The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 07 - 2025

Legal Risks and Accountability in Defi Ecosystems

[1] Marufjon Yoqubjonov
[1] Lecturer at the Training Institute for Lawyers, Uzbekistan

Received: 20th Nov 2025 | Received Revised Version: 11th Dec 2025 | Accepted: 24th Dec 2025 | Published: 29th Dec 2025

Volume 07 Issue 12 2025 | Crossref DOI: 10.37547/tajpslc/Volume07Issue12-21

Abstract

Decentralized finance (DeFi) represents a novel financial ecosystem built on open blockchain networks and smart contracts, enabling the provision of financial services without traditional intermediaries. This article examines the conceptual foundations of DeFi, its legal nature, associated risks, and regulatory challenges through a comparative analysis of international practice and the emerging legal framework of Uzbekistan. Particular attention is paid to the composability of DeFi protocols, the legal uncertainty surrounding smart contracts, and the difficulty of identifying responsible parties in decentralized systems. The study analyzes scholarly perspectives, including those of Schär and Zetzsche, and reviews regulatory responses in the United States and the European Union, with a focus on enforcement actions and AML/CFT concerns. It further evaluates risks such as cyberattacks, fraud, money laundering, and consumer harm, highlighting the systemic vulnerabilities of DeFi infrastructures. The article argues that while DeFi offers transparency and innovation, effective regulation requires balancing technological neutrality with robust consumer protection and compliance mechanisms. The findings suggest that Uzbekistan may adopt a cautious, technology-integrated regulatory approach to harness DeFi's potential while mitigating legal and financial risks.

Keywords: Decentralized finance (DeFi); smart contracts; legal liability; AML/CFT; regulatory challenges; blockchain regulation; financial innovation.

Cite This Article: Marufjon Yoqubjonov. (2025). Legal Risks and Accountability in Defi Ecosystems. The American Journal of Political Science Law and Criminology, 7(12), 130–132. https://doi.org/10.37547/tajpslc/Volume07Issue12-21

1. Introduction

Decentralized finance (DeFi) is a new financial ecosystem that automates financial services without intermediaries based on open blockchain networks and smart contracts. DeFi enables lending, insurance, payments, and various financial transactions through smart contracts signed on platforms such as Ethereum. Schär stated that DeFi is a "set of open, unauthorized, and highly interconnected protocols" that replicates traditional financial services in a more transparent manner by eliminating intermediaries.[1] This article provides a comparative analysis of the essence of the DeFi ecosystem, its legal aspects, risks, and the possibilities of implementing DeFi in Uzbekistan. The analysis applies the legislation of the USA, the European, as well as relevant decisions and opinions of legal scholars in Uzbekistan.

DeFi is a set of decentralized financial services; it operates on the basis of digital assets (blockchains) and code-based contracts. Swiss scientist Schär notes that DeFi performs traditional financial services via code, not through intermediaries (banks, clearing centers, etc.) [1]. For example, in the DeFi ecosystem, it is possible to buy stablecoins for the value of USD, transfer them to an open loan platform with interest, and then add the acquired assets to the market to generate income. In this case, all agreements are recorded in a transparent blockchain and are automatically executed through "smart contracts."

The DeFi (decentralized finance) ecosystem consists of several separate, but interconnected financial services.

These services include, among other things, decentralized exchanges, lending platforms, and mechanisms aimed at generating income. These platforms operate without traditional financial institutions, that is, without banks or brokers, through smart contracts.

An important feature of DeFi is that all its components work "combined" with each other. That is, one DeFi protocol can use a token or digital asset created by another protocol in its operation. For example, a user buys a stablecoin on a decentralized exchange, places it on a lending platform, and in return receives a special token (an asset representing the user's right of claim). Subsequently, this token can again be used as a source of liquidity on another platform.

From a legal point of view, this process creates a complex chain of legal relations. Because one user interacts with several protocols simultaneously, but these relationships are not clearly defined: the specific Contracting Party, the scope of rights and obligations, the subject of responsibility. In customary law, such relationships are regulated by separate agreements, whereas in DeFi, all obligations arise automatically through the code.

According to Professor Zetzsche of the University of Luxembourg and his co-authors, DeFi is actually a form of providing financial services not within one organization or one country, but through different jurisdictions and multiple participants[2]. This creates problems from the point of view of law enforcement: the question of which country's law will be applied, which court will consider the dispute, and who will be held responsible remains open.

Transactions in the DeFi infrastructure are carried out in the form of a "smart contract." However, there is a problem with responsibility: in the traditional sense, the contract is a legally binding obligation freely agreed upon between the two parties, but it is often impossible to establish the identity of the developer or smart contract user who wrote the code in DeFi. According to leading experts in the field, Bassan and Rabitti, due to the unclear legal status of smart contracts, many legal disputes have arisen. They note that the concept of "smart contracts" does not fully comply with the legislation, as well as the problems of their implementation under judicial supervision. And the lawyers of Industria Business Lawyers LLP listed the legal difficulties of smart contracts: such traditional terms of the contract as offer and acceptance, quantitative compensation, intent of the parties are "packaged" in the code, however, in this procedure, it is impossible to be sure that both parties fully understood the terms[4]. For example, in the USA, the CFTC ("Commission for the Sale of Company Goods") in 2022 conducted a case against a decentralized trading platform called Ooki DAO: in court, it was noted that transactions made through smart contracts in the Ooki DAO blockchain violated financial regulation laws[4].

Along with the freedom of DeFi, there are also significant risks. The main risks include hacking, fraud, and money laundering. According to new research, due to technical vulnerabilities in DeFi (smart-contractual shortcomings, oracle-dependencies), users suffered losses of about $153 million in 2020, and in 2021, Ethereum assets worth $610 million were stolen in one major attack (PolyNetwork case) [5]. Due to the vulnerability of DeFi protocols, according to the 2021 Elliptic study, users lost a total of more than $10 billion in cases of fraud and promotion (rug pull). As a unique phenomenon in the securities market, the collision of DeFi (the irreversibility of final contracts) also causes serious damage to investors.

DeFi also uses fraudulent (ponzi schemes, "project flows" - rug pull) and fraudulent investment offers. For example, in the "rug pull" scheme, the creators of the project attract an investor to make a bet, and then disappear with the savings. The absence of restrictions and code openness in DeFi creates a favorable environment for scammers. According to regulators' concerns, DeFi services are also being used for money laundering and terrorist financing[6]. Although DeFi is not considered a money transfer enterprise or financial institution under US law, illegal funds can be channelled through blockchain through anonymous "bridges" on DeFi. External studies also note that DeFi platforms serve as a "magnet" for illegal financial transactions. This indicates that KYC/AML (knowing the client) rules are not mandatory for all users in DeFi, as well as the lack of control over international financial transactions. Fraud and scam projects represent the most widespread type of crime in DeFi ecosystems. In these projects, criminals create fake DeFi platforms, collect money from investors, and then disappear. This is carried out through a scheme called a "rug pull." According to the 2022 report from the Cyber Crime Division of the Federal Bureau of Investigation (FBI) of the United States, fraud cases related to DeFi increased by 600% in 2022

compared to 2021 [7]. One of the most damaging projects was the "Squid Game token" scam that occurred in 2021. This project exploited the name of a popular Korean series to collect 3.38 million dollars from investors, after which the creators disappeared [8].

Daniel Richman, Professor of Criminal Law at Columbia University in New York, emphasizes that detecting and prosecuting fraud in DeFi ecosystems is extremely difficult because criminals operate under pseudonyms and often utilize multiple jurisdictions. Unlike fraud in traditional finance, there are no Know Your Customer (KYC) requirements in this space [9].

Uzbek researchers Makhamadkhujaeva, relying on international experience, emphasizes the need to combine AML/CFT and consumer protection methods in DeF control[10].

Conclusion

DeFi is a technological approach that revolutionizes the traditional financial system and can provide transparency and global access. However, DeFi tends to violate legal norms due to its decentralization and anonymity. Foreign experience shows that DeFi requires real-world regulation. According to Zetzsche and his co-authors, when DeFi reduces centralization, "less regulated" other parts appear; Therefore, control should be directed towards such parts. Similarly, to increase DeFi capabilities in Uzbekistan, it will be important to harmonise AML/CFT requirements with modern technology, integrate into code for regulation (such approaches as "digital license to blockchain"). So far, the biggest limitation on the implementation of DeFi is legal uncertainty and strict control. However, considering that our country has started regulating stablecoins from 2026, there may be an opportunity to introduce DeFi mechanisms under simplified CFT/AML conditions in the future.

References

1. Fabian Schär, "Decentralized Finance: On Blockchain-and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74. https://doi.org/10.20955/r.103.153-74;
2. Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley, Decentralized Finance, Journal of Financial Regulation, Volume 6, Issue 2, 20 September 2020, Pages 172-203, https://doi.org/10.1093/jfr/fjaa010;
3. Bassan, Fabio and Rabitti, Maddalena, From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation (November 6, 2023). Available at SSRN: https://ssrn.com/abstract=4624640 or http://dx.doi.org/10.2139/ssrn.4624640;
4. Industria Business Lawyers LLP. (2024, November 14). Legal challenges in defining and regulating smart contracts. Industria Business Lawyers LLP. https://ibl.law/legal-challenges-in-defining-and-regulating-smart-contracts;
5. Kaur S, Singh S, Gupta S, Wats S. Risk analysis in decentralized finance (DeFi): a fuzzy-AHP approach. Risk Management. 2023. 25 (2):13. doi:10.1057/s41283-023-00118-0. Epub 2023 Apr 10. PMCID: PMC10088710.;
6. U.S. Department of the Treasury. (2023). Illegal finance risk assessment of decentralized finance. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf;
7. Federal Bureau of Investigation. (2022). Internet Crime Report 2022. U.S. DepartmentofJustice.https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf;
8. Chen, Y., & Bellavitis, C. (2023). Decentralized finance: Blockchain technology and the quest for an open financial system. Journal of Business Venturing Insights, 19, e00379. https://doi.org/10.1016/j.jbvi.2023.e00379;
9. Richman, Daniel C., The (Immediate) Future of Prosecution (March 5, 2023). Fordham Urban Law Journal, Forthcoming, Columbia Public Law Research Paper No. 4378890, Available at SSRN: https://ssrn.com/abstract=4378890;
10. Makhamadkhujaeva, M. (2023). Crafting Balanced Regulations for Decentralized Finance: Comparative Analysis and Policy Recommendations. International Journal of Accounting, Finance and Risk Management, 8 (4), 111-118.;