


Promise of AI in DeFi, a Systematic Review

Nafiz Sadman ¹, Md Manjurul Ahsan ², Abdur Rahman ¹, Zahed Siddique ³ and Kishor Datta Gupta ^{4,*}¹ Silicon Orchard Ltd., Dhaka 1206, Bangladesh; nafiz@siliconorchard.com (N.S.); rahman@siliconorchard.com (A.R.)² Industrial and Systems Engineering, University of Oklahoma, Norman, OK 73019, USA; ahsan@ou.edu³ School of Aerospace and Mechanical Engineering, University of Oklahoma, Norman, OK 73019, USA; zsiddique@ou.edu⁴ Department of Computer Science, University of Memphis, Memphis, TN 38152, USA

* Correspondence: kgupta1@memphis.edu

Abstract: Decentralized Finance (DeFi) is an emerging and revolutionizing field with notable uncertainties of reliability to be used on a mass scale. On the other hand, Artificial Intelligence (AI) has proved to be a crucial helping tool in numerous domains. In this study, we present a systematic review of the utility of AI in DeFi in terms of impact, reliability, and security and conduct exhaustive analysis. The review was motivated by an in-depth investigation of recently published literature that prioritized AI and DeFi in their research. This research, like many prior studies, examined the articles in terms of impact, reliability, and security. In addition, a new relevance score is introduced to better comprehend the quality of the content. According to investigation, the combination of AI and DeFi is one of the trending research topics that lacks adequate interpretations of black-box methodologies. Furthermore, it was discovered that one of the primary issues in DeFi is security, and numerous technologies, including blockchain technology and machine learning approaches, have been used to minimize such challenges. We hope that the gap addressed throughout this review will give insights to future researchers and practitioners, ultimately leading to new research opportunities in AI to bridge the gap of trust between peers and make the integration of DeFi more agile in the near future.



Citation: Sadman, N.; Ahsan, M.M.; Rahman, A.; Siddique, Z.; Gupta, K.D. Promise of AI in DeFi, a Systematic Review. *Digital* **2022**, *2*, 88–103. <https://doi.org/10.3390/digital2010006>

Academic Editor: David J. Edwards

Received: 4 January 2022

Accepted: 9 March 2022

Published: 12 March 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: decentralized finance; artificial intelligence; security; reliability

1. Introduction

Artificial Intelligence (AI) and decentralized finance (DeFi) are two technological developments that have gained tremendous traction in the last couple of years. The increasing use of AI in business has significant benefits for large and small organizations [1]. One famous example is chatbots—software applications that can interact with human users through conversations in natural language. This allows managers to automate some types of basic interactions with customers or employees, including answering frequently asked questions or scheduling appointments. Automating these tasks helps companies increase efficiency while also improving customer experience by providing more consistent information with fewer mistakes [2].

The accelerating pace at which artificial intelligence (AI) is developed has led many people to view it as one of the most significant technological developments of our time. AI is being developed to automate more tasks traditionally performed by humans (including administrative, managerial, and professional tasks). Likewise, the use of decentralized finance (DeFi) has grown exponentially in recent years. DeFi describes financial tools that are built on top of open blockchains [3] like Ethereum; these allow decentralized applications to interact with each other without requiring trusted intermediaries or centralized entities [4].

Initially, the Bitcoin system was used for creating the most popular cryptocurrencies with Bitcoin's features. Later it became clear that Bitcoin is not fully scalable and flexible

enough, so decentralized applications (DApp) developers started moving to the Ethereum blockchain platform because of its better technical capabilities [5].

Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality. It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), to execute scripts using an international network of public nodes. Ethereum also provides a cryptocurrency token called “ether”, which can be transferred between accounts and used to compensate participant nodes for computations performed [6].

Decentralized Finance (DeFi) is inspired by FinTech (FinTech: Financial Technology; Any technology that delivers financial services through software.) and the practical applicability of blockchain technology. Blockchain technology offers a decentralized, transparent platform for finance with no intermediaries for exchanges [7]. Lee et al. (2018) in their journal defines FinTech and disruption of FinTech in modern times: the digital evolution of financial services provided to customers. The authors uphold some contemporary challenges of FinTech, such as offering incentivized packages to customers and making the payment process more manageable [8]. The emergence of alternative peer-to-peer (P2P) lending, digital banking, mobile banking, smart contracts, and open banking APIs all come to offer additional options to customers. However, FinTech is vulnerable to cyberattacks and security breaches. Thus a decentralized system can help mitigate some of the existing problems of traditional FinTech. This decentralization is what we term as Decentralized Finance or DeFi in short. The decentralization and transparency provided by blockchain technology have led to disruption of DeFi [9]. It can provide transparency, innovation, low cost of a transaction, and borderlessness among peers from different geography. However, the counter to these facilities can be overexposing of privacy, open-source could lead to new manipulation technologies, and no specific body to be held accountable for if the system is abused. Malicious smart contracts and exploited audit protocols [10–12] are a few of the many primary concerns of DeFi users. The acceptance of DeFi is challenged by its very own characteristics. Absolute transparency is questionable to many legal terms till date since it seeks to demolish a controlled (centralized) system. zetzsche et al. (2020) dived into uncharted waters of DeFi where they proposed it requires regulation as any other financial body. The authors pointed three perspectives from which DeFi faces legal obstacles: “Legal jurisdiction and applicable law, enforcement, and data protection and privacy” [7]. Despite falling short on such terms, interest in DeFi has been ever increasing and led to the derivation of conceptually useful applications like DEX (decentralized exchange platforms) [13] for instance, where cryptocurrencies or crypto assets [14] can be exchanged. Unsurprisingly, DEX is not protected from security concerns such as replication of the platform to fool users [15]. Risk and hostility of crypto-assets [16], POW (proof-of-work) and POS(proof-of-stake) [17] fall under the same radar. Some scholars [18–20] have studied possible attacks on DeFi, while some scholars [21–23] have studied secure trading on DEX.

Artificial intelligence (AI) has helped many technologies mitigate security issues, which also includes blockchain. Utilizing artificial intelligence on the blockchain has been around for quite some time. A survey analysis by [24] of different machine learning adoption in blockchain technology discusses how specific ML techniques can be applied to counter the attacks on the blockchain network and also noted some practical use cases of these two technologies in autonomous vehicles, smart cities, and healthcare. Giudici and Polinesi (2021) conduct an analysis of the dynamics of crypto-currency price exchanges between bitcoin and traditional marketplaces. Their major study indicates that the greatest exchanges are facilitated through bitstamp [25].

A systematic survey following a detailed taxonomy of goal-oriented, layers-oriented, counter-measures, and applications of machine learning and blockchain technology has also been presented. Another work by [26] proposed an incentivized approach to build a decentralized data sharing and incremental model learning platform for users. The framework encourages quality data to be provided by the users for more accurate model training. However, the framework is vulnerable to data manipulation and hacks. The

framework requires 10% of data shared to be pre-exposed for validation by each user of the blockchain network. Moreover, the model that will be trained will also be exposed to the network. This creates a loophole for adversary attacks. Some scholars have studied applications of deep learning in blockchains [27,28], while others [29,30] have discussed the integrative perspective of one another and the convergence of two technologies that can be beneficial for improved services.

However, privacy remains a persisting issue in such kinds of settings and thus exists as a researchable topic as of today. Chen et al. (2018) introduced decentralized training of machine learning algorithms that follows the concept of blockchain technology, with a new concept of gradient calculation which they termed as LearningChain. They propose their architecture combined with an ‘l-nearest aggregation’ algorithm is resilient to byzantine attacks. The authors evaluated their architecture on three different datasets and concluded that their system would work as long as Byzantine attackers do not exceed 51% in numbers. The paper does not provide any practical implementation in the domain of decentralized finance, however, their research can act as a building block towards ‘better AI’ in DeFi [31]. One such technology is “RegTech” [8], a regulatory technology driven by AI, that can prevent such attacks.

While both AI and DeFi present significant business opportunities, they also pose potentially significant threats to established business models. Managers in all industries need to be aware of the potential impact of AI and Defi on their companies’ strategies, operations, HR/recruitment strategies, accounting records, etc. As the applications and domains of AI evolve fast, so does decentralized finance; hence, an up-to-date overview will provide new academics and practitioners with valuable insights. This study selected articles using a hybrid technique. Apart from the standard bibliometric analysis and qualitative synthesis, a few research employed novel methodologies. For example, Wadesango et al. (2020) employed a methodology called the desktop approach, which is quite distinct from empirical research [32].

The majority of systematic reviews employed two to three databases to identify articles, which frequently raised concerns about the result’s bias [33]. On the other hand, Google Scholar keeps a substantial volume of literature that is frequently difficult to utilize for systematic literature reviews (SLR) but serves as a significant source for the article [34]. Additionally, Google Scholar indexes many new and significant papers earlier than any other resource. As a result, we began this effort by utilizing Google Scholar as our primary database. The first evaluation was conducted methodically, with up to 50 searched google scholar pages in length, and further pertinent papers were included. Additionally, we implemented a new rating system in our review process, which may help future researchers and practitioners avoid ambiguity when comparing newly published papers to previously published material.

In this study, we perform a hybrid systematic literary analysis on some of the recent and most relevant research on the use of artificial intelligence in decentralized finance in terms of impact, reliability, and security. The analysis include extensively studying each literature, authors’ claim on impact, reliability, and security, and, our distributed yet consensus agreement on the claims. We also compute a relevance score that utilizes citation, year of publication and the ranking of the publication platform. While proceeding with this study, we have seen that integration of AI in DeFi is still at the infant stage of research. There are few several methods [35–37] to measure relevance and impact of scientific research. However, we demonstrate our own criteria. We further conclude from our extensive literature review that we can identify possible new research opportunities in AI to bridge the gap of trust between peers and more agile the integration of DeFi in the near future.

The contribution of this study includes:

- A systematic study of various recent research publications based on the use of artificial intelligence in decentralized finance.

- Insights to such research publications according to impact, reliability, and security. A relevance score calculated on the basis of year of publication, citation, and ranking of the publication platform.
- A trend analysis as to where DeFi could be heading with AI.

The organization of this research is as follows. In Section 2, we briefly define some technical backgrounds related to the paper and our methods of conducting this study. In Section 3, a literary analysis is presented. A summary of key takeaways are distinctly presented in Section 4. Section 5 describes the future possibility of AI in DeFi. Finally, in Section 6 concludes with some of the related work that potentially contributed in DeFi.

2. Materials and Methods

2.1. Technical Backgrounds

In this section, we briefly talk about three technical terms relevant to our research topic for the convenience of the readers. Table 1 can assist readers in understanding abbreviations used in this paper.

Table 1. List of Abbreviations used throughout the paper.

Term	Full Form
FinTech	Financial Technology
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DLT	Distributed Ledger Technology
AI	Artificial Intelligence

2.1.1. Blockchain

Blockchain is a method of storing data in such a way that it is difficult or impossible to change, hack, or deceive it. A blockchain is a digital log of transactions that is duplicated and distributed across the blockchain's complete network of computer systems [38]. Each block on the chain contains a number of transactions, and whenever a new transaction occurs on the blockchain, a record of that transaction is added to the ledger of each participant. Distributed Ledger Technology is a decentralized database that is administered by various people (DLT). Blockchain is a sort of distributed ledger technology in which transactions are recorded using a hash, which is an immutable cryptographic signature [39].

2.1.2. FinTech

The term “fintech” refers to new technology that aims to improve and automate the delivery and usage of financial services. Fintech, at its most basic level, is used to help organizations, company owners, and individuals better manage their financial operations, procedures, and lives through the use of specialized software and algorithms that run on computers and, increasingly, smartphones. The term “fintech” is a mix of “financial technology” and “financial innovation.” Fintech was coined in the twenty-first century to describe the technology used in the back-end systems of established financial organizations [40]. However, since then, there has been a shift toward more consumer-focused services and, as a result, a more consumer-focused definition. Fintech today spans a variety of sectors and industries, including education, retail banking, nonprofit fundraising, and investment management, to mention a few [41].

2.1.3. Decentralized Finance

Decentralized finance, in its most basic form, is a system in which financial items are made available on a public decentralized blockchain network, making them accessible to anybody rather than going through intermediaries such as banks or brokerages [7,42]. Unlike a bank or brokerage account, DeFi does not require a government-issued ID, Social

Security number, or proof of address. DeFi refers to a system in which buyers, sellers, lenders, and borrowers connect peer to peer or with a strictly software-based middleman rather than a firm or organization conducting a transaction using software developed on blockchains [43]. To achieve the goal of decentralization, a variety of technologies and protocols are employed. A decentralized system, for example, might be made up of open-source technologies, blockchain, and proprietary software. These financial products are made possible by smart contracts, which automate agreement terms between buyers and sellers or lenders and borrowers. DeFi solutions are designed to eliminate intermediaries between transacting parties, regardless of the technology or platform used.

2.2. Methodology

Compared to research on AI in blockchain and its various applications, AI in DeFi is still at its infant stage. Since the emergence of Bitcoin in 2009, many other cryptocurrencies have followed. However, cryptocurrency is one of the many applications of DeFi. To truly understand the current status of Defi-AI, we have used the global research publication search engine “Google Scholar” (scholar.google.com) to research published work on the field. Interestingly, not much work has been done related specifically to AI in DeFi. Our search keywords were combination of “Artificial Intelligence”, “Decentralized Finance”, “Machine Learning”, “AI”, and “DeFi”. About 103,000 results came in from which maximum publications were not related to the topic of this study but were more related to blockchain technology and AI. For this study, our scope of search was confined to Google Scholar since it is by far the first go-to place to look for research articles compared to Scopus or WoS according to Google Trends shown in Figure 1. However, WoS and Scopus can assist a systematic research search in terms of category and placement of the publication.

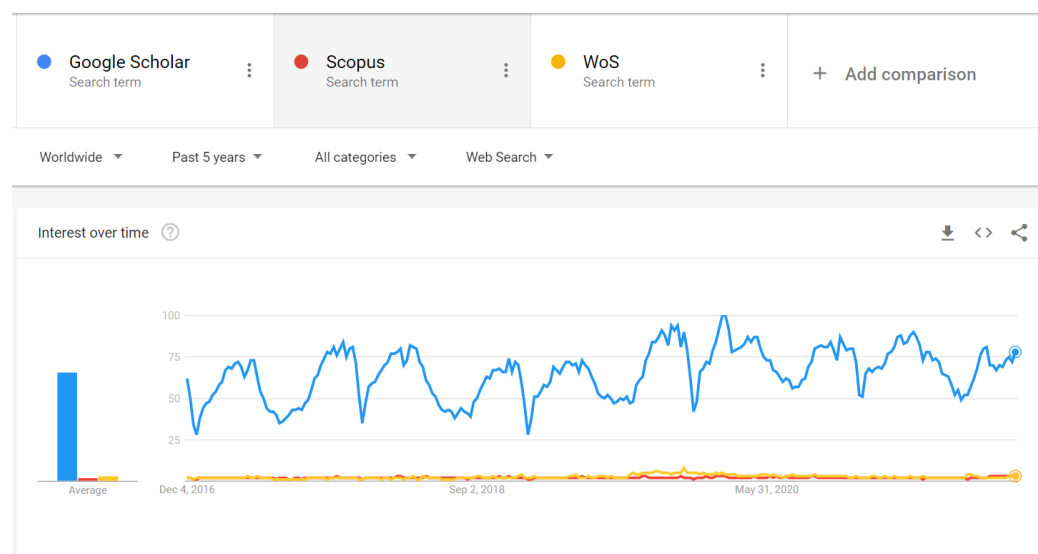


Figure 1. Google Trends comparison between Google Scholar, Scopus, and WoS.

To narrow our search, we surfed the first 50 pages of the results as they were arranged in order of relevance. Moreover, we maintained some ground rules. A publication is selected if it met the following criteria:

1. Title, abstract contains the term “AI” and “DeFi”.
2. Only English article.
3. Not book or book chapter
4. Published from the year 2011 till 2021.
5. Publicly available.
6. Published in conferences or journals.

The reason for selecting 2011 or later was due to the massive advancement of blockchain technology and artificial intelligence in terms of computation and security since that period [9]. Even though the implementation phase took time to come to light, much theoretical research was already being conducted. In this study, we aimed to look at the advancement of AI in DeFi over the last decade.

Each of the collected publications is thoroughly read to interpret the impact, reliability, and security of the use of AI in DeFi. These three categories are not scored; rather they are based on a summarized understanding of the paper to minimize the probability of interpretation bias. Figure 2 shows a workflow of what we have considered from a publication while grading them according to the aforementioned categories. Moreover, a relevance score is computed using citations, year of publication, and the ranking of the publication platform.

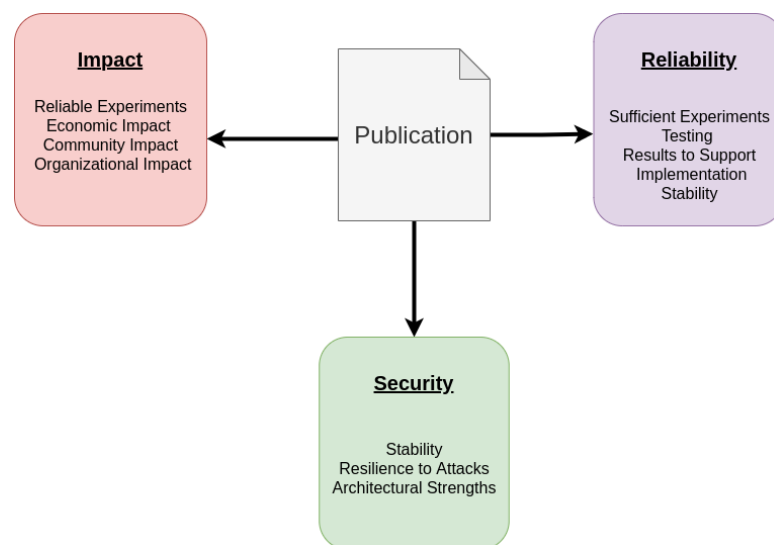


Figure 2. Mental map to grade impact, reliability, and security of a publication.

2.2.1. Grading *Impact*, *Reliability*, and *Security*

A publication proposal is graded to have *Impact* if the authors introduced well-structured and reproducible experiments, addressed the economic, community, organizational impact of their work which all parties can be benefited in some ways. These may be directly or indirectly addressed in their research. *Reliability* of a publication depends on many factors. However, we focus on the reproducibility of the experiments, hypothesis testing, result analyses to support the experiments and hypothesis, and implementation stability. *Security* is by far the most significant concern of any new research involving human participation. Therefore, we looked for the presence of resilience to adversaries and architectural strengths in publications. Adversaries may include machine learning model attacks and possible misuse of the system proposed by the authors. Architectural strengths include a well-rounded system design that can protect its users and has a backup strategy in case of system failure.

All of these three criteria are graded according to:

- Yes: All the points are met.
- Subject to experiment: Authors addressed the points partially, which can be overcome with more experiments.
- No: None of the points were addressed in the publication.

We are aware that some interpretation bias will be present due to variance in human interpretation. However, we have tried to maintain fairness with due diligence to the respected authors. The summaries are checked with two university professors and five undergraduate students from the computer science department (specifics were requested

to be anonymized). This grading system does not undermine the contribution of the publications to any extent; instead, it might be used to improve upon for a better future.

2.2.2. Scoring Relevancy of a Publication

We apply a generalized Equation (1) to measure the relevance of a published paper depending on the impact of the medium (conference or journal) of publication and the number of times it was cited. However, we do not want to undermine the fact that recent publications are more often likely to have fewer citations or none. Therefore, we consider the year of publication and length of time since then till the current year of this study, i.e., 2021 as the normalizing factor. However, we add β to avoid division by zero. In this study we consider $\beta = 1$.

$$relevance_{score} = \frac{impact + citation}{\beta + (2021 - publication_{year})} \quad (1)$$

The impact of conference papers is measured differently than that of the journal papers. Conference papers are ranked from A* to C (<http://portal.core.edu.au/conf-ranks/>, accessed on 12 March 2021). Journals on the other hand, have impact factors categorized from Q1 to Q4 (<https://www.scimagojr.com/journalrank.php?order=sjr&ord=asc>, accessed on 12 March 2021). To bring them together under our term (impact), we used the following marking scheme:

- Conference (A*) and Journal (Q1): ≥ 9.0
- Conference (A) and Journal (Q2): $\geq 8.0 < 9$
- Conference (B) and Journal (Q3): $\geq 6.0 < 8.0$
- Conference (C) and Journal (Q4): $\geq 4.0 < 6.0$
- Unranked: 0.0

The scale ranges from 0.0 to 9.0. A score close to 0 means less relevance. A score close to 9 represents high relevance as well as impact. For preprints or arXiv papers with citations greater than 0, we will only consider recent 2021 papers, and we shall assign 'NA' (Not Applicable) for impact. This formulation is our personal contribution which can be used as standardized evaluation for a publication. A* and Q1 publications are harder to achieve compared to B and Q3 publications. The difference in scoring therefore can be justified with this hypothesis. However, we have also cross verified that the number of B and Q3 publications per year far exceeds than the number of A* and Q1 publications. A and Q2 publications are somewhat considerably closer to A* and Q1 publications, therefore can be assigned with a score closer to latter.

We would also like to assert that the scoring system does not personally undermine any publisher of any degree. This is to be only used as an assistance to evaluating metric for the relevancy of a publication. We would also like to assert that the relevance score is computed considering the date of writing this paper. In future, the score is subjected to change with citations and year.

2.2.3. Validity of Our Methodology

There are few several ways to rank scientific literature. Citation counts [44–46] and graph-based ranking [47,48] are more popular ways to rank articles. There are also deep learning and reinforcement learning based ranking systems [49,50]. Dunaiski et al. (2016) tested several ranking algorithms and concluded that citation-based ranking are best next to PageRank ranking algorithms [51]. However, all these algorithms view articles as an interdependent network, i.e., the impact of one publication is dependent on the impact it has on the network of other publications. Sometimes, it is also seen that a hint of bias persists from the publisher [52]. A research published in Q3 journal might have more impact than a research published in Q1. More often we notice star research groups (Google Research, Microsoft Research, etc.) publish in ArXivs to avoid lengthy peer-review process that cuts down the importance of getting their research to the community.

In our study, we viewed each article as individual contributing entity. We have used two levels of analysis: content analysis of each articles, and using statistics. For the first part, we read the articles without discussing among ourselves. The grading is then made based on the agreement of our common grounds. We also reached out to university professors and undergraduate students (who requested to be anonymous) to validate our findings.

3. Literary Analysis

Publication Overview

In this section, we review and try to excavate some of the relevant research publications of Artificial Intelligence in Decentralized Finance. We summarize our literary analysis in Table 2.

Table 2. Literary Analysis of different research publication related to AI in DeFi. The table is organized according to the proceeding description.

Publications	Year	Impact	Reliability	Security	Relevance Score
[53]	2021	Subject to experiments	No	Subject to experiments	NA
[54]	2018	Yes	Subject to experiments	No	2.00
[28]	2018	Yes	Subject to experiments	Subject to experiments	18.00
[55]	2019	Yes	Subject to experiments	No	9.33
[56]	2019	Subject to experiments	Subject to experiments	Yes	4.33
[57]	2018	Subject to experiments	Subject to experiments	Subject to experiments	70.75
[58]	2020	Yes	Yes	Subject to experiments	2.50
[59]	2019	Yes	Yes	Subject to experiments	2.33
[60]	2017	Subject to experiments	Subject to experiments	No	28.80
[61]	2019	Yes	Subject to experiments	Yes	5.0
[62]	2018	Subject to experiments	Subject to experiments	Subject to experiments	5.75
[63]	2021	Yes	Subject to experiments	No	2.0
[64]	2020	Subject to experiments	Subject to experiments	Yes	1.0
[65]	2014	Yes	Subject to experiments	No	27.75
[66]	2019	Yes	Subject to experiments	Yes	4.00
[67]	2020	Yes	Yes	Yes	12.00
[68]	2018	Yes	Subject to experiments	Yes	41.00

Table 2. *Cont.*

Publications	Year	Impact	Reliability	Security	Relevance Score
[69]	2019	Yes	Subject to experiments	Subject to experiments	2.33
[70]	2020	Subject to experiments	Subject to experiments	No	2.50

Raheman et al. (2021) proposed a compact architecture that combines several machine learning predictive models with distinct tasks like portfolio planner, strategy evaluator, pool weighting, signal generator, and sentiment watcher to construct an automated agent for active portfolio management in decentralized finance [53]. Together they form an intelligent profile for an investor using CEX or DEX for trading. The authors tested their architecture on Binance CEX data with incremental training and prediction. However, their architecture oversimplifies the behavior of real market scenarios. The runtime of their architecture may pose a problem to few investors as enough time needs to be given for training on historical data. No specific time has been described in the paper. Sigova et al. (2018) identified usage of AI-driven prediction mechanisms (deep learning) coexisting with decentralized financial platforms to support consumers in making their calls. The article addressed two aspects of using blockchain in forecasting financial markets using “collective knowledge” and digitizing assets of market participants based on blockchain [54]. To observe market fluctuations, the authors studied Augur and Stox, a forecasting interface that leverages crowd forecasts. The machine learning algorithms used for forecasting in Augur are comparatively effective. The authors’ purpose was to concentrate on the rise of forecasting tools used in distributed ledger technology. Another work by [28] mentioned in Chapter 5 that deep learning algorithms are needed for the modern blockchain-based crypto secured data which is rendered trustable and interoperable through standardized formats and validation. The machine learning algorithms can be used for setting fees, and peer-to-peer nodes might provide deep learning services as they provide transaction hosting and confirmation, news hosting, and banking services. The author also asserts the convergence of AI and DeFi by stating that the mutual symbiosis is played by one another. An application by [55] proposed a deep learning stock prediction system using LSTM in a blockchain setting of stock data distributed among buyers and sellers, where a transaction between two peers is initiated by calling a smart contract. The predictive modeling is kept separate from the smart contract. However, it can only be activated through transactions via a smart contract. The outcome of the model is fed back to an agent that monitors the transaction and allows change before committing to the network. The authors experimented on an open-source data set and concluded with about 99% accuracy. The authors state this methodology of encapsulating the stock market in a blockchain technology assisted by machine learning predictive modeling is more secure than existing online centralized stock markets. Similar work has been done by [56] on Bitcoin, a widely used cryptocurrency, to evaluate how well machine learning techniques such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN) can predict prices and if abnormal risks can be adjusted using aforementioned strategies. Their study found that traders can earn returns on the risk-adjusted strategy. The techniques can identify short-term complex and non-linear patterns. Their experiments demonstrated that SVM performed better in return than ANN, thereby concluding investors can utilize SVM who are willing to achieve conservative returns. However, the authors do not address the downfalls of bitcoin and the drawbacks of possible attacks in machine learning techniques. Moreover, given their length of experiments, the risk factor is significant to decide whether the techniques can be reliable in the long term. McNally et al. (2018) used Bayesian recurrent neural network and long short term memory network to predict Bitcoin prices. The models are compared with ARIMA, a forecasting tool, and it was found that the models outperformed the tool

with a classification accuracy of 52%. The authors need to address security issues with their model with elaborated experiments and the scope of their work in the advancement of AI in DeFi [57]. Dietzmann et al. (2020) studied integration of AI with Distributed Ledger Technology (DLT) to assist the end-to-end lending process. They proposed a renovation of end-to-end lending design and assessed the impact of the framework in terms of 9 different criteria, which ranges from standardization, automatization, data frequency and sensitivity, process patterns, interaction, and others [58]. A comparative overview of the impact on the respective sub-processes has been elaborated to conduct principles for the design and development of future distributed-ledger-based AI applications. Their study is sufficient to prove the convergence of DLT and AI, but they conclude with an open-ended regarding the applicability of their proposal on autonomous services and organizations. Setiawan et al. (2019) proposed a tree-based classification method for predicting whether the quality of a loan is to be approved. They developed a Binary Particle Swarm Optimization with SVM with Extremely Randomized Tree (ERT) and Random Forest (RF) as the classifiers. The authors concluded that the algorithm outperformed random forest in terms of execution time, with the reduction of time needed being approximately 46% [59]. An intelligent portfolio management system for trading is proposed by [60], where they used a reinforcement learning agent trained with convolutional neural network (CNN) on stock price data with the promising outcome. Moreover, it can be re-trained on recent data to stay relevant. The drawback came from limited testing, and cannot practical usability cannot be determined with a small sample size and constrained scenario.

Cryptocurrency exchange platforms are the new 'currency exchange bank' of DeFi. Boonpeam et al. (2021) explored profits that can be earned from decentralized cryptocurrency exchange platforms (DEX) and propose the arbitrage system that can reveal the profits from trading token routes on different DEXs. Statistical arbitrage is a technique to find an opportunity for profitable trading. The automatic arbitrage system applies the procedures by adapting the state space-search algorithm [63]. It is capable of searching every possible route of the listed tokens and finding the maximum profit route. Lo et al. (2020) introduced an automated market maker that aims to bridge the gap between on-chain transactions and trust-based decentralized exchanges by applying ARDL and VAR on Uniswap V2 exchange containing 154 days of Ether-Tether trading data. The model is robust and reserves the ratio of Ether and USDT, which moves towards the model equilibrium at 99.9% statistical significance. The authors signify the requirement to emphasize the decentralization of blockchain and its applications in DEX. The paper is well established on aspects of security [64]. The need for AI systems for information translation in smart contracts and DEX has also been addressed by [65], which paved the way for digitized legislation. Numerous scams and misuses are present in smart contracts, which can be leveraged to loot millions of dollars worth of cryptocurrencies. SoliAudit (Solidity Audit) [66] is a machine learning and fuzz testing is driven vulnerability check for smart contracts to classify 13 types of vulnerabilities using Solidity machine code as learning features. Moreover, the authors constructed a gray-box fuzz testing mechanism for online transaction verification. The results showed that SoliAudit's accuracy can reach 90 percent and that fuzzing can help identify potential flaws such as reentrancy and arithmetic overflow. A similar work by [67] leveraged and customized Graph Neural Networks to detect vulnerabilities in Smart Contracts, which they refer to as contract graph. It consists of a degree-free graph convolutional neural network and temporal message propagation network to normalize and detect vulnerabilities through graph nodes. Infamous Ponzi scheme detection method is proposed by [68] using data mining from sampled Ponzi smart contract code and XGBoost for classification. The classification used account features and code features. The findings revealed that code features contributed more towards accurate classification with gas limit as the dominant feature. The authors also identified 400 possible Ponzi schemes on the Ethereum network and proposed to create a unified platform to detect further scams. Another framework called DOORchain [69] aims to combine Deep learning, Ontology, and Operation Research for detecting intrusions and maliciousness. DOORchain formalizes

and detects network maliciousness using operation research and detects behavioral maliciousness using ontology. The result is fed to deep learning for transaction classification in the blockchain.

In terms of algorithmic design, ref. [61] proposed a novel design to accommodate real-world events (oracles) in a decentralized, trustless, and transparent Ethereum blockchain which they term as Infochain. Infochain is an incentivized gamified approach towards peer consistency that can elicit valid information from peers (termed as agents) and discourage any misinformation being fed to the network. The interesting fact is the proposal of providing incentives to peers for being truthful. This process is done by an individual peer who updates “beliefs” about another peer for providing correct information. Tracking malicious accounts is equally important as tracking malicious transactions on a blockchain network. Several works question the anonymity of users in cryptocurrency. One such work by [62] addressed features (address statistical by features and address transaction history features), which is fed to a deep neural network Gated RNN after being transformed to vector representations and normalized. The authors construct a 3-layered fully connected called MainNet to achieve address-user mapping on Bitcoin users. The authors identified owners of addresses through address verification, recognition, and clustering, where the implementation relies directly on the distance between address feature vectors. The aim of the paper is to map individual owners of a certain address and excavate patterns of the users. Golubev et al. (2020) in their paper presented an overview of theoretical and empirical studies of the introduction of decentralized finance in the banking sector in Russia. Moreover, an analysis of official statistics of the Bank of Russia was carried out in their paper by which the authors concluded that there is an increase in the need for modernized banking solutions. Their work, despite portraying just one use case of blockchain-AI in bank, shows that the application of DeFi-AI is indeed possible [70]. However, it cannot be determined if the application of DeFi-AI has led to any security concerns.

While the black-box approach of AI is still a significant concern, none of the reference literature provides any validation regarding the interpretability of their model. However, a recent study conducted by Giudici and Raffinetti (2021) proposed explainable AI algorithms based on Shaply for cyber risk management. The suggested technique is based on Lorenz Zonoids, which are appropriate for ordinal measurement variables that may be used to account for cyber risk [71].

For each of the publications studied in this section, we have computed the relevance scores using Equation (1). The scores can be normalized between 0 to 1; however, we have decided not to change it for this study. The scores give us a brief idea about the relevance and importance of the paper in terms of where it was published and the number of times it was cited. Moreover, it also gives us a hint where the knowledge of AI-DeFi is mostly based. In the next section, we will summarize our findings from this literary analysis.

4. Discussions

This paper reviewed many recent significant studies on the progress of AI and DeFi. Two primary ways may be utilized to improve decentralized finance: two-factor authentication and AI-assisted digital advice and investing. While two-factor authentication is not new, it is gaining popularity in decentralized apps due to the fact that it enables users to maintain total control over their accounts without requiring an extensive technical understanding of cybersecurity best practices. Users just install software, such as Google Authenticator, that enables them to authenticate transactions by entering in the program’s generated numbers on their phone. By incorporating a second factor into the authentication process, users may easily and intuitively add a layer of physical security to their accounts. Another extension of this method is the development of decentralized apps that make use of what are known as zero-knowledge proofs. In many instances, two-factor authentication enables users to confidently validate transactions or authenticate information without actually viewing the underlying data. On the other side, the cryptocurrency industry is booming. Digital currencies, decentralized exchanges, automated investing

platforms, and decentralized loans are examples of blockchain's practical applications in decentralized finance.

The literature we reviewed in this study to grasp where the future is headed for AI in DeFi is limited. However, we can point out some critical information as noted below:

- Security concern remains the most persisting problem. This could be a major barrier to entry for DeFi itself, and with AI.
- Not enough subsistent experiments are being conducted to support applicability in financial institutions. Again, this could be a byproduct of security concerns which does not permit for such experiments.
- The relevance score does not necessarily imply the importance of the literature studied in this paper, but it can also give us a brief idea of where the knowledge of DeFi-AI is mostly based.
- Higher relevance score does not necessarily imply that the publication satisfies the criteria mentioned in Section 2.2.1. The relevance score is significant on the number of citations and the year of publication. The same is true for vice-versa.
- About 63% of the publications completely satisfied *Impact*, 16% satisfied *Reliability*, and 21% satisfied *Security*.
- Reliability and Security are mutually inclusive in the studied domain. Investing research on security will subsequently increase the reliability of the work.
- Compared to DeFi as a standalone entity, utilization of AI has proved to be more significant in driving integration and bridging the gap of reliability.

From the detailed analysis of the research we have elaborated in the preceding section, we can devise some research questions to understand the future research directions for AI in DeFi. These are:

1. Does AI's utilization in the DeFi add value to the original purpose?
2. Will the utilization of AI comply /compromise with security that is at stake?
3. What will be the trade-off between the robustness (impact and reliability) and the trustworthiness (security) of the system (AI in DeFi).

While most of the studied articles attempted to address one or more of these questions, we believe security will have much attention in this sector as financial matters are 'eyed' upon very seriously. Both intrinsic and extrinsic security research will likely go up in future work.

Our research has a few drawbacks as well:

1. Google Scholar returns around 1000 results in our initial search, making it impossible to study owing to time constraints. As a result, we've chosen the first 50 pages. The author's consensus determined the selection of 50 pages for surfing. If the surfing range is expanded, however, the analysis should be more thorough.
2. Only one data source was used during the article selection process: Google Scholar. Other databases, such as Scopus and the Web of Science, as well as Google Scholar for article searching, will be examined in the near future.

5. Concluding Remarks

This study presents a systematic literary analysis of various research publications related to Artificial Intelligence(AI) in Decentralized Finance (DeFi). We observe that the field is still at an infant stage but increasing nevertheless. We have designed some criteria to grade the literature in terms of impact, reliability, and security. To help minimize the bias, we formulated a generalized equation. The analysis shows that the concern of security has persisted compared to the impact and reliability of the proposals. Even though AI has been around for quite a long time, the convergence of AI and DeFi is under dark waters, given DeFi itself poses few uncertainties, as discussed in the introduction. Most of the research publications demonstrated how AI could assist one or more functions of DeFi. However, we believe AI can also bridge the gap of security concerns of DeFi. For instance, a distributed reinforcement learning agent can communicate with each other to govern transactions and

monitor peer-to-peer activities. A research problem does exist when we talk about DeFi and AI. The concept of decentralized finance is yet to be trusted by governments given its previous records of scams and thefts, and AI is yet to reach absolute interpretability for the general people. Such issues create barrier to entry for revolutionizing technologies. But these barriers are also being addressed in recent research [72–74]. However, despite the fact that the requirement of explainable AI is at the top of the list, relatively few articles in DeFi fields considered its significance. One such explanation is the difficulty in merging the DeFi with interpretable machine learning. It will be fascinating to observe how the future researcher overcome the AI model's pre and post hoc constraints when applying it in DeFi.

In the future, we shall extend our research to propose a deep reinforcement learning framework for DeFi to strengthen the design security of DEX, and make the integration of DeFi more agile to organizations.

6. Related Work

Surveys are vital to research as they contribute to various insights into a research topic. Our study on the use of AI in DeFi is a systematic analysis on a trending topic that holds future uncertainties as of yet. There has been previous collective research on DeFi. The benefits of DeFi and its limitations are studied by Chen et al. [9]. A similar work is presented by Zetzsche et al. [7], where they demonstrated several perspectives of how DeFi differed from traditional financial systems. They have gathered resources to architect the security concerns that DeFi poses to institutions and people and summarizes how DeFi can be regulated. A systematization of knowledge is presented by Werner et al. [75] where they detailed DeFi protocols according to operation types and the security in technical and economic perspectives. Lockl et al. [76] conducted a behavioral study where they accumulated several propositions of prior studies in the context of DeFi to understand the distrust that people have in banks. They also proposed the existence of a trust paradox in distributed ledger technology (DLT) and found no evidence to support that this distrust had led to the adoption of DeFi.

On the other hand, several research [8,24,26,31] have shown that AI can be useful to blockchain applications. On the opposite, Salah et al. [77] review different literatures of blockchain applications of AI and how blockchain can benefit AI systems. Research on AI in DeFi, however, is apparently rare to find. In this study, we analyze existing research on AI in DeFi in a systematic way that can provide insights to where DeFi is headed.

Author Contributions: Conceptualization, N.S. and A.R.; methodology, N.S. and A.R.; software, N.S.; validation, M.M.A., K.D.G. and Z.S.; formal analysis, M.M.A. and Z.S.; investigation, K.D.G.; resources, N.S. and A.R.; data curation, N.S.; writing—original draft preparation, N.S. and A.R.; writing—review and editing, K.D.G., M.M.A. and Z.S.; visualization, K.D.G. and Z.S.; supervision, K.D.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Centobelli, P.; Cerchione, R.; Esposito, E.; Raffa, M. The revolution of crowdfunding in social knowledge economy: Literature review and identification of business models. *Adv. Sci. Lett.* **2016**, *22*, 1666–1669. [\[CrossRef\]](#)
2. Sharma, V.; Goyal, M.; Malik, D. An intelligent behaviour shown by chatbot system. *Int. J. New Technol. Res.* **2017**, *3*, 263312.
3. Centobelli, P.; Cerchione, R.; Esposito, E.; Oropallo, E. Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. *Technol. Forecast. Soc. Chang.* **2021**, *165*, 120463. [\[CrossRef\]](#)
4. Bahga, A.; Madiseti, V.K. Blockchain platform for industrial internet of things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [\[CrossRef\]](#)
5. Wu, K. An empirical study of blockchain-based decentralized applications. *arXiv* **2019**, arXiv:1902.04969.

6. Wickström, J.; Westerlund, M.; Pulkkis, G. Smart contract based distributed IoT security: A protocol for autonomous device management. In Proceedings of the 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid), Melbourne, Australia, 10–13 May 2021; pp. 776–781.
7. Zetzsche, D.A.; Arner, D.W.; Buckley, R.P. Decentralized finance. *J. Financ. Regul.* **2020**, *6*, 172–203. [CrossRef]
8. Lee, M.R.; Yen, D.C.; Hurlburt, G.F. Financial technologies and applications. *IT Prof.* **2018**, *20*, 27–33. [CrossRef]
9. Chen, Y.; Bellavitis, C. Blockchain disruption and decentralized finance: The rise of decentralized business models. *J. Bus. Ventur. Insights* **2020**, *13*, e00151. [CrossRef]
10. CoinDesk. Defi Lender bZx Loses 8M in Third Attack this Year. 2020. Available online: <https://www.coindesk.com/defilender-bzx-third-attack> (accessed on 12 July 2021).
11. Cointelegraph. Akropolis DeFi Protocol ‘Paused’ as Hackers Get Away with 2M in DAI. 2020. Available online: <https://cointelegraph.com/news/akropolis-defi-protocol-paused-ashackers-get-away-with-2m-in-dai> (accessed on 12 July 2021).
12. CoinDesk. Cover Protocol Attack Perpetrated by ‘White Hat,’ Funds Returned, Hacker Claims. 2020. Available online: <https://www.coindesk.com/cover-protocol-attackperpetrated-by-white-hat-all-funds-returned-hacker-claims> (accessed on 12 July 2021).
13. Lin, L.X.; Budish, E.; Cong, L.W.; He, Z.; Bergquist, J.H.; Panesir, M.S.; Kelly, J.; Lauer, M.; Prinster, R.; Zhang, S.; et al. Deconstructing decentralized exchanges. *Stanf. J. Blockchain Law Policy* **2019**, *2*, 1.
14. Schär, F. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB St. Louis Rev.* **2021**, *103*, 153–174. [CrossRef]
15. Smith, S.S. Blockchain-Based Decentralized Exchanges Are Growing, But There Still Are Significant Risks. 2020. Available online: <https://www.forbes.com/sites/seansteinsmith/2021/02/24/blockchain-based-decentralized-exchanges-are-growing-but-there-still-are-significant-risks/> (accessed on 12 July 2021).
16. Abramova, S.; Voskobojnikov, A.; Beznosov, K.; Böhme, R. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2021; pp. 1–19.
17. Bonneau, J. Hostile blockchain takeovers (short paper). In Proceedings of the International Conference on Financial Cryptography and Data Security, Nieuwpoort, Curacao, 26 February–2 March 2018; pp. 92–100.
18. Heilman, E.; Narula, N.; Tanzer, G.; Lovejoy, J.; Colavita, M.; Virza, M.; Dryja, T. Cryptanalysis of curl-p and other attacks on the IOTA cryptocurrency. *IACR Trans. Symmetric Cryptol.* **2020**, *2020*, 367–391. [CrossRef]
19. Qin, K.; Zhou, L.; Livshits, B.; Gervais, A. Attacking the defi ecosystem with flash loans for fun and profit. In Proceedings of the International Conference on Financial Cryptography and Data Security, Virtual Event, 1–5 March 2021; pp. 3–32.
20. Gandal, N.; Hamrick, J.; Moore, T.; Vasek, M. The rise and fall of cryptocurrency coins and tokens. *Decis. Econ. Financ.* **2021**, *44*, 981–1014. [CrossRef]
21. Zhou, L.; Qin, K.; Torres, C.F.; Le, D.V.; Gervais, A. High-frequency trading on decentralized on-chain exchanges. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 428–445.
22. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; et al. On scaling decentralized blockchains. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; pp. 106–125.
23. Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Syta, E.; Ford, B. Omniledger: A secure, scale-out, decentralized ledger via sharding. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–23 May 2018; pp. 583–598.
24. Tanwar, S.; Bhatia, Q.; Patel, P.; Kumari, A.; Singh, P.K.; Hong, W.C. Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. *IEEE Access* **2019**, *8*, 474–488. [CrossRef]
25. Giudici, P.; Polinesi, G. Crypto price discovery through correlation networks. *Ann. Oper. Res.* **2021**, *299*, 443–457. [CrossRef]
26. Harris, J.D.; Waggoner, B. Decentralized and collaborative AI on blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 368–375.
27. Rabah, K. Convergence of AI, IoT, big data and blockchain: A review. *Lake Inst. J.* **2018**, *1*, 1–18.
28. Swan, M. Blockchain for business: Next-generation enterprise artificial intelligence systems. *Adv. Comput.* **2018**, *111*, 121–162. [CrossRef]
29. Atlam, H.F.; Walters, R.J.; Wills, G.B. Intelligence of things: Opportunities & challenges. In Proceedings of the 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2–4 July 2018; pp. 1–6.
30. Rathore, S.; Kwon, B.W.; Park, J.H. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.* **2019**, *143*, 167–177. [CrossRef]
31. Chen, X.; Ji, J.; Luo, C.; Liao, W.; Li, P. When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2018; pp. 1178–1187.
32. Wadesango, N.; Charity, M.; Blessing, M.; Haufiku, H. The effects of corporate governance on financial performance of commercial banks in a turbulent economic environment. *Acta Univ. Danubius. CEconomica* **2020**, *16*, 164–191.
33. Ganann, R.; Ciliska, D.; Thomas, H. Expediting systematic reviews: Methods and implications of rapid reviews. *Implement. Sci.* **2010**, *5*, 1–10. [CrossRef]

34. Kuhrmann, M.; Fernández, D.M.; Daneva, M. On the pragmatic design of literature studies in software engineering: An experience-based guideline. *Empir. Softw. Eng.* **2017**, *22*, 2852–2891. [CrossRef]
35. Sutherland, W.J.; Goulson, D.; Potts, S.G.; Dicks, L.V. Quantifying the impact and relevance of scientific research. *PLoS ONE* **2011**, *6*, e27537. [CrossRef] [PubMed]
36. University, P. Ways to Measure Research. 2021. Available online: <https://www.cs.purdue.edu/homes/dec/essay.research.measure.html> (accessed on 12 July 2021).
37. Connect, E.L. Quick Reference Cards for Research Impact Metrics Regarding Potential Opportunity for Graduate Student. 2020. Available online: https://libguides.cam.ac.uk/ld.php?content_id=31682519 (accessed on 12 July 2021).
38. Pilkington, M. Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016.
39. Kuznetsov, A.; Shekhanin, K.; Kolhatin, A.; Kovalchuk, D.; Babenko, V.; Perevozova, I. Performance of hash algorithms on GPUs for use in blockchain. In Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 18–20 December 2019; pp. 166–170.
40. Kagan, J. Financial technology–fintech. *Datum Pristup. Dok.* **2020**, *13*, 2020.
41. Gomber, P.; Kauffman, R.J.; Parker, C.; Weber, B.W. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *J. Manag. Inf. Syst.* **2018**, *35*, 220–265. [CrossRef]
42. Abdulhakeem, S.A.; Hu, Q. Powered by Blockchain technology, DeFi (Decentralized Finance) strives to increase financial inclusion of the unbanked by reshaping the world financial system. *Mod. Econ.* **2021**, *12*, 1. [CrossRef]
43. Michalikova, K.F.; Poliakova, A. Decentralized finance. In Proceedings of the 21st International Scientific Conference Globalization and its Socio-Economic Consequences 2021, SHS Web of Conferences, Zilina, Slovakia, 13–14 October 2021; EDP Sciences: Les Ulis, France, 2020; Volume 129, p. 03008.
44. Garfield, E. Citation analysis as a tool in journal evaluation. *Science* **1972**, *178*, 471–479. [CrossRef] [PubMed]
45. Nerur, S.; Sikora, R.; Mangalaraj, G.; Balijepally, V. Assessing the relative influence of journals in a citation network. *Commun. ACM* **2005**, *48*, 71–74. [CrossRef]
46. Hirsch, J.E. An index to quantify an individual’s scientific research output. *Proc. Natl. Acad. Sci. USA* **2005**, *102*, 16569–16572. [CrossRef]
47. Ding, Y.; Yan, E.; Frazho, A.; Caverlee, J. PageRank for ranking authors in co-citation networks. *J. Am. Soc. Inf. Sci. Technol.* **2009**, *60*, 2229–2243. [CrossRef]
48. Wang, Y.; Tong, Y.; Zeng, M. Ranking scientific articles by exploiting citations, authors, journals, and time information. In Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence, Bellevue, WA, USA, 14–18 July 2013.
49. Kanellos, I.; Vergoulis, T.; Sacharidis, D.; Dalamagas, T.; Vassiliou, Y. Ranking papers by their short-term scientific impact. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021; pp. 1997–2002.
50. Wang, S.; Xie, S.; Zhang, X.; Li, Z.; Yu, P.S.; Shu, X. Future influence ranking of scientific literature. In Proceedings of the 2014 SIAM International Conference on Data Mining, Philadelphia, PA, USA, 24–26 April 2014; pp. 749–757.
51. Dunaiski, M.; Visser, W.; Geldenhuys, J. Evaluating paper and author ranking algorithms using impact and contribution awards. *J. Inf.* **2016**, *10*, 392–407. [CrossRef]
52. Callaham, M.; Wears, R.L.; Weber, E. Journal prestige, publication bias, and other characteristics associated with citation of published studies in peer-reviewed journals. *JAMA* **2002**, *287*, 2847–2850. [CrossRef] [PubMed]
53. Raheman, A.; Kolonin, A.; Goertzel, B.; Hegykozi, G.; Ansari, I. Architecture of Automated Crypto-Finance Agent. *arXiv* **2021**, arXiv:2107.07769.
54. Sigova, M.V.; Klioutchnikov, I.K.; Zatevakhina, A.V.; Klioutchnikov, O.I. Approaches to evaluating the function of prediction of decentralized applications. In Proceedings of the 2018 International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI), Nicosia, Cyprus, 31 October–2 November 2018; pp. 1–6.
55. Bansal, G.; Hasiija, V.; Chamola, V.; Kumar, N.; Guizani, M. Smart stock exchange market: A secure predictive decentralized model. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
56. de Souza, M.J.S.; Almudhaf, F.W.; Henrique, B.M.; Negredo, A.B.S.; Ramos, D.G.F.; Sobreiro, V.A.; Kimura, H. Can artificial intelligence enhance the Bitcoin bonanza. *J. Financ. Data Sci.* **2019**, *5*, 83–98. [CrossRef]
57. McNally, S.; Roche, J.; Caton, S. Predicting the price of bitcoin using machine learning. In Proceedings of the 2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Cambridge, UK, 21–23 March 2018; pp. 339–343.
58. Dietzmann, C.; Heines, R.; Alt, R. The convergence of distributed ledger technology and artificial intelligence: An end-to-end reference lending process for financial services. In Proceedings of the Twenty-Eighth European Conference on Information Systems (ECIS2020), Marrakech, Morocco, 15–17 June 2020; Association for Information Systems: Atlanta, GA, USA, 2020.
59. Setiawan, N.; Suhajito, S.; Diana. A comparison of prediction methods for credit default on peer to peer lending using machine learning. *Procedia Comput. Sci.* **2019**, *157*, 38–45. [CrossRef]
60. Jiang, Z.; Liang, J. Cryptocurrency portfolio management with deep reinforcement learning. In Proceedings of the 2017 Intelligent Systems Conference (IntelliSys), London, UK, 7–8 September 2017; pp. 905–913.

61. Goel, N.; van Schreven, C.; Filos-Ratsikas, A.; Faltings, B. Infochain: A Decentralized, Trustless and Transparent Oracle on Blockchain. *arXiv* **2020**, arXiv:1908.10258.
62. Shao, W.; Li, H.; Chen, M.; Jia, C.; Liu, C.; Wang, Z. Identifying bitcoin users using deep neural network. In Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing, Guangzhou, China, 15–17 November 2018; pp. 178–192.
63. Boonpeam, N.; Werapun, W.; Karode, T. The Arbitrage System on Decentralized Exchanges. In Proceedings of the 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 19–22 May 2021; pp. 768–771.
64. Lo, Y.C.; Medda, F. Uniswap and the Rise of the Decentralized Exchange. SSRN 3715398. 2020. Available online: <https://mpira.ub.uni-muenchen.de/103925/> (accessed on 12 July 2021).
65. Omohundro, S. Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters* **2014**, *1*, 19–21. [[CrossRef](#)]
66. Liao, J.W.; Tsai, T.T.; He, C.K.; Tien, C.W. Soliaudit: Smart contract vulnerability assessment based on machine learning and fuzz testing. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 458–465.
67. Zhuang, Y.; Liu, Z.; Qian, P.; Liu, Q.; Wang, X.; He, Q. Smart Contract Vulnerability Detection Using Graph Neural Network. In Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20), Yokohama, Japan, 11–17 July 2020; pp. 3283–3290.
68. Chen, W.; Zheng, Z.; Cui, J.; Ngai, E.; Zheng, P.; Zhou, Y. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In Proceedings of the 2018 World Wide Web Conference, Lyon, France, 23–27 April 2018; pp. 1409–1418.
69. El-Dosuky, M.A.; Eladl, G.H. DOORchain: Deep ontology-based operation research to detect malicious smart contracts. In Proceedings of the World Conference on Information Systems and Technologies, Galicia, Spain, 16–19 April 2019; pp. 538–545.
70. Golubev, A.; Ryabov, O.; Zolotarev, A. Digital transformation of the banking system of Russia with the introduction of blockchain and artificial intelligence technologies. In Proceedings of the IOP Conference Series: Materials Science and Engineering, St. Petersburg, Russian Federation, 21–22 November 2019; IOP Publishing: Bristol, UK, 2020; Volume 940, p. 012041.
71. Giudici, P.; Raffinetti, E. Explainable AI methods in cyber risk management. *Qual. Reliab. Eng. Int.* **2021**, *1–9*. [[CrossRef](#)]
72. Hamon, R.; Junklewitz, H.; Sanchez, I. *Robustness and Explainability of Artificial Intelligence*; Publications Office of the European Union: Luxembourg, 2020.
73. Gade, K.; Geyik, S.C.; Kenthapadi, K.; Mithal, V.; Taly, A. Explainable AI in industry. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Anchorage, AK, USA, 4–8 August 2019; pp. 3203–3204.
74. Goebel, R.; Chander, A.; Holzinger, K.; Lecue, F.; Akata, Z.; Stumpf, S.; Kieseberg, P.; Holzinger, A. Explainable ai: The new 42? In Proceedings of the International Cross-Domain Conference for Machine Learning and Knowledge Extraction, Hamburg, Germany, 27–30 August 2018; pp. 295–303.
75. Werner, S.M.; Perez, D.; Gudgeon, L.; Klages-Mundt, A.; Harz, D.; Knottenbelt, W.J. Sok: Decentralized finance (defi). *arXiv* **2021**, arXiv:2101.08778.
76. Lockl, J.; Stoetzer, J.C. Trust-free Banking Missed the Point: The Effect of Distrust in Banks on the Adoption of Decentralized Finance. In Proceedings of the 29th European Conference on Information Systems (ECIS), Marrakech, Morocco, 15–17 June 2021.
77. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. *IEEE Access* **2019**, *7*, 10127–10149. [[CrossRef](#)]