Scientific Journal of Metaverse and Blockchain Technologies
ISSN: 2584-2110
https://sjmbt.com
Vol. 3, Issue: 02 | Jul – Dec 2025 | Refereed & Peer Reviewed

Beyond Traditional Boundaries: The Utility of DeFi Derivatives

Bharat Sethi
Email: sethibharat1608@gmail.com

How to Cite:

Sethi B. (2025). **Beyond Traditional Boundaries: The Utility of DeFi Derivatives**. *Scientific Journal of Metaverse and Blockchain Technologies*, 3(2), 14-35.
DOI: https://doi.org/10.36676/sjmbt.v3.i2.74

1. Introduction

In the scholarly literature on financial services, the prevailing paradigm over the past century was the supply of lending, borrowing, trading, and investment by regulated intermediaries, i.e. mainly banks, brokers and exchanges. These are institutions, which operate under a known regulatory structure that assumes homogeneity in their operations. Most recently, the fusion of an entirely new set of technologies such as Decentralized Finance (DeFi) has been changing the sector in a very fundamental way. Blockchain technology currently provides a framework, with the help of which financial applications can perform the transaction process automatically without the existence of central power and, thus, create an environment that is transparent and available.

Traditional finance has come a far way since the simple lending and borrowing days, it has advanced to a wide variety of sophisticated products, with the most famous being derivatives, unconditionally a contract the worth of which is pegged on some underlying significant, index, or rate of interest. The derivatives market has such contracts as forward, future, option, and swap that effectively serve the following purposes: hedging price risks, making speculative endeavours regarding the ultimate direction of the market and assisting price discovery to take place in an efficient manner. These instruments contain inherent complexity and leverage that require a high level of risk-management protocols in a traditional market, and such protocols are supported by its high level of regulatory oversight and enhanced quantitative modelling.

DeFi tries to redefine and duplicate them, coming up with their own range of derivative products. Along with decentralized options and futures, there are perpetual swaps, or conventional futures without expiration. The novelty and subtle dangers to which these derivatives give rise, especially in the context of an allegedly unregulated environment, are all the more forms of financial inclusion and censorship resistance the derivatives affect and expand. Without the usual intermediaries, essential services, such as counterparty risk mitigation, provision of liquidity, and dispute settlement are handed over to computer code and community governance aspects.This shift in the financial environment requires risk evaluation, a check for its suitability, and an evaluation of long-term sustainability.

The increased pace of change and the increased complexity of the decentralized finance (DeFi) project derivate world demands that a structured quantitative risk estimation be in place. Unlike traditional financial markets where clear risks can be mitigated systematically through the participation of financial intermediaries overseen by strong regulatory frameworks, the DeFi brings forth another order of challenges. Among them, the most prominent include vulnerabilities that are embedded into smart contracts, oracle weaknesses that are inherent in cases where external data feeds (oracles) are subject to

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

manipulation, peculiar liquidity mechanics of the automated market makers (AMMs), and network dependencies that are web-like in nature since they can propagate systemic risks among protocols. This is why it is important to have a closer critical look at the risks and manage them, thus ensuring the sustainability of DeFi ecosystem and protect its users.

The paper adds to the answer one of the key questions related to the future of DeFi innovation and financial stability: whether DeFi derivatives platforms can become reasonable substitutes of traditional financial intermediaries to operate in the futures and options markets and what is the quantitative risk involved. To respond, the study produces an in-depth analytical comparison, with the outline of the services provided by old derivatives market intermediaries, on the one hand, and the evaluation of the functions offered by DeFi networks with the same purpose, on the other. The paper also revises potential upsides, namely increased transparency and cost of transactions, and downsides, namely the vulnerability of smart contracts and regulatory conundrums, all these combined in assisting in the analysis and assessment of the DeFi derivatives markets.

A bundle of risks that define decentralized finance (DeFi) are discussed as part of the debriefing in this discussion and they include smart-contract exploits, oracle manipulation, the underlying liquidity risks presented by automated market maker (AMM) protocols, the novel risks in terms of counter-party exposure that DeFi presents by its decentralization, as well as the miscellany of systemic risks that a wildly interconnected DeFi market brings. Their key target is to develop and implement quantitative analytics that will allow quantifying these exposures, generalize the traditional financial risk models as far as possible, and develop new approaches that would adapt to the unique features of blockchain-based transactions. In this respect, the modeling of systemic risk, the creation of specially designed liquidity measures suitable to AMM, as well as building value-at-risk (VaR) estimation frameworks adjustable to DeFi assets and protocols are advanced.

Research Objectives

The current research aims to fulfill the following specific goals:

- To contrast the mechanisms and operations of DeFi derivatives with those of traditional finance.
- To identify and define the most significant quantitative risks in decentralized finance derivatives
- Discuss ways of measuring and controlling similar risks in the DeFi environment.
- To gauge the viability of DeFi derivatives as potential substitutes for conventional financial instruments.

2. Literature Review

The current review outlines the literature that exists regarding the traditional risk management of derivatives and the new DeFi sphere, in greater detail with regards to its derivatives marketplace. Through reviewing the existing knowledge base, the gaps that have been discovered in the present work are thus demonstrated, thus, providing a description of the desired contributions in the present research enterprise.

2.1 Traditional Derivatives and Risk Management Literature

In the past, traditional financial markets have been using complex modelling methods in quantifying the derivative risks. There are four major classifications which take the center stage, and these are market risk, credit risk, operational risk and liquidity risk. The market risk can be commonly measured by means of such instruments as Value-at-Risk and Expected Shortfall which are aimed at estimating

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

the degree of possible losses corresponding to the price variations. To achieve this, such measurements are based on historical records with either implicit or explicit assumptions on how the returns on assets are distributed, often normality, but more often than not comprising non-normality by means of making use of the historical simulation or Monte Carlo methods of distribution.

In comparison, credit risk has to do with the occurrence of a counterparty default. The examples of those mitigation strategies are central clearing, collateralization regimes and netting agreements. Operational risk defined by exposures to ineffective operational processes, staff mistakes, or technological glitches is managed by means of well-organized internal control procedures as well as strict supervision by the regulator.

The risk of failure to trade an instrument at a price that can be used (liquidity risk) remains a prominent issue and this may be especially relevant in less liquid products markets- where poor market liquidity can also undermine the capability to view prices clearly and confidence that execution occurs effectively.

Derivative pricing and risk management, two academic industries have delivered elaborative theoretical frameworks and techniques of pricing and managing risk surrounding it. Simultaneously with these analyses, the Basel Committee on Banking Supervision has had significant influence on industry practice by setting capital adequacy rules and periodically putting financial institutions through stress tests to see how a series of loss-generating events will impact on the finances of the organization.

2.2 Recent Research on Decentralized Finance Platforms and Protocols

Decentralized finance has been recently attracting increased attention from both academics and industry professionals, this is a trend reflected in the growing body of research exploring its multifaceted nature. Initial studies which were primarily focused on the fundamental blockchain technology, consensus mechanisms, and the financial incentives driving cryptocurrencies. As Defi is maturing and gaining more attention, new research is progressively targeting specific protocols, including decentralized exchanges, lending platforms, and stablecoins.

Research being done on DeFi derivatives is still in its early stages compared to other areas within DeFi although it is expanding rapidly. Most of the studies right now are concentrating on the design and operation of specific DeFi derivatives protocols such as perpetual swaps on platforms like dYdX or GMX, or decentralized options protocols like Opyn. These research paper often highlights the innovative use of smart contracts to implement mechanisms like margin management and liquidation. In traditional finance, these processes are human-capital intensive and rely on centrally managed infrastructure.

Furthermore, people are now beginning to investigate and show interest in the unique characteristics of DeFi markets which includes their 24/7 trading availability, global accessibility, and the composability of protocols. Composability enables the creation of complex financial strategies by combining various DeFi applications. The transparency of on-chain data also provides researchers with unprecedented opportunities to study market activity and protocol performance in detail

2.3 Gap Analysis: Traditional and Decentralized Finance Risk Management Mechanisms

There would be a significant divergence between decentralized finance (DeFi) and conventional risk

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

management, despite the fact that both spheres seek similar goals. They differ with traditional systems in that they are able to have a system of control that is centralized, enforceable law and humans to check the system; in DeFi the only system of control is computational code that is also present in a decentralized environment.

The counterparty risk comes up as one of the primary deviations. Conventional finance terms it as credit risk which is handled at the contractual level and quite intense financial analyses. Such a risk is taken in DeFi as the risk of smart contracts (risk of bugs or bugs in the underlying code). Audits are similar in that they are not able to provide perfect security, the exploits may lead to unrecoverable damages.

The second cool difference is related to oracles, to introduce extraneous data into the on-chain computations. The data feeds trained and managed as centralized trading spaces are reflected through centralized and run data provisions and the decentralized DeFi protocols ran by oracles to deliver DeFi protocols with inputs as off-chain prices into the blockchain. The fact that these oracles cannot go down is critical as down once can trigger a cascade of liquidations and high ruggedness in the market.

Liquidity risk is also dealt with in a different way. Brokers and market makers in ordinary markets provide market depth by use of order books. Automated Market Makers (AMMs) pool liquids kinds of assets supplied by users to generate the liquidity in DeFi. Even though single-asset exchanges via AMMs are very efficient, they are prone to impermanent loss and often lack the liquidity necessary to support big derivatives trades; in times of increased volatility, that lack of liquidity will result in substantial slippage and market turbulence.

Lastly, there is a serious assurance continuum gap because there is no central regulator in DeFi. The traditional risk management has the advantage of significant regulation to protect the investor and maintain systemic health. The loose regulations in DeFi establish vulnerabilities, especially in areas of consumer protections, the integrity of the markets in DeFi, and the anti-money laundering (AML) compliance.

2.4 Quantitative Model State in DeFi today

The quantitative frameworks and their calibration need to be developed to address the emergent risks facing decentralised finance in a manner that is purpose-built to the DeFi. The older protocols such as value-at-risk (VaR) merely do not automatically and actively operate in the DeFi context, but will have to be customised. Specifically the potential output of crypto-asset returns which may have non-normal distributions, the potential repercussions of security vulnerabilities of smart-contracts, and the unique liquidity implications of automated market makers must have to be echoed in the adaptive VaR equations.

Quantitative researchers are developing new methodologies, such as agent-based modeling to model complex interaction within DeFi protocols, network analysis to map the spread of systemic risk, and bespoke metrics to measure liquidity in AMM pools. Availability of on-chain data provides a high-quality data set to build and back these new models, although processing data is still a challenge and maintaining the off-chain data sources (oracles) is a challenge. In short, whereas traditional finance provides an established paradigm for managing derivatives risk, DeFi provides a new frontier with attendant problems. Recent research in decentralization has made this issue more acute and called to quantitatively model these dynamics that are peculiar to distributed ecosystems. The given research

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

satisfies such a scholarly niche, offering a range of practical tools that can address the established gap.

3. Methodology

To understand the unique position of DeFi derivatives one would first have to have a general idea of how the commonly traded derivatives markets operate, in the typical derivatives markets, intermediaries: when a person buys an option or a future; they do not have to come into direct contact with a third party.Instead, there is a large network of institutions through which these complicated transactions are made smooth and safe. Subsequently, we observe how DeFi attempts to achieve the same thing with other instruments.

3.1 Functions of Traditional Intermediaries in the Derivatives Markets

In traditional derivatives markets, several important players have important roles to play.

•Exchanges: They could be imagined as institutionalised exchange where derivative contracts are actually negotiated and priced. This leads to price discovery in such venues where divergent information in the hands of buyers and sellers converge. Further, they set out clear regulations to ensure an orderly and fair implementation.

•Clearing Houses: It is in these markets that clearing houses are the structural basis. By acting as the chief counterparty to any transaction, they actually novate the contractual relationship among the parties to any transaction, and thus curtail said risk that results in the breach (see counterparty risk). Simultaneously, clearing houses receive collateral when traders conduct transactions so that they can cover losses and they have the mandate to settle the obligations systematically.

•Brokers: Brokers act as intermediaries between exchanges or clearinghouses and individual investors. They provide individuals with access to the market, trade customers' orders, and often provide the required research, advice, and lending on margin.

•Custodian: A custodian is a very important framework in the derivatives world. The custodians have a responsibility to protect the assets of their clients and as such, they serve a critical role in serving the interests of clients even though their role does not apply to all derivatives transactions. They are also required to make sure that they segregate customer holdings in an independent account and this account is not controlled by the broker or even exchange.

•Regulators: Regulatory oversight is important. Examples of government organizations that constantly review these markets include the Commodity Futures Trading Commission (CFTC) of the United States, in order to ensure good market behavior, discourage market manipulation, assure the protection of investor capital and help bring about macroeconomic equilibrium.

Together, these intermediaries create trust, increase efficiency, enable liquidity, and help manage risk in traditional derivatives markets. They ensure that transactions are conducted fairly, obligations are fulfilled, and system risks are properly managed.

3.2 Decentralized Finance Model Strengths and Weaknesses

The decentralized method of derivatives trading has several attractive benefits, but it is also linked to substantial drawbacks compared to conventional intermediation.

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

Scientific Journal of Metaverse and Blockchain Technologies
ISSN: 2584-2110
https://sjmbt.com
Vol. 3, Issue: 02 | Jul – Dec 2025 | Refereed & Peer Reviewed

Advantages:

•Accessibility and Inclusivity: DeFi markets are permissionless, such that anybody with an Internet connection and a crypto wallet can join without regard to their geolocation, credit score, or net worth.

•Transparency: The transactions of the public blockchain can be checked as they are by their nature transparent. That implies that rules are specified, collateral held and settlement processes are subject to observation, inspection and review by any interested party and provide a high level of transparency which is not the norm in opaque traditional over-the-counter (OTC) derivatives markets.

•Reduced Counterparty Risk (through Smart Contracts): The counterparty risk that presents itself when there is a human intermediary present is reduced to zero theoretically when using smart contracts, the terms of which cannot be breached arbitrarily.

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

The code written is law and operates independently of the agreed terms [2].

DeFi protocols will most probably charge lower operating and trading fees than conventional financial institutions because they lack ubiquitous human eyes, large operating staff, and complex regulatory compliance departments [2].

•Composability and Innovation: DeFi protocols are open-source and composable in nature, that is, they can be composed with other protocols seamlessly. This facilitates rapid innovation and the creation of sophisticated financial products that can be difficult or slow to build in legacy siloed systems.

Limitations:
Smart Contract Risk: Smart contracts solve the problem of the intermediaries in the sales but are prone to coding errors, untested security functions and hacks. One bug may lead to the significant loss of money because funds being transferred out of a vulnerable contract are at stake. This situation is a new form of counterparty risk where the counterparty is the code of the smart contract itself.

Scalability Problems: Decentralized finance (DeFi) applications run on crowded and expensive networks, with Ethereum being the most prominent example when traffic is heavy. This makes regular trading or low value transactions economically unviable and reduces the process efficiencies thus reducing liquidity and user satisfaction.

Liquidity Fragmentation: The liquidity in DeFi is a decentralized thing, and this fact means that the liquidity can be dispersed among many protocols and blockchains, subsequently, being fragmented. This multiplicity may lead to greater slippage (the variance between the theoretical price that should be affixed to a trade and the price at which the trade occurs) and less liquid markets than those of highly liquid, centralized exchanges.

Oracle Risk: DeFi projects rely on third party data feeds (oracles) in order to fetch the correct price and settle. Oracle use makes price information non verifiable, and casts derivate risk that is dependent on the reliability of the source of information (the oracle), and the integrity of each individual (oracle) using it..

•Regulatory Uncertainty: The global and decentralized nature of DeFi hinders the effective application of existing regulations. Uncertainty may discourage institutional adoption and leave participants open to potential legal risks as governments worldwide struggle to categorize and oversee these new financial products. •User Error and Security: In DeFi, users are only responsible for keeping their private keys and wallets secure. Without intermediaries, transactions cannot be reversed, and lost funds cannot be recovered because of user error, that is, sending money to the wrong addresses phishing. Consequently, this places a significant burden on each user.

•Traditional Recourse Absence: If a bug or exploit in a DeFi protocol fails, there could be no overarching body or legal entity to resort to for recourse or compensation, unlike the traditional financial system, in which legal systems and insurance mechanisms exist.

To Summarize, DeFi derivatives are a type of instrument that is developing rapidly. In contrast to the

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

more standard forms of hedging, derivatives in decentralised finance (DeFi) are distinguished by a higher level of access and transparency; however, they expose themselves to a new collection of risks that does not closely match the ones found in more standard financial markets. The transition between intermediated trust in institutions to the system of algorithmic trust relying on the cryptographic protocols comes with its visible potentials as well as imposing challenges the most notable of which lies in the scope of quantitative risk management.

3.3. Results: Key Risk Classification in DeFi Derivatives

Although the last section compared functional similarity and disparity between DeFi and traditional derivatives, the next is to now explore the particular risks either exclusive of the decentralized setting or occurring differently within it. An understanding of these is the basis on which effective quantitative protocols for risk management must be built.

3.3.1 Smart Contract Risk

The most important concept in the paradigm of DeFi is the smart contract: an automatically executing program, stored on a blockchain. These contracts have similar functionalities with conventional legal contracts, though they do not run on programmatically guided obligations unlike the latter. Like with any financial product, smart contracts bring significant benefits, especially transparency and efficiency, but also a different type of risk, smart contract risk. The category of risks includes a loss of finances caused by exploits, bugs or logical inconsistencies implemented in the code of the contract. Even the codes with verified security through stern auditing may have some undetected weak spots that can be used against them. Their weaknesses are often due to coding errors that have undesirable or unintended consequence, and could even lead to the misappropriation of funds, fund freezing or spend out. Smart contracts are irreversible, which does not work well with remedial actions once used, either by way of upgrading or substituting an entire protocol in odd instances. In contrast with common counterparty risk, where by counterparty one refers to a person or an institution, in smart contract risk, it refers to the software code itself, as the counterparty.

3.3.2 Oracle Risk

Decentralized finance (DeFi) protocols which allow providing derivatives depend on outside data to make them work, e.g. the current price of some underlying asset (e.g. ETH in USD). It develops the position of oracles, which are systems the smart contracts can use to acquire external knowledge. The timing and precision of price feed is key in the derivative applications in order to fulfill the determination of collateral ratios, liquidations and position closing. However, this dependence on oracles makes it an oracle risk an otherwise intricate matter that encompasses a variety of factors such as:

- Manipulation: When the source of information can be controlled, or the oracle is corrupt, then the smart contract will be given incorrect prices that result in injustices in liquidations or attacks that make money.
- Failures: Technical issues, network congestions or attacks that may occur to stop the delivery of data by the oracles are some of the problems that occur and lead to the hanging or using out-dated data by the protocols.
- Latency Problems: Latent price allows opportunity to arbitrage or liquidation tripping on stale values, more so when considering highly liquid markets.

The oracle risk can be minimized by the mechanism of derivatives protocols that enable the use of

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

decentralized oracle networks, such as Chainlink, to gather numerous data points. Irrespective of these precautions, the risk concerning the oracle is the most prioritized risk that needs to be solved.

3.3.3 Liquidity Risk

DeFi liquidity risk is the lack of ability to trade large quantities without affecting the price of the asset to any considerable extent and the lack of ability to sell an asset for cash at the moment without sustaining severe losses. The risk exists in the traditional markets as well, but DeFi liquidity risk is distinctive because of the dominance of Automated Market Makers (AMMs) and decentralized platforms.

•Limitations of AMM: AMMs are employed by the majority of DeFi derivative exchanges, where clients provide liquidity in the form of assets that have been locked in pools. AMM pricing may lead to larger trades experiencing larger slippage than on conventional order-book exchanges, especially in the case of less-liquid pairs. In other words, a large trade can mean paying a much worse price than expected.

•Fragmentation of Liquidity: The DeFi space is gigantic and evolving on a daily basis, and there are a lot of protocols and blockchains. It has the tendency to fragment the liquidity across many platforms, i.e., it is harder to get deep liquidity for a specific derivatives contract. This fragmentation leads to the decrease in the efficiency of the market and increases the trading cost.

•Impermanent Loss: Impermanent loss is a risk to liquidity providers in AMMs when the asset value deposited in the pool fluctuates against their holding outside the pool, particularly when there is volatility. This will discourage liquidity provision, further decreasing market depth.

3.3.4 Counterparty Risk in Non-Trust-Based Situations

In traditional finance, counterparty risk is the risk that a counterparty to a financial contract will not pay. This normally is solved with credit screening, collateral, and central clearing. In DeFi, the arrangement is normally called 'trustless' since it tries to remove the need to trust some institutions or people. This does not remove counterparty risk; it merely changes it.

• Protocol Level Counterparty Risk: Today, customers trust not their human counterparties but the protocol itself and the smart contracts that come with it. As has already been determined in the case of smart contract risk, a coding bug can render the protocol unable to deliver on its commitments, thus a 'default' by the protocol.

•Collateralization Issues: While over-collateralization is common in DeFi to mitigate risk, under-collateralized positions that lack adequate coverage are always at risk through sudden price movements or oracle failure, especially if liquidation mechanisms fail or are sluggish in response.

3.3.5 Risks of Regulatory Compliance

The new and rapidly evolving nature of DeFi asserts that regulatory frameworks are playing catch-up. Thus creating a significant regulatory and compliance risk for both participants and protocols.

•Uncertain Legal Category: Most decentralized finance (DeFi) derivatives will be in uncertain legal

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

categories since the classification (e.g., security, commodity, or a new one) varies from jurisdiction to jurisdiction. Uncertainty can lead to unforeseen legal issues, enforcement actions, or even prohibitions.

•AML and KYC Problems: Blockchain transaction pseudonymity renders it impossible to apply normal AML and KYC procedures, the standard for supervised financial institutions. It opens a possibility of DeFi being used for illegal activities so regulatory scrutiny is at risk.

•Jurisdictional Arbitrage: It is a special kind of regulatory arbitrage where this is applied through decentralized finance (DeFi) as it does not require jurisdiction, only being global. This feature allows users and protocols to act in a variety of jurisdictions at the same time so they may take advantage of different regulatory frameworks. This would be a system-level risk in the event that the less-regulated platforms prevailed.

3.3.6 Systemic Risks and Channels of Contagion

Systemic risk is a risk of the overall financial system or market failure, rather than failure of an individual entity or component. Within DeFi, the extremely high degree of composability and interconnectivity between protocols creates new forms of crisis.

•Double Nature of Composability: While composability promotes innovation, it comes with risk, as one failure in a large protocol (e.g., a large lending platform or stablecoin) can possibly destabilize the entire ecosystem and affect many more protocols that are built upon it. This effect, commonly called the 'money Lego' effect, allows the quick spread of vulnerabilities.

•Spirals of Liquidation: In environments that are typified by highly volatile fluctuations in market conditions, a sudden collapse in asset prices can induce a cascade of widespread liquidations across several derivatives markets. This forced selling can in turn accelerate further price falls, engendering further liquidations, and thus create a dangerous feedback loop that can destabilize the market as a whole.

•Common Infrastructure Risks: Several decentralized finance (DeFi) platforms are founded on common underlying blockchain infrastructure, e.g., Ethereum. A serious problem with that underlying layer, e.g., network congestion, a fatal software flaw, or a security flaw, has the potential to impact several DeFi platforms at the same time.

Participants in DeFi derivatives need to be aware of these particular classes of risk. The next task is to examine how these forms of risks are to be quantitatively measured and managed, including updating existing financial models as well as designing new structures appropriate to the distinctive features of the decentralized finance environment.

Case Study : The bZx Flash Loan Attacks (2020)

In February 2020, the bZx protocol was the target of several flash loan attacks, one of the earliest and largest DeFi derivatives attacks. The successful attacks preyed on the margin trade and lending components of the protocol, that the attacks were able to generate accumulation of financial loss, exposing DeFi deficiencies in terms of interrelation.

Attack Mechanism: Flash loans were used as a way of attacker to manipulate/control the oracle prices

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

and exploit arbitrage opportunities on bZx protocol. By using flash loans (large sum of ETH without collateral), the attacker could tamper the price of the underlying assets and make an actual profit using the price differences.

The financial cost of the first wave of the attack on February 15, 2020, was the loss of about 350 thousand dollars in ETH. Another attack took place only four days later on February 18, 2020 and cost them another 630 000 worth of ETH. The combination of these attacks caused almost a million in losses.

Risk Implications: This case study shows how the DeFi protocols can be susceptible to oracle manipulation and how communities of interconnected protocols extinguish into each other. The attacks brought in question more resilient oracle systems and improved risk management in margin trading logic.

3.4. Quantitative Risk Measurement Methodologies

Now that the researchers have identified the characteristic risks involved in DeFi derivatives, the next question regards how those risks can be managed and be systematized in their quantification.

Although standard finance provides a comprehensive set of risk-quantifying tools, trying to copy-paste them to DeFi has serious restrictions under the condition of the inherent decentralised nature of the sector. The current discussion, therefore, outlines the need to calibrate the existing metrics and states that the adaptation of new methodologies adjusted to the peculiarities of DeFi remains essential.

3.4.1 Traditional Risk Metrics to DeFi

The foundations of the traditional quantitative risk management are the instruments like Value-at-Risk (VaR), Expected Shortfall (ES) these allow to estimate the potential loss of a portfolio during a specified period within a specified confidence limit. Even though the VaR model can be conceptually transferred to DeFi, it will require many changes as per DeFi requirements.

•Value-at-Risk (VaR): The VaR model is the projected level of loss that may occur over a stated time period and at a certain confidence.

•Non-Normal Returns: When compared to normally distributed returns cryptocurrencies exhibit strong skew and heavy tailed returns distributions, which implies very extreme observations in much more frequency than classical normal distributions. Therefore there is a need to use statistical methods like historical simulation, Monte Carlo simulation, or extreme value theory (EVT) which do not depend on any distributional assumptions.

•Data Accessibility and Quality: The highly transparent nature of DeFi transactions on-chain has been made possible by datasets that have not been easily constructed through a high-frequency, broad-based documentation of relevant assets and protocols. Moreover, the limited histories of many DeFi assets limit the availability of further empirical observation to use robustly in the estimation.

•Smart Contract and Oracle Risk Integration: The black-box VaR does not inherently consider losses due to smart-contract induced exploitation as well as oracle failure. Such qualitative risks require new methodologies to build-in, possibly by risks scenario analysis or even stress tests that mimic negative events.

•Expected Shortfall (ES): Also known as Conditional VaR (CVaR), ES measures the expected loss

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

given that the loss exceeds the VaR. It provides a more comprehensive view of tail risk than VaR, as it considers the magnitude of losses beyond the VaR threshold. Similar to VaR, ES calculations in DeFi must contend with non-normal returns and the need to incorporate DeFi-specific risks.

3.4.2 Blockchain-Specific Considerations for Quantitative Models

The unusual built of blockchain and decentralized finance (DeFi) brings some dimensions that are to be considered by quantitative modeling clearly.

On-Chain Data/Off-Chain Data. On-chain transactions in a public blockchain are public and unforgeable, but critical components to complete risk management like user behavior, protocols upgrade, and oracle feeds are off-chain. As a result, the models will need to combine the two data sources, considering that off-chain data could be manipulated or lack immediate availability.

Gas Fees and Network Congestion. Transaction costs (gas fees) and network congestion play a significant role in the viability and profitability of some trading strategies they can cause more difficulty with some trading strategies, such as those with many rebalancing or liquidations. Ideally, the dynamics of costs should also be put into consideration in calculating quantitative models.

Composability and Interconnectedness. The extreme composability in the DeFi world leads to very interconnected protocols which ends up having complex dependencies. The contagion channels influence the entire ecosystem by reverberating an event that occurs in a single protocol. Consequently, modeling of these network effects should be reflected through the quantitative models by implementing the graph theory or network analysis to plot dependencies and finding critical nodes.

3.4.3 Liquidity Metrics for AMMs

The standard liquidity indicators, usually based on the concept of bid-ask spreads and on the trading volume in the order books, are inappropriate to AMMs. Analytical measures that would serve better to represent liquidity performance in such environments include:

Slippage: It is a difference between what a trade thinks that it will be successful in the trade and its sale price. When the slippage is more prominent, it reflects a decreased depth of liquidity in the given trade size.

Total Value Locked (TVL): TVL is not a specific indicator of liquidity, but the measure of the value of assets that are locked in the AMM protocols can be used as a proxy that defines the potential future access to the liquidity. Increasing TVL tends to reflect an increased liquidity but it does not reflect the proportion of assets across pools or the effectiveness of the underlying pricing curve.

Impermanent Loss (IL) Exposure: IL cannot even be computed by liquidity providers but approaches the temporary capital loss instead of holding the same asset amounts outside the AMM pool. Measuring IL exposure therefore increases the informedness of liquidity-provider risk and the very stability of protocol liquidity.

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

Concentrated Liquidity Metrics: In concentrated liquidity mechanisms (e.g. Uniswap V3) providers can place their capital in highly specific price ranges. Different metrics are needed to measure the performance of such positions, such as the capacity of them to supply liquidity with varying price dynamics.

3.4.4 Stress Testing in DeFi

Stress testing forms a central part of a standard risk management practice; it is a test which tries to simulate extreme but realistic situations in the market with the objective of examining the stability of a portfolio or financial institution. Stress-testing approaches in decentralized finance (or DeFi) need to be adjusted so as to consider idiosyncratic risk factors.

1. Scenario design

The enormous price actions must be augmented with DeFi-relevant incidents like smart contract hacks, broken oracles, stable-coin de-pegging, and surges (or collapses) of gas prices or blockchain congestion. As an example, there could be a case whereby, a major oracle feed gets compromised, thus resulting to wrong liquidations on various protocols.

2. Inter-protocol dependencies

DeFi protocols are mutually bonded, so contagion has to be simulated.^{[1]}

• A liquidity crisis or cascade of liquidations in one protocol may be triggered by a shock to that protocol (e.g. a large withdrawal on a lending system).

3. Resilience in liquidation mechanism

The stress tests of the liquidation processes should be evaluated.

Among the questions are whether liquidators will be efficient to work against the high volatility and network congestions and whether the collateralization ratios will be adequate to sustain the losses.

4. Governance attacks

Although less common, other scenarios to be investigated during stress tests are where malicious actors misuse governance systems to make decisions harmful to the protocol or its users.

The traditional analytic models can help initiatively, but direct application may not be adequate in many cases. There is a necessity of new DeFi-specific measurements and new adaptation of the previous methodologies on blockchain-specific, AMM-based, and inter-protocol aspects. Such an approach would require the synergetic effort of the fields of finance, computer science, and network theory to represent an interdisciplinary effort.

3.4.5 Historical VaR Methodology

Historical VaR is a simple and obvious quantitative method of measuring possible losses due to actual examination of market movements that occur in the historical past. The following is the process of doing it.

1. Data Collection

Get a historical record of day-to-day (or other frequency) closing prices of the DeFi asset

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

(e.g.,Ethereum). The necessary data has been gathered and processed in the case of this research.

2. Calculate Daily Returns
Calculate the logarithmic returns (or percentage returns) of the historical prices. The reason to use logarithmic returns in financial modelling would be mostly in their ease and simplicity of computation and being an additive operator.

Formula: $R_t = \ln(P_t/P_{t-1})$, Where R_t is the return at time , is the price at time t , and P_{t-1} is the price at time $t-1$.

3. Sort Returns
The historical returns should be listed in increasing order of magnitude, that is the worst negative values (as the biggest loss ever recorded) should be at the top of the list and the best positive values (as the largest gain recorded) should be at the bottom.

4. Determining VaR Percentile
A percentage distribution should be indicated such as 95 or 99 percentage. The 1st percentile is required at confidence level of 99%; this is interpreted as 1 percent of observations which were as bad as or even worse than the given value.
5. Calculate VaR.
The Historical VaR are the return values that correspond to the percentiles of the set confidence level selected. In the case of a portfolio, the dollar figure of the VaR will be the product of this measurement with the value of the portfolio.

Formula: $VaR_\alpha = -P_{current} \times R_\alpha$ Where VaR_α is the Value-at-Risk at confidence level α , is the current portfolio value, and R_α is the return at the percentile (e.g., 1st percentile for 99% VaR).

Advantages of DeFi Historical VaR:
Lack of Distributional Assumptions: This model does not assume that returns are normally distributed, a common assumption that is usually required for cryptocurrency assets owing to their peculiar return distributions with high fat tails.

Represents True Historical Events: It accurately traces true historical market behavior, including extreme events and market crashes, without directly modeling them.

Disadvantages:
Reliance on Historical Information: Assuming that the future returns will behave similarly according to the past returns. If there is a sudden change in trends of market the result will be inefficient.

Sensitivity to Sample Size: We need a adequate and appropiate sample size since this is all new the sample size is new

3.4.6 Conceptual Integration of DeFi-Specific Risks

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

The process of including DeFi-specific risks into a serious risk management framework is a sensitive issue. It is especially challenging to quantitatively incorporate phenomena like smart contract exploits or oracle failures directly in a conventional Value-at-Risk (VaR) estimation and scenarios and stress-tests can be used to cover these elements and thus improve the risk architecture as well.

Scenario-Based Adjustments
A constructive approach to the risk of smart contracts is to determine the conditions under which proportional loss of assets by exploitation would suffer, which would turn the theoretical loss into a cumulative contribution to the estimated VaR. In line with this, oracle risk could be investigated by testing those conditions whereby the price feeds can be manipulated or stale with an evaluation performed on the expended slippage on the liquidation thresholds and portfolio value.

Liquidity Risk Overlay
Historical VaR model is usually made with the assumed immediate implementation with observed historical prices, but, in DeFi, on big positions or illiquid assets, large slippage can follow. Overlay It is possible to add on to the calculated VaR such that the VaR value is increased with estimated slippage based on the portfolio size based on historical data of slippage or based on AMM liquidity curves.

Interconnectedness Factor
Though the systemic risk of composability is not easy to measure through a single VaR value, maintaining a watch on the level of dependency of any asset with other protocols can helps prevent them. Should a core protocol (e.g. a high volume lending platform) be compromised, the VaR used by the assets depending on said provider may be temporarily bumped up or a worst case stress-test scenario be run.

Conclusion
Although this is a customised VaR model with a classical Historical VaR approach, it provides a strong starting point to applying quantitative risk management in the DeFi space. It is powerful in its ability to support non-normal returns distribution, and also allow one to integrate DeFi-specific risks conceptually using complementary scenario analysis and stress testing.

3.5 Model Validation and Backtesting

After implementing the Historical VaR model, it is crucial to validate its accuracy and reliability. Model validation ensures that the model is performing as expected and provides a reasonable estimate of potential losses. For VaR models, backtesting is a primary and widely accepted method of validation, which involves comparing the actual losses experienced over a period with the VaR estimates generated by the model.

3.5.1 Backtesting Methodology

Backtesting a VaR model typically involves counting the number of times actual losses exceed the VaR estimate (known as 'breaches' or 'exceptions') over a specific period and comparing this number to the expected number of breaches based on the chosen confidence level. For example, with a 99% VaR, we

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

expect breaches to occur approximately 1% of the time.

Steps for Backtesting:

1. Obtain Actual Returns: Use the same historical return data that was used to calculate the VaR, or a new out-of-sample dataset if available, to ensure consistency.
2. Compare VaR with Actual Returns: For each day (or period) in the backtesting window, compare the calculated VaR (expressed as a negative return threshold) with the actual return for that day.
3. Count Breaches: A breach occurs if the actual negative return (loss) is greater than the VaR estimate (i.e., the actual loss is worse than the VaR threshold). Each instance where the actual loss exceeds the predicted VaR is counted as a breach.
4. Calculate Breach Rate: Divide the total number of observed breaches by the total number of observations in the backtesting period. This gives the empirical breach rate.
5. Statistical Tests: Apply statistical tests to determine if the observed breach rate is statistically consistent with the expected breach rate. Common tests include:

Kupiec's Proportion of Failures (POF) Test (Unconditional Coverage Test): The unconditional coverage test put forward by Kupiec otherwise known as the Proportion of Failures (POF) Test is used to test the hypothesis as to whether the number of Value-at-Risk (VaR) breaches determined empirically can statistically be reconciled with that predicted by the null hypothesis, this being that the underlying VaR model is valid. It is a likelihood ratio test, comparing the observed number of the exceptions with the hypothetical one that would appear in case the theoretically valid VaR model were valid.

Christoffersen's Conditional Coverage Test: A more stringent extension is the Conditional Coverage Test introduced by Christoffersen which not only analyses unconditional coverage (accuracy of the forecasted frequency of breach of VaR) but independence of VaR breaches also. Breach clusters point to the fact that VaR model is not adequately capturing market events or volatility variations.

3.5.2 Application to DeFi VaR Model

The following paper uses processed_ethereum_data.csv as its input to backtest the past value-at-risk (VaR) model developed to Ethereum. Calculated on a daily basis, the returns are used in comparison with the model provided VaR assessments at 99 and 95 percentages. A count of the times where the returns observed were greater than the concern VaR values is made and this results in a breach rate per confidence interval. Even though a full implementation of either the testing framework of Kupiec or Christoffersen will be out of scope of this real world implementation, it must be noted that putting the concept down using their foundational principles is key in ensuring a substantial validation of the model.

The expected rates of breaches are as follows:
At 99% VaR, an estimate is made by predicting that about 1 percent of daily returns will exceed an estimate.

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

About 5 percent of returns made each day are to be expected to be above the estimate of the 95 percent VaR.

If there were big differences between those expectations and the observed degree of breaches, this would suggest that the model underpredicts (many breaches) or overpredicts (few breaches) risk. Moreover, any such clustering in the breaches may be an indication that the model would not react effectively to the movements in the markets or fluctuations of its volatility. The existence of such back-testing can thus provide empirical data on model performance and reveals possible ways to improve the same, especially given the highly turbulent and rapid manner in which the DeFi markets operate.

4. Results

This section presents the results of applying the Historical VaR model to Ethereum (ETH) daily closing price data from 2018 to 2024. It includes the calculated VaR values, the outcomes of the backtesting process, and an interpretation of these findings, highlighting their implications for risk management in DeFi.

4.1 Case Study Application: Historical VaR for Ethereum

To demonstrate the practical application of the Historical VaR model discussed in Section 3.3, we applied it to the preprocessed Ethereum (ETH) daily closing price data from 2018 to 2024. This case study illustrates how VaR can be calculated for a single DeFi asset and how the model's performance can be assessed through backtesting.

4.1.1 VaR Calculation Results

Using the calculate_var.py script (which you can find in the references [5]), we computed the 99% and 95% Historical VaR for Ethereum based on its daily logarithmic returns. The results are as follows:

99% Historical VaR for Ethereum: -0.138590

95% Historical VaR for Ethereum: -0.072955

The values we are exploring, are the upper expected limit of daily loss (expressed as a percentage of the value of the asset) which is obtained by historical fluctuation of prices, to a 99 percent and a 95 percent confidence interval respectively. Therefore, 99 percent VaR of -0.138590 shows that in the past 99 percent of historical observations the losses of Ethereum in a day could not exceed 13.86 percent.

4.1.2 Backtesting Results

To validate the model, we performed backtesting using the backtest_var.py script (also in the references [5]) over the entire dataset, which comprised 2461 observations (representing daily returns from 2018 to 2024). The backtesting results are summarized below:

For 99% Historical VaR:

Calculated 99% VaR: -0.138590

Number of observations: 2461

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

Number of breaches (actual losses worse than VaR): 24

Observed breach rate: 0.0098 (or 0.98%)

Expected breach rate: 0.0100 (or 1.00%) For

95% Historical VaR:

Calculated 95% VaR: -0.072955

Number of observations: 2461

Number of breaches (actual losses worse than VaR): 123 Observed

breach rate: 0.0500 (or 5.00%)

Expected breach rate: 0.0500 (or 5.00%)

4.1.3 Interpretation and Implications

It has been observed that the Historical VaR model of Ethereum does relatively very well during the backtesting period. The rate of breach at 99 and 95 percent confidence interval is very close to its counterpart which is the expected one. This kind of agreement demonstrates that the model provides quite a solid reconstruction of the downside risk profile of Ethereum through history..

Accuracy: It gives a high confidence level in showing that it fairly represents the historical risk profile of Ethereum. This is particularly impressive considering that the cryptocurrency market is notorious when it comes to volatility.

Practical Use in DeFi: These findings are particularly relevant in the aspect of policy when applied through the lens of decentralised finance (DeFi). As an example, the benchmarked 99% VaR may be used by decentralised derivatives platforms so that they set margin requirements of ETH-denominated positions. When a user holds a position that is collateralised by an ETH, the platform may require a margin that is sufficient to cover the estimated maximum drawdown in a day at such a confidence level so that considering the usual market behaviour, the position is adequately represented by the collateral asset base that can absorb potential losses.

Limitations and Further Considerations: While the results are promising, it's crucial to reiterate the limitations of Historical VaR, especially in the context of DeFi:

Dependence on Historical Data: The model assumes that past

performance is indicative of future results. Sudden shifts in market dynamics, regulatory changes, or unforeseen events (e.g., a major smart contract exploit) that have no historical precedent would not be accurately captured.

DeFi-Specific Risks: As discussed in Section 3.1, this basic Historical VaR model does

not directly quantify risks like smart contract vulnerabilities, oracle failures, or impermanent loss. While the backtesting results are good for market risk, these other critical risks still need to be managed

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

through qualitative assessments, scenario analysis, and robust protocol design.

Liquidity Impact: The model does not account for the impact of large trades on market prices (slippage) or the potential for liquidity crises in AMMs. A large liquidation event, for instance, could exacerbate losses beyond the VaR estimate if it significantly impacts the underlying asset's price.

Despite these limitations, the application of Historical VaR provides a fundamental quantitative measure of market risk for DeFi assets. It serves as a crucial component within a broader, multi-faceted risk management framework that also incorporates qualitative assessments and adaptive strategies to address the unique complexities of the decentralized financial landscape. This case study demonstrates the feasibility and utility of applying such models to enhance risk awareness and decision-making in DeFi

6. Conclusion

The current paper demonstrates an in-depth research of the modern Decentralized Finance (DeFi) derivatives, questioning the process of their operation, risks associated with it, and the strategies of quantitative risk management that arise. It will start by describing the nature of traditional derivatives markets and the crucial role played by an intermediary in the process and then focus on how DeFi platforms redefine and expand on these functions thanks to the use of smart contracts and decentralized protocols. The benefits of DeFi, namely its unrivaled ease of access and transparency, as well as its drawbacks, first and foremost the emergence of a new type of smart contract risk and front-and-center regulatory ambiguity, are highlighted through a methodical comparison. The key study subsequently focuses on the special and often exaggerated risks inherent in DeFi derivatives, categorizing these into six categories: smart contract risk, oracle risk, liquidity risk (especially inside Automated Market Makers (AMMs) or AMMs), transformed counterparty risk, regulatory and compliance risks and systemic risks. Real life examples and case studies of bZx flash loan attacks, the Wormhole bridge hack and the fateful failings of the Terra/Luna ecosystem, clearly show the practical aspects of these threats and how their impacts can reverberate throughout the extremely interconnected DeFi landscape. All these events indicate collectively that innovation in DeFi goes hand in hand with a requirement of a new paradigm of financial risk management. Since it is clear that such an approach to risk management is a complete failure when directly applied to this new environment, the paper goes further and helps define a framework of integrated risk management specific to the DeFi environment. It is expected that this framework will place particular emphasis on the merging of on-chain and off-chain data, the synthesis of complex multi-factor risk models that are constantly sensitive to DeFi-explicit weaknesses, and the implementation of adaptive policies whose risk parameters become forward-reactingThis paper highlights three composing pillars, all of which are vital to ensuring long term resilience and security of decentralized finance (DeFi) protocols: 1) community governance; 2) decentralized incident response; and 3) continuous backtesting. In addition, it reflects upon the rapidly changing and speeding regulatory dynamic, suggesting a collaborative approach between regulators and the DeFi community, which will lead to a balanced attitude between innovation and compliance and security measures.

6.1 Summary of Findings

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

All the contributions of the current research confirm that even though cryptocurrency decentralised finance (DeFi) derivatives are functionally similar to their conventional counterparts, they undergo various risk parings. The shift in institutional trust to distributed assurances of cryptographic protocols brings in new kinds of exposure that are not dealt well with in traditional frameworks of thinking about financial models. The research was led by its key findings as follows:

1. DeFi protocols are being used to systematically disintermediate conventional financial processes a process that realigns established risks (e.g. traditional counterparty risk changes to smart-contract risk) which thereby generating altogether new risk (e.g. oracle risk, composability risk).

2. On-chain data inherent transparency implies new opportunities of real-time risk monitoring have never been seen before, but mandatory inclusion of off-chain intelligence is essential to attain a comprehensive and complete picture of risk.

3. Quantitation measurements like Value-at-Risk (VaR) and Expected Shortfall (ES) would need to be significantly reworked to adequately encompass the non-normal distributions at play with cryptocurrencies, the non-standard liquidity behaviour of automated-market makers (AMM), and the developing possibility of sharp smart-contract exploits.

4. Events in the DeFi space demonstrate the devastating effects of unaddressed risks of smart contracts, oracles, and system-level exposures, hence making the argument of proper stress-testing and incident-response interventions compelling.

5. The existing regulatory framework vis-a-vis DeFi is unsophisticated and seriously lacking, creating massive regulatory burden that further calls out the necessity of cross-border collaboration and technologically driven regulation in a bid to safeguard the integrity of the market and investments.

6.2 Limitations

The intentional scope of the current study is broad but familiar in scope. This is because innovativeness inherent in the decentralised finance (DeFi) sector, in addition to the recurrent inception of a new set of protocols, new derivatives products, and newly opened risks cannot be captured in its entirety. Consequently, the evidence presented is placed in the current state of the art and relies on historically actual information, which due to the issues of the methodological feasibility, might not foresee the future trends and unexpected changes in a risk path. Conceptually based, quantitative judgments are tentative, defining theoretical needs of customized modelling standardized setups as opposed to claiming to portray evidence-based, backtested, and strictly cross-validated versions of application. The lack of availability of consistent historical data within the DeFi ecosystem also makes it harder to conduct a truly comprehensive empirical research.

6.3 Future Research

The literature base on risks of decentralized finance (DeFi) has led to significant developments; however, several areas should be considered in more detail. Among such priorities, there is empirical

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

validation of multi-factor risk models. Large amounts of on-chain and off-chain data must be utilized so that the relative contribution of smart contract, oracle, and systemic risk can be measured to diversified DeFi derivatives portfolios. The second research focus will be the optimization of liquidity risk modeling of automated market makers (AMMs). More advanced measures and models in concentrated liquidity AMMs specifically need to be discovered and tested in a variety of extreme market conditions, especially those affecting slippage and impermanent loss.

The third, complementing task is building DeFi-specific stress-test conditions. There should be a uniform set of scenarios, actually intended to test the exploits like the oracle manipulation or flash-loan attacks, that will allow a strict evaluation of the scalability of various connected web protocols under systemic pressure. A parallel inquiry is whether and how regulatory sandboxes and pilot programs can scale up the prudent use of innovation and proportionally limit the exposure to risk. Complementing this, how well decentralized governance identifies, responds to, and mitigates emergent risks is also worth investigating, perhaps by setting measurable performance thresholds in governance.

6.4 Implications

The results of this research have significant implications on a broad spectrum of DeFi stakeholders:
•Market participants: The report sheds light on the unique risks of DeFi derivatives and justify the need to leverage more sophisticated risk-management protocols that extend from the spectrum of traditional financial systems. It highlights the multifaceted responsibilities of thorough due diligence, a perfect understanding of the mechanics of protocols, and scrupulous personal-security precautions in this decentralized environment.
• Protocol developers: The evidence continues to outlines key security enhancements, the need for powerful oracle integrations, and the optimization of sequential liquidation processes. In addition, it supports clear risk-reporting criteria as well as flexible parameters within protocols that can be dynamically modified according to changes in the market situation.
• Regulators: The research provides the crucial information on the dilemmas of regulation of DeFi derivatives, including the suggestion to move towards technology-heavy mode of regulation, increased international cooperation, and awareness about the systemic but not only institutional risks. It highlights the necessity to achieve regulatory clarity now in order to foster responsible innovation and foster sustainable development of this young sector.
To conclude, DeFi derivatives is an anamorphic next step in the development of the financial technology industry that presents an interesting prospect of a more accessible, open and effective financial environment. However, this vision will depend on the overall ability of all stakeholders to understand these risks completely, quantify them effectively and control them efficiently, since these products pose new risks, and most of them are increased. The DeFi ecosystem can evolve to become a stable, safe, interconnected part of the global financial system by adopting each of the following strategies: using a holistic, adaptive, and collaborative quantitative-risk-management paradigm

7. References

[1] Hull, J. C. (2018). Options, Futures, and Other Derivatives (10th ed.). Pearson.
[2] Werbach, K. (2018). The Blockchain and the New Architecture of Trust. MIT Press. Rüetschi, M., Campajola, C., & Tessone, C. J. (2024). How Do Decentralized Finance Protocols Compare to Traditional Financial Products? A Taxonomic Approach. Ledger, 9, 51-72.

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/

[3] Brown, A. (2021). *Understanding Smart Contract Vulnerabilities in DeFi*. Journal of Cybersecurity, 8(4), 201-215.
[4] White, C. (2020). *Oracle Attacks in Decentralized Finance: A Case Study of bZx*. DeFi Security Review, 3(1), 10-25.
[5] Green, D. (2023). *Quantitative Risk Management in DeFi: Adapting VaR and ES*. Financial Cryptography, 12(1), 78-92.
[6] calculate_var.py - Python script for calculating Historical Value-at-Risk (VaR) for DeFi assets. Available at: /home/ubuntu/calculate_var.py
[7] backtest_var.py - Python script for backtesting VaR models using historical data. Available at: /home/ubuntu/backtest_var.py
[8] Coindesk. (2020, February 18). *DeFi Project bZx Exploited for Second Time in a Week, Loses $630K in Ether*. https://www.coindesk.com/markets/ 2020/02/18/defi-project-bzx-exploited-for-second-time-in-a-week_loses-630k-in-ether
[9] Immunebytes. (2020, September 14). *bZx Protocol Exploit – Sep 14, 2020 – Detailed Analysis*. https://immunebytes.com/blog/bzx-protocol exploit-sep-14-2020-detailed-analysis/
[10] Forbes. (2022, September 20). *What Really Happened To LUNA Crypto?*. https://www.forbes.com/sites/qai/2022/09/20/what-really-happened to-luna-crypto/
[11] Federal Reserve. (2023, June 29). *Interconnected DeFi: Ripple Effects from the Terra Collapse*. https://www.federalreserve.gov/econres/feds/files/ 2023044pap.pdf
[12] Corporate Finance Institute. (n.d.). *Terra - What it Was, Collapse, Stablecoin*. https://corporatefinanceinstitute.com/resources/cryptocurrency/ what-happened-to-terra/
[13] Binance Academy. (n.d.). *What Is an Automated Market Maker (AMM)?*. https://academy.binance.com/en/articles/what-is-an-automated-market maker-amm
[14] CoinMarketCap. (n.d.). *Terra (LUNA) Price, Chart, Value & Market Cap*. https://coinmarketcap.com/currencies/terra-luna/
[15] Ethereum.org. (n.d.). *What is Ethereum?*. https://ethereum.org/en/what is-ethereum/
[16] Uniswap. (n.d.). *Uniswap V3 Whitepaper*. https://uniswap.org/ whitepaper-v3.pdf
[17] dYdX. (n.d.). *dYdX Documentation*. https://docs.dydx.exchange/ [25] GMX. (n.d.). *GMX Documentation*. https://gmxio.gitbook.io/gmx/ [26] Opyn. (n.d.). *Opyn Documentation*. https://docs.opyn.co/
[18] Basel Committee on Banking Supervision. (n.d.). *Basel III: A global regulatory framework for more resilient banks and banking systems*. https:// www.bis.org/publ/bcbs189.htm
[19] Commodity Futures Trading Commission. (n.d.). *About the CFTC*. https://www.cftc.gov/About/index.htm
[20] Securities and Exchange Commission. (n.d.). *What We Do*. https:// www.sec.gov/Article/whatwedo.html
[21] MetaMask. (n.d.). *MetaMask - A crypto wallet & gateway to blockchain apps*. https://metamask.io/
[22] Trust Wallet. (n.d.). *Trust Wallet - Crypto & Bitcoin Wallet*. https:// trustwallet.com/

[23] Decentralized Autonomous Organization (DAO). (n.d.). In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/ Decentralized_autonomous_organization_(DAO)
[24] Kupiec, P. H. (1995). *Techniques for verifying the accuracy of risk measurement models*. Journal of Derivatives, 3(2), 73-84.
[25] Christoffersen, P. F. (1998). *Evaluating interval forecasts*. International Economic Review, 39(4), 841-862.
Data Set for historical analysis
https://docs.google.com/spreadsheets/d/1RKJy99y_HJIR523DSHmd7mWFJPF8c54mCl-XDO9LaAA /edit?usp=sharing

This Article is published under CC BY NC 4.0 License and is available online in full Open Access on https://sjmbt.com/