doi:10.20944/preprints202110.0136.v1

Article

Promise of AI in DeFi, a Literary Analysis

Nafiz Sadman [1], Abdur Rahman [2] and Kishor Datta Gupta [3,*]

[1] Silicon Orchard Ltd, Bangladesh; nafiz@siliconorchard.com
[2] Silicon Orchard Ltd, Bangladesh; a.rahman@siliconorchard.com
[3] University of Memphis, Memphis, TN USA; kgupta1@memphis.edu
[*] 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. 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 make the integration of DeFi more agile in the near future.

Keywords: Decentralized finance ; Artificial Intelligence ; Security ; Reliability

check for updates

Citation: Sadman, N.; Rahman, A.; Gupta, K.D. . *Preprints* , , .

Received:
Accepted:
Published:

1. Introduction

Decentralized Finance (DeFi) is inspired by FinTech[1] and the practical applicability of blockchain technology. Blockchain technology offers a decentralized, transparent platform for finance with no intermediaries for exchanges [1]. Lee et al., in their journal [2] 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. 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 [3]. 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 [4–6] 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. dived into uncharted waters of DeFi where they proposed it requires regulation as any other financial body [1]. The authors pointed three perspectives from which DeFi faces legal obstacles: "Legal jurisdiction and applicable law, enforcement, and data protection and privacy". 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) [7] for instance, where cryptocurrencies or crypto assets [8] can be exchanged. Unsurprisingly, DEX is not protected from security concerns such as replication of the platform to fool users [9]. Risk and hostility of crypto-assets [10], POW (proof-of-work) and POS(proof-of-stake) [11] fall under the same radar. Some scholars [12–14] have studied possible attacks on DeFi, while some scholars [15–17] have studied secure trading on DEX.

[1] FinTech: Financial Technology; Any technology that delivers financial services through software.

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 [18] 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. 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 [19] 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 [20,21], while others [22,23] 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. [24] 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. One such technology is "RegTech" [2], a regulatory technology driven by AI, that can prevent such attacks.

In this study, we perform a literary analysis on some of the recent research on the use of artificial intelligence in decentralized finance in terms of impact, reliability, and security. 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 [25–27] 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 trend analysis as to where DeFi could be heading with AI.

The organization of this research is as follows. In section II, we briefly define some technical backgrounds related to the paper. Few relevant works that we have identified during our study are presented in section III. In section IV, we present our methods of conducting this study. In section V, a literary analysis is presented. A summary of key takeaways are distinctly presented in section VI We conclude our study in section VII with a future possibility of AI 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. 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.

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. 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.

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. 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. 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.

Materials and Methods should be described with sufficient details to allow others to replicate and build on published results. Please note that publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.

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"[2] 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.

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. Published from the year 2011 till 2021.
2. Publicly available.
3. 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 [3]. 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 1 shows a rough mental picture of what we have considered from a publication while grading them according to the aforementioned categories.

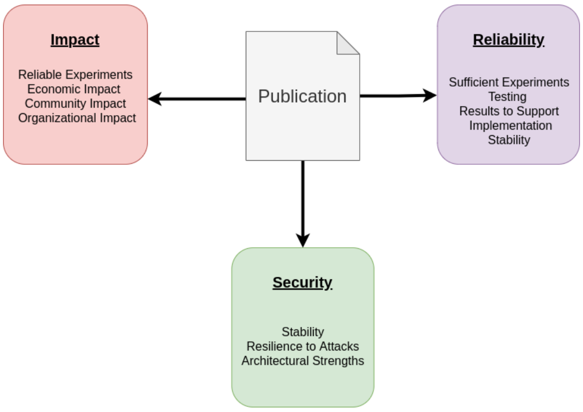

Figure 1. Mental map to grade impact, reliability, and security of a publication.

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

[2] scholar.google.com

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 $\beta = 1$.

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

The impact of conference papers is measured differently than that of the journal papers. Conference papers are ranked from A* to C[3]. Journals on the other hand, have impact factors categorized from Q1 to Q4[4]. 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): 8.0
- Conference (B) and Journal (Q3): 6.0
- Conference (C) and Journal (Q4): 4.0
- 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, we will only consider recent 2021 papers, and we shall assign 0 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.

[3] http://portal.core.edu.au/conf-ranks/

[4] https://www.scimagojr.com/journalrank.php?order=sjr&ord=asc

3. Literary Analysis

3.1. 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
Raheman et al.[28]	2021	Subject to experiments	No	Subject to experiments	0.00
Sigova et al.[29]	2018	Yes	Subject to experiments	No	2.00
Swan et al.[21]	2018	Yes	Subject to experiments	Subject to experiments	18.00
Bansal et al.[30]	2019	Yes	Subject to experiments	No	9.33
Souza et al.[31]	2019	Subject to experiments	Subject to experiments	Yes	4.33
McNally et al.[32]	2018	Subject to experiments	Subject to experiments	Subject to experiments	70.75
Dietzmann et al.[33]	2020	Yes	Yes	Subject to experiments	2.50
Setiwan et al.[34]	2019	Yes	Yes	Subject to experiments	2.33
Jiang et al. [35]	2017	Subject to experiments	Subject to experiments	No	28.80
Goel et al.[36]	2019	Yes	Subject to experiments	Yes	5.0
Shao et al.[37]	2018	Subject to experiments	Subject to experiments	Subject to experiments	5.75
Boonpeam et al.[38]	2021	Yes	Subject to experiments	No	2.0
Lo et al.[39]	2020	Subject to experiments	Subject to experiments	Yes	1.0
Steve Omohundro [40]	2014	Yes	Subject to experiments	No	27.75
Liao et al. [41]	2019	Yes	Subject to experiments	Yes	4.00
Zhuang et al. [42]	2020	Yes	Yes	Yes	12.00
Chen et al. [43]	2018	Yes	Subject to experiments	Yes	41.00
El-Dosuky et al. [44]	2019	Yes	Subject to experiments	Subject to experiments	2.33
Golubev et al.[45]	2020	Subject to experiments	Subject to experiments	No	2.50

The paper [28] 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. 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. The paper [29] 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. 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 [21] 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 [30] 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 Souza et al. [31] 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. The authors in the paper [32] 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.

Dietzmann et al. [33] 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. 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. Setiwan et al. [34] 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%. An intelligent portfolio management system for trading is proposed by Jiang et al. [35], 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. The authors [38] explore 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. It is capable of searching every possible route of the listed tokens and finding the maximum profit route. The authors [39] introduced an automated market marker 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. The need for AI systems for information translation in smart contracts and DEX has also been addressed by the authors in the paper [40], 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) [41] 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 the authors [42] 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 in this paper [43] 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 Etherium network and proposed to create a unified platform to detect further scams. Another framework called DOORchain [44] 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, the authors [36] propose 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 [37] 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. [45] 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. However, it cannot be determined if the application of DeFi-AI has led to any security concerns.

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.

3.2. Key Takeaways

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.

4. 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 area 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.

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.

5. 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. [3]. A similar work is presented by Zetzsche et al. [1], 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. [46] where they detailed DeFi protocols according to operation types and the security in technical and economic perspectives. Lockl et al. [47] 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 [2,18,19,24] have shown that AI can be useful to blockchain applications. On the opposite, Salah et al. [48] 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.

References

1. Zetzsche, D.A.; Arner, D.W.; Buckley, R.P. Decentralized finance. *Journal of Financial Regulation* **2020**, *6*, 172–203.
2. Lee, M.R.; Yen, D.C.; Hurlburt, G.F. Financial technologies and applications. *IT Professional* **2018**, *20*, 27–33.
3. Chen, Y.; Bellavitis, C. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights* **2020**, *13*, e00151.
4. CoinDesk. Defi lender bzx loses 8m in third attack this year. Available at https://www.coindesk.com/defilender-bzx-third-attack (2020), 2020.
5. Cointelegraph. Akropolis defi protocol 'paused' as hackers get away with 2m in dai. Available at https://cointelegraph.com/news/akropolis-defi-protocol-paused-ashackers-get-away-with-2m-in-dai (2020), 2020.
6. CoinDesk. Cover protocol attack perpetrated by 'white hat,' funds returned, hacker claims. Available at https://www.coindesk.com/cover-protocol-attackperpetrated-by-white-hat-all-funds-returned-hacker-claims (2020), 2020.
7. Lin, L.X.; Budish, E.; Cong, L.W.; He, Z.; Bergquist, J.H.; Panesir, M.S.; Kelly, J.; Lauer, M.; Prinster, R.; Zhang, S.; others. Deconstructing decentralized exchanges. *Stanford Journal of Blockchain Law & Policy* **2019**, *2*.
8. Schär, F. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review* **2021**.
9. Smith, S.S. Blockchain-Based Decentralized Exchanges Are Growing, But There Still Are Significant Risks. Available at https://www.forbes.com/sites/seansteinsmith/2021/02/24/blockchain-based-decentralized-exchanges-are-growing-but-there-still-are-significant-risks/ (2021), 2020.
10. Abramova, S.; Voskobojnikov, A.; Beznosov, K.; Böhme, R. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, pp. 1–19.
11. Bonneau, J. Hostile blockchain takeovers (short paper). International Conference on Financial Cryptography and Data Security. Springer, 2018, pp. 92–100.
12. 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 Transactions on Symmetric Cryptology* **2020**, pp. 367–391.
13. Qin, K.; Zhou, L.; Livshits, B.; Gervais, A. Attacking the DeFi ecosystem with flash loans for fun and profit. *arXiv preprint arXiv:2003.03810* **2020**.
14. Gandal, N.; Hamrick, J.; Moore, T.; Vasek, M. The rise and fall of cryptocurrency coins and tokens. *Decisions in Economics and Finance* **2021**, pp. 1–34.

15. Zhou, L.; Qin, K.; Torres, C.F.; Le, D.V.; Gervais, A. High-frequency trading on decentralized on-chain exchanges. *arXiv preprint arXiv:2009.14021* **2020**.
16. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; others. On scaling decentralized blockchains. International conference on financial cryptography and data security. Springer, 2016, pp. 106–125.
17. Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Syta, E.; Ford, B. Omniledger: A secure, scale-out, decentralized ledger via sharding. 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 583–598.
18. 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.
19. Harris, J.D.; Waggoner, B. Decentralized and collaborative AI on blockchain. 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 368–375.
20. Rabah, K. Convergence of AI, IoT, big data and blockchain: a review. *The lake institute Journal* **2018**, *1*, 1–18.
21. Swan, M. Blockchain for business: Next-generation enterprise artificial intelligence systems. In *Advances in computers*; Elsevier, 2018; Vol. 111, pp. 121–162.
22. Atlam, H.F.; Walters, R.J.; Wills, G.B. Intelligence of things: opportunities & challenges. 2018 3rd Cloudification of the Internet of Things (CIoT). IEEE, 2018, pp. 1–6.
23. Rathore, S.; Kwon, B.W.; Park, J.H. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications* **2019**, *143*, 167–177.
24. Chen, X.; Ji, J.; Luo, C.; Liao, W.; Li, P. When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. 2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018, pp. 1178–1187.
25. Sutherland, W.J.; Goulson, D.; Potts, S.G.; Dicks, L.V. Quantifying the impact and relevance of scientific research. *PloS one* **2011**, *6*, e27537.
26. University, P. Ways To Measure Research. Available at https://www.cs.purdue.edu/homes/dec/essay.research.measure.html (2021), 2021.
27. Connect, E.L. Quick Reference Cards for Research Impact Metrics Regarding potential opportunity for graduate student. Available at https://libguides.cam.ac.uk/ld.php?content_id=31682519 (2021), 2020.
28. Raheman, A.; Kolonin, A.; Goertzel, B.; Hegykozi, G.; Ansari, I. Architecture of Automated Crypto-Finance Agent. *arXiv preprint arXiv:2107.07769* **2021**.
29. Sigova, M.V.; Klioutchnikov, I.K.; Zatevakhina, A.V.; Klioutchnikov, O.I. Approaches to evaluating the function of prediction of decentralized applications. 2018 International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI). IEEE, 2018, pp. 1–6.
30. Bansal, G.; Hasija, V.; Chamola, V.; Kumar, N.; Guizani, M. Smart stock exchange market: a secure predictive decentralized model. 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019, pp. 1–6.
31. 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. *The Journal of Finance and Data Science* **2019**, *5*, 83–98.
32. McNally, S.; Roche, J.; Caton, S. Predicting the price of bitcoin using machine learning. 2018 26th euromicro international conference on parallel, distributed and network-based processing (PDP). IEEE, 2018, pp. 339–343.
33. 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. Proceedings: Twenty-Eighth European Conference on Information Systems (ECIS2020). Association for Information Systems, 2020.
34. Setiawan, N.; others. A comparison of prediction methods for credit default on peer to peer lending using machine learning. *Procedia Computer Science* **2019**, *157*, 38–45.
35. Jiang, Z.; Liang, J. Cryptocurrency portfolio management with deep reinforcement learning. 2017 Intelligent Systems Conference (IntelliSys). IEEE, 2017, pp. 905–913.
36. Goel, N.; van Schreven, C.; Filos-Ratsikas, A.; Faltings, B. Infochain: A decentralized, trustless and transparent oracle on blockchain. *arXiv preprint arXiv:1908.10258* **2019**.
37. Shao, W.; Li, H.; Chen, M.; Jia, C.; Liu, C.; Wang, Z. Identifying bitcoin users using deep neural network. International Conference on Algorithms and Architectures for Parallel Processing. Springer, 2018, pp. 178–192.

doi:10.20944/preprints202110.0136.v1

38. Boonpeam, N.; Werapun, W.; Karode, T. The Arbitrage System on Decentralized Exchanges. 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). IEEE, 2021, pp. 768–771.
39. Lo, Y.C.; Medda, F. Uniswap and the rise of the decentralized exchange. *Available at SSRN 3715398* **2020**.
40. Omohundro, S. Cryptocurrencies, smart contracts, and artificial intelligence. *AI matters* **2014**, *1*, 19–21.
41. Liao, J.W.; Tsai, T.T.; He, C.K.; Tien, C.W. Soliaudit: Smart contract vulnerability assessment based on machine learning and fuzz testing. 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE, 2019, pp. 458–465.
42. Zhuang, Y.; Liu, Z.; Qian, P.; Liu, Q.; Wang, X.; He, Q. Smart Contract Vulnerability Detection using Graph Neural Network. IJCAI, 2020, pp. 3283–3290.
43. Chen, W.; Zheng, Z.; Cui, J.; Ngai, E.; Zheng, P.; Zhou, Y. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. Proceedings of the 2018 world wide web conference, 2018, pp. 1409–1418.
44. El-Dosuky, M.A.; Eladl, G.H. DOORchain: deep ontology-based operation research to detect malicious smart contracts. World Conference on Information Systems and Technologies. Springer, 2019, pp. 538–545.
45. Golubev, A.; Ryabov, O.; Zolotarev, A. Digital transformation of the banking system of Russia with the introduction of blockchain and artificial intelligence technologies. IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2020, Vol. 940, p. 012041.
46. Werner, S.M.; Perez, D.; Gudgeon, L.; Klages-Mundt, A.; Harz, D.; Knottenbelt, W.J. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778* **2021**.
47. Lockl, J.; Stoetzer, J.C. Trust-free Banking Missed the Point: The Effect of Distrust in Banks on the Adoption of Decentralized Finance. *arXiv* **2021**.
48. 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.