Journal of
Risk and Financial Management

MDPI

Article

Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance

Tim Weingärtner [1,*], Fabian Fasser [1], Pedro Reis Sá da Costa [1] and Walter Farkas [2,3,4]

[1] School of Computer Science and Information Technology, Lucerne University of Applied Sciences and Arts, 6343 Rotkreuz, Switzerland
[2] Department of Banking and Finance, University of Zürich, 8032 Zürich, Switzerland
[3] Department of Mathematics, ETH Zürich, 8032 Zürich, Switzerland
[4] Swiss Finance Institute, 8006 Zürich, Switzerland
* Correspondence: tim.weingaertner@hslu.ch

Abstract: Decentralized finance (DeFi) promises a revolution in financial accessibility, transparency, and automation. Yet, its very novelty exposes participants to a number of additional risks and challenges. This study aims to address the risks associated with DeFi, while also conducting a comparative analysis to those of classical/traditional finance (TradFi). After introducing DeFi and its defining characteristics, such as the use of smart contracts, blockchain technology, and decentralized governance, the paper outlines the principal risks associated with DeFi. Drawing insights from an extensive literature review of 200 recent articles, of which 50 were thoroughly analyzed, the study compares risks of DeFi and TradFi, categorizing these into systematic and unsystematic risks. Furthermore, we introduce the 'risk wheel', an innovative tool tailored to understand and navigate the subtleties of DeFi risks, finding potential applications in risk assessment, management, and even education. This paper's primary objective is to provide a detailed and impartial examination of the risks associated with DeFi and their comparison to traditional finance in order to assist stakeholders in making informed decisions and mitigating possible losses.

Keywords: decentralized finance; DeFi; risk management; literature review; risk classification; risk wheel

check for updates

Citation: Weingärtner, Tim, Fabian Fasser, Pedro Reis Sá da Costa, and Walter Farkas. 2023. Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. *Journal of Risk and Financial Management* 16: 454. https://doi.org/10.3390/jrfm16100454

Academic Editor: Svetlana Drobyazko

Received: 3 October 2023
Revised: 12 October 2023
Accepted: 16 October 2023
Published: 20 October 2023

1. Introduction

The emergence of decentralized finance (DeFi) has brought many innovations and benefits to the financial industry, such as increased accessibility, transparency, and automation. DeFi protocols and applications offer new ways to lend, borrow, trade, and invest. However, they also introduce unique risks that need careful consideration. In this research, we will compare the risks associated with DeFi to those of traditional finance.

We will focus on systematic and unsystematic risks, which are often used in finance to characterize the causes and effects of risk. Systematic risks, usually referred to as market risks, are inherent to the market as a whole and influence all market assets. It is difficult to diversify or hedge systemic risks, which are driven by external factors such as economic conditions, political events, and technological advancements. Inflation, deflation, recession, and conflicts are examples of systematic risks. Unsystematic risks, often known as specific risks, are asset- or industry-specific risks that can be diversified or hedged. They are generated by internal factors such as the quality of management, the performance of the asset, and the rivalry in the industry.

First, we explain DeFi and highlight its most pivotal products, emphasizing its foundational technologies and functionalities. The third section focuses on the risk landscape. We explain the risk categories prevalent in traditional finance. Drawing from a robust analysis of academic literature—encompassing a quantitative review of 50 selected papers from a pool of 200—we elaborate on the multifaceted risks intrinsic to DeFi. Following this, the fourth section introduces a novel risk categorization that divides DeFi risks into systematic and unsystematic categories, paving the way for a more nuanced understanding. In Section 5, we present our 'risk wheel', a tool designed to assess DeFi risks. We highlight the diverse range of applications of this concept, with a particular focus on its effectiveness in the realms of risk assessment and risk management. We conclude with a rigorous discussion of our findings, obtained from our research. Overall, this paper aims to provide a comprehensive and balanced analysis of the risks of DeFi and a tool to visualize and assess them.

2. Decentralized Finance

Decentralized finance (DeFi) is a recent paradigm in the financial sector that combines blockchain technology and smart contracts to provide financial services without intermediaries. DeFi is a rapidly expanding segment of the crypto financial industry that offers numerous advantages over traditional financing.

The following DeFi features stand out from traditional finance:

- Decentralization: DeFi is based on decentralized networks, notably blockchain, which is a decentralized and distributed ledger technology that records transactions across multiple computers securely, transparently, and immutably, as well as peer-to-peer networks. These technologies function without a central authority or intermediaries.
- Smart contracts: DeFi relies on smart contracts, defined as self-executing contracts, where the terms are directly written into code and run on a blockchain, ensuring that they are not only tamper-proof but also automatically enforceable without the need for a centralized authority. These blockchain-encoded, self-executing, and enforceable computer programs enable DeFi to automate complex operations, remove the need for intermediaries, and increase efficiency and trust;
- Crypto assets: DeFi makes use of crypto assets, such as cryptocurrencies and tokens, as a means of exchanging and storing wealth. Crypto assets provide DeFi products with higher liquidity, flexibility, increased speed and accessibility than conventional assets, allowing DeFi to offer innovative financial products and services;
- Open finance: Open finance is the use of open protocols, standards, and networks to facilitate financial innovation and interoperability. Open finance enables DeFi to offer more inclusive, interoperable, and decentralized financial services than traditional finance;
- DeFi applications: Decentralized applications, also known as dApps, provide the user interface for financial services that run on blockchain systems. DeFi-powered decentralized applications include decentralized exchanges, lending systems, stablecoins, insurance, and prediction markets;
- DeFi ecosystem: The DeFi ecosystem includes blockchain technology and cryptocurrencies , platforms, and communities. Developers, users, investors, academics, regulators, and other stakeholders all contribute to the development and evolution of DeFi.

DeFi is the umbrella term for a variety of products that incorporate many or all of the features described above. Examples include Stablecoins, Liquidity Pools, Lending Pools, Staking, Insurance Products, Digital Exchanges (DEXs), or Automated Market Makers (AMMs). Some of these products are briefly described below to help readers better understand the subsequent content.

2.1. Stablecoins

Stablecoins are a type of token tied to a stable asset, such as a fiat currency, a commodity, or a diversified portfolio of assets. Stablecoins are intended to offer greater predictability and stability than other cryptocurrencies or tokens, which are frequently volatile and susceptible to changes.

There are various types of stablecoins based on the underlying asset to which they are linked. These are some of the most prevalent types of stablecoins:

1. Fiat-backed stablecoins: Stablecoins are backed by fiat currencies, such as the US dollar, the euro, or other currencies. They are issued and maintained by centralized entities that hold reserves of the corresponding fiat currency;
2. Commodity-backed stablecoins: Stablecoins backed by a commodity, like gold or oil. They are also issued and maintained by centralized entities and are supported by reserves of the respective commodity;
3. Algorithmic stablecoins: These stablecoins use computer algorithms to keep their value stable. They are not backed by real-world assets but rely on tech solutions instead. Decentralized systems, such as MakerDAO[1] and Frax[2], issue and control algorithmic stablecoins (Kjäer et al. 2021).

Stablecoins serve as a medium of commerce, unit of account, store of value, and collateral for loans, among other functions. Other DeFi products such as decentralized exchanges, loan systems, and prediction markets utilize them. Stablecoins offer DeFi greater liquidity, stability, and accessibility than other cryptocurrencies, allowing DeFi to offer new financial products and services.

2.2. Liquidity Pools

Liquidity pools, integral to DeFi protocols, allow decentralized applications (dApps) to operate and provide crypto investors with a way to earn yield on their digital assets. A liquidity pool represents a collection of digital assets in a smart contract that is used to facilitate trades between the assets on a decentralized exchange (DEX). Instead of traditional markets of buyers and sellers, many DeFi platforms use Automated Market Makers (AMMs), which allow digital assets to be traded in an automatic and permissionless manner through the use of liquidity pools.

As an essential part of DEXes, liquidity pools provide the liquidity that is necessary for these exchanges to function. They are created when users lock their cryptocurrency into smart contracts, which then enable them to be used by others. In exchange for providing liquidity, those who fund this pool earn a percentage of transaction fees for each interaction by users. Without liquidity, AMMs would not be able to match buyers and sellers of assets on a DEX, and the whole system would grind to a halt.

Liquidity pools use smart contracts to make trades. But if there is a mistake in the code, it can be exploited by hackers (Rivas 2022). They play a crucial role in attacks, as they often become the mechanism for price manipulation that leads to flash loan (Qin et al. 2021) and vampire attacks (Xu et al. 2022) to drain the liquidity of the pools.

2.3. Lending Pools

Lending protocols, which are decentralized, provide the rules, algorithms, and incentives governing the lending process within lending pools (Bartoletti et al. 2021). A lending pool is an instrument that facilitates the involvement of several borrowers and lenders in a decentralized lending market. Lending pools are utilized regularly in DeFi to provide liquidity, accessibility, and transparency to the lending market.

Like other DeFi products, lending pools fundamentally operate on decentralization, use smart contracts, and involve the exchange and collateralization of crypto assets. A lending pool must have adequate liquidity in order to issue loans. Thus, lending pools often depend on liquidity pools to maintain the necessary liquidity.

2.4. Automated Market Makers

Automated Market Makers (AMMs) are decentralized protocols that allow the creation and oversight of liquidity pools within a decentralized exchange (DEX) (Mohan 2020; Pourpouneh et al. 2020). AMMs utilize algorithms and smart contracts to automatically connect buyers and sellers, as well as to decide the prices and quantities of assets in the liquidity pool. They offer fair, transparent, and secure pricing on the DEX market.

AMMs serve multiple functions, including providing liquidity to the DEX market, letting users trade assets swiftly and easily, and allowing liquidity providers to make returns on their assets.

3. Risks in Traditional Finance and DeFi

DeFi is a fresh and game-changing approach to the financial sector offering a suite of financial services without the need for traditional intermediaries such as banks, brokers, or insurance companies. Accessibility, financial inclusion, transparency, self sovereign control over assets, and programmability are only some of the benefits that come with DeFi. Nevertheless, it also comes with its own set of risks, mixing new tech challenges with the usual challenges of handling money and finance. This section presents a comparative overview of the risks inherent in traditional finance (TradFi), which have been extensively studied and documented over an extended period, and the risks associated with Decentralized Finance (DeFi). We conducted both a qualitative analysis and a quantitative literature review on DeFi risks.

3.1. Risk Categories in TradFi

The Basel III risk categories are a set of rules that banks and other financial institutions use to manage and reduce their risks (King and Tarbert 2011; Shakdwipee and Mehta 2017). These criteria are established by the Basel Committee on Banking Supervision (BCBS) (Basel Committee on Banking Supervision 2011), an international regulatory body whose mission is to enhance financial system stability and integrity.

The main risk categories according to the Basel III regulatory framework are:

- Credit risk: This is the risk of default or loss on a loan or investment due to the borrower's or issuer's inability or reluctance to make regular payments. Credit risk is the primary risk category in traditional finance. It is managed through the establishment of appropriate capital requirements, implementing credit rules and processes, and conducting thorough credit risk assessments;
- Market risk: This is the risk of loss resulting from changes in market pricing or conditions, including interest rates, exchange rates, and stock prices. Market risk is controlled by imposing limitations on market exposure, developing frameworks for market risk management, and conducting routine stress testing;
- Operational risk: This is the risk associated with inadequate or failing internal processes, people, and systems, or external occurrences. Operational risk is managed by creating robust risk management frameworks, conducting regular internal audits, and executing effective contingency plans;
- Liquidity risk: This risk addresses the danger of incurring a loss or being unable to meet financial obligations owing to a lack of liquid assets or finances. Liquidity risk is managed by setting appropriate liquidity ratios, performing liquidity stress tests, and maintaining adequate funding sources;
- Concentration risk: This is the risk of loss resulting from a concentration of exposures to a single counterparty, sector, or geographic region. To manage concentration risk, diversification techniques are implemented, concentration limits are established, and exposures are regularly reviewed and monitored.

3.2. Qualitative Analysis of Risks in DeFi

Decentralized finance contains unique and novel financial risks for a variety of reasons. First, DeFi, being a nascent and rapidly growing sector of the financial industry, faces significant uncertainty and volatility. Several DeFi programs and methods are experimental in nature, and there is considerable doubt regarding their long-term feasibility and sustainability. Second, since DeFi relies on blockchain technology and smart contracts, it introduces additional risks and challenges not typically found in traditional financial systems. For instance, DeFi projects and protocols are often independent and decentralized, meaning there is no central authority or mediator that can provide oversight or control.

This can make it more challenging to manage and mitigate risks and expose DeFi users to new forms of threats, such as fraud and hacking. Third, since DeFi frequently involves the usage of digital assets, such as cryptocurrencies and tokens, the offered financial services can be extremely volatile and subject to substantial price swings. This means that DeFi users may be exposed to substantial financial risks, such as the possibility of losing their investment or the value of their assets.

In recent years, several publications have analyzed the risks associated with DeFi. The first systematic literature review of DeFi research directions was conducted by Meyer et al. (2022). While Werner et al. (2021) give a general overview of DeFi and also the mostly technical risks associated with it, Zhou et al. (2023) specifically addresses DeFi attacks. In their article, Schär (2021) explains the architecture, market mechanisms and price calculations of some DeFi products and also addresses the associated new risks. The survey of DeFi security by Li et al. (2022) also focuses primarily on technical aspects. However, the article also includes governance risks like inappropriate key management.

Much of the current literature focuses on the technical risks that arise with the new technology, some of which are fundamentally different from previous financial risks. Some, like Qin et al. (2021), address market manipulation with new technological features like flash loans. Comprehensive risk assessments which also include economical and market risks are rarely found, as in Meegan (2020) or Carter and Jeng (2021). Only recently, a first approach on a categorization of risks was presented by Chang et al. (2022). They present a framework of six main risk categories in their paper: smart contract risks, cybersecurity operational risks, blockchain infrastructure risks, social and people risks, financial risks, and societal risks.

In the following sections, we summarize the risks from the literature to provide a comprehensive overview that is not limited to technological risks.

3.2.1. Technology Risks

Risks from Smart Contracts

While smart contract technology is reshaping traditional industries and business processes, there are several potential hazards associated with its misuse in DeFi. We categorize these challenges according to the life cycle of smart contracts.

- Creation risks: Contract creation is an important step to implement smart contracts. Developers have to code their own contracts and then deploy them in various blockchain platforms. Translating the smart contract using the programming languages, can introduce exploitable vulnerabilities or errors. There might also be arithmetic vulnerabilities, which are types of vulnerabilities caused by flaws or errors in the contract's arithmetic computations. Other vulnerabilities in this category are re-entrancy vulnerability (Li et al. 2020), block randomness vulnerability (Bonneau et al. 2015), and overcharging (Chen et al. 2017).
- Deployment risks: Smart contracts need to be checked carefully before deploying on blockchain platforms to avoid potential bugs that can be exploited by malicious behaviors. However, it is challenging to verify the correctness of smart contracts due to the complexity of modeling smart contracts, it is of vital importance to evaluate the correctness of smart contracts before the formal deployment (Luu et al. 2016).
- Execution risks: The execution phase is pivotal to smart contracts, as it determines the final state of smart contracts. Since smart contracts cannot work without real-world information, it is necessary to rely on a trustworthy oracle (Al-Breiki et al. 2020). Also, the dependence of the order of transactions is challenging to solve it in smart contracts, and developers should be aware to mitigate potential losses (Mavridou and Laszka 2017). Finally, smart contracts are executed in serialization, which limits the system performance. There are some software transactional memory systems that help to improve the execution efficiency of smart contracts (Bragagnolo et al. 2018), but more work needs to be performed.

- Completion risks: The proliferation of smart contracts brings additional concerns. Most current smart contract and blockchain platforms lack privacy-preserving mechanisms, especially concerning transactional privacy. Consequently, all the transactions are visible to everyone in the networks. Although some blockchain systems use pseudonymous public keys to improve the anonymity of the transactions, most transaction data are still publicly visible (Ron and Shamir 2013).

Risks from the Blockchain Protocol

DeFi products operate on a distributed ledger system. Therefore, they heavily rely on the blockchain's underlying protocol and its flawless and ongoing functioning (Carter and Jeng 2021). Possible protocol errors could be:

- Changes to the protocol: Changes to the blockchain protocol can happen via hard forks, soft forks, protocol upgrades, or modifications from a governance process. A hard fork is a modification to the blockchain protocol that is not backward-compatible, requiring all network participants to update to the latest version of the program. A soft fork is a backward-compatible update to the blockchain protocol that may be executed without needing all users to upgrade their software. Some blockchain protocols, including Ethereum, have a method for executing protocol upgrades. Depending on the nature of the modifications being made, these enhancements may be introduced via a hard fork or a soft fork. Some blockchain networks provide a governance procedure that enables users to propose and vote on protocol modifications. The execution method for these modifications depends on the specific network, the type of proposed change, and the community's social structure. They can be implemented through a hard fork, a soft fork, or another method. There is the risk of fraud or sub-optimal outcomes of these change processes, as described in Barrera and Hurder (2018).
- Centralization: Consensus protocols, such as proof-of-work (PoW) or proof-of-stake (PoS), might be susceptible to centralization, which occurs when a small number of users control a considerable majority of the network's computational capacity (Gencer et al. (2018)). This is called a 51% attack. PoS protocols depend on a limited set of validators to validate transactions and establish consensus on the blockchain's state. If these validators are hacked or do not function in the best interests of the network, it might pose a risk to DeFi users. Further risks specific to the used consensus protocols are: selfish mining, pool hopping attack, Sybil attack, or nothing at stake attack.
- Performance and scalability: DeFi products can also be affected by the speed and scalability of a consensus mechanism. If the protocol cannot manage a huge amount of transactions or has a high latency, it might cause DeFi users to experience delays and other issues.
- Front running: Front running is a method of trading that includes profiting on knowledge of a future deal. This risk already existed in traditional finance (Cai 2003). A person or entity can engage in front running in the context of decentralized finance (DeFi) if they are able to monitor a trade that is about to be performed on a blockchain and then arrange their own trade ahead of it to gain an advantage. Often, the transaction pool (mempool) is used for front running. We also include attacks like sandwich attacks this category.

Risks from the Use of Oracles

Oracles are entities that supply smart contracts on a blockchain with external data (Caldarelli 2020). Since smart contracts cannot access anything outside of a blockchain, oracles must provide all required data from external sources. They serve as a link between the smart contract and the "outside world", providing the contract with the necessary data to execute its conditions.

Oracles do not provide the robust security properties of native blockchain protocols. Therefore, they can be manipulated by either technical or social vulnerabilities (Li et al. 2020). Yet, they are very sensitive and need always to be accurate.

Padding oracle attacks (Rorot 2014) and compression oracle attacks (Rorot 2013) are an example of oracle attacks that exploit the system's availability. Recently, an attack on the Solend lending platform incurred a debt of USD 1.26 million (Hines 2022). The hacker exploited a weakness in the platform's price data oracle, stole funds, and increased the value of the assets. This attack impacted three loan pools that held stablecoins.

There are solutions that try to provide strong guarantees of data authenticity. PADVA (Szalachowski 2019) and TownCrier (Zhang et al. 2016) are oracles that provide cryptographically checkable information as they attest to the content of websites accessed using the Hypertext Transfer Protocol Secure (HTTPS) protocol. The underlying idea behind these oracles is that they verify attestations due to the use of transport layer security (TLS). However, TLS does not guarantee that every visitor to the site sees the same information. Additionally, a website could maliciously alter its output to influence on-chain attestations, creating a centralized point of failure in the system.

Augur is a prediction market platform that uses an oracle to determine the outcomes of events (Peterson et al. 2018). The platform pays participants based on the outcome determined by the oracle. To ensure accurate reporting, the oracle may require certain users to report the outcome at designated times or face a financial penalty. If a user intentionally reports incorrect results, they may be subject to a dispute resolution process. However, Augur's oracle does not allow users to easily enter or leave the system, which can negatively impact the usability of the platform.

Risks from the Use of Liquidity Pools

Liquidity pools remove a lot of the risk that centralized exchanges have. However, there are still risks that can be serious problems for the crypto world:

- Impermanent loss: During extreme market fluctuations, liquidity pools risk impermanent loss. In simple terms, impermanent loss means that the FIAT value of a user's crypto assets deposited to a pool could decline over time.
- Smart contract vulnerabilities: Once assets have been added to a liquidity pool, they are controlled exclusively by a smart contract, with no central authority or custodian. So, if a bug or some vulnerability is exploited, they could lose the coins for good.
- Liquidation risk: As liquidity pools are often leveraged, there is a risk of forced liquidation if the price of the assets devalues. The highly volatile market of the crypto-currencies and the vulnerabilities can lead to liquidity problems. Recently, the missing payments on USD 17.7 million of loans from lending pools after a sudden implosion of FTX percolated to creditors on lending protocols (Sandor 2022). Solend, a decentralized lending protocol on the Solana network, has narrowly avoided having 95% of the SOL deposits in its lending pool liquidated (Elliot 2022). As the price of SOL continued to drop and the collateral is used for liquidation, Solend almost ended with no SOL.
- Flash loan attack: Flash loans are unlimited and non-collateralized loans in which a user borrows funds and returns them in the same transaction. Malicious actors use flash loans to manipulate the price of the market, resulting in the theft of assets. In 2021, a flash loan attack caused the value of the token to drop 95% (Crawley 2021). The attacker profited USD 3 million and left the company to adapt their strategy to prioritize security instead of product release. These attacks are becoming a serious problem in cryptocurrency and are increasing yearly. In 2021, attackers gained over USD 3.2 billion in various attacks, hacks, and scams. In 2022, this value raised to USD 3.7 billion (Malwa 2022).
- Vampire attack: Although unusual, vampire attacks can lead to the depletion of a liquidity pool. This attack drains the liquidity from one exchange to another source. Uniswap has become a victim of a vampire attack when a cloned exchange called SushiSwap siphoned USD 1.2 billion in liquidity (Kelly and Balakrishnan 2020). Although SushiSwap returned USD 14 million in Ether, this attack cast a shadow on the confidence of DeFi's community in this DEX.

Risks from the Use of Lending Pools

Lending pools (LPs) allow mutually untrusted users to lend and borrow crypto assets. All the parameters of a loan, like its interests, maturity periods or token prices, are determined by a smart contract, which also includes mechanisms to incentivize correct behavior.

Similar to smart contracts, lending pools are inherently complicated to design. Besides the typical difficulty of implementing secure smart contracts Zhao et al. (2017), lending pools feature complex economic incentive mechanisms, which makes it difficult to understand when a lending pool actually achieves the economic goals it was designed for. Recently, a cross-contract reentrancy attack on a lending pool allowed the exploiter to redeem the assets at inflated prices (Sovryn 2022).

But there are other risks that are serious problems for LPs:

- Liquidity risk: Currently, the main depositors contribute to most liquidity in LPs (Gudgeon et al. 2020) and a small group of borrowers account for most loans. For instance, when dual-role users supply stablecoins, they can launch illiquidity risks by withdrawing their deposits and not repay the loans. Aave protocol benefit from more revenue when potential risks are higher. This is consistent with the logic around LPs. LPs rely on users to provide liquidity. Therefore, these dual-role users can booster the growth of Aave by depositing their stablecoins. In contrast, this protocol faces negative consequences when the risk of potential illiquidity increases, because it can lead to devaluations of Aave protocol.
- Counterparty risk: Counterparty risk happens when one party in a financial transaction cannot fulfill their commitments. A reentrancy attack can be used as a tool to drain the liquidity. Since blockchain allows smart contracts to work without the need to trust any party except the smart contract itself, the untrusted contract then calls back to the original function in an attempt to drain funds. To avoid this risk, the security of a smart contract is a vital in DeFi.

Risks from Internet and Online Access

The internet and online access to DeFi and blockchain in general bring several concerns. Cybersecurity is a significant threat, as these systems are susceptible to hackers and theft. By getting access to users' private keys or by exploiting flaws in the smart contracts that operate on blockchain networks, hackers may attempt to steal users' assets.

In Distributed Denial of Service (DDoS) attacks, a network of hacked computers is used to flood a website or network with traffic, rendering it unreachable to authorized users. This can render a DeFi platform inaccessible, preventing users from accessing their cash or engaging in transactions.

3.2.2. Market and Financial Risks

Market and financial risks arise from either the financial market itself or the participants involved in financial transactions. Many of these risks are similar to risks of traditional finance. Nevertheless, the reasons are often different since DeFi uses a decentralized and often anonymous environment.

- Counterparty risk: Since DeFi depends on an interconnected network of smart contracts and other applications, the failure of a single component can have cascading effects on the entire system. The term for this is counterparty risk.
- Volatility and leverage: The values of cryptocurrencies and other assets utilized in DeFi often have an enormous leverage effect and can be extremely volatile, meaning that users may incur substantial losses if the value of their assets declines.
- Liquidity risk: Some DeFi systems and protocols may have restricted liquidity, making it challenging for users to purchase or sell particular assets. This can generate liquidity risk, since consumers may be unable to readily transfer their assets into cash or other kinds of value.

- Credit risk: Certain DeFi products, including decentralized exchanges (DEXs) and lending platforms, extend credit to customers. This can create credit risk, as there is a chance that borrowers will default on their loans or that the value of the collateralized assets would drop. Credit risks in DeFi differ from traditional finance because loans are typically overcollateralized.

3.2.3. Operational Risks

Operational risks are the risks of loss caused by poor or failing internal processes, people, or systems, or by external events that can interrupt the flow of corporate operations. The financial losses may be direct or indirect. Due to the fact that the functioning of DeFi products is fundamentally distinct from conventional finance, operational risks also vary substantially.

- Governance risks: Governance risks in DeFi relate to the uncertainties associated with the procedures and mechanisms that are used to make decisions concerning the operation and development of DeFi platforms and protocols. This could be the lack of transparency, making it difficult for consumers to comprehend how and by whom decisions are made Makridis et al. (2023). Also, some DeFi governance organizations may not be responsible to users, meaning that consumers may have few options if anything goes wrong or if they disagree with the decisions made. If a small number of persons or entities has disproportionate control over DeFi governance procedures, this might pose hazards for DeFi users, since these individuals or businesses may be able to make choices that are not in the best interests of the larger community. These decision-making processes utilized by DeFi governing bodies may be inefficient or susceptible to bias, which might result in subpar decision-making and cause hazards for DeFi users.
- Inappropriate key management: One aspect of governance risk involves the mishandling of private keys. The vast majority of DeFi smart contracts permit an update or even a trade halt. These transactions are performed using the product administrators' wallet and private keys. Any unauthorized use or theft of these private keys might lead to the loss of all funds. These may occur both intentionally and accidentally.
- Prospectus risks: "Depending on the country and legal structure of the underlying tokens, DeFi products might fall in the category of securities or asset tokens. For example, in Switzerland this token category result in prospectus requirements under the Swiss Code of Obligations" (FINMA 2018, pp. 6/11). This means that missing prospectus or errors in the descriptions can have legal consequences for the issuer.

3.2.4. Legislative, Regulatory and Governance Risks

The legislative and regulatory environment for DeFi is very challenging. Not only is this a very new and innovative technology, it must also be taken into account that DeFi products are available worldwide. Therefore, any country-specific laws must be taken into account.

- Legal status of smart contracts: Since smart contracts are self-executing, there is typically no legal redress when anything goes wrong. This implies that it may be difficult or impossible to remedy the issue if a contract is abused or a mistake is made in the code.
- Legal, regulatory, and compliance risk: DeFi is a very new and mostly unregulated field, which implies that there is a lack of legal and regulatory control. This can pose dangers for DeFi users, since they may have little options if something goes wrong. These risks can arise if either already existing legal requirements are not complied with or if the legal framework changes but the DeFi product is not or cannot be adapted.

3.2.5. Strategic and Reputational Risks

Strategic and reputational risks in DeFi are issues related to the long-term survival and reputation of DeFi platforms, protocols, and associated companies. DeFi is a fast expanding and very competitive industry, and new platforms and protocols are continuously being created. Risks associated with this category include:

- Changes in technology: the DeFi area is characterized by fast technical development, and platforms and protocols that do not keep up with these changes risk becoming obsolete or less appealing to consumers;
- Reputational risk: the reputation of a DeFi platform or protocol is crucial to its success, and any unfavorable press or security breaches might harm its reputation and reduce its appeal to users;
- Leave risk: if a DeFi platform or protocol encounters substantial issues or loses the confidence of its users, there is a danger that users would "exit" the platform, which might result in a loss of value or the platform's demise.

3.3. Quantitative Literature Review of DeFi Risks

To gain a deep understanding of DeFi-associated risks, we thoroughly analyzed pertinent academic literature. We conducted a comprehensive search in two academic databases, namely Google Scholar and Scopus, utilizing a carefully constructed search string to identify relevant scholarly literature pertaining to the diverse risks associated with DeFi. After our initial review, we excluded medical papers because they often referenced "defibrillators," causing terminological overlaps. The search string utilized for our final analysis was:

«Risk» OR «Risks» AND «Decentralized Finance» OR «Defi» NOT Defibrillator -Medicine -Health -Diabetes -Disease -Cancer

Due to the extensive search results, we sorted them by the number of references, limiting ourselves to the top 200 outcomes and focusing on publications from 2020 to 2023. Out of the 200 obtained results, 46 entries were excluded from consideration due to either incongruent titles or unavailability. Initially, we reviewed the literature based on the relevance of their titles, specifically looking for those that matched the topic "Risks of Decentralized Finance". We deemed a title relevant if it pertained to Traditional Finance (TradFi) or if it highlighted specific DeFi protocols. In this first step, we focused on the core principles of DeFi described above. Using this approach, we narrowed down our list from 154 publications to 96.

Subsequently, the abstracts of the remaining 96 publications were analyzed. To ensure a thorough evaluation, a set of criteria was established. Two researchers independently assessed each abstract based on these criteria. Their evaluations were then combined to derive a final score for each publication, ensuring a comprehensive comparison and identification of the most relevant works. The following scoring system was utilized: a score of 0 indicates no relevance, a score of 1 indicates some level of relevance, and a score of 2 indicates high relevance (see Table A1). Using this scoring system, we efficiently evaluated and compared various publications, assessing their importance in terms of DeFi domains, associated risks, protocols, and their connection to TradFi.

The articles that received the highest score from the evaluation process were selected for inclusion in the paper. Articles with a score of 4 or higher were included in this group. Consequently, the literature review thus resulted in a total of 50 publications. These remaining publications underwent a comprehensive analysis, wherein the described risks were carefully documented. This detailed analysis can be found in Appendix A.

Based on our analysis, Figure 1 highlights the ten most prominent risks. This figure represents the frequency of each risk's mention across the 50 selected publications and is also summarized at the end of Appendix A.

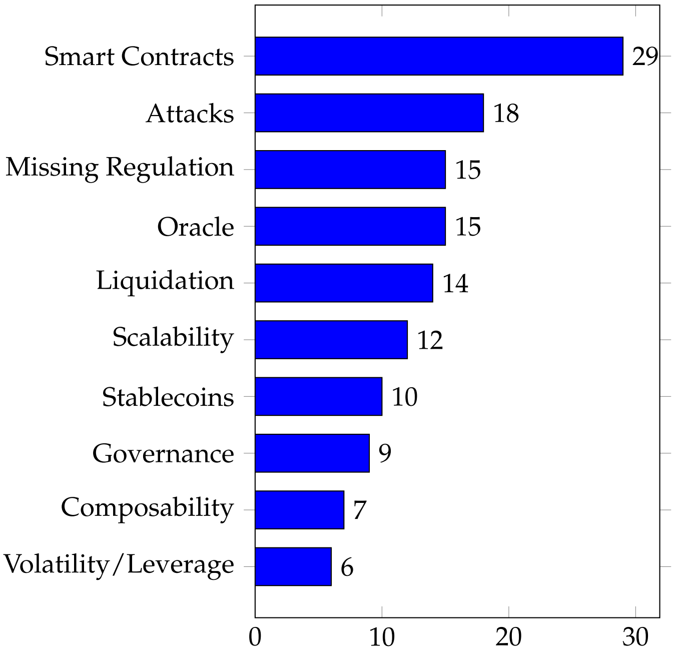

Figure 1. The ten most-mentioned DeFi risks in the literature (see Table A1 in Appendix A).

4. Classification of Risks in DeFi

The classification of risks provides a clear and structured overview, making it simpler to comprehend and communicate about various risk types. In their 1952 work "Portfolio Selection" (Markowitz 1952), economist Harry Markowitz introduced the distinction between systematic and unsystematic risk, laying the foundation for modern portfolio theory. Examples of systematic risk include recessions, political instability, and natural disasters. In contrast, unsystematic risk is unique to a given asset or firm and is uncorrelated with the market as a whole. Unsystematic risk examples include company-specific financial performance, changes in management, and regulatory measures.

Drawing from Markowitz's framework, we categorize risks associated with DeFi into systematic and unsystematic categories, the latter being those risks that can be managed or influenced by the DeFi product creator. We developed a further risk classification based on the findings of the qualitative and quantitative analysis described in Section 3.

We categorize operational risk under unsystematic risk as it can be managed by the DeFi smart contract's creator. From a technological perspective, there are risks categorized as controllable, aligning them with systematic risks, such as all risks associated with the development of the smart contract, as well as unsystematic risks, which stem primarily from the protocol or external technological aspects, such as oracles or cryptography. With measures such as collateralization, certain financial risks can be addressed or at least mitigated, while other financial risks are indeed market-dependent and systemic. A similar principle is applicable to legislative and regulatory risks. Compliance with present rules is a risk that can be managed; however, regulatory changes are exogenous and hence unmanageable. In this uncertain landscape, it is even more important to seek a stable regulatory environment and proactively anticipate potential changes. Comparisons with traditional financial products and their regulatory conditions can help.

Figure 2 provides a detailed visualization of our categorized risks. The left half of the figure represents unsystematic risks, whereas the right half illustrates systematic risks. The inner colored circle denotes the level 1 categories, as detailed in Section 3.2. The outer circle delineates the level 2 risk categories, which are aligned with the level 1 risk categories based on their positioning. Notably, the top ten risks from Figure 1 are highlighted in yellow.

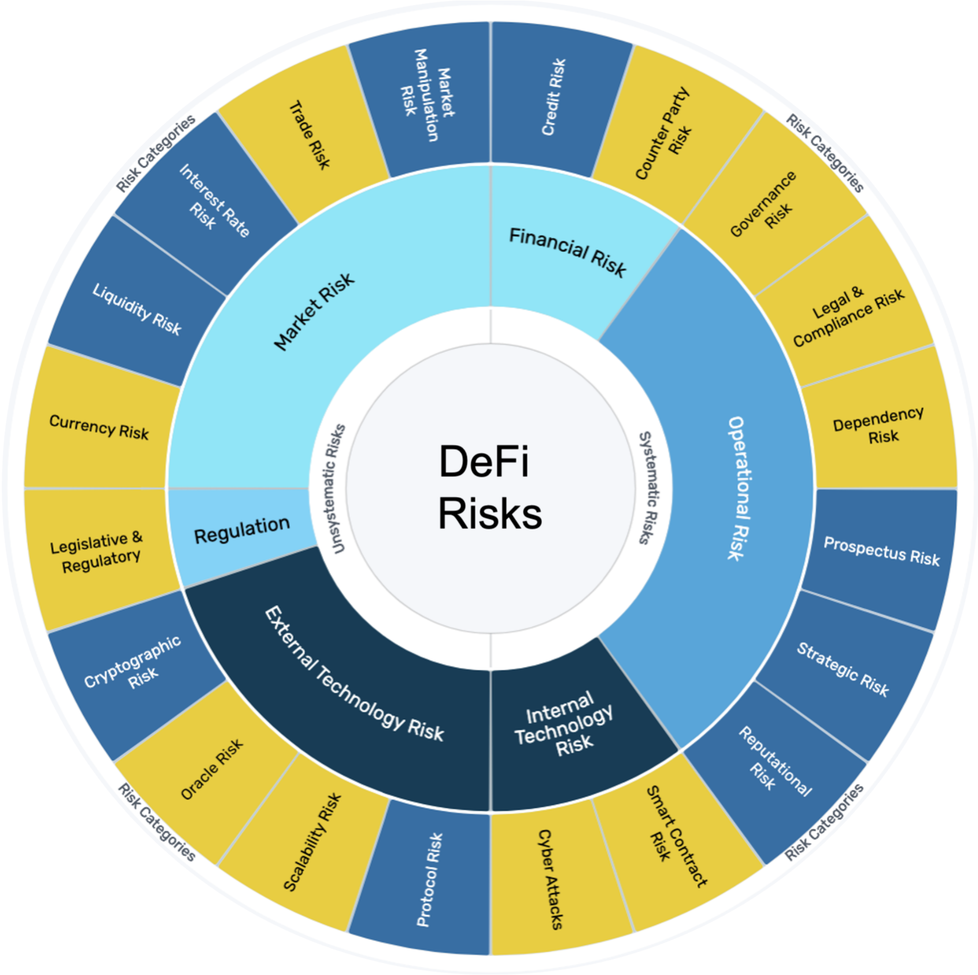

Figure 2. Suggested risk categories for DeFi. Yellow indicates the top ten risks from the literature (see Figure 1). The colors within the inner circle differentiate the DeFi risk categories as outlined in Section 3.2.

In the following section, we focus on the question how those risks can be measured and managed.

5. Assessing Risks in DeFi

Drawing inspiration from the principles of supply chain risk assessment and the risk wheel framework presented by Handfield and McCormack (2007), we formulated a parallel framework tailored for the DeFi sector. The DeFi risk categories, as illustrated in Figure 2, play a crucial role in streamlining this process. These categories serve as the foundation for multiple risk management tasks.

The risk wheel introduced here is versatile, applicable to tasks encompassing risk assessment, monitoring, and communication, as elaborated in the subsequent sections.

5.1. Static Risk Assessment

In practical scenarios, a common methodology is the risk matrix approach, which factors in the likelihood of a risk occurring (probability) and the potential fallout or damage should the risk manifest (impact). The risk wheel offers the possibility to visualize the varying probabilities and impacts of occurrences within their respective categories. As seen in Figure 3, the relevant areas can be visually represented in the risk wheel. This gives a comprehensive risk view at a glance.

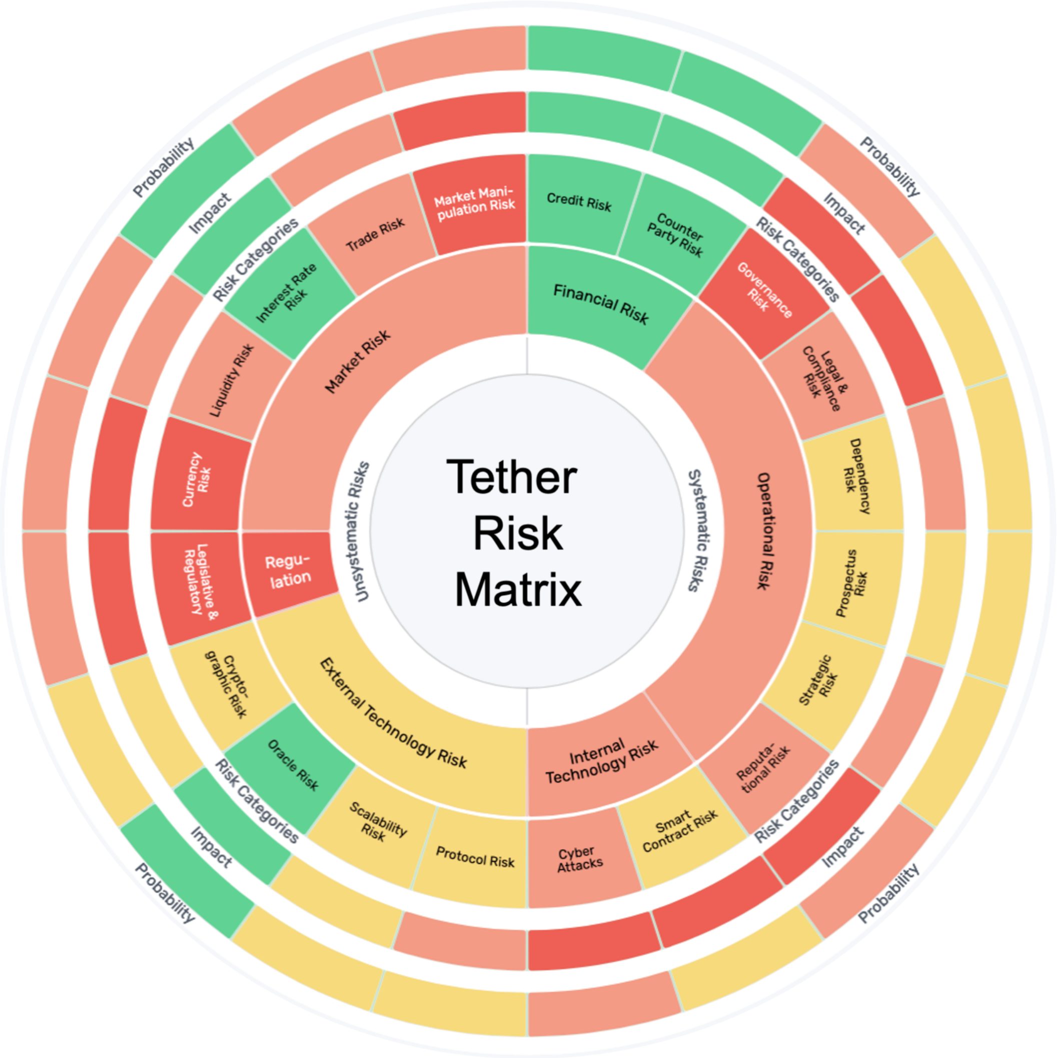

Figure 3. This risk wheel provides a static risk analysis of the Tether stablecoin. The color-coded system is as follows: Red (high risk), light red (medium risk), yellow (low risk), green (no risk). The colors assigned to the categories reflect the risks determined by both probability and impact. The shades of the inner circle collectively represent all risk categories associated with these primary (level 1) classifications.

5.2. Continuous Risk Monitoring

Dynamic risk factors refer to variables that are subject to change over time, influencing the likelihood and ramifications of potential risks. For instance, within DeFi, dynamic elements might include the total value locked (TVL) in a specific protocol or prevailing market sentiments influencing market risks. A sudden increase in TVL might increase the impact of a smart contract vulnerability. Also, traditional risk factors, like the Value at Risk (VaR), could be used.

The risk categories and risk wheel described in this study can facilitate the process of continuous monitoring and offers the opportunity to include quantitative data. This offers the chance of visualizing both real risk events and simulated risk scenarios like stress tests. To deepen the understanding of how risks interplay, interactive tools like the one offered by Plandisk[3] can be employed.

5.3. Risk-Based Comparison of DeFi Products

The risk wheel offers a thorough and all-encompassing perspective on the myriad risk factors linked to a DeFi product. Through the structured, circular presentation of risks, the vast spectrum and multifaceted nature of potential challenges and vulnerabilities for each product are more readily graspable. The more risks concentrated in specific sections of the wheel for a particular product, the more apparent its vulnerabilities in those areas.

For stakeholders unfamiliar with the intricacies of blockchain and DeFi, the risk wheel offers a more intuitive and accessible way to understand the risk landscape. It can act as a focal point in discussions, meetings, or presentations. Given their objective to provide a holistic perspective, researchers or analysts are less inclined to miss out on detailing risks. By visualizing and comparing risks of various DeFi products, the risk wheel can inform decisions about investment, product adoption, or risk mitigation strategies.

5.4. Subsequent Analysis of Risk Incidents

Since the risk wheel provides a 360-degree view of the risks, this tool can also be used for subsequent analysis of risk incidents. Following a risk incident, stakeholders can consult the risk wheel to pinpoint the pertinent segment the incident aligns with, determining if it was a previously recognized risk, an under-emphasized one, or an entirely unexpected occurrence. This helps in quickly pinpointing the specific category or intersection of risk factors implicated, thereby streamlining subsequent forensic analysis and response.

With a clear visual representation of the risks at hand, developers and protocol architects are better positioned to craft precise mitigation strategies. For instance, if oracle manipulation is a prominently represented risk, efforts can be directed towards developing more secure oracle mechanisms.

5.5. Educational Tool

Finally, the risk wheel stands as a valuable tool in elevating the learning journey, particularly when navigating complex topics such as DeFi. It provides a holistic view of the entire DeFi risk landscape and offers a snapshot of the diverse challenges and uncertainties inherent to the DeFi ecosystem. The above described interactive digital versions of risk wheels allows the users to click on specific risks to delve deeper into definitions, examples, or case studies. This interactivity can further engage learners, promoting a more in-depth exploration of the subject. By presenting risks visually and highlighting their interrelations, the risk wheel can encourage learners to think critically about the complexities of DeFi, prompting deeper exploration and understanding.

6. Discussion

Our study contributes several significant insights to the current body of research in the DeFi domain. Firstly, we highlight an increase in the number of publications addressing DeFi risks, as seen by 50 out of the 200 assessed articles being published during the period spanning from 2020 to 2023. This observed increase in research activity likely mirrors the growing interest and academic attention towards this sector. The comprehensive literature review identified the ten most often cited risks associated with DeFi: smart contracts, attacks, absence of regulation, oracles, liquidation, scalability, stablecoins, governance, composability, and volatility/leverage. This compiled inventory provides clarity in a complex and rapidly evolving landscape.

Secondly, we introduce a detailed risk wheel, adeptly categorizing the various DeFi risks, hence providing a visual tool to enhance comprehension and facilitate navigation within the complexities of this financial domain. The applications of this risk wheel are manifold, spanning basic risk assessment, quantitative risk evaluation, DeFi product comparison based on risk factors, subsequent analysis following risk incidents, and its utility as an educational tool.

Finally, our research provides an in-depth exploration of DeFi-associated risks, adopting both qualitative and quantitative methodologies. Nonetheless, we must recognize a few constraints inherent to our study. Similar to systematic reviews, our sample selection and interpretation of results may have been impacted by possible biases. Furthermore, in order to ensure concentration and adhere to limitations in terms of quantity, we made the decision to select a subset of 50 articles from the total pool of 200, therefore removing several prospective perspectives from the larger collection. Future studies might potentially explore the possibility of broadening the scope of this review by integrating related research domains, or doing more comprehensive analyses of the risk categories that have been identified.

By consolidating and presenting these insights, our work aims to offer a foundational framework for various stakeholders within the DeFi ecosystem to understand and address the numerous risks inherent to decentralized finance. Each group brings unique concerns and insights based on their distinct roles and interactions with DeFi systems. Investors, for instance, are concerned with profitability and the stability of their investments. Their concerns might focus on the robustness of smart contracts, potential vulnerabilities, the likelihood of large-scale breaches, and the clarity of regulations. Developers play a critical role in building and maintaining the infrastructure of DeFi systems. Their main concerns revolve around creating secure and efficient code, ensuring interoperability across various platforms, and keeping up with rapid technological advancements. Regulators are tasked with the challenging job of ensuring that DeFi platforms operate within legal boundaries while not stifling innovation. Their concerns include ensuring consumer protection, preventing money laundering or other illicit activities, and creating a regulatory framework that can adapt to the rapid evolution of the DeFi sector. Lastly, users of DeFi platforms, whether they are borrowers, lenders, or traders, are interested in the usability, security, and reliability of these systems. They are concerned with transaction fees, the transparency of protocols, the security of their assets, and the potential for improved financial returns or services compared to traditional finance.

Given the transformative potential of this financial system, it is also worth emphasizing the ethical and societal impact of DeFi, which has not been covered by our research yet. Aspects such as financial inclusion, privacy, and security play critical roles in shaping the future of DeFi. These considerations are especially crucial when evaluating the implications for vulnerable populations. Ensuring that DeFi systems are both transparent and inclusive, and that they prioritize the safety and privacy of users, is vital in fostering an equitable financial ecosystem. Future research could delve deeper into these ethical dimensions, examining the balance between innovation, risk, and societal benefit in the DeFi sector.

Author Contributions: Conceptualization, T.W. and W.F.; methodology, T.W. and W.F.; literature review, F.F.; DeFi description, T.W. and P.R.S.d.C.; validation, T.W. and W.F.; writing—original draft preparation, T.W.; writing—review and editing, W.F.; visualization, T.W.; funding acquisition, T.W. and W.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the SNSF Bridge project *Data Driven Financial Risk and Regulatory Reporting (DaDFiR3)* Grant Nr. 40B2-0_203617. The authors would like to express their gratitude to the Swiss National Science Foundation (SNSF) for their support and for making this research possible.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Literature analysis.

Title	Reference	Year	DeFi	DeFi Risks	DeFi Protocol	TradFi	Total	Smart Contracts	Attacks	Missing Regulation	Oracle	Liquidation	Scalability	Stablecoins	Governance	Composability	Volatility/Leverage	Other Risks
DeFi protocol risks: the paradox of DeFi	Carter and Jeng (2021)	2021	2	2	2	2	8	X		X			X	X				Operational Risk
DeFi risks and the decentralisation illusion	Aramonte et al. (2021)	2021	2	2	1	2	7					X		X			X	
A Risk Classification Framework for Decentralized Finance Protocols	Chang et al. (2022)	2022	2	2	2	1	7	X	X									MEV, network effect
Decentralized Finance (DeFi): Foundations, Applications, Potentials, and Challenges	Gramlich et al. (2022)	2022	2	2	2	1	7	X	X	X		X	X					
Security and efficiency of collateral in decentralized finance	Harz (2022)	2022	2	2	2	1	7				X	X			X			Governance, technical security
Risks in DeFi-Lending Protocols-An Exploratory Categorization and Analysis of Interest Rate Differences	Huber and Treytl (2022)	2022	2	2	2	1	7	X			X		X		X			Operational risk
A Survey of DeFi Security: Challenges and Opportunities	Li et al. (2022)	2022	2	2	2	1	7	X			X							Cybersecurity, design issues
An empirical study of DeFi liquidations: Incentives, risks, and instabilities	Qin et al. (2021)	2021	2	2	2	1	7					X						Flash loans

Table A1. *Cont.*

Title	Reference	Year	DeFi	DeFi Risks	DeFi Protocol	TradFi	Total	Smart Contracts	Attacks	Missing Regulation	Oracle	Liquidation	Scalability	Stablecoins	Governance	Composability	Volatility/Leverage	Other Risks
Deceptive Assurance? A Conceptual View on Systemic Risk in Decentralized Finance (DeFi)	Bekemeier (2021)	2021	1	2	1	2	6	X		X	X	X	X		X	X		
DeFi Potential, Advantages and Challenges	Borisov (2022)	2022	1	2	2	1	6	X		X	X		X			X		Infrastructure risk
Decentralized Finance (DeFi): Transformative Potential & Associated Risks	Carapella et al. (2022)	2022	1	2	2	1	6	X	X	X	X	X	X		X	X		
Security analysis of DeFi: Vulnerabilities, attacks and advances	Li et al. (2022)	2022	1	2	2	1	6	X			X							
Cryptocurrencies and decentralized finance (DeFi)	Makarov and Schoar (2022)	2022	2	1	1	2	6	X						X				Leverage
Flash crash for cash: Cyber threats in decentralized finance	Oosthoek (2021)	2021	2	2	2	0	6	X	X									
Speculative multipliers on DeFi: Quantifying on-chain leverage risks	Wang et al. (2022)	2022	2	2	2	0	6	X	X							X		
Centralized and decentralized finance: Coexistence or convergence?	Wieandt and Heppding (2023)	2023	2	1	1	2	6	X		X	X		X	X				
Defining DeFi: Challenges & pathway	Amler et al. (2021)	2021	1	1	1	2	5	X		X	X		X			X		Data protection, infrastructure

Table A1. *Cont.*

Title	Reference	Year	DeFi	DeFi Risks	DeFi Protocol	TradFi	Total	Smart Contracts	Attacks	Missing Regulation	Oracle	Liquidation	Scalability	Stablecoins	Governance	Composability	Volatility/Leverage	Other Risks
Embedded Supervision: How to Build Regulation Into Decentralized Finance	Auer (2022)	2022	1	1	1	2	5							X				Exchanges
DeFi Survival Analysis: Insights into Risks and User Behavior	Green et al. (2022)	2023	1	2	2	0	5										X	Lending protocol
SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance	Heimbach and Wattenhofer (2022)	2022	1	2	2	0	5		X									
Advantages and disadvantages of decentralized financial (DeFi) services	Kirvesoja (2022)	2022	2	1	0	2	5			X	X		X					Flash loans, illegal activities, systemic risk
Stablecoins and Their Risks to Financial Stability	MacDonald and Zhao (2022)	2022	1	1	2	1	5							X				
Risks and benefits of centralized and decentralized cryptocurrency exchanges and services	Nummelin (2022)	2022	2	2	0	1	5		X									Fraud, scams
Decentralized finance (DeFi)–the lego of finance	Popescu (2020)	2020	2	1	2	0	5	X									X	Fraud
Decentralized finance: On blockchain-and smart contract-based financial markets	Schär (2021)	2021	2	2	1	0	5	X			X		X			X		
Decentralized finance (DeFi)	Zetzsche et al. (2020)	2020	2	1	0	2	5				X							Lack of support in times of crisis, technological dependency, price manipulation

Table A1. *Cont.*

Title	Reference	Year	DeFi	DeFi Risks	DeFi Protocol	TradFi	Total	Smart Contracts	Attacks	Missing Regulation	Oracle	Liquidation	Scalability	Stablecoins	Governance	Composability	Volatility/Leverage	Other Risks
SoK: lending pools in decentralized finance	Bartoletti et al. (2021)	2021	1	2	1	0	4	X	X			X						
Governing Decentralized Finance (Defi)	Bhambhwani (2023)	2022	1	1	2	0	4								X			
A deep dive into crypto financial risks: stablecoins, DeFi and climate transition risk	Born et al. (2022)	2022	0	1	2	1	4			X		X		X			X	Risk appetite, spillover effect
Risk Analysis of Crypto Assets	Botte and Nigro (2021)	2021	0	2	1	1	4											Correlation, complexability,
Flashot: a snapshot of flash loan attack on DeFi ecosystem	Cao et al. (2021)	2021	2	1	1	0	4	X	X									Flash loans
Blockchain disruption and decentralized finance: The rise of decentralized business models	Chen and Bellavitis (2020)	2020	2	1	1	0	4			X							X	Data protection
Decentralized finance (DeFi): an emergent alternative financial architecture	Chohan (2021)	2021	1	1	1	1	4	X	X	X								Arbitrage, manipulationen, money laundry
Do we still need financial intermediation? The case of decentralized finance–DeFi	Grassi et al. (2022)	2022	1	1	1	1	4	X	X									Technology risks
Manage Risk in DeFi Portfolio	Inzirillo and De Quénetain (2022)	2022	1	2	1	0	4	X	X			X		X				Double Spending attack
An introduction to decentralized finance (DeFi)	Jensen et al. (2021)	2021	1	2	1	0	4	X					X		X	X		
Stablecoins 2.0: Economic foundations and risk-based models	Klages-Mundt et al. (2020)	2020	1	1	1	1	4	X		X				X	X			Stability, counterparty risk

Table A1. *Cont.*

Title	Reference	Year	DeFi	DeFi Risks	DeFi Protocol	TradFi	Total	Smart Contracts	Attacks	Missing Regulation	Oracle	Liquidation	Scalability	Stablecoins	Governance	Composability	Volatility/Leverage	Other Risks
MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance')	Maia and Vieira dos Santos (2021)	2021	2	1	1	0	4		X			X						
DeFi Risk Transfer: Towards A Fully Decentralized Insurance Protocol	Nadler et al. (2022)	2022	1	1	2	0	4	X	X		X				X			
Decentralized Finance & Centralized Finance Analogy	Pardhi et al. (2022)		2	1	0	1	4	X										Missing customer service
Liquidations: DeFi on a Knife-edge	Perez et al. (2021)	2021	1	1	2	0	4					X						
Attacking the DeFi ecosystem with flash loans for fun and profit	Qin et al. (2021)	2021	1	2	1	0	4				X							
Challenges and approaches to regulating decentralized finance	Salami (2021)	2021	1	1	1	1	4			X				X				Know-Your-Customer Challenge
Decentralized finance (DeFi) compliance and operations	Scharfman and Scharfman (2022)	2022	2	1	1	0	4		X	X								
DeFi: decentralized finance-an introduction and overview	Schueffel (2021)	2021	2	0	1	1	4	X				X	X					
P2P-The Key Behind Regulatory Framework of DeFi Services	Shalini et al. (2023)	2023	1	2	0	1	4	X	X	X					X		X	
Liquidity Risks in Lending Protocols (LPs): Evidence from Aave Protocol	Sun (2022)	2022	1	1	2	0	4					X						

Table A1. *Cont.*

Title	Reference	Year	DeFi	DeFi Risks	DeFi Protocol	TradFi	Total	Smart Contracts	Attacks	Missing Regulation	Oracle	Liquidation	Scalability	Stablecoins	Governance	Composability	Volatility/Leverage	Other Risks
Rethinking the Rule and Role of Law in Decentralized Finance	Wang (2022)	2022	1	1	1	1	4					X						Unstable loss, arbitrage
Blockeye: Hunting for DeFi attacks on blockchain	Wang et al. (2021)	2021	1	2	1	0	4	X	X									
Sok: Decentralized finance (DeFi) incidents	Zhou et al. (2023)	2023	1	1	2	0	4	X	X		X							Cyber risks, front running
50 sources								29	18	15	15	14	12	10	9	7	6	

Notes

[1] https://makerdao.com/ (accessed on 20 December 2022).

[2] https://frax.finance/ (accessed on 20 December 2022).

[3] https://plandisc.com/ (accessed on 3 October 2023).

References

Al-Breiki, Hamda, Muhammad Habib Ur Rehman, Khaled Salah, and Davor Svetinovic. 2020. Trustworthy blockchain oracles: Review, comparison, and open research challenges. *IEEE Access* 8: 85675–85. [CrossRef]

Amler, Hendrik, Lisa Eckey, Sebastian Faust, Marcel Kaiser, Philipp Sandner, and Benjamin Schlosser. 2021. Defi-ning DeFi: Challenges & pathway. Paper presented at the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, September 27–30, pp. 181–84.

Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf. 2021. Defi Risks and the Decentralisation Illusion. *BIS Quarterly Review*, December 6. Available online: https://www.bis.org/publ/qtrpdf/r_qt2112b.htm (accessed on 29 January 2023).

Auer, Raphael. 2022. Embedded supervision: How to build regulation into decentralized finance. *Cryptoeconomic Systems* 2: 1–48. [CrossRef]

Barrera, Cathy, and Stephanie Hurder. 2018. Blockchain Upgrade as a Coordination Game. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192208 (accessed on 29 January 2023). [CrossRef]

Bartoletti, Massimo, James Hsin-yu Chiang, and Alberto Lluch Lafuente. 2021. Sok: Lending pools in decentralized finance. In *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, Revised Selected Papers 25*. Berlin and Heidelberg: Springer, pp. 553–78.

Basel Committee on Banking Supervision. 2011. Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems. [Revised Version: June 2011; Online]. Available online: https://www.bis.org/publ/bcbs189.pdf (accessed on 29 January 2023).

Bekemeier, Felix. 2021. Deceptive assurance? a conceptual view on systemic risk in decentralized finance (DeFi). Paper presented at the 2021 4th International Conference on Blockchain Technology and Applications, Xi'an, China, December 17–19, pp. 76–87.

Bhambhwani, Siddharth M. 2023. Governing Decentralized Finance (DeFi). Available online: https://ssrn.com/abstract=4513325 (accessed on 17 July 2023).

Bonneau, Joseph, Jeremy Clark, and Steven Goldfeder. 2015. On Bitcoin as a Public Randomness Source. Cryptology ePrint Archive, Paper 2015/1015. Available online: https://eprint.iacr.org/2015/1015 (accessed on 1 October 2023).

Borisov, Svetoslav. 2022. Defi–potential, advantages and challenges. *Economic Studies* 31: 33–54.

Born, Alexandra, and Josep M. Vendrell Simón 2022. A Deep Dive into Crypto Financial Risks: Stablecoins, DeFi and Climate Transition Risk. *Macroprudential Bulletin*. Available online: https://ideas.repec.org/a/ecb/ecbmbu/20221.html (accessed on 1 October 2023).

Botte, Alex, and Mike Nigro. 2021. Risk Analysis of Crypto Assets. *TwoSigma*, July. Available online: https://www.twosigma.com/wp-content/uploads/2021/07/Using-Factors-to-Explain-Risk-in-Crypto-Assets-3.pdf (accessed on 1 October 2023).

Bragagnolo, Santiago, Henrique Rocha, Marcus Denker, and Stephane Ducasse. 2018. Smartinspect: Solidity smart contract inspector. Paper presented at the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, March 20, pp. 9–18. [CrossRef]

Cai, Fang. 2003. Was There Front Running during the Ltcm Crisis? Available online: https://ssrn.com/abstract=385560 (accessed on 19 October 2023) [CrossRef]

Caldarelli, Giulio. 2020. Understanding the blockchain oracle problem: A call for action. *Information* 11: 509. [CrossRef]

Cao, Yixin, Chuanwei Zou, and Xianfeng Cheng. 2021. Flashot: A snapshot of flash loan attack on DeFi ecosystem. *arXiv* arXiv:2102.00626.

Carapella, Francesca, Edward Dumas, Jacob Gerszten, Nathan Swem, and Larry Wall. 2022. Decentralized Finance (DeFi): Transformative Potential & Associated Risks. August 2022. FEDS Working Paper No. 2022-57. Available online https://www.federalreserve.gov/econres/feds/decentralized-finance-defi-transformative-potential-and-associated-risks.htm (accessed on 19 October 2023).

Carter, Nic, and Linda Jeng. 2021. Defi protocol risks: The paradox of DeFi. *Regtech, Suptech and Beyond: Innovation and Technology in Financial Services" RiskBooks–Forthcoming Q 3 2021*. Available online: https://ssrn.com/abstract=3866699 (accessed on 19 October 2023) [CrossRef]

Chang, Tara, Joe Ho, Zachary Tirrell, Gwen Weng, and Jo You. 2022. A Risk Classification Framework for Decentralized Finance Protocols. Available online: https://www.soa.org/resources/research-reports/2022/decentralized-finance-protocols/ (accessed on 6 January 2023).

Chen, Ting, Xiaoqi Li, Xiapu Luo, and Xiaosong Zhang. 2017. Under-optimized smart contracts devour your money. Paper presented at the 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), Klagenfurt, Austria, February 20–24, pp. 442–46. [CrossRef]

Chen, Yan, and Cristiano Bellavitis. 2020. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights* 13: e00151. [CrossRef]

Chohan, Usman W. 2021. Decentralized finance (DeFi): An emergent alternative financial architecture. *Critical Blockchain Research Initiative (CBRI) Working Papers*. Available online: https://ssrn.com/abstract=3791921 (accessed on 19 October 2023). [CrossRef]

Crawley, Jamie. 2021. Flash Loan Attack Causes DeFi Token Bunny to Crash over 95%. Available online: https://www.coindesk.com/markets/2021/05/20/flash-loan-attack-causes-defi-token-bunny-to-crash-over-95/ (accessed on 20 December 2022).

Elliot, Stacy. 2022. How a Solend Whale with a $108 M Loan Nearly Crashed the Solana Network. Available online: https://decrypt.co/103489/solend-whale-108m-loan-nearly-crashed-solana (accessed on 22 December 2022).

FINMA, Swiss Financial Market Supervisory Authority. 2018. Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (icos). Available online: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf (accessed on 20 January 2023).

Gencer, Adem Efe, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. 2018. Decentralization in bitcoin and ethereum networks. In *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, Revised Selected Papers 22*. Berlin and Heidelberg: Springer, pp. 439–57.

Gramlich, Vincent, Marc Principato, Benjamin Schellinger, Johannes Sedlmeir, Julia Amend, Jan Stramm, Till Zwede, Jens Strüker, and Nils Urbach. 2022. Decentralized Finance DeFi: Foundations, Applications, Potentials, and Challenges. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4535868 (accessed on 20 January 2023).

Grassi, Laura, Davide Lanfranchi, Alessandro Faes, and Filippo Maria Renga. 2022. Do we still need financial intermediation? the case of decentralized finance–DeFi. *Qualitative Research in Accounting & Management* 19: 323–47.

Green, Aaron, Christopher Cammilleri, John Erickson, Oshani Seneviratne, and Kristin Bennett. 2022. DeFi survival analysis: Insights into risks and user behavior. In *The International Conference on Mathematical Research for Blockchain Economy*. Cham: Springer International Publishing.

Gudgeon, Lewis, Sam Werner, Daniel Perez, and William J Knottenbelt. 2020. Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. Paper presented at the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, October 21–23, pp. 92–112.

Handfield, Robert, and Kevin P. McCormack. 2007. *Supply Chain Risk Management: Minimizing Disruptions in Global Sourcing*. Boca Raton: CRC Press.

Harz, Dominik Lucas. 2022. Security and Efficiency of Collateral in Decentralized Finance. Dissertation. Available online: http://hdl.handle.net/10044/1/101394 (accessed on 2 January 2023). [CrossRef]

Heimbach, Lioba, and Roger Wattenhofer. 2022. Sok: Preventing transaction reordering manipulations in decentralized finance. *arXiv* arXiv:2203.11520.

Hines, Richard. 2022. Attackers Hijack $1.26 Million from Solend Lending Platform. Available online: https://heraldsheets.com/attackers-hijack-1-26-million-from-solend-lending-platform/ (accessed on 2 January 2023).

Huber, Marco, and Vinzenz Treytl. 2022. Risks in DeFi-lending protocols-an exploratory categorization and analysis of interest rate differences. In *Database and Expert Systems Applications-DEXA 2022 Workshops: 33rd International Conference, DEXA 2022, Vienna, Austria, 22–24 August 2022, Proceedings*. Berlin and Heidelberg: Springer, pp. 258–69.

Inzirillo, Hugo, and Stanislas De Quénetain. 2022. Manage risk in DeFi portfolio. *arXiv* arXiv:2205.14699.

Jensen, Johannes Rude, Victor von Wachter, and Omri Ross. 2021. An introduction to decentralized finance (DeFi). *Complex Systems Informatics and Modeling Quarterly* 26: 46–54. [CrossRef]

Kelly, Liam, and Ashwath Balakrishnan. 2020. All You Need to Know about DeFi's SushiSwap Saga. Available online: https://cryptobriefing.com/all-you-need-know-about-defis-sushiswap-saga/ (accessed on 14 January 2023).

King, Peter, and Heath Tarbert. 2011. Basel iii: An overview. *Banking & Financial Services Policy Report* 30: 1–18.

Kirvesoja, Ville. 2022. Advantages and Disadvantages of Decentralized Financial (DeFi) Services. Master's Thesis, University of Jyväskylä, Jyväskylä, Finland. Available online: http://urn.fi/URN:NBN:fi:jyu-202206153332 (accessed on 20 February 2023).

Kjäer, Martin, Monika Di Angelo, and Gernot Salzer. 2021. Empirical evaluation of makerdao's resilience. Paper presented at the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, September 27–30, pp. 193–200.

Klages-Mundt, Ariah, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. 2020. Stablecoins 2.0: Economic foundations and risk-based models. Paper presented at the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, October 21–23, pp. 59–79.

Li, Wenkai, Jiuyang Bu, Xiaoqi Li, and Xianyi Chen. 2022. Security analysis of DeFi: Vulnerabilities, attacks and advances. Paper presented at the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, August 22–25, pp. 488–93.

Li, Wenkai, Jiuyang Bu, Xiaoqi Li, Hongli Peng, Yuanzheng Niu, and Xianyi Chen. 2022. A Survey of DeFi Security: Challenges and Opportunities. *arXiv* arXiv:2206.11821.

Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems* 107: 841–53. [CrossRef]

Luu, Loi, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making smart contracts smarter. In *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. New York: Association for Computing Machinery, pp. 254–69. [CrossRef]

MacDonald, Cameron, and Laura Zhao. 2022. *Stablecoins and Their Risks to Financial Stability*. Bank of Canada Staff Discussion Paper 2022-20. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466522 (accessed on 20 February 2023). [CrossRef]

Maia, Guilherme C., and João Vieira dos Santos. 2021. MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). In *Blockchain and the Law: Dynamics and Dogmatism, Current and Future*. N. 2, Vol. 28. Available online: https://ssrn.com/abstract=3875355 (accessed on 17 July 2023).

Makarov, Igor, and Antoinette Schoar. 2022. *Cryptocurrencies and Decentralized Finance (DeFi)*. Technical Report. Cambridge: National Bureau of Economic Research. [CrossRef]

Makridis, Christos A., Michael Fröwis, Kiran Sridhar, and Rainer Böhme. 2023. The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. *Journal of Corporate Finance* 79: 102358. [CrossRef]

Malwa, Shaurya. 2022. 2022 Crypto Attacks Were Least in December, with $62 M Lost in Heists, Certik Says. Available online: https://www.msn.com/en-us/money/markets/2022-crypto-attacks-were-least-in-december-with-62m-lost-in-heists-certik-says (accessed on 3 January 2023).

Markowitz, Harry. 1952. Portfolio selection. *Journal of Finance* 7: 77–91.

Mavridou, Anastasia, and Aron Laszka. 2017. Designing secure ethereum smart contracts: A finite state machine based approach. *arXiv* arXiv:1711.09327.

Meegan, Xavier. 2020. *Identifying Key Non-Financial Risks in Decentralised Finance on Ethereum Blockchain*. Milano: MIP Politecnico di Milano.

Meyer, Eva, Isabell M. Welpe, and Philipp G. Sandner. 2022. Decentralized finance—A systematic literature review and research directions. ECIS 2022 Research Papers. 25. Available online: https://ssrn.com/abstract=4016497 (accessed on 19 October 2023) [CrossRef]

Mohan, Vijay. 2020. Automated market makers and decentralized exchanges: A DeFi primer. *Financial Innovation* 8: 1–48.

Nadler, Matthias, Felix Bekemeier, and Fabian Schär. 2022. Defi risk transfer: Towards a fully decentralized insurance protocol. *arXiv* arXiv:2212.10308.

Nummelin, Sami. 2022. Risks and Benefits of Centralized and Decentralized Cryptocurrency Exchanges and Services. Bachelor Thesis. Available online: https://www.theseus.fi/bitstream/handle/10024/786568/Nummelin_Sami.pdf (accessed on 20 February 2023).

Oosthoek, Kris. 2021. Flash crash for cash: Cyber threats in decentralized finance. *arXiv* arXiv:2106.10740.

Pardhi, Sarika, Sakshi Mohale, Nikhil Ganorkar, Aman Jadhao, and Sonal V. Sawarkar. Decentralized finance & centralized finance analogy. In *2022 IJCSPUB, Volume 12, Issue 1 January 2022*. Available online: https://ijcspub.org/papers/IJCSP22A1008.pdf (accessed on 22 March 2023).

Perez, Daniel, Sam M. Werner, Jiahua Xu, and Benjamin Livshits. 2021. Liquidations: Defi on a knife-edge. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5. 2021, Revised Selected Papers, Part II 25*. Berlin and Heidelberg: Springer, pp. 457–76.

Peterson, Jack, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander. 2018. *Augur: A Decentralized Oracle and Prediction Market Platform*. *arXiv* arXiv:1501.01042. [CrossRef]

Popescu, Andrei-Dragoş. 2020. Decentralized finance (DeFi)—The lego of finance. *Social Sciences and Education Research Review* 7: 321–49.

Pourpouneh, Mohsen, Kurt Nielsen, and Omri Ross. 2020. Automated Market Makers. IFRO Working Paper No. 2020/08. Available online: https://www.econstor.eu/handle/10419/222424 (accessed on 3 March 2023).

Qin, Kaihua, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. An empirical study of DeFi liquidations: Incentives, risks, and instabilities. Paper presented at the 21st ACM Internet Measurement Conference, Virtual, November 2–4, pp. 336–50.

Qin, Kaihua, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the DeFi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security*. Berlin and Heidelberg: Springer, pp. 3–32.

Rivas, Ricardo. 2022. DeFi Algorand Based Platform Tinyman Lost $3 Million During an Exploit. Available online: https://www.fxempire.com/news/article/defi-platform-tinyman-lost-3-million-during-an-exploit-855009 (accessed on 6 January 2023).

Ron, Dorit, and Adi Shamir. 2013. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*. Berlin and Heidelberg: Springer, pp. 6–24.

Rorot. 2013. The BREACH Attack. Available online: https://resources.infosecinstitute.com/topic/the-breach-attack/ (accessed on 7 January 2023).

Rorot. 2014. Padding Oracle Attack. Available online: https://resources.infosecinstitute.com/topic/padding-oracle-attack-2/ (accessed on 25 July 2014).

Salami, Iwa. 2021. Challenges and approaches to regulating decentralized finance. *American Journal of International Law* 115: 425–29. [CrossRef]

Sandor, Krisztian. 2022. Crypto Trading Firm Auros, Hit by FTX Collapse, Discloses Provisional Liquidation. Available online: https://www.coindesk.com/markets/2022/12/20/crypto-trading-firm-auros-hit-by-ftx-collapse-discloses-provisional-liquidation/ (accessed on 20 December 2022).

Schär, Fabian. 2021. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis. Review* Available online: https://ssrn.com/abstract=3843844 (accessed on 19 October 2023). [CrossRef]

Scharfman, Jason, and Jason Scharfman. 2022. Decentralized finance (DeFi) compliance and operations. In *Cryptocurrency Compliance and Operations: Digital Assets, Blockchain and DeFi*. Cham: Palgrave Macmillan, pp. 171–86.

Schueffel, Patrick. 2021. Defi: Decentralized finance-an introduction and overview. *Journal of Innovation Management* 9: I–XI. [CrossRef]

Shakdwipee, Pushpkant, and Masuma Mehta. 2017. From basel i to basel ii to basel iii. *International Journal of New Technology and Research (IJNTR)* 3: 66–70.

Shalini, H. S., K. Ravichandran, and P. V. Raveendra. 2023. P2p-the key behind regulatory framework of DeFi services. In *Recent Advances in Blockchain Technology: Real-World Applications*. Berlin and Heidelberg: Springer, pp. 267–79. [CrossRef]

Sovryn. 2022. October 2022 Lending Pool Exploit Postmortem. Available online: https://www.sovryn.app/blog/october-2022-lending-pool-exploit-postmortem (accessed on 20 December 2022).

Sun, Xiaotong. 2022. Liquidity risks in lending protocols (lps): Evidence from aave protocol. *arXiv* arXiv:2206.11973.

Szalachowski, Pawel. 2019. Padva: A blockchain-based tls notary service. Paper presented at the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, December 4–6, pp. 836–43. [CrossRef]

Wang, Andre. 2022. Rethinking the rule and role of law in decentralized finance. Paper presented at the 2022 IEEE 24th Conference on Business Informatics (CBI), Amsterdam, The Netherlands, June 5–17, vol. 2, pp. 118–25.

Wang, Bin, Han Liu, Chao Liu, Zhiqiang Yang, Qian Ren, Huixuan Zheng, and Hong Lei. 2021. Blockeye: Hunting for DeFi attacks on blockchain. Paper presented at the 2021 IEEE/ACM 43rd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), Madrid, Spain, May 25–28, pp. 17–20.

Wang, Zhipeng, Kaihua Qin, Duc Vu Minh, and Arthur Gervais. 2022. Speculative multipliers on DeFi: Quantifying on-chain leverage risks. In *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, 2–6 May 2022, Revised Selected Papers*. Berlin and Heidelberg: Springer, pp. 38–56.

Werner, Sam M., Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. 2021. Sok: Decentralized finance (DeFi). *arXiv* arXiv:2101.08778.

Wieandt, Axel, and Laurenz Heppding. 2023. Centralized and decentralized finance: Coexistence or convergence? In *The Fintech Disruption: How Financial Innovation Is Transforming the Banking Industry*. Berlin and Heidelberg: Springer, pp. 11–51.

Xu, Jiahua, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2022. SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. *ACM Computing Surveys* 55: 1–50. [CrossRef]

Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. 2020. Decentralized finance (DeFi). *Journal of Financial Regulation* 6: 172–203. [CrossRef]

Zhang, Fan, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. 2016. Town crier: An authenticated data feed for smart contracts. In *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. New York: Association for Computing Machinery, pp. 270–82. [CrossRef]

Zhao, Xiangfu, Zhongyu Chen, Xin Chen, Yanxia Wang, and Changbing Tang. 2017. The DAO attack paradoxes in propositional logic. Paper presented at the 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, November 11–13, pp. 1743–746. [CrossRef]

Zhou, Liyi, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. Sok: Decentralized finance (DeFi) attacks. Paper presented at the 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 22–24, pp. 2444–61. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.