks such as phishing attacks.

Additionally, DeFi faces risks from the government as many platforms may need to be change due to legal challenges as the regulation surrounding cryptocurrencies continues to transform due to the novelty of these technologies. Additional regulations could hinder access to services which would impact the ability of users to create DeFi projects [18]. These issues need to be considered when using DeFi applications, which is why we also need a security model as well.

C. Security Model

While many risks are imposed in the field of decentralized finance, they can be addressed and ultimately mitigated to a certain extent. To mitigate smart contract vulnerabilities, developers need to make precautions when developing smart contacts and follow specific procedures to reduce their vulnerabilities to attacks. This can be done through code audits and extensive testing of contracts before deploying them on the Ethereum network. Additionally, including bug bounty programs for contracts would also help find vulnerabilities before they can be exploited.

To mitigate Oracle manipulation vulnerabilities, DeFi developers can make sure that they are using Oracles from highly reputable sources that have been thoroughly tested and have a history of being secure. Additionally, Oracle developers can add data verification mechanisms to ensure that data hasn't been tampered with by outside sources. The number of phishing attacks can also be reduced by more education on the subject, as well as through secure authentication measures such as dual authentication.

Finally, Defi applications can reduce risks faced with regulatory uncertainties by communicating with authorities. Developers should consult with legal professionals on the subject matter to gain insights into what they believe may happen in the future regarding regulations. Additionally, DeFi developers should implement necessary compliance measures in their applications to ensure they are following current rules and regulations like a centralzied bank. A popular compliance measure for centralized banks is know your client (KYC) measures, which ensures that banks take the necessary precautions to ensure user verification and report any suspicious activities. However, it's important to know which compliance measures to follow as following certain compliance measures may lead to the centralization of DeFi.

D. System and Security Assumptions

There are several assumptions for the system and security of DeFi. Firstly, it is assumed that the underlying structures of DeFi which include blockchain, smart contracts, and cryptocurrencies are all completely decentralized. Secondly, it is assumed that once transactions are posted on the blockchain, they cannot be altered or changed. Thirdly, DeFi relies heavily on transparency as anyone can see transaction history and smart contract history to reduce concerns and create a fair system. DeFi also assumes permissionless access meaning that anyone with internet access and a crypto wallet can use applications. Additionally, DeFi is built around open-source development, which means that the community can contribute to the Ethereum codebase to help improve operability and security. Finally, DeFi assumes resistance to cybersecurity attacks, however, these should still be considered to protect against when developing applications.

V. Research Methodology

In this research, we aim to explore the implementation of decentralized finance (DeFi) protocols. Our methodology is designed to provide a comprehensive understanding of these protocols, their design, operation, and potential impact on the DeFi landscape.

A. Approach to Address the Problem

Our approach involves a detailed study and analysis of the protocols. We will dissect their smart contracts, understand their functionalities, and examine their interaction with the Ethereum blockchain.

B. High-Level Idea and Intuition

At a high level, Uniswap, SushiSwap, Curve Finance, and Balancer are all DeFi protocols built on the Ethereum blockchain, each serving as automated liquidity protocols that facilitate decentralized trading of cryptocurrencies.

Uniswap, as a pioneering protocol in this space, introduced the automated market maker (AMM) model, allowing users to trade directly from their wallets. SushiSwap, initially a fork of Uniswap, has since introduced additional features and unique tokenomics, while maintaining the core AMM model.

Curve Finance, on the other hand, specializes in stablecoin trading, offering low slippage and low fee swaps between different stablecoins, optimizing for users who want to trade between assets with relatively stable prices.

Balancer takes the AMM model a step further by allowing liquidity providers to create pools with up to 8 tokens in any ratio, introducing the concept of programmable liquidity.

By understanding these protocols, we can gain insights into the operation and potential of DeFi, particularly the evolution and innovation in the space of decentralized exchanges.

C. Protocol Designs/Algorithms

In this study, we delve into the specifics that power prominent DeFi protocols such as Uniswap V3, Sushiswap, Curve Finance, and Balancer. We focus on smart contract design, security measures, governance, liquidity, slippage, risks, and interoperability.

D. Analysis of Protocol Designs

In the direct evaluation of protocols, we focus on several key metrics:

- **Operational Efficiency** - Operational efficiency in DeFi protocols involves computational and storage efficiency. It can be evaluated by examining the complexity of the protocol's operations and how well its data storage is optimized.
- **Security Infrastructure** - The security infrastructure of a DeFi protocol is assessed by examining the security mechanisms it employs. This includes understanding how the protocol safeguards against prevalent risks in the DeFi sector, such as smart contract vulnerabilities, and price manipulation.
- **Risk Exposure** - Identifying potential vulnerabilities within a DeFi protocol and understanding how they can be mitigated is crucial. This includes analyzing the protocol's smart contracts for potential exploits and assessing the protocol's governance model for potential risks.

- **Liquidity** - For decentralized exchanges, liquidity is a key metric. High liquidity generally leads to better price stability and less slippage, which can attract more users.
- **User Adoption** - The number of active users and the volume of transactions can indicate a DeFi protocol's popularity and trustworthiness.
- **Protocol Governance** - Understanding how decisions are made within a DeFi protocol, who has voting rights, and how changes are implemented can provide insight into the protocol's long-term viability and adaptability.

VI. Implementation and Experiments

A. Uniswap V3 Protocol

- **Implementation Details** - The Uniswap V3 protocol is implemented using Solidity, and is a noncustodial automated market maker implemented for the Ethereum Virtual Machine (EVM). The protocol is implemented using smart contracts that are persistent, and non-upgradeable. They are designed to prioritize security, and to function without (trusted) intermediaries. They are designed to function with 100% uptime, assuming the underlying blockchain remains functioning.
- **Evaluation Metrics** - The evaluation of Uniswap was conducted using several metrics which are
  - **Operational Efficiency** - Uniswap V3 is an automated market maker model which uses the formula $x * y = k$ where x and y represents the quantity of two tokens in the liquidity pool, and k is a constant. This formula is used to reduce drastic changes in prices (slippage) and that the pool remains balanced. However since the Uniswap V3 algorithm is used on the EVM, any operations used can be affected by problems with the Ethereum network, such as congestion (lots of transactional activity) and gas fees (usually high during periods of large transactional activity).
  - **Security Infrastructure** - Uniswap uses smart contracts that are open source, and have been audited by multiple third party sources. Uniswap uses a bug bounty program, which encourages individuals to find and report security vulnerabilities, so any vulnerability, when found will likely be reported, and patched fairly quickly.
  - **Risk Exposure** - There are several risks that Uniswap users may be exposed to. One is called impermanent loss, which can occur when the prices of tokens within the liquidity pool change. When a user attempts to withdraw their share from a pool that has decreased significantly, they may receive less of it, than if they had just stored their tokens outside of the pool.
  - **Liquidity** - The liquidity in Uniswap is determined by the total value of the liquidity pools. This means that more tokens in the pools, results in an increase in the liquidity. The higher the liquidity, the lower the slippage (lower = better for slippage), as described in the next section.
  - **Slippage** - The slippage is defined as the difference between the expected price of a trade, and the price at which the trade is executed. The liquidity is defined as how "easily" an asset can be bought or sold without causing a major price change. In Uniswap the amount of liquidity can be calculated using a formula

$$(x + L\sqrt{p_b})(y + L\sqrt{p_a}) = L^2$$

    The x and y are the quantities of the two tokens in the liquidity pool. L is the amount of liquidity provided, which is equal to $\sqrt{k}$. p_a and p_b are the prices that define the range in which liquidity is provided. Liquidity is inversely proportional to slippage in the Uniswap protocol. If there is a lot of liquidity in a pool, a trade is less likely to cause a major change in the price of the tokens, and vice versa. Trade size matters when using the Uniswap protocol. If the liquidity becomes too small, then a a trade will result in high slippage, and exponentially higher prices. In that respect, if the pools used have relatively small liquidity, it would be preferable to use another AMM that might better protect against this. In practice it is highly unlikely that liquidity will be this small, but it is something to consider.
  - **Price Oracle Accuracy** - The price oracle in Uniswap V3 is used to track the geometric TWAP rather than the TWAP as used in V2. It works by accumulating the current sum of the current tick index, which is the logarithm of the price for base 1.0001. The value is precise up to a single basis point. This method of tracking prices in Uniswap V3 means that the users of the protocol don't need to track separate accumulators for two tokens, which was previously required in V2. The accumulator is also stored more efficiently since it stores $log(p)$ as opposed p. Overall the geometric TWAP is more accurate of the average price over time when compared to the TWAP, and the storage of the data is significantly more efficient since it uses the log representation.
  - **User Adoption** - The Uniswap protocol is in use extensively across multiple chains, primarily Ethereum. In March of 2024, it processed $\$90.11$ billion in monthly volume, and earned market makers about $\$159.25$ million in fees. Liquidity was up to $\$7.19$ billion, which decreases slippage, resulting in more efficient transactions.
  - **Protocol Governance** - Uniswap is governed by UNI ticket holders. The more UNI (a token) a user holds, the greater voting power. This is an example of decentralized governance, and the decisions about the protocol are made by the users of the protocol. While this is very secure in practice, in theory, this kind of governance is theoretically vulnerable to a Sybil attack, where an individual can create multiple identities. In

practice this is highly improbable based on the sheer scale of Uniswap.

B. Kyber Network Protocol

- **Implementation Details** - Kyber Network is a protocol that allows for instant, decentralized token exchange. It operates on the Ethereum blockchain and is powered by smart contracts. The protocol maintains a reserve of all tokens in the network, which are held by Reserve Entities. These entities can be public or private, and they contribute liquidity to the network. When a user wants to exchange one token for another, the protocol automatically finds the best rate among all the reserves.
- **Evaluation Metrics** - The evaluation of the Kyber Network protocol was conducted using several metrics which are
  - **Operational Efficiency** - Kyber Network's on-chain nature ensures high operational efficiency. This means that operations like transacting, and executing smart contracts are completed on the blockchain which is more transparent, and secure. The liquidity pool is also on-chain which means that the reserves are stored on the primary blockchain. It eliminates the need for an order book, which is a common feature in traditional exchanges. This means that users can perform token swaps in a single transaction, without needing to deposit funds into an exchange and wait for a matching order.
  - **Security Infrastructure** - The protocol is built on the Ethereum blockchain, which means it benefits from Ethereum's security model. All transactions are transparent and can be verified on the blockchain. The smart contracts used by Kyber Network have been audited by third-party security firms. The blockchain is decentralized, without a single point of failure. It is permission-less which allows anyone to contribute liquidity. There is price manipulation protection since smart contracts verify that the conversion rate is not too dissimilar from the market rate.
  - **Risk Exposure** - The on-chain nature of Kyber Network reduces the risk of counter-party default. Users don't need to trust an intermediary with their funds, as transactions are peer-to-peer. There could be vulnerabilities in the smart contracts that are executed, but there have been numerous audits to minimize this risk.
  - **Liquidity** - Kyber Network aggregates liquidity from various sources into a single pool, which it calls a "decentralized liquidity network". This includes token projects, liquidity pools, and market makers. This ensures that the network can always provide competitive rates. The network looks through the multiple reserves, and selects one that can provide the best market rate for the trade. The structure of the Kyber network, allows anyone to contribute liquidity, by setting up a reserve. This increases the overall liquidity, and decreases the change of slippage as a result. There is an incentive to provide liquidity, which encourages more participants in liqudity. This improves the rates for all users, which is a major benefit of Kyber.
  - **Slippage** - Slippage refers to the difference between the expected price of a trade and the price at which the trade is executed. High slippage usually occurs in low liquidity environments. However, because Kyber aggregates liquidity from various sources, it can minimize slippage, even for large trades.
  - **Price Oracle Accuracy** - Kyber Network provides an on-chain price feed, which is updated with every trade. This makes it resistant to price manipulation. The price feed can be used by other DeFi protocols that need reliable, on-chain price information.
  - **User Adoption** - Kyber Network is widely adopted due to its versatility. It can be integrated into any application, including wallets, websites, and DeFi dapps. This makes it easy for users to perform token swaps without leaving their preferred environment.
  - **Protocol Governance** - Kyber Network has transitioned to a decentralized autonomous organization (DAO) model for governance. This means that decisions about the network are made by KNC token holders. They can vote on various proposals, including changes to network parameters and the allocation of network fees.

C. Curve Finance

- **Implementation Details** - Curve Finance is a protocol running on the Ether blockchain primarily implemented using Solidity that uses smart contracts to automate and optimize stablecoin trading. The platform uses an automated market maker (AMM) model designed specifically for stablecoins, which helps minimize slippage and maintain efficient pricing. Curve's liquidity pool is essentially a reserve of different stablecoins, which can be dynamically adjusted to ensure that rates within the platform correlate closely with actual market rates. This mechanism allows Curve to offer its users a low slippage rate and higher trading efficiency than traditional exchanges. Users provide liquidity to these reserves and receive transaction fees and rewards in return, which improves the overall liquidity and stability of the platform [8].
- **Evaluation Metrics** - The evaluation of the Curve Finance protocol was conducted using several metrics which are
  - **Operational Efficiency** - Curve Finance is often considered very efficient in its operations thanks to its dedicated Automated Market Maker AMM algorithms that are optimized for stablecoins. Curve's focus on the stablecoin market also allows it to maintain low volatility and provide predictable returns, which is essential for maintaining high operational efficiency in the often volatile cryptocurrency environment.

- **Security Infrastructure** - Curve Finance strengthens its security through regular and rigorous audits of its smart contracts by reputable third-party companies, decentralized governance of security decisions made by the community, and decentralized insurance protocols to cover potential losses due to breaches . Additionally, the focus on stablecoin trading limits the risk of extreme market volatility and provides a safer trading environment. Together, these measures strengthen the platform's security infrastructure and are designed to effectively protect user investments.
- **Risk Exposure** - Curve Finance faces several risks typical of decentralized finance platforms, including smart contract vulnerabilities, which may remain exploitable despite extensive audits. The platform also faces liquidity risks, with mass withdrawals potentially destroying pool balances, as well as short-term losses, particularly in pools involving non-stable coins. Regulatory changes are another significant risk, as changes in legislation could impact operations or asset values. Additionally, Curve's integration with other DeFi protocols introduces systemic risk of potential vulnerabilities in these platforms. These factors require users and investors to exercise constant vigilance regarding Curve's risk management practices and the broader DeFi environment [9].
- **Liquidity** - Curve's liquidity pool is powered by users who deposit assets into it to earn transaction fees and sometimes additional rewards in the form of CRV tokens (Curve's native cryptocurrency). This incentive structure promotes a high level of liquidity supply. Curve also incorporates a governance system that allows CRV token holders to vote on a wide range of decisions related to the development and operation of the platform, such as changes to the fee structure or the addition of new liquidity pools. . This decentralized governance helps align the interests of those involved and maintain the adaptability and security of the protocol.
- **Slippage** - Curve Finance focuses on stablecoins and assets of similar value, which effectively reduces slippage. The design of its AMM is optimized for these asset types, ensuring that trades can be executed close to market averages without significantly impacting prices. This design is particularly beneficial in high-volume trading environments, where the protocol maintains price stability and reduces the gap between expected prices and actual trade execution prices, making it the platform of choice for users looking to trade stablecoins with minimal losses.
- **Price Oracle Accuracy** - Curve Finance uses a trusted external price tipster to ensure the accuracy of its price data, which is essential for fair and stable trading of stablecoins and similar assets. This configuration helps avoid price manipulation and provides reliable market rates, thereby increasing the security and efficiency of the platform.
- **User Adoption** - With its efficient stablecoin trading mechanism and low slippage rate, Curve Finance has been widely adopted by users, attracting both individual and institutional players in the DeFi space. The focus on liquidity and integration with other DeFi protocols strengthens its attractiveness.
- **Protocol Governance** - Curve Finance is governed by its Decentralized Autonomous Organization (DAO) which uses CRV tokens. Token holders can suggest and vote on changes to the deal, influencing decisions on fee structures, liquidity pools, and other key aspects. This model promotes community engagement and aligns with the decentralized principles of DeFi, allowing Curve to dynamically adapt based on participant contributions.

D. Balancers

- **Implementation Details** - Balancer is a decentralized protocol running on the Ether blockchain that uses smart contracts to automate multi-asset market making. The protocol allows users to create liquidity pools comprising up to eight different tokens, each with adjustable weights to meet specific portfolio strategies. These pools dynamically adjust their balances through trading activity, supporting automatic trading and rebalancing. [**?**]
- **Evaluation Metrics** - The evaluation of the Curve Finance protocol was conducted using several metrics which are
  - **Operational Efficiency** - Balancer's operational efficiency stems from its customizable liquidity pool on the Ether blockchain, which allows users to set different weightings for up to eight different tokens. This flexibility allows precise control of asset exposure and rebalancing, which increases trading efficiency and reduces slippage. The protocol also uses intelligent order routing to ensure that trades are executed in different pools at the best available price, thereby optimizing trading costs. Additionally, incentivizing liquidity providers through transaction fees and BAL tokens ensures a steady supply of liquidity, further improving market efficiency.
  - **Security Infrastructure** - Balancer uses multiple strategies to protect its decentralized finance (DeFi) platform. It leverages ongoing, comprehensive smart contract audits conducted by respected companies in the blockchain security spaces, such as Trail of Bits, ConsenSys Diligence, and OpenZeppelin, to ensure vulnerabilities are identified and mitigated by timely. Additionally, the protocol uses a modular architecture that isolates different functions and minimizes the risk of system failure. Balancer also includes license-free and custodial-free features that allow users to maintain control of their assets without an intermediary, reducing the risk of centralized points of failure. All of these

measures strengthen Balancer's security, making it a resilient platform in the DeFi ecosystem.

- **Risk Exposure** - Balancers' risk exposure is multi-faceted and arises from smart contract vulnerabilities, market volatility and regulatory changes. Despite rigorous audits carried out by reputable companies to mitigate risks associated with code, there may still be inherent vulnerabilities that can be exploited. The fact that the protocol relies on external price predictions also introduces risks related to price manipulation or incorrect predictions. Market risks include significant fluctuations in asset prices, which can result in short-term losses for liquidity providers. Additionally, the evolving regulatory environment introduces compliance risks that could impact operational stability and user confidence [9].
- **Liquidity** - Balancer's liquidity is enhanced by its unique protocol design, which allows the creation of multi-asset liquidity pools with customizable ratios. Balancer's dynamic fee adjustment mechanism also optimizes transaction fees based on market conditions, further incentivizing liquidity provision by ensuring providers are properly compensated for risk.
- **Slippage** - The combination of Balancer's customizable pool weights and dynamic fees helps ensure that slippage on the platform remains competitive, even in volatile market conditions, increasing the platform's appeal to traders and liquidity providers.
- **Price Oracle Accuracy** - Balancer's price prediction accuracy is enhanced by the integration with Chainlink, which provides robust and reliable market data for its trading algorithms. This partnership allows Balancer to access decentralized and tamper-proof price information, which is essential for maintaining the integrity of transactions in its liquidity pool. Using multiple independent sources of pricing information helps mitigate risks associated with single points of failure or price manipulation. Additionally, Balancer's asset pools can be designed to include a variety of differently weighted assets, which inherently promotes price stability by spreading risk exposure and reducing the impact of abnormal price movements in any single asset.
- **User Adoption** - Balancer has demonstrated significant user adoption in the DeFi space, attracting approximately 25,000 liquidity providers and managing over $3 billion in locked liquidity. This level of participation highlights Balancer's role as a decentralized exchange and a major player in the liquidity provision market.
- **Protocol Governance** - Balancer's protocol governance is implemented through a decentralized autonomous organization (DAO), which uses its native BAL token to give token holders voting rights on key protocol decisions. Governance recommendations can range from adjusting fee structures and protocol upgrades to changing the distribution of mining liquidity.

VII. Conclusion

Throughout our research on decentralized finance protocols, we've determined that there is not a single solution for every protocol-related problem. Through the evaluation of the protocols described above we can see that they are all thoroughly vetted using third-parties which is necessary for confidence in the protocol, and security. They do face similar risks across all the protocols analyzed including smart contract vulnerabilities, and the fact that integration with other protocols means that the attack surface is increased. The biggest differences observed between the protocols was the methods of maintaining liquidity, and reducing slippage. In terms of liquidity, some protocols focused on aggregating liquidity from various sources, while others focused on other methods such as multi-asset liquidity pools. Methods of slippage also were a notable difference between the protocols, with some focusing on dynamic fees for changing market conditions, while others focused on using stable-coins to reduce slippage.

VIII. Statement of Work

A. Vincent DiPerna

Vincent DiPerna was primarily focused on the Research Methodology, and Implementation and Experiments section. He detailed how the protocols would be analyzed. He included information explaining the high level ideas, and analysis of the protocols in several respects. He focused on two protocols in particular, which were the Uniswap V3 protocol, and the Kyber Network protocol. He researched both of these protocols in depth, and compiled a database of information on the protocol focusing primarily on operational efficiency, security infrastructure, risk exposure, liquidity analysis, user adoption, and protocol governance. He focused on these aspects specifically since they can be evaluated for a wide range of protocols, and allow for a comprehensive analysis of the protocol.

B. Gautham Gali

Gautham Gali was helpful in the Literature Review and Analysis part, where he critically reviewed and analyzed a wide range of scholarly literature relevant to Decentralized Finance (DeFi). He selected and curated relevant publications, offered critical analysis on a variety of topics, including security concerns and regulatory consequences, and performed comparison studies to better understand changing research trends. His rigorous documenting and integration of findings created the research process, which influenced the experimental designs used by his team. Gautham's thorough approach guaranteed that the study was based on a sound theoretical foundation and represented the most recent advances in DeFi, therefore increasing the overall depth and quality of the research.

C. Alexander Marrero

Alexander Marrero primarily focused on the Introduction and Model sections. In the introduction section, Alexander

compared Centralized Finance (CeFi) to Decentralized Finance (DeFi) and also explained the main objects of the paper. In the model section, Alexander explained the System Model for DeFi, as well as the Threat Model, Security Model, and Assumptions that are already made when analyzing DeFi. Alexander also wrote the DeFi overview section in the Preliminaries section, which details how cryptocurrencies are used in DeFi and how services can interact together. Additionally, Alexander also helped write the Conclusion, Abstract, and Index Terms sections.

D. Xinbei Zhu

Xinbei Zhu focused on the detailed analysis of two prominent DeFi protocols: Curve Finance and Balancer. Specifically, her investigation delved into the operational efficiency, security infrastructure, risk exposure, liquidity, user adoption, and protocol governance of Curve Finance and Balancer. By examining these areas, she aimed to compile a robust information system that will serve as a foundational resource for understanding and comparing the mechanisms and impacts of these protocols.

REFERENCES

[1] Radhakrishna Dodmane, et al., *Blockchain-Based Automated Market Makers for a Decentralized Stock Exchange*, Information [Basel], vol. 14, no. 5, May 2023, Available at: here. Accessed 26 Apr. 2024.

[2] Andry Alamsyah, et al., *A Review on Decentralized Finance Ecosystems*, Future Internet, vol. 16, no. 3, Feb. 2024, Available at: here. Accessed 26 Apr. 2024.

[3] Vijay Mohan, *Automated market makers and decentralized exchanges: a DeFi primer*, Financial Innovation, vol. 8, no. 1, 14 Feb. 2022, Available at: here. Accessed 26 Apr. 2024.

[4] Petar Radanliev, *The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse*, Financial Innovation, vol. 10, no. 1, Dec. 2024, Available at: here. Accessed 26 Apr. 2024.

[5] Tim Weingärtner, et al., *Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance*, Journal of Risk and Financial Management, vol. 16, no. 10, Oct. 2023, Available at: here. Accessed 26 Apr. 2024.

[6] Bikramaditya Ghosh, et al., *Do Automated Market Makers in DeFi Ecosystem Exhibit Time-Varying Connectedness during Stressed Events?*, Journal of Risk and Financial Management, vol. 16, no. 5, Apr. 2023, Available at: here. Accessed 26 Apr. 2024.

[7] Bikramaditya Ghosh, Dimitrios Paparas, *Is There Any Pattern Regarding the Vulnerability of Smart Contracts in the Food Supply Chain to a Stressed Event? A Quantile Connectedness Investigation*, Journal of Risk and Financial Management, vol. 16, no. 2, Jan. 2023, Available at: here. Accessed 26 Apr. 2024.

[8] Shuangge Wang, Bhaskar Krishnamachari, "Optimal Trading on a Dynamic Curve Automated Market Maker", 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China: IEEE, May. 2022, pp. 1-5.

[9] J. Chen et al., "Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild," 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, Netherlands, 2023, pp. 332-351.

[10] N. Ivanov, Q. Yan and A. Kompalli, "TxT: Real-Time Transaction Encapsulation for Ethereum Smart Contracts," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1141-1155, 2023.

[11] J. Su, J. Liu, Y. Nan and Y. Li, "Security Evaluation of Smart Contracts based on Code and Transaction - A Survey," 2022 International Conference on Service Science (ICSS), Zhuhai, China, 2022, pp. 41-48.

[12] S. S, A. R. Saxena, Y. R. Saxena, M. S. M. Sana, S. Verma and S. Roy, "Decentralized Finance and Cross-Chain Interoperable Automated Market Maker - Using BlockChain," 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 2024, pp. 1-9.

[13] D. Churiwala and B. Krishnamachari, "QLAMMP: A Q-Learning Agent for Optimizing Fees on Automated Market Making Protocols," 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait, Kuwait, 2023, pp. 274-281.

[14] Y. Zhao, X. Kang, T. Li, C. -K. Chu and H. Wang, "Toward Trustworthy DeFi Oracles: Past, Present, and Future," in IEEE Access, vol. 10, pp. 60914-60928, 2022, doi: 10.1109/ACCESS.2022.3179374. keywords: Blockchains;Insurance;Soft sensors;Feeds;Flowcharts;Finance;Smart contracts;DeFi;oracles;blockchain;trustworthiness,

[15] B. Sriman and S. G. Kumar, "Decentralized finance (DeFi): The Future of Finance and Defi Application for Ethereum blockchain based Finance Market," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-9, doi: 10.1109/ACCAI53970.2022.9752657. keywords: Privacy;Protocols;Buildings;Finance;Organizations; Bitcoin;Blockchains;Blockchain;Decentralized Financial [Defi];Ethereum platform;Crypto-coins;Digital Ledgers

[16] L. Zhou et al., "SoK: Decentralized Finance (DeFi) Attacks," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 2444-2461, doi: 10.1109/SP46215.2023.10179435. keywords: Privacy;Smart contracts;Ecosystems;Finance;Decentralized applications;Frequency measurement;Security,

[17] H. Teng, W. Tian, H. Wang and Z. Yang, "Applications of the Decentralized Finance (DeFi) on the Ethereum," 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2022, pp. 573-578, doi: 10.1109/IPEC54454.2022.9777543. keywords: Computers;Technological innovation;Image processing;Conferences;Supply chains;Smart contracts;Insurance;Decentralized Finance;blockchain technology;cryptocurrency,

[18] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner and B. Schlosser, "DeFi-ning DeFi: Challenges & Pathway," 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 2021, pp. 181-184, doi: 10.1109/BRAINS52497.2021.9569795. keywords: Economics;Smart contracts;Finance;Blockchains;Financial services;blockchain;finance;contracts;distributed ledgers,

[19] W. Li, J. Bu, X. Li and X. Chen, "Security Analysis of DeFi: Vulnerabilities, Attacks and Advances," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 488-493, doi: 10.1109/Blockchain55522.2022.00075. keywords: Economics;Protocols;Ecosystems;Finance;Blockchains;Security;Optimization;Smart contract;Ethereum;Decentralized finance;DeFi,

[20] M. Nadler, F. Bekemeier and F. Schär, "DeFi Risk Transfer: Towards A Fully Decentralized Insurance Protocol," 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, 2023, pp. 1-9, doi: 10.1109/ICBC56567.2023.10174937. keywords: Economics;Protocols;Insurance;Finance;Trustless services;Peer-to-peer computing;Proposals;Blockchain;DeFi;Decentralized Insurance;Risk Transfer;Smart Contracts,

[21] M. Hodgson, "Designing Matrix: A Global Decentralised End-To-End Encrypted Communication Network," 2023 SREcon23 EMEA, Www.usenix.org, 2023, www.usenix.org/conference/srecon23emea/presentation/hodgson. keywords: Communications; Security; Encryption; Network Architecture; Distributed Systems; Privacy; Open Source Software,

[22] M. Andoni, et al., "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities," Renewable and Sustainable Energy Reviews, vol. 100, no. 1, Feb. 2019, pp. 143-174, www.sciencedirect.com/science/article/pii/S1364032118307184, doi: 10.1016/j.rser.2018.10.014. keywords: Blockchain; Energy Sector; Systematic Review; Renewable Energy; Sustainable Energy; Technological Innovation; Energy Markets,

[23] M. Bijlsma, et al., "What Triggers Consumer Adoption of CBDC?" SSRN Electronic Journal, 2021, doi: 10.2139/ssrn.3836440. keywords: Central Bank Digital Currency (CBDC); Consumer Behavior; Financial Technology; Adoption Factors; Digital Payments; Monetary Policy; Economic Innovation,

[24] N. Z. Aitzhan and D. Svetinovic, ”Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, 1 Sept. 2018, pp. 840-852, doi: 10.1109/tdsc.2016.2616861. keywords: Decentralized Systems; Energy Trading; Blockchain Technology; Security; Privacy; Multi-Signatures; Anonymous Communications,

[25] C. Ferreira Torres, F. Willi, and S. Shinde, ”Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3,” presented at USENIX Security Symposium, ETH Zurich, 2023, https://www.usenix.org/conference/usenixsecurity23/presentation/torres. keywords:Web3; Privacy; Cryptocurrency Wallets; Blockchain Technology; Cybersecurity; Digital Identity; Financial Privacy,

[26] F. Miedema, K. Lubbertsen, V. Schrama, and R. van Wegberg, ”Mixed Signals: Analyzing Ground-Truth Data on the Users and Economics of a Bitcoin Mixing Service,” presented at USENIX Security Symposium, Delft University of Technology, 2023, https://www.usenix.org/conference/usenixsecurity23/presentation/miedema. keywords: Bitcoin; Cryptocurrency; Mixing Services; Financial Privacy; User Behavior; Blockchain Analytics; Economic Analysis,

[27] P. Raghunathan, S. Shibu, and P. Rekha, ”Design of Blockchain DApps to Simplify GST and Letter of Credit Processes in Deregulated Financial Services,” 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 2022, pp. 1-6, doi: 10.1109/ASIANCON55314.2022.9908740. keywords: Technological innovation;Scalability;Smart contracts;Government;Finance;Banking;Decentralized applications;Blockchain Technology;Decentralized Applications;DApps;Ethereum;Decentralized Finance Systems;DeFi,

[28] C. Busayatananphon and E. Boonchieng, ”Financial Technology DeFi Protocol: A Review,” 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT and NCON), Chiang Rai, Thailand, 2022, pp. 267-272, doi: 10.1109/ECTIDAMT-NCON53731.2022.9720373. keywords: Operating systems;Smart contracts;Finance;US Department of Transportation;Decentralized applications;Blockchains;Financial services;DeFi Protocol;Smart Contract;Centralized Exchange;Binance;Ethereum Virtual;Proof-of-work;Proof-of-stake;Staking;Market Capitalization Decentralized Application;EcoSystem;Liquidity Pool;Liquidity Mining,

[29] B. Wang et al., ”DeFiScanner: Spotting DeFi Attacks Exploiting Logic Vulnerabilities on Blockchain,” IEEE Transactions on Computational Social Systems, vol. 11, no. 2, April 2024, pp. 1577-1588, doi: 10.1109/TCSS.2022.3228122. keywords: Feature extraction;Ash;Semantics;Blockchains;Security;Smart contracts;Ecosystems;Attacks detection;blockchain;decentralized finance;deep learning,

[30] A. V. Pomogalova, A. A. Martyniuk, and K. E. Yesalov, ”Key Features and Formation of Transactions in the Case of Using UTxO, EUTxO and Account Based Data Storage Models,” 2022 International Conference on Modern Network Technologies (MoNeTec), Moscow, Russian Federation, 2022, pp. 1-7, doi: 10.1109/MoNeTec55448.2022.9960753. keywords: Solid modeling;Codes;Smart contracts;Buildings;Memory;Public key;Decentralized applications;UTxO;EUTxO;Account Based storage;blockchain;transaction;Cardano;Ethereum,

[31] N. Balpande and S. Prasad, ”Blockchain Solutions: Blockchain as a Service and Implementation Strategies,” 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 1349-1354, doi: 10.1109/ICAISS58487.2023.10250735. keywords: Industries;Technological innovation;Supply chain management;Scalability;Finance;Consensus algorithm;Writing;Blockchain;Smart-contract;Blockchain as a service (BAAS);Decentralised Finance (DeFi);Ethereum;Use case,