Risk Management (2023) 25:13
https://doi.org/10.1057/s41283-023-00118-0

ORIGINAL ARTICLE

Risk analysis in decentralized finance (DeFi): a fuzzy-AHP approach

Sandeepa Kaur[1] · Simarjeet Singh[2] · Sanjay Gupta[3] · Sangeeta Wats[4]

Accepted: 30 March 2023 / Published online: 10 April 2023

Abstract

Decentralized finance is disrupting the financial ecosystem through innovative, transparent, and interoperable financial solutions. Based on distributed ledger technology, decentralized finance is a nascent and rapidly evolving area. Decentralized finance protocols are witnessing a perfect storm (in terms of growth). However, this emerging area needs sober consideration as these financial technologies possess unique risks for users, makers, regulators, and other stakeholders. The current research aims to identify and prioritize risks in decentralized finance. The present study conducted an extensive survey of the literature to identify various risks involved in decentralized finance. For empirical analysis, the study collected data from 90 experts. A fuzzy analytical hierarchical process (F-AHP) was applied to prioritize various risks in decentralized finance. Pairwise comparison and weights of all the criteria and sub-criteria revealed that technical risks are the most significant ones, followed by legal, regulatory, and financial risks. Among the sub-risks, financial risks are at the highest level, followed by smart contract risks and transaction risks. The outcomes of this research have several implications for regulators, policymakers, entrepreneurs, technologists, and practitioners. These stakeholders can focus on these vulnerabilities and offer more sustained solutions in the future.

Keywords Decentralized finance (DeFi) · Fuzzy analytical hierarchy process (F-AHP) · Smart contract · Oracle risks · Rug pulls

Introduction

Modern-day financial systems are managed and operated by centralized systems and governing bodies (Vereckey 2021). Consumers must deal with a stack of financial intermediaries to access these financial systems. From stock and bond trading to mortgages and auto loans, consumers have to pay a percentage of every financial

✉ Sanjay Gupta
researchsaccm@gmail.com

Extended author information available on the last page of the article

transaction to these intermediaries (Mörke 2022). In addition to this, legacy financial institutions lack transparency, interoperability, and efficiency. Decentralized finance (DeFi) aims to overcome these challenges by empowering the general public through distributed ledger technologies (Harvey et al. 2021). Through open-access blockchain-based protocols and smart contracts, DeFi intends to provide an alternative financial system that will be more accessible, cost-effective, interoperable, and transparent than legacy financial systems (Buterin 2013). Decentralized financial protocols have already disrupted the traditional financial world as total value locked (TVL) in these protocols has grown over $121.74 billion[1] by the mid of September 2021 as compared to $21.87 billion by the year ending 2020 (Huilgolkar 2020). Based on open-access protocols and decentralized applications (Dapps), DeFi infrastructure requires the negligible role of clearing house, custodians, or escrow services as all these roles, by and large, are taken up by Smart Contracts. Smart contracts, coined initially as executable codes, run on a blockchain to facilitate, execute, and enforce an agreement between untrustworthy parties without the involvement of a trusted third party (Szabo 1994; Buterin 2013).

Nevertheless, the exponential growth in DeFi has also brought some novel operational, technical, and regulatory challenges (Sood et al. 2023). DeFi vulnerabilities like smart contract risks, oracle risks, and miner risks have caused investors a loss over $153 million in 2020 and perpetrated a whopping $610 million worth of Ethereum in one single hack in August 2021. The dependence of DeFi on nascent blockchain technology has made these open-access protocols a soft target for hackers. In addition to this, massive speculative investments in DeFi protocols carry contagion risks (Gudgeon et al. 2020; Liu et al. 2020).

DeFi protocols have also raised serious concerns for regulators. Due to the fact that most DeFi protocols are unregulated, DeFi has become a magnet for money laundering and fraud (Vereckey 2021). Being unregulated, DeFi protocols also lack consumer safeguards; According to a report by Elliptic research, consumers lost $10 billion in 2021 due to DeFi scams. In addition to this, the collection of taxes is also a major concern in DeFi protocols. Since most of the protocols are built on pseudonymous and permissionless ledgers, traceability of DeFi transactions is a difficult task. According to one estimate by Barclays, internal revenue services may miss a revenue of $50 billion due to the pseudonymous nature of DeFi protocols. Further, developers of most DeFi protocols often lack the required financial expertise and knowledge (Montaz 2022). In short, all these hurdles are a significant challenge in the mainstream adoption of DeFi protocols.

Based on the above discussion, it is requisite to identify various risks and subrisks that hinder the growth of DeFi protocols. Several researchers have made attempts to ascertain DeFi risks (Aramonte et al. 2021; Carter and Jeng 2021; Werner et al. 2021). However, the majority of these research studies are conceptual and stress on one or two categories of risks. The current research fills this gap by conducting a comprehensive and empirical study on DeFi risks. In short, the present research tries to answer the following research questions.

[1] Total value locked (TVL) in DeFi as on 19.09.2021 source https://dappradar.com/defi.

RQ1: what are the risks decentralized finance (DeFi) may pose?

To achieve this goal, the authors conducted a structured multivocal literature review (MLR). MLR helped us in getting both academic and industrial insights on DeFi risks. Further, with the help of the consistency ratio, the study ensured content validity.

RQ2: how to assign priorities to these risk criteria and sub-criteria in line with significance in driving the decentralized, programmable, and composable structure of DeFi?

The present research applied fuzzy analytical hierarchy process (F-AHP) techniques to examine the relative significance of all the risk criteria and the sub-criteria. Priorities were assigned based on a pairwise comparison analysis of all the selected risk criteria and the sub-criteria.

In light of this, the current study contributes to nascent literature in numerous manners. Firstly, the study is one of the pioneer studies in the digital finance literature that utilized a unique blend of multivocal literature review and fuzzy analytical hierarchy process. Second, by revealing the relative importance of various DeFi risks and sub-risks, the study offers unique insights for investors, entrepreneurs, developers, researchers, consumers, regulators, and policymakers. Finally, the study offers the first empirical evidence of DeFi risks.

Review of literature

This section is divided into two major parts. First, the study used the MLR technique and employed "Preferred Reporting Items for Systematic Reviews and Meta-Analyses" (PRISMA) criteria to identify, screen, and select the academic and industrial literature on DeFi risks. In the next part, the study thoroughly examined the literature and classified the research studies into various risk categories.

Article selection

The study relied on the MLR technique to identify literature on DeFi risks. The rationale behind this particular review was twofold: (a) this technique offers novel insights both from academia and industry (Singh et al. 2021), (b) MLR is preferred when academic literature on a particular topic is very limited (Sood et al. 2023). MLR considers both white literature (peer-reviewed articles and conference proceedings) and grey literature (white papers, technical papers, government reports, and policy recommendations). The authors conducted the entire article selection process in three sequential phases: literature identification, screening, and selection.

The literature identification phase began with the identification of relevant keywords. The authors run several pilot searches before deciding on the final keywords (Yadav and Desai 2016; Singh et al. 2021). After finding the appropriate keywords

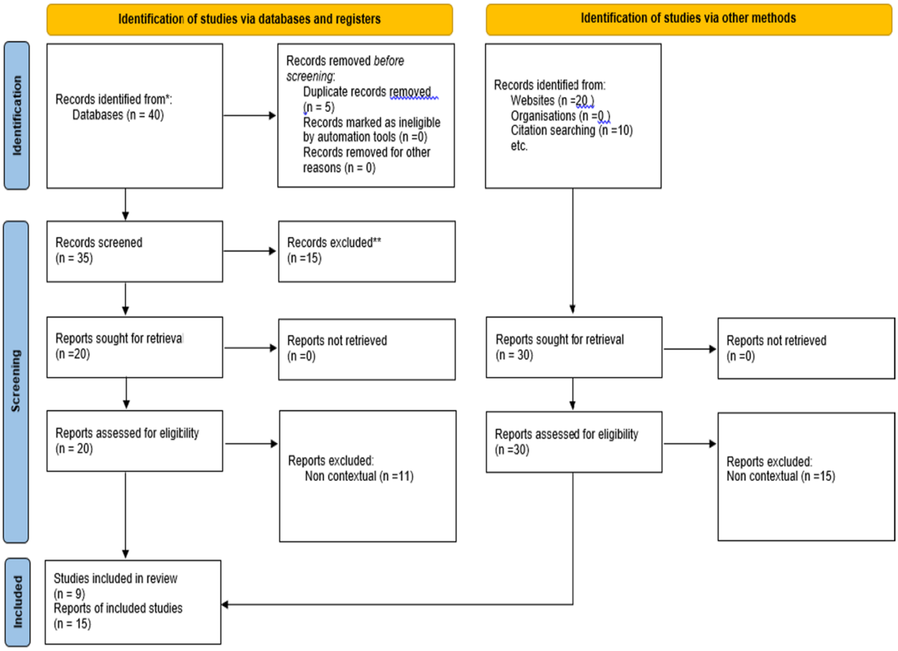
Identification of studies via databases and registers
Identification of studies via other methods
Identification
Records identified from*:
Databases (n = 40)
Records removed before screening:
Duplicate records removed (n = 5)
Records marked as ineligible by automation tools (n =0)
Records removed for other reasons (n = 0)
Records identified from:
Websites (n =20)
Organisations (n =0)
Citation searching (n =10)
etc.
Screening
Records screened (n = 35)
Records excluded** (n =15)
Reports sought for retrieval (n =20)
Reports not retrieved (n =0)
Reports sought for retrieval (n = 30)
Reports not retrieved (n =0)
Reports assessed for eligibility (n = 20)
Reports excluded: Non contextual (n =11)
Reports assessed for eligibility (n =30)
Reports excluded: Non contextual (n =15)
Included
Studies included in review (n = 9)
Reports of included studies (n = 15)

Fig. 1 Article selection process

such as “DeFi risks”, “smart contracts vulnerabilities”, “DeFi scams”, “cyber security”, “threat intelligence”, and “DeFi attacks”, the authors run search queries on bibliometric databases such as the EBSCOhost, Scopus, and Web of Science. For grey literature search, the study used the Google search engine. In a preliminary search, the study identified 40 academic studies and 30 industrial records. Due to quality concerns, the study considered only Tier-1 grey literature. In the next phase, the authors screened these studies on the basis on their titles and abstracts. This title and abstract screening resulted in the elimination of 15 academic and 12 industrial records. Finally, we did a deep screening (full content readings) and selected total 24 studies (9 research papers and the rest industrial literature). The whole process is depicted in Fig. 1.

Factor selection scheme

The articles and review papers were read, and the factors were figured out. A list of the critical risks was made, which was addressed in different research works and found to have a significant impact on the DeFi architecture. The white paper of the World Economic Forum on Decentralized Finance Policy Maker Toolkit (forwarded by Deshmukh et al. 2021) listed the important risks along with the papers which found them to be significant. This gives us the path to do further research in this field.

Operational risks

The analysis of international research studies offered a strong impact of various operational risks impacting DeFi. Under the head of Operational Risks, Finality Risks, Loss of Private Keys, Upgradation Risks, Governance Risks, and Composability Risks are catered. The finality of the transaction is when all network nodes receive the transaction and agree on its validity. It also captures that a transaction made is stored on the blockchain and cannot be modified or reversed (Meegan and Koens 2021; Miller et al. 2016). However, finality enhances security and immutability, but it comes at the cost of greater settlement and liquidity risks. In traditional financing, these risks are insured by the government, but that assurance is not possible in DeFi (Meegan 2020; Muzzy 2020; Smith and Crown 2019; Buterin 2016).

Another risk is efficiently and securely managing keys for cryptographic systems, which is named as the risk of loss of private keys (key management). The overall security of these cryptosystems in DeFi depends on how anyone can keep their private keys secure. Suppose an intruder by any mechanism, namely bruit force, physical access of the system, side-channel attack, or weak encryption, discovers the keys. In that case, they can steal everything or erase all money from the targeted system or account. Moreover, since it is a decentralized system, thus there is no way to recover stolen currency from anywhere (Ramos et al. 2021; Zetzsche et al. 2020; Casino et al. 2019).

Upgradation risk is the next to fall in this category. Many times, attacks or controversial situations (community conflict) may lead to the forking of a cryptocurrency (Ramos et al. 2021). Forking is the split of the blockchain into two separate branches following a change in the rules of the system. There are multiple reasons, sometimes as a response to a major hack (DAO Case) or sometimes due to disagreements among the user and developer communities (increasing the block size in case of Bitcoin cash) (Islam et al. 2019).

Protocols that implement some decentralized governance mechanisms tend to rely upon governance tokens, which empower token holders to propose and vote on protocol upgrades (Werner et al. 2021; Zetzsche et al. 2020). Protocol upgrades come through proposals in the form of executable code, on which governance token holders vote. For a protocol to be executed, a minimum number of votes is required, commonly referred to as a quorum. An attacker may obtain a number of governance tokens sufficient to propose and execute malicious contract code and steal a contract's funds (Gudgeon et al. 2020; Werner et al. 2021). However, composability is a system design principle that enables applications to be created from component parts (Zetzsche et al. 2020). Composability is often referred to as money legos in the DeFi ecosystem, as its code can be selected and assembled in multiple combinations (MakerDAO Blog 2020; Nystrom 2019). Composability in DeFi exposes the ecosystem to 'financial contagion'. Financial contagion in DeFi can be best described as the potential damage that could be done to all protocols relying on an underlying protocol. Thus, composability exposes DeFi to a potential risk that can undo all of the innovation in DeFi as fast as it has accelerated it (Meegan and Koens 2021; Gudgeon et al. 2020; Meegan 2020).

Technical risks

Ethereum is the largest public blockchain and has significantly avoided breaches, but the blockchain-based wallets or centralized exchanges and DApps have been targeted for technical risks and hacks. Under this head, we encounter four major types of risks: smart contract risks, miner risks, transaction attacks, and Oracle risks. Smart contracts are executable codes that run on blockchain to execute, enforce, and facilitate an agreement between untrustworthy parties without involving any trusted third party (Khan et al. 2021; Klages-Mundt et al. 2020; Li et al. 2020; Buterin 2013). Various early research focussed on security incidents with smart contracts, smart contract vulnerabilities, and surveyed older incidents, such as the DAO and Parity multi-sig attacks (Atzei et al. 2021; Praitheeshan et al. 2020; Chen et al. 2020; López Vivar et al. 2020; Wang et al. 2019) provided that smart contract risks deal with code that does not execute as intended. More specifically, some other authors have surveyed specific vulnerabilities such as integer overflows (Lai and Luo 2020; Gao et al. 2019), reentrancy (Qian et al. 2020), solidity weaknesses (SWC Registry Online; Dingman et al. 2019), the Decentralized Application Security Project (Dasp Co. Online), and high-level smart contract languages and their security characteristics (Harz and Knottenbelt 2018). However, Perez and Livshits (2020) regarded vulnerabilities against their real-world impact and found that of 23,327 vulnerable contracts, only 1.98% had been exploited.

Another risk in this category is miner risk which deals with the possibility that transaction processing entities behave maliciously towards certain transactions. In blockchain systems, users typically send a transaction to the network along with a fee to the miner that successfully processes it into a block. Miners take proposed transactions and decide the order in which to execute them (Consensys, The q1 2020). However, a miner can choose to execute a lower-fee transaction ahead of a higher-fee transaction if that transaction is particularly valuable to them or in return for a side payment from the originator of the lower-fee transaction (Obadia 2020). On black Thursday, 2020, when global markets crashed, signalling the beginning of the COVID-19 recession, attackers manipulated Ethereum's mempool of transactions waiting to be mined and confirmed.[2]

Transaction risks are limitations or failures of the underlying blockchain network. If the base-layer settlement network is successfully attacked, allows for double-spending, becomes too expensive for transactions, or lacks the necessary throughput, those failures will affect the application layer. The long-planned upgrade to Eth2 (Ethereum version 2.0), which aims for significant performance improvements, thus represents an important development for DeFi.[3] This upgrade will also shift Ethereum to proof-of-stake consensus, which does not require the intensive energy usage of proof-of-work mining.

One class of vulnerabilities deserving special attention relates to failures resulting from oracles. In DeFi, oracles are service providers that provide outside information to a smart contract. The most common usage of oracles is to transmit market prices drawn from one or many exchanges to a DeFi protocol that relies on outside pricing

[2] https://www.blocknative.com/blog/mempool-forensics.

[3] Ethereum 2.0 (Eth2) vision | ethereum.org.

information (Caldarelli 2021; Peaster 2020). As Liu et al. (2020) note, oracles introduce risk in a number of ways: their mechanics are opaque and unaccountable; they introduce critical nexuses of trust and dependency into DeFi, and malicious oracles can cause catastrophic harm. As pointed out by Werner et al. (2021), market dislocations at spot exchanges feed into oracles and affect DeFi systems built atop these price feeds.

Financial risks

The DeFi service segment also inherits the Financial Risks, i.e. the depletion of funds which is caused by the transactional behaviour of users concerning the digital assets in the DeFi services. These vulnerabilities are majorly classified into three categories, viz., Liquidity Risk, Market Risk, and Credit Risk. The 'liquidity risk' is the possibility of insufficiency of funds to realize the value of a financial asset. DeFi services often incentivize market makers to liquidate under-collateralized loans, performing a function analogous to a foreclosure auction for real estate. If the liquidation incentive structures fail, however, original counterparties and liquidity providers hold unanticipated default risk. On centralized exchanges, in the event of flash crashes, the trading was taken offline until the market settled. Such last-resort remedies may not be available for decentralized services.[4]

Another feather in the financial risk category is 'Market Risk' is the possibility that asset value will decline over a period of time due to investors' idiosyncratic behaviours, new information, or market conditions. DeFi's ease in fund transferring and its novel yet complex instruments pave the way for the increased possibility of abuses by DeFi protocol creators, operators of exchanges, or third-party manipulators (Werner et al. 2021; white paper of World Economic Forum forwarded by Deshmukh et al. 2021). These attacks would generally trigger liquidations by manipulating an asset's price in the context of stablecoins (Klages-Mundt and Minca 2019). There is also a lack of standardized price discovery mechanisms found in digital currency markets, which in turn is a driver of overall volatility and valuation swings in DeFi.

The last risk in this category is 'Credit risk' or 'Counterparty risk' is the probability of counterparties default on their obligations to a financial instrument. Credit risk is a very particular problem in DeFi, where the volatility of underlying digital assets produces under-collateralization, the ease of credit creation leads to excessive leverage, or the algorithmic determination of interest produces inaccuracies. The lack of fixed identities in a pseudonymous network presents additional challenges in terms of determining creditworthiness (Werner et al. 2021; World Economic Forum White Paper forwarded by Deshmukh et al. 2021; Meegan 2020).

Legal & regulatory risks

Use of DeFi to engage in illicit activity or to evade regulatory obligations falls into the category of 'Legal & Regulatory Risks'. Money laundering, for example,

[4] https://www.coindesk.com/tech/2020/02/19/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack/.

is a problem for established centralized cryptocurrency exchanges as well as DeFi DEXs. This category has sub-classifications as Regulatory arbitrage, Fraud through Rug Pulls, Disclosure Risks, and Financial Crimes. Regulatory risk is the risk that any DeFi protocol can be affected by the government, with either laws being made that affect how a DeFi protocol operates or laws being made effectively shutting down DeFi protocols (Meegan 2020). It means failing to meet regulatory obligations by carrying out similar functions in a different technical manner. In general, the greatest amount of regulatory attention so far has focussed on traditional concerns of investor and customer protection, particularly in the case of cryptocurrencies and ICOs, not on DeFi (Zetzsche et al. 2020). Regulatory arbitrage could amplify all risks mentioned so far in this paper if, 1 day, a regulatory crackdown was to happen.

The Frauds through Rug Pulls involve deliberate misappropriation, hacks, attacks, scams, and other efforts to take advantage of investors. This involves all such activities enabled and carried out by DeFi developers themselves rather than third-party attacks. For example, “rug pulls” or exit scams involve convincing users to place funds into a seemingly legitimate DeFi service, from which they are drained by the developers, who then disappear (Cylynx 2021; Xia et al. 2021; L and AU 2021).

Another risk encountered is Disclosure risks which arise as in DeFi systems, there is no involvement of regulatory authorities in any jurisdiction. This puts investors in the DeFi segment at the risk of non-disclosure of the entities involved in the transactions (Meegan 2020). The financial crime involves a breach of anti-money laundering/countering the financing of terrorism (AML/CFT) restrictions, financial sanctions, and similar legal regimes. The use of virtual currencies in cybercrime and in money laundering typologies is well documented. DeFi transactions involving natively digital assets may be difficult to regulate through traditional AML/CFT controls because transactions are resistant to blockage, users are pseudonymous by default, many transactions involve non-custodial wallets not directly tied to individuals, and assets are resistant to seizure (Werner et al. 2021; World Economic Forum White Paper forwarded by Deshmukh et al. 2021; Meegan 2020). Although DeFi transactions are generally transparent and traceable, new privacy-enhancing protocols and/or tools may create additional regulatory challenges. Terrorist actors who have used Bitcoin may see its pseudonymity as useful. After all, posting a Bitcoin address to a social media account or public channel on a messaging platform is likely advantageous to posting bank account details online (Keatinge et al. 2018).

Nascent risks

Nascent risks are budding risks that have started displaying signs of potential vulnerabilities in stuff related to Decentralized Financing. This category includes ‘financial illiteracy risks’, black swans & dynamic interactions. DeFi strives to be more accessible to the global community and is open for anyone to build products. And thus, DeFi transforms traditional financial products into products operating without an intermediary via smart contracts on the Ethereum blockchain (Meegan 2020). A serious risk arises from the fact that these platforms are generally developed by programmers belonging to non-financial backgrounds who have no financial knowledge about the financial implications of the product they are creating and have users investing in the product without considering the risks. This is against traditional finance, where products were created by certified financial engineers and traded by specialized institutions. Currently, there is no certification in the DeFi environment to prove someone knows exactly what they are programming or investing into. Various risks mentioned in this study might be mitigated if any certification or course was required for participation in DeFi (Cylynx 2021). However, this offset DeFi's goal to be accessible to everyone no matter their education. However, as we have already seen, sometimes all decentralized ideals are not fully complied by DeFi platforms, so perhaps in the future, we will also see some barriers to entering DeFi, defying the DeFi's accessibility ideal, for the future adoption of DeFi (Xia et al. 2021; L and AU 2021; Zetzsche et al. 2020).

Another risk in this category is named 'black swans' or flash crashes or price cascades, which may occur in extremely volatile or rough market conditions and are exacerbated by leverage in the DeFi system. When Ethereum has seen isolated smart contract attacks in the past, over the 'DeFi summer' of 2020 adversaries 'flash crashed' compositions of DeFi protocols and cashed out lavishly (Werner et al. 2021; Meegan and Koens 2021; Oosthoek 2021; Meegan 2020). Unlike traditional markets, where manual intervention was possible in case of concurrent defaults and manipulations, the algorithmic permissionless nature of DeFi does not allow to stop cascading crashes. In the situation of the flash crash, the markets tend to be high on volatility, and there may be so many liquidations and precipitous drops in the price of the collateral that liquidators or others will face significant losses, and black swans will gain (Oosthoek 2021; Meegan 2020; Harvest Online 2021).

The last type of risk is classified as 'dynamic interactions', among a potentially endless number of interconnected DeFi components that may produce risks that are not present in any individual service. Since, DeFi operates in a global environment, unless regulators can effectively limit cross-border DeFi activity, firebreaks to the contagion of systemic defaults may be more limited than for traditional finance. As DeFi services begin to interoperate with traditional financial platforms, the interaction risks will also grow (Shen 2021).

The criterion and sub-criteria of DeFi were selected through the literature review and shown in the two levels of hierarchy in F-AHP (Fig. 2).

Research methodology

Criteria and sub-criteria selection and model development

For criteria (risks) and sub-criteria (sub-risks) selection, the authors conducted an extensive survey of the literature. Initially, the study identified 22 sub-risks grouped into six main categories. Afterwards, for validation, we consult with six academic experts. These academic experts consist of academicians from finance and computer science backgrounds having at least 8–10 years' research experience in distributed ledger technologies, open finance, and financial technologies. The authors first introduce them

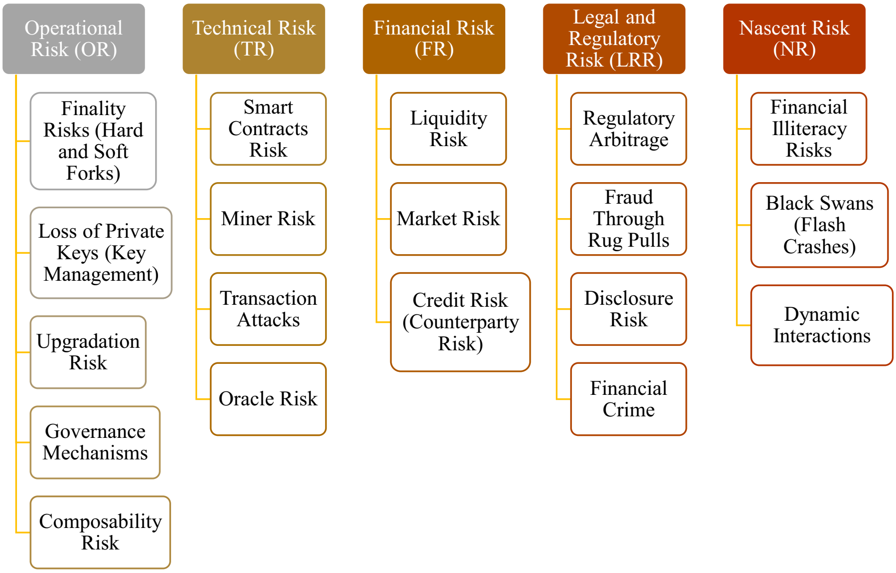

Fig. 2 Multicriteria model of DeFi (Decentralized Finance)

objectives of the research. Afterwards, they provided their responses based on the Fuzzy linguistic scale (shown in Table 2). Further, following the suggestions of Saaty (1980), the study also computed consistency ratios to avert any divergence in the pairwise comparison matrix. Pilot testing confirmed the reliability of the results as the consistency ratio was below the cut-off point (0.10). Eventually, the study finalized five main criteria and 19 sub-criteria. Figure 3 depicts the entire research approach used in this study in the form of a flowchart.

Data collection and sample design

The present research relied on the pairwise comparison-based survey to prioritize the DeFi risks. To construct a pairwise comparison matrix, the study used a nine-point fuzzy linguistic scale (as shown in 'Table 2 and Appendix'). For data collection, the current study relied on experts who have in-depth knowledge of blockchain and DeFi technologies and who are involved in various DeFi projects. The data collection process proved problematic as there exists a narrow pool of specialists who have profound knowledge of Defi and practical exposure to implementing DeFi projects. Following the recommendations of Singh et al. (2021), the study used a couple of screening questions to confirm the expertise of the respondent. These questions include a broader overview of the fundamentals of DeFi, such as DeFi spectrum and protocols and relevant technical, policy and regulatory areas of focus. For sampling purposes, the present paper employed non-probabilistic sampling techniques. The authors initially approached 130 respondents consisting of academicians, consultants, policymakers, entrepreneurs, technologists, and regulatory experts involved in DeFi projects. Out of these 130 respondents, 24 failed to clear the screening criteria. Thereafter, the authors

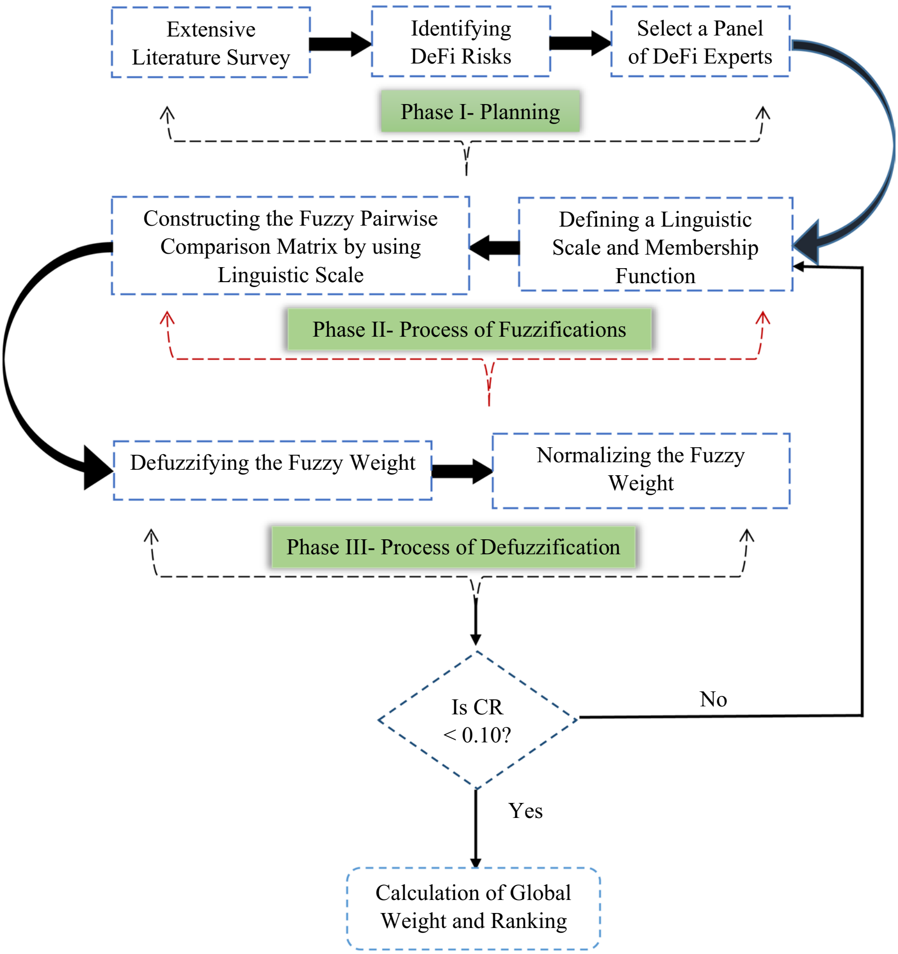
Extensive Literature Survey
Identifying DeFi Risks
Select a Panel of DeFi Experts
Phase I- Planning
Constructing the Fuzzy Pairwise Comparison Matrix by using Linguistic Scale
Defining a Linguistic Scale and Membership Function
Phase II- Process of Fuzzifications
Defuzzifying the Fuzzy Weight
Normalizing the Fuzzy Weight
Phase III- Process of Defuzzification
Is CR < 0.10?
No
Yes
Calculation of Global Weight and Ranking

Fig. 3 Methodology flowchart

contacted the remaining 106 respondents, and 16 respondents did not fill the complete nine-point fuzzy linguistic scale. Eventually, the data were collected from 90 respondents. The sample size is appropriate as the study relied on the expert-based MCDM method (Fu et al. 2006). Table 1 represents the demographic details of the experts.

Fuzzy analytical hierarchy process (fuzzy-AHP)

In 1980, Saaty gave the concept of the analytical hierarchy process (AHP) that assists in evaluating the importance of criteria and sub-criteria. According to Badhotiya et al. (2021), AHP can be applied to calculate the global weights for ranking the main criteria and sub-criteria. According to Deng (1999), AHP

Table 1 Demographic profile of experts

Demographic classification	Category	Number of experts
Business/Industry	Academicians	25
	DeFi entrepreneurs	20
	Financial and Legal practitioners	12
	Technologist	25
	Regulatory experts	08
Continent	Asia	20
	Europe	35
	North America	25
	Australia	10
Years of experience	0–5 year	15
	5–10 year	32
	10–15 year	20
	15–20 year	13

does not take into account the degree of uncertainty in the expert or decision-maker’s opinion. Zadeh (1996) has given the concept of fuzzy-AHP to deal with vagueness or uncertainty in the decision makers’ opinion. Fuzzy-AHP has been a widely used technique to solve problems deals in multiple criteria evaluations.

In Eq. 1, $\tilde{A}$ represents the triangular fuzzy numbers (TFNs) i.e. (l,m,u), where ‘l’ represents lower value, ‘m’ represents middile value, and ‘u’ respresents upper value.

$$\boldsymbol{\mu}_{\tilde{A}(\boldsymbol{x})} = \begin{cases} 1, & x = m \\ \frac{(x-l)}{(m-l)}, & \text{If } l \le x \le m \\ \frac{(u-x)}{(u-m)}, & \text{If } m \le x \le u \\ 0, & \text{Other Cases} \end{cases} \tag{1}$$

$\widetilde{A}$ represents the fuzzy set i.e. = $\{(x, \boldsymbol{\mu}_{\widetilde{A}(\boldsymbol{x})}) | x \in X\}$, so that $\boldsymbol{\mu}_{\widetilde{A}}$: $P \rightarrow [0,1]$. Zadeh (1965) has given the concept of arithmetic operations which has been applied on two triangular fuzzy numbers i.e. TFNs (Fig. 4) is given below:

Addition of two TFNs

$$\widehat{A_1} \oplus \widehat{A_2} = \left(l_1, m_1, u_1\right) \oplus \left(l_2, m_2, u_2\right) = \left(l_1 + l_2, m_1 + m_2, u_1 + u_2\right).$$

Subtraction of two TFNs

$$\widehat{A}_1 \ominus \widehat{A}_2 = \left(l_1, m_1, u_1\right) \ominus (l_2, m_2, u_2) = (l_1 - l_2, m_1 - m_2, u_1 - u_2).$$

Multiplication of two TFNs

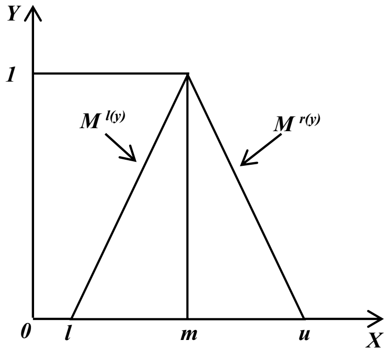

Fig. 4 Triangular fuzzy membership function

$$\widehat{A_1} \otimes \widehat{A_2} = \left(l_1, m_1, u_1\right) \otimes \left(l_2, m_2, u_2\right) = \left(l_1 \times l_2, m_1 \times m_2, u_1 \times u_2\right).$$

Division of two TFNs

$$\widehat{A_1} \emptyset \widehat{A_2} = \left(l_1, m_1, u_1\right) \emptyset \left(l_2, m_2, u_2\right) = \left(l_1/u_2, m_1/m_2, u_1/l_2\right).$$

Inverse of TFNs

$$\widetilde{A}_1^{-1} = \left(l_1, m_1, u_1\right)^{-1} = \left(\frac{1}{u_1}, \frac{1}{m_1}, \frac{1}{l_1}\right).$$

The following steps have been applied to explain the process of fuzzy-AHP (Lesniak et al. 2018)

Step 1 *Constructing the Fuzzy pairwise comparison matrix* Triangular fuzzy numbers (TFNs) (Table 2) have been used to prepare the pairwise comparison matrix (Eq. 2). Three values i.e. *l*, *m*, *u* are based on the linguistic scale of 1–9 and follow fuzzy logic.

$$\tilde{A} = \begin{bmatrix} 1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ \vdots & 1 & \ddots & \vdots \\ {}^{1}/_{\tilde{a}_{12}} & {}^{1}/_{\tilde{a}_{23}} & 1 & \tilde{a}_{3n} \\ {}^{1}/_{\tilde{a}_{1n}} & {}^{1}/_{\tilde{a}_{24}} & \cdots & 1 \end{bmatrix}, \tag{2}$$

where

$$\tilde{a}_{ij} = \begin{cases} \tilde{1}, \tilde{3}, \tilde{5}, \tilde{7}, \tilde{9} & \text{When element } \}i' \text{ is more significant than element } \}j' \\ 1 & \text{When element } \}i' \text{ is equally significant than element } \}j' \\ \tilde{9}^{-1}, \tilde{7}^{-1}, \tilde{5}^{-1}, \tilde{3}^{-1}, \tilde{1}^{-1} & \text{When element } \}i' \text{ is less significant than element } \}j' \end{cases}$$

Step 2 *Fuzzy weight calculation* In F-AHP, the geometric mean (Csutora and Buckley 2001) method is applied to aggregate group judgments (Eq. 3).

Table 2 Fuzzy-AHP Scale

Linguistic terms	Non-fuzzy number	Scale of fuzzy numbers (*l*, *m*, *u*)	Inverse of fuzzy number
Equally important	1	(1,1,1)	(1,1,1)
Weakly important	3	(2,3,4)	(1/4,1/3,1/2)
Fairly important	5	(4,5,6)	(1/6,1/5,1/4)
Strongly important	7	(6,7,8)	(1/8,1/7,1/6)
Absolutely important	9	(9,9,9)	(1/9,1/9,1/9)
The intermittent values between two adjacent scales	2	(1,2,3)	(1/3,1/2,1)
	4	(3,4,5)	(1/5,1/4,1/3)
	6	(5,6,7)	(1/7,1/6,1/5)
	8	(7,8,9)	(1/9,1/8,1/7)

Source Sachdeva et al. (2021)

$$l_{ij} = \left(\prod_{m=1}^{M} l_{ij}^{m}\right)^{1/M}, m_{ij} = \left(\prod_{m=1}^{M} m_{ij}^{m}\right)^{1/M}, u_{ij} = \left(\prod_{m=1}^{M} u_{ij}^{m}\right)^{1/M}, \tag{3}$$

where l_{ij}^{m}, l_{ij}^{m}, u_{ij}^{m} represents the fuzzy sample and the ranking of each sample have been evaluated by applying the geometric mean method, which is shown in Eqs. 4 and 5.

$$\tilde{r}_i = \left(\prod_{j=1}^{n} \tilde{a}_{ij}\right)^{\frac{1}{n}} \tag{4}$$

$$\tilde{\boldsymbol{w}}_{\boldsymbol{i}} = \tilde{\boldsymbol{r}}_{\boldsymbol{i}} \otimes \left(\sum_{i=1}^{n} \tilde{r}_i\right)^{-1}, \quad i = 1, 2, \ldots, n. \tag{5}$$

Step 3 *Calculation of defuzzified weight* A review of literature has suggested various methods for Defuzzifying the fuzzy weight i.e. Largest of Maximum (LOM), Mean of Maximum (MOM), Center of Area (COA), Smallest of Maximum (SOM), and Bisector of Area (BOA). In this study, we have applied (Eq. 6) the center of Area (COA) method for calculating the best non-fuzzy performance value (BNP).

$$\mathrm{BNP} = w_i \frac{\left[\left(U\tilde{w}_i - L\tilde{w}_i\right) + \left(M\tilde{w}_i - L\tilde{w}_i\right)\right]}{3} + L\tilde{w}_i \ldots \forall i. \tag{6}$$

Step 4 *Normalizing the defuzzified weight* To normalizing the fuzzy weight, Eq. 7 has been applied to defuzzified the fuzzy weight.

Table 3 Normalized pairwise comparison matrix of main criteria for DeFi

Goal	OR	TR	FR	LRR	NR	Normalized weight	Global ranking
OR	1,1,1	0.11,0.12,0.17	6.00,7.00,9.00	0.13,0.15,0.20	7.00,8.00,9.00	0.139	4
TR	6.00,8.33,9.00	1,1,1	0.11,0.14,0.20	6.00,8.00,9.00	7.00,8.00,9.00	0.317	1
FR	0.13,0.14,0.17	5.00,7.33,9.00	1,1,1	0.13,3.10,9.00	0.13,2.77,9.00	0.236	3
LRR	5.00,6.67,8.00	0.11,0.13,0.17	0.11,4.70,8.00	1,1,1	7.00,8.67,9.00	0.259	2
NR	0.11,0.13,0.14	0.11,0.13,0.14	0.11,4.38,8.00	0.11,0.12,0.14	1,1,1	0.049	5

Operational Risk (OR); Technical Risk (TR); Financial Risk (FR); Legal and Regulatory Risk (LRR); Nascent Risk (NR)

Consistency Ratio = 0.0789 which is less than 0.10

$$\mathrm{NW_i} = \frac{BNP}{\sum(\mathrm{BNP})}. \tag{7}$$

Step 5 *Checking the consistency ratio* (*CR*) Saaty (1980) has given the concept of consistency ratio through which we can check the consistency of all individuals by applying Eqs. 8 and 9.

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{8}$$

$$\mathrm{CI} = \frac{1}{n(n-1)}\sum_{i=1}^{n}\sum_{j=1}^{n}\left(a_{ij}\frac{w_j}{w_i} - 1\right), \tag{9}$$

where CI represents consistency index and RI shows a random index.

Results and discussions

The study applied the AHP approach under fuzzy conditions to evaluate the pairwise comparison matrix constructed on the basis of the DeFi risks preference of the experts. This approach helps the researchers in prioritizing criteria and sub-criteria related to a field. As discussed in step 1, crisp values were used to formulate a comparison matrix. To ensure reliability, a consistency ratio (CR) has been computed. The outcomes of CR proved that the comparison matrix is consistent as its value is less than 0.10. In Table 3, the authors have represented the pairwise comparison of the major criteria. The outcomes of the research corroborate the existing literature on Defi.

It is clear from this Table 3; the priority order is TR > LRR > FR > OR > NR. Echo, technical risk (relative preference weight = 0.317) was the most significant

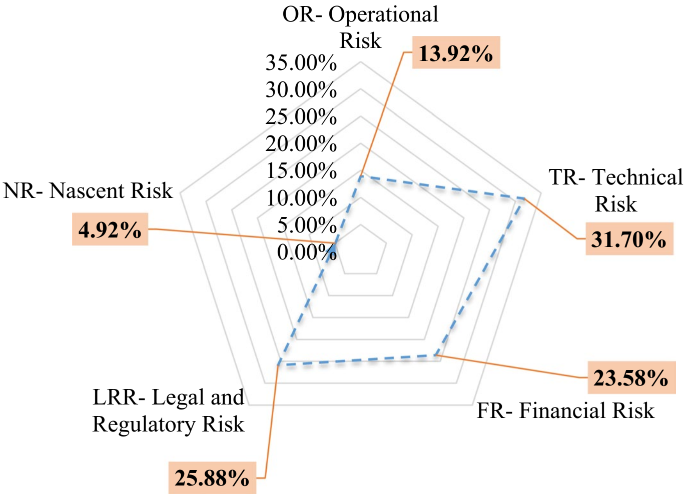

Fig. 5 Radar chart showing criterion global weight

Defi risk. Figure 5 also verifies the supremacy of technical risk. Reliance on immature blockchain designs seems to be the major reason for technical risks (Liu et al. 2021). Further, among the various sub-categories of technical risk, smart contracts risks are the most substantial risk (as shown in Table 4). Experts feel that reentrancy attacks are a major hurdle in the mass adoption of smart contracts. Legal and regulatory risks, i.e. regulatory arbitrage, disclosure risk, and financial crime proved to be the second most substantial DeFi risk (relative preference weight = 0.259). Most DeFi protocols do not fulfil compliance requirements as they are not regulated by financial regulators. Unregulated DeFi protocols pose consumer protection risks that will hinder the mass adoption of DeFi protocols. The recent collapse of FTX crypto exchange demonstrates the negative consequences of deregulation. According to our experts, regulated DeFi startups such as Swarm markets (regulated by German financial regulator BaFin) will be more successful as they can resolve the issue of lacking trust. The next two DeFi risks are financial and operational risks. Among financial risks, liquidity risk (global weight = 0.0928) was the most significant risk. Financial specialists argue that slippage due to low market liquidity is the major shortcoming of present decentralized exchanges. Governance mechanism and Finality risks were found to be the most significant operational risks. Betwixt the nascent risks, flash crashes get the maximum consideration. Automated Market Maker-based decentralized exchanges should consider open-source arbitrageur bots and limit orders to avoid these crashes.

Apart from the above discussions, the authors also prioritize all the sub-criteria. Table 4 reports the global weight and ranking of all the sub-criteria. Financial crime (global weight = 0.1437) proved the utmost important sub-criteria, followed by smart contract risks (global weight = 0.1394), transaction risks (global weight = 0.1355), and liquidity risks (global weight = 0.0928). Legal practitioners argue that perceived anonymity in P2P

Table 4 Global weight and ranking of all the sub-criteria with respect to main criteria of DeFi

Goal	OR	TR	FR	LRR	NR
Finality risks (hard and soft forks)	*0.0330 (9)*				
Loss of private keys (key management)	*0.0259 (13)*				
Upgradation risk	*0.0265 (12)*				
Governance mechanisms	*0.0362 (8)*				
Composability risk	*0.0176 (17)*				
Smart contracts risk		*0.1394 (2)*			
Miner risk		*0.0206 (16)*			
Transaction attacks		*0.1355 (3)*			
Oracle risk		*0.0215 (15)*			
Liquidity risk			*0.0928 (4)*		
Market risk			*0.0704 (6)*		
Credit risk (counterparty risk)			*0.0727 (5)*		
Regulatory arbitrage				*0.0305 (10)*	
Fraud through rug pulls				*0.0587 (7)*	
Disclosure risk				*0.0258 (14)*	
Financial crime				*0.1437 (1)*	
Financial illiteracy risks					*0.0119 (18)*
Black swans (flash crashes)					*0.0272 (11)*
Dynamic interactions					*0.0100 (19)*
Total	*1.00*	*1.00*	*1.00*	*1.00*	*1.00*
Consistency ratio (CR)	*0.0874 <0.10*	*0.0786 <0.10*	*0.0941 <0.10*	*0.0689 <0.10*	*0.0841 <0.10*

transactions can lead to AML/CFT breaches. Logical bugs, integer manipulations, and other operational vulnerabilities are major hurdles in the smooth functioning of smart contracts. In addition to this, financial illiteracy risks and dynamic interactions were at the bottom of the list.

Theoretical and managerial implications

The outcomes of current research have several implications for DeFi entrepreneurs, policymakers, DeFi developers, programmers, and investors. With the advent of blockchain-based smart contracts, decentralized finance is rewiring the working of financial systems. Several disruptors and incumbents are adopting these permissionless, non-custodial, and open-source solutions. Nevertheless, DeFi is a nascent area, and there are several vulnerabilities that need to be addressed to ensure its mass adoption. The findings of the present research motivate developers, programmers, and entrepreneurs to understand several DeFi risks and come up with sustainable mechanisms to manage these risks. For regulators, DeFi masquerades unique challenges. Too much anonymity in DeFi protocols can have sinister consequences, i.e. money laundering and illicit activities. Stringent regulations can hamper innovations. The current research highlights the high-priority regulatory vulnerabilities that regulators need to consider first, although, several regulators are proposing different regulatory frameworks to regulate DeFi protocols. However, global regulatory frameworks would be more effective, therefore global regulatory coordination is the need of the hour. Further, there should be a standardized framework for asset tokenization that will assist regulators to perform technical due diligence. ERC 1400 is the latest development in this field. ERC 1400 is a security token standard that can incorporate intricate regulations in smart contracts. From financial practitioner's point of view, the study underpins the importance of slippage risk that may arise due to low liquidity. In short, technical, legal, and financial risks are substantial DeFi risks; to address these risks global solution networks may be a potential solution. These networks consist of standard, advocacy, watchdog, knowledge, policy, and delivery networks.

Apart from managerial implications, the study also offers novel insights for academicians. With the help of multivocal literature review, the present research reviewed various technical notes, peer-reviewed studies, white papers, government papers, and policy reports and provided a comprehensive state-of-the-art understanding of key issues in the mass adoption of DeFi protocols. The study's findings revealed that technical and regulatory risks are the major obstacle in the growth of DeFi protocols. These findings corroborate the ideas of Hayek's theory of money, which claimed that monopolies of central banks on money could be challenged by the novel, effective, and solvent solutions by private players (Hayek 1980). In addition to this, the study will guide the researchers working in the field of DeFi to propose novel pathways to overcome DeFi risks. Finally, by using a novel combination of MLR and F-AHP, the study also contributes to methodology.

Conclusion and future scope

DeFi is disintermediating financial services through both familiar and novel mechanisms. DeFi is witnessing a perfect storm and it has been accentuated to an $80 billion industry in 2021 (Wu 2021). In this study, the authors identified several DeFi risks through an extensive literature survey and segregated these risks into five major categories. These major categories were considered as the main criteria. In addition to this, the present study also considered several sub-criteria for every major criterion. With the help of F-AHP, the relative importance of each criterion and sub-criteria has been computed. Global weights have been calculated for all the sub-criteria. Financial crimes, smart contract risks, transactions risks, and liquidity risks are key vulnerabilities that policymakers and industry practitioners should consider initially.

To achieve the true potential of DeFi, these risks need to be addressed. Stringent regulations will not work for DeFi as it is a new and immature area. Strict regulations will stifle innovations. Academicians, financial practitioners, non-state organizations, technologists, policy experts, governments, co-operations, and non-government organizations should come together and build a collaborative ecosystem to fulfil the true promise of DeFi, i.e. financial democracy. The sustainable future of DeFi will depend upon the collective capabilities of different stakeholders to address technical, operational, financial, and legal vulnerabilities.

The current research highlights various risks and sub-risks that hinder the growth of DeFi; future researchers may offer feasible solutions to these obstacles that will help in the evolution of this nascent field. Future studies can employ advanced multi-criteria decision-making techniques such as Pythagorean fuzzy analytical hierarchy, Pythagorean fuzzy Delphi, MICMAC to investigate and validate the various DeFi risk categories. Further, the present study explores the overall DeFi risks; future studies can investigate risks in narrow DeFi areas such as lending and borrowing protocols, payment protocols, and insurance protocols.

Appendix

Identifying and prioritizing decentralized finance (DeFi) risks: a fuzzy-AHP approach

Questionnaire survey

1. Name: _______________ (Optional)
2. Kindly indicate your gender: Male □ Female □

Part A: general information

Part B: survey questions In the following sheet, we would like to stimulate your opinion in order to select among the alternatives. The pairwise comparison scale is used to express the importance of one element over another.

Explanation	Numeric value
If *Option A* and *Option B* are equally important: Insert	1
If *Option A* is moderately more important than *Option B*: Insert	3
If *Option A* is strongly more important than *Option B*: Insert	5
If *Option* **A** is very strongly more important than *Option B*: Insert	7
If *Option A* is extremely more important than *Option B*: Insert	9
Use even numbers for intermediate judgments	2,4,6,8

Comparison of various factors affecting decentralized finance

Please indicate your response to the relationship between all the critical success factors of Decentralized Finance are given below. Rate them on a scale of 1–9 (Tables 5, 6, 7, 8, 9, and 10).

Table 5 Main criteria

Operational risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Technical risk
Operational risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Financial risk
Operational risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Legal and regulatory risk
Operational risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Nascent risk
Technical risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Financial risk
Technical risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Legal and regulatory risk
Technical risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Nascent risk
Financial risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Legal and regulatory risk
Financial risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Nascent risk
Legal and regulatory risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Nascent risk

Table 6 Sub-criteria of operational risk

Finality risks (hard and soft forks)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Loss of private keys (key management)
Finality risks (hard and soft forks)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Upgradation risk
Finality risks (hard and soft forks)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Governance mechanisms
Finality risks (hard and soft forks)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Composability risk
Loss of private keys (key management)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Upgradation risk
Loss of private keys (key management)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Governance mechanisms
Loss of private keys (key management)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Composability risk
Upgradation risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Governance mechanisms
Upgradation risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Composability risk
Governance mechanisms	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Composability risk

Table 7 Sub-criteria of technical risk

Smart contracts risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Miner risk
Smart contracts risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Transaction attacks
Smart contracts risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Oracle risk
Miner risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Transaction attacks
Miner risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Oracle risk
Transaction attacks	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Oracle risk

Table 8 Sub-criteria of financial risk

Liquidity risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Market risk
Liquidity risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Credit risk (counterparty risk)
Market risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Credit risk (counterparty risk)

Table 9 Sub-criteria of legal regulatory risk

Regulatory arbitrage	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Fraud through rug pulls
Regulatory arbitrage	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Disclosure risk
Regulatory arbitrage	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Financial crime
Fraud through rug pulls	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Disclosure risk
Fraud through rug pulls	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Financial crime
Disclosure risk	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Financial crime

Table 10 Sub-criteria of nascent risk

Financial illiteracy risks	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Black swans (flash crashes)
Financial illiteracy risks	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Dynamic interactions
Black swans (flash crashes)	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Dynamic interactions

References

Aramonte, S., W. Huang, and A. Schrimpf. 2021. DeFi Risks and the Decentralization Illusion. https://www.bis.org/publ/qtrpdf/r_qt2112b.htm.

Atzei, N., M. Bartoletti, and T. Cimoli. 2021. A survey of attacks on Ethereum smart contracts. *IACR Cryptology* ePrint Archive, 2016: 1007

Badhotiya, G.K., S. Avikal, G. Soni, and N. Sengar. 2021. Analyzing Barriers for the Adoption of Circular Economy in the Manufacturing Sector. *International Journal of Productivity and Performance Management*. https://doi.org/10.1108/IJPPM-01-2021-0021.

Buterin. 2013. Ethereum Whitepaper. *GitHub Repository*. https://ethereum.org.

Buterin, V. 2016. *On Settlement Finality*. *Ethereum Foundation Blog*. https://blog.ethereum.org/2016/05/09/on-settlement-finality.

Caldarelli, G. 2021. Wrapping Trust for Interoperability: A Preliminary Study of Wrapped Tokens. *Information* 13 (1): 1. https://doi.org/10.3390/info13010006.

Carter, N., and L. Jeng. 2021. *DeFi Protocol Risks: The Paradox of DeFi* (SSRN Scholarly Paper No. 3866699). https://doi.org/10.2139/ssrn.3866699.

Casino, F., T.K. Dasaklis, and C. Patsakis. 2019. A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. *Telematics and Informatics* 36: 55–81. https://doi.org/10.1016/j.tele.2018.11.006.

Chen, H., M. Pendleton, L. Njilla, and S. Xu. 2020. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. *ACM Computing Surveys* 53 (3): 67:1-67:43. https://doi.org/10.1145/3391195.

ConsenSys The q1. 2020. ConsenSys Year in Review 2020. *ConsenSys*. https://consensys.net/year-in-review-2020/.

Csutora, R., and J.J. Buckley. 2001. Fuzzy Hierarchical Analysis: The Lambda-Max Method. *Fuzzy Sets and Systems* 120: 181–195. https://doi.org/10.1016/S0165-0114(99)00155-4.

Cylynx. 2021. Introducing Cylynx Cryptocurrency News API. https://www.cylynx.io/blog/introducing-our-cryptocurrency-news-api/.

Deng, H. 1999. Multicriteria Analysis with Fuzzy Pairwise Comparison. *International Journal of Approximate Reasoning* 21 (3): 215–231.

Deshmukh, S., S. Warren, and K. Warbach. 2021. *Decentralized Finance (DeFi) Policy-Maker Toolkit*. World Economic Forum.

Dingman, W., A. Cohen, N. Ferrara, A. Lynch, P. Jasinski, P.E. Black, and L. Deng. 2019. Defects and Vulnerabilities in Smart Contracts, a Classification Using the NIST Bugs Framework. *International Journal of Networked and Distributed Computing* 7 (3): 121–132. https://doi.org/10.2991/ijndc.k.190710.003.

Fu, H., Y. Ho, R.C.Y. Chen, T. Chang, and P. Chien. 2006. Factors Affecting the Adoption of Electronic Marketplaces: A Fuzzy AHP Analysis. *International Journal of Operations & Production Management* 26 (12): 1301–1324. https://doi.org/10.1108/01443570610710560.

Gao, J., H. Liu, C. Liu, Q. Li, Z. Guan, and Z. Chen. 2019. EASYFLOW: Keep Ethereum Away from Overflow. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, 23–26. https://doi.org/10.1109/ICSE-Companion.2019.00029.

Gudgeon, L., D. Perez, D. Harz, A. Gervais, and B. Livshits. 2020. The decentralized financial crisis. In *2020 crypto valley conference on blockchain technology (CVCBT)* (pp. 1-15). IEEE.

Harvest Online. 2021. Harvest: Earn Passive Yield on Your Crypto. https://www.harvest.finance/. Accessed 2 Apr 2023.

Harvey, C.R., A. Ramachandran, and J. Santoro. 2021. *DeFi and the Future of Finance* (SSRN Scholarly Paper ID 3711777). Social Science Research Network. https://doi.org/10.2139/ssrn.3711777.

Harz, D., and W. Knottenbelt. 2018. Towards Safer Smart Contracts: A Survey of Languages and Verification Methods. https://arxiv.org/abs/1809.09805v4.

Hayek, F.A. 1980. *Individualism and Economic Order*. Chicago: University of Chicago Press.

Huilgolkar, H. 2020. Designing the Most Secure Oracle for the Decentralized Finance. *Coinmonks*. https://medium.com/coinmonks/designing-the-most-secure-oracle-for-the-decentralized-finance-9853237f0c37.

Islam, A.K.M.N., M. Mäntymäki, and M. Turunen. 2019. Why Do Blockchains Split? An Actor-Network Perspective on Bitcoin Splits. *Technological Forecasting and Social Change* 148: 119743. https://doi.org/10.1016/j.techfore.2019.119743.

Keatinge, T., D. Carlisle, and F. Keen. 2018. Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses. EPRS: European Parliamentary Research Service. Belgium. Retrieved April 8, 2023 from https://policycommons.net/artifacts/1332623/virtual-currencies-and-terrorist-financing/1936307/

Khan, S.N., F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani. 2021. Blockchain Smart Contracts: Applications, Challenges, and Future Trends. *Peer-to-Peer Networking and Applications* 14 (5): 2901–2925. https://doi.org/10.1007/s12083-021-01127-0.

Klages-Mundt, A., D. Harz, L. Gudgeon, J.-Y. Liu, and A. Minca. 2020. *Stablecoins 2.0: Economic Foundations and Risk-Based Models*, 59–79. https://doi.org/10.1145/3419614.3423261.

Klages-Mundt, A., and A. Minca. 2019. (In)Stability for the Blockchain :Deleveraging Spirals and Stablecoin Attacks. *Cryptoeconomic Systems*. https://doi.org/10.21428/58320208.e46b7b81.

L and AU. 2021. DeFi Cryptocurrency Rug Pulls. *CyberTalk*. https://www.cybertalk.org/2021/09/02/defi-cryptocurrency-rug-pulls/.

Lai, E., and W. Luo. 2020. Static Analysis of Integer Overflow of Smart Contracts in Ethereum. In *Proceedings of the 2020 4th International Conference on Cryptography*, *Security and Privacy*, 110–115. https://doi.org/10.1145/3377644.3377650.

Lesniak, A., D. Kubek, E. Plebankiewicz, K. Zima, and S. Belniak. 2018. Fuzzy AHP Application for Supporting Contractors' Bidding Decision. *Symmetry*. https://doi.org/10.3390/sym10110642.

Li, X., P. Jiang, T. Chen, X. Luo, and Q. Wen. 2020. A Survey on the Security of Blockchain Systems. arXiv [Cs]. http://arxiv.org/abs/1802.06993.

Liu, B., P. Szalachowski, and J. Zhou. 2021. A First Look into DeFi Oracles. *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)* 2021: 39–48. https://doi.org/10.1109/DAPPS52256.2021.00010.

Liu, Q., L. Yu, and C. Jia. 2020. MovER: Stabilize Decentralized Finance System with Practical Risk Management. In *2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, 55–56. https://doi.org/10.1109/BRAINS49436.2020.9223274.

López Vivar, A., A.T. Castedo, A.L. Sandoval Orozco, and L.J. García Villalba. 2020. An Analysis of Smart Contracts Security Threats Alongside Existing Solutions. *Entropy* 22 (2): 203. https://doi.org/10.3390/e22020203.

Maker Dao Blog. 2020. MakerDAO's Year in Review: 2020. https://blog.makerdao.com/makerdaos-year-in-review-2020/.

Meegan, X. 2020. Identifying Key Non-financial Risks in Decentralized Finance on Ethereum Blockchain. https://doi.org/10.13140/RG.2.2.27175.57769.

Meegan, X., and T. Koens. 2021. Lessons Learned from Decentralized Finance (DeFi). 22.

Miller, A., Y. Xia, K. Croman, E. Shi, and D. Song. 2016. The Honey Badger of BFT Protocols. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 31–42. https://doi.org/10.1145/2976749.2978399.

Mörke, M. 2022. Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro: DeFi and the Future of Finance. *Financial Markets and Portfolio Management*. https://doi.org/10.1007/s11408-022-00418-7.

Muzzy. 2020. What Happens to My ETH on Ethereum 2.0?*ConsenSys*. https://consensys.net/blog/ethereum-2-0/what-happens-to-my-eth-on-ethereum-2/.

Nystrom. 2019. 2019 Was The Year of DeFi (and Why 2020 Will be Too). *ConsenSys*. https://consensys.net/blog/news/2019-was-the-year-of-defi-and-why-2020-will-be-too/.

Obadia, A. 2020. Flashbots: Frontrunning the MEV Crisis. *Medium*. https://medium.com/flashbots/frontrunning-the-mev-crisis-40629a613752.

Oosthoek, K. 2021. Flash Crash for Cash: Cyber Threats in Decentralized Finance. arXiv [Cs]. http://arxiv.org/abs/2106.10740.

Peaster. 2020. Biggest DeFi Hacks in 2020. https://defiprime.com/hacks2020.

Perez, D., and B. Livshits. 2020. Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited. arXiv [Cs]. http://arxiv.org/abs/1902.06710.

Praitheeshan, P., L. Pan, J. Yu, J. Liu, and R. Doss. 2020. Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey. arXiv [Cs]. http://arxiv.org/abs/1908.08605.

Qian, P., Z. Liu, Q. He, R. Zimmermann, and X. Wang. 2020. Towards Automated Reentrancy Detection for Smart Contracts Based on Sequential Models. *IEEE Access*. https://doi.org/10.1109/access.2020.2969429.

Ramos, S., F. Pianese, T. Leach, and E. Oliveras. 2021. A Great Disturbance in the Crypto: Understanding Cryptocurrency Returns Under Attacks. *Blockchain: Research and Applications*. https://doi.org/10.1016/j.bcra.2021.100021.

Saaty, T.L. 1980. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. New York: McGraw-Hill International Book Co.

Sachdeva, M., R. Lehal, S. Gupta, and A. Garg. 2021. What Make Investors Herd While Investing in the Indian Stock Market? A Hybrid Approach. *Review of Behavioral Finance*. https://doi.org/10.1108/RBF-04-2021-0070.

Shen, M. 2021. Maker Price Passes $4K for First Time, as MakerDAO Brings Real Estate to DeFi—CoinDesk. https://www.coindesk.com.

Singh, S., N. Walia, S. Saravanan, P. Jain, A. Singh, and J. Jain. 2021. Mapping the Scientific Research on Alternative Momentum Investing: A Bibliometric Analysis. *Journal of Economic and Administrative Sciences* 38 (4): 619–636. https://doi.org/10.1108/JEAS-11-2020-0185.

Smith and Crown. 2019. The oracle problem and mixicles. sci.smithandcrown.com/ research/ oracle-problem-and-mixicles.

Sood, K., Singh, S., Behl, A., Sindhwani, R., Kaur, S., and Pereira, V. 2023. Identification and prioritization of the risks in the mass adoption of artificial intelligence-driven stable coins: The quest for optimal resource utilization. *Resources Policy* 81: 103235.

Szabo. 1994. Smart Contracts. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Vereckey, B. 2021. Decentralized Finance: 4 Challenges to Consider. *MIT Sloan*. https://mitsloan.mit.edu/ideas-made-to-matter/decentralized-finance-4-challenges-to-consider.

Wang, S., L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang. 2019. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49 (11): 2266–2277. https://doi.org/10.1109/TSMC.2019.2895123.

Werner, S.M., D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W.J. Knottenbelt. 2021. SoK: Decentralized Finance (DeFi). arXiv [Cs, Econ, q-Fin]. http://arxiv.org/abs/2101.08778.

Wu, E. 2021. Why DeFi Could be an $800 Billion Industry Next Year, According to a Crypto Expert | Currency News | Financial and Business News | Markets Insider. Markets Insider. https://markets.businessinsider.com/news/currencies/defi-crypto-800-billion-industry-billionaire-decentralized-finance-vesper-2021-08.

Xia, P., H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu. 2021. Demystifying Scam Tokens on Uniswap Decentralized Exchange. arXiv [Cs]. http://arxiv.org/abs/2109.00229.

Yadav, G., and T.N. Desai. 2016. Lean Six Sigma: A Categorized Review of the Literature. *International Journal of Lean Six Sigma* 7 (1): 2–24. https://doi.org/10.1108/IJLSS-05-2015-0015.

Zadeh, L.A. 1965. Fuzzy Sets. *Information and Control* 8 (3): 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X.

Zadeh, L.A. 1996. On Fuzzy Algorithms. In *Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems*, vol. 6, 127–147. Singapore: World Scientific. https://doi.org/10.1142/9789814261302_0010.

Zetzsche, D.A., D.W. Arner, and R.P. Buckley. 2020. *Decentralized Finance (DeFi)* (SSRN Scholarly Paper ID 3539194). Social Science Research Network. https://doi.org/10.2139/ssrn.3539194.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Sandeepa Kaur[1] · **Simarjeet Singh**[2] · **Sanjay Gupta**[3] · **Sangeeta Wats**[4]

Sandeepa Kaur
sandeepakaur@gmail.com

Simarjeet Singh
jeetsimarkamal93@gmail.com

Sangeeta Wats
sangeeta.wats@sbm.nmims.edu

[1] Department of Management, Jagannath International Management School, Kalkaji, New Delhi, India

[2] Great Lakes Institute of Management, Gurgaon, Gurugram, Haryana, India

[3] Sri Aurobindo College of Commerce and Management, Ludhiana, Panjab University, Chandigarh, India

[4] School of Business Management, Narsee Monjee Institute of Management Studies University, (NMIMS University), Mumbai, India