ISSN (онлайн): 2663-8959 | ISSN (друк): 2308-6912
УДК 336.76:004.056
DOI: https://doi.org/10.17721/apmv.2026.167.1.178-185

CYBER THREATS TO TOKENIZED ASSETS IN INTERNATIONAL FINANCE: "REACTIVATION"

КІБЕРЗАГРОЗИ ТОКЕНІЗОВАНИМ АКТИВАМ У МІЖНАРОДНИХ ФІНАНСАХ: «ПОВТОРНА АКТИВАЦІЯ»

Serhii Tsyhanov
Doctor of Economics, Professor, Educational and scientific institute of international relations
ORCID: 0000-0002-9032-7829
e-mail: S_Tsyganov@knu.ua

Bohdan Khyzhnyak
Postgraduate student, Educational and scientific institute of international relations
ORCID: 0009-0007-9252-5830
e-mail: khyzhnyakbohdan@gmail.com

Сергій Циганов
Доктор економічних наук, професор кафедри міжнародних фінансів, Навчально-науковий інститут міжнародних відносин
ORCID: 0000-0002-9032-7829
e-mail: S_Tsyganov@knu.ua

Богдан Хижняк
Аспірант, Навчально-науковий інститут міжнародних відносин
ORCID:0009-0007-9252-5830
e-mail: khyzhnyakbohdan@gmail.com

Abstract. *The rapid development of blockchain technologies has led to the emergence of tokenized assets, which is already claiming the title of one of the key innovations in international finance. Although tokenization is a promising direction for the development of the international financial system, it also introduces new cyber risks associated with vulnerabilities in smart contracts. This article examines one of the most influential risks, "reactivation" attacks, and assesses their impact in the context of international financial relations. The study highlights the economic consequences of smart contract vulnerabilities, including financial losses, reduced investor confidence, and systemic risks for global financial markets. Based on the results of the analysis, a list of recommendations has been formed to minimize the likelihood of occurrence and spreading of understanding of the consequences of the "reactivation" vulnerability. The conclusions emphasize the need to improve security standards and spread understanding of the threat to ensure the sustainable development of tokenized financial instruments.*

Keywords. *tokenized assets; smart contracts; reactivation vulnerability; cyber risk; blockchain; international financial relations; digital finance; financial stability; systemic risk; decentralized finance (DeFi); smart contract security; global financial markets*

Анотація. *Швидкий розвиток блокчейн-технологій призвів до появи токенізованих активів, що вже претендує на звання однієї з ключових інновацій в міжнародних фінансах. Хоча токенізація і є перспективним напрямком розвитку міжнародної фінансової системи, вона також вводить нові кіберризики, які пов'язані з вразливостями смарт-контрактів. У цій статті досліджується один із найбільш впливових ризиків, атаки «повторної активації», та оцінюється їх вплив у контексті міжнародних фінансових відносин. У дослідженні висвітлюються економічні наслідки вразливостей смарт-контрактів, включаючи фінансові втрати, зниження довіри інвесторів та системні ризики для світових фінансових ринків. За результатами аналізу сформовано список рекомендацій для мінімізації імовірності виникнення та поширення розуміння наслідків вразливості «повторної активації». Висновки підкреслюють необхідність удосконалення стандартів безпеки та поширення розуміння загрози для забезпечення сталого розвитку токенізованих фінансових інструментів.*

https://doi.org/10.17721/apmv.2026.167.1.178-185

Ключові слова. *токенізовані активи; смарт-контракти; вразливість «повторної активації»; кіберризик; блокчейн; міжнародні фінансові відносини; цифрові фінанси; фінансова стабільність; системний ризик; децентралізовані фінанси (DeFi); безпека смарт-контрактів; світові фінансові ринки*

Introduction. Trading of financial assets is evolving under the influence of the rapid evolution of technology – from the adaptation of banks to the emergence and spread of the Internet and high-speed mobile communications to the most modern developments – artificial intelligence and blockchain technologies. Tokenized assets – traditional assets represented on a programmable platform – are one such technology.

Asset tokenization is one of modern directions of development of the market for financial assets, which utilizes blockchain technology. Although it is believed that tokenization could reduce the barriers associated with the issuance, circulation, trading, and settlements for certain classes of assets, the process is not perfect (Bank for International Settlements & Committee on Payments and Market Infrastructures, 2024). Despite the fact that tokenized assets are partially protected from the risks inherent in traditional asset circulation, they face no less serious risks inherent to them. Here are just some of these risks: logic imperfections and code errors, incorrect authorization, exploits of protocol's vulnerabilities, dependence of libraries on third parties, exploiting of cross-bridge vulnerabilities, cyberattacks, and others.

Each of the listed risks can take different forms. A clear understanding of their root causes, how they work, and potential losses is essential to ensure the continued safe development of the tokenized assets market. This article examines one of the most serious threats – the "reactivation" vulnerability.

The goal of this article is to develop a list of recommendations to minimize the likelihood of occurrence of the "reactivation" vulnerability and to spread understanding of its consequences. The objectives of this article are: identify the threat of "reactivation" and determine root causes of its occurrence; study the real-world case of the "reactivation" vulnerability; analyse the impact of the threat on tokenized assets; formulate a list of appropriate recommendations

To achieve set objectives and goal, a comprehensive literature analysis was conducted.

Literature review. Asset tokenization and its implications for financial markets is discussed in publications by international organizations and academic studies. In particular, the report by the Bank for International Settlements highlights the potential of tokenization to transform financial systems by increasing efficiency, programmability, and reducing dependence on intermediaries. It also emphasizes the emergence of new operational and technological risks (Bank for International Settlements & Committee on Payments and Market Infrastructures, 2024).

In addition, asset tokenization is being actively explored by companies focused on the development of blockchain technologies, such as Ethereum, as this direction is promising for further development of their technologies and increasing profits. Technical documentation in the Ethereum ecosystem describes "reactivation" attacks as a consequence of incorrect sequence of operations in smart contracts and emphasizes the need for secure design patterns and protection mechanisms (ethereum.org, n.d.).

However, the existing literature has largely focused on the technical aspects of vulnerabilities of smart contracts, while their broader economic implications for international finance remain underexplored. This gap highlights the relevance of further research into cyber-threats to tokenized assets in the context of international finance.

Results. For a comprehensive understanding of the article, it is necessary to define the meanings of key terms employed herein:

1. "Contract," as used in this article, is defined as a set of programmed actions aimed at performing operations on a tokenized asset, including purchase, sale, transfer, modification of properties, etc.
2. "Liquidity pool" refers to a collective aggregation of cryptocurrencies or tokenized assets that are locked within a smart contract (Chainlink, 2026).
3. "Node" is a participant in a blockchain network that takes part in the formation of new blocks.
4. "Hard fork" is defined as a modification of a blockchain protocol or blocks' structure,

implemented with the consensus of a majority of participating nodes that exercise control over the network.

Contract's "reactivation" refers to a state in which the current condition of a contract does not correspond to the instructions received from subsequent stages of the protocol (i.e., downstream contracts). This inconsistency enables an attacker to repeatedly "reactivate" the contract and assume control over it by exploiting the mismatch (LlamaRisk, 2023; Vyperlang Team, 2023). Exploitation of this vulnerability allows the attacker to trigger the "withdraw" function within the contract in a manner that facilitates a so-called "infinite asset issuance," whereby all available funds are drained from the contract until either the victim's balance is exhausted or the attacker's balance required to cover transaction execution fees (commonly referred to as "gas fees") is depleted (Nervos Network, 2025; Ethereum.org, n.d.). This vulnerability is most commonly exploited in asset depositories and liquidity pools.

Below is a schematic representation of how an attack based on contract's "reactivation" is carried out. The contract from which funds are to be extracted is referred to as the "Victim," while the hacker's contract is referred to as the "Attacker." The scheme for exploiting this vulnerability is presented below:

The "Attacker" deposits 1 ETH into the balance of the "Victim" → the "Attacker" submits a request to transfer 1 ETH from the balance of the "Victim" → the "Victim" executes «withdraw()» function and transfers 1 ETH to the "Attacker" → upon receiving 1 ETH the "Attacker" invokes the «fallback()» function, thereby submitting a new request to transfer 1 ETH from the balance of the "Victim" → the "Victim" again executes the «withdraw()» function and transfers 1 ETH to the "Attacker" (ethereum.org, n.d.).

The "Attacker" is able to withdraw all funds from the "Victim's" balance (or the maximum amount for which sufficient gas fees can be covered) before the initial withdrawal request is completed. This occurs because the "Attacker's" balance within the "Victim" contract is not reset to zero prior to the completion of the function's execution; consequently, subsequent withdrawal requests are successfully processed, allowing the same amount to be withdrawn multiple times. Through this mechanism, malicious actors are able to drain all liquidity from liquidity pools or asset depositories.

Multiple options for "reactivation" attacks exist, including cross-contract reentrancy and so-called "view-only" methods, among others. The scheme described above represents a basic model within "reactivation" attack scenarios; however, it is sufficient for identifying the core nature of the threat, determining its root causes, assessing the potential consequences of its exploitation, and formulating appropriate recommendations for mitigating the risk of this type of attacks.

The exploitation of this vulnerability is possible because of imperfections in the execution of the function within the targeted contract. However, such imperfections do not arise from a single error. Rather, multiple factors contribute to the emergence of "reactivation" vulnerabilities, and these factors may affect the contract's susceptibility either collectively or independently. The underlying causes and their descriptions are discussed below.

Imperfect protocol logic. This vulnerability was particularly characteristic of earlier protocols, prior to the point at which "reactivation" became widely recognized among developers. Flawed protocol logic constitutes one of the primary causes that may render contracts susceptible to "reactivation" attacks, as the root of the issue originates at the stage of designing and implementing the protocol's core logic. "Imperfect logic" means an incorrect ordering of contract's operations or interactions as encoded within the protocol. The presence of such flaws creates opportunities for "reactivation" by enabling the contract to be re-invoked during execution phases that follow the initial activation (i.e., in subsequent stages of the protocol's execution flow) (Solidity Authors, n.d.). As noted above, this vulnerability was more prevalent in early protocols; however, as awareness of the scale and implications of the issue has increased, a growing number of protocols have been designed from the outset with logic intended to mitigate such attacks or their developers have incorporated built-in protective mechanisms against this class of vulnerability. A particularly notable case is the attack on the DAO (Decentralized Autonomous Organization) in 2016, which will be examined in greater detail further.

Absence of dedicated safeguards against "reactivation" attacks. This is another common cause

particularly prevalent in earlier protocols, although it remains relevant today. This factor is more specific in scope than imperfect protocol logic. Contemporary protocol developers typically implement protective mechanisms known as "reactivation guards," which are designed to prevent the concurrent or repeated execution of the same function. However, given the wide range of "reactivation" attack variants, developers may fail to anticipate certain specific attack vectors and consequently may not implement appropriate specialized defenses. A notable example of the consequences of insufficient protection is the case of Rari Capital, where approximately $80 million was lost during an attack. Although the attack mechanism was more complex than the basic scheme described above, its underlying principle remained unchanged (CertiK, 2022; REKT, 2022). It should also be noted that this cause is closely related to another factor: *the use of increasingly sophisticated techniques by attackers to circumvent established security mechanisms*. While existing safeguards can effectively protect protocols against many forms of attack, hackers continuously refine their methods to bypass these defenses, as the potential reward from successful exploitation often outweighs the cost associated with discovering and leveraging protocol's vulnerabilities. In light of the rapid growth of the tokenized asset market, where the capitalization of tokenized public equities alone reached approximately $16 million as of March 2025, the incentives for attackers to exploit protocols' vulnerabilities are expected to increase further. This, in turn, will likely drive the development of new attack methods as well as refinement of existing techniques for bypassing protocol security mechanisms (World Economic Forum, 2025).

Code "bugs" that occur during protocol updates. The issue of software bugs is, in itself, a complex and multifaceted problem. For the purposes of this study, it is sufficient to define "bugs" as errors in code that lead to its incorrect or unintended functioning, and they emerge during the development stage when the code is initially written (Britannica, 2026). It is also important to note that "bugs" may occur not only during the initial development phase, but also during subsequent protocol updates. However, their emergence during the update phase is more likely to result in vulnerabilities. This is due to the possibility of altering protocol architecture during updates, particularly through the modification of contract logic using proxy mechanisms. While such functionality enables developers to improve and extend existing systems, it also introduces new risks: newly implemented logic may interact improperly with legacy components that have not been updated, thereby creating vulnerabilities that were not characteristic of earlier protocol versions (OpenZeppelin, 2020). Among these is the "reactivation" vulnerability.

Insufficient testing of protocols. Testing refers to the evaluation of how a protocol functions under both standard operating conditions and scenarios involving non-standard use. Continuous and rigorous testing is one of the key prerequisites for ensuring correct functionality and an adequate level of system security. The execution of comprehensive tests enables early detection of flaws in protocol logic, identification of software bugs, and assessment of vulnerabilities to various forms of attack. However, due to a range of factors, the level of testing may fall short of what is considered optimal, thereby increasing the likelihood of issues, including susceptibility to "reactivation" attacks (ethereum.org, n.d.). Several factors may influence the adequacy of testing, including the completeness of test case design at initial stages, the availability of sufficient time to conduct thorough testing, the alignment between the complexity of tasks and the expertise of testing personnel, etc. Moreover, the required depth and rigor of testing are also contingent upon the incentives faced by potential attackers. The greater the perceived benefits of exploiting a protocol, the more comprehensive and sophisticated the testing procedures should be. As a project evolves and its user base expands, the complexity and scope of testing should increase accordingly to maintain an appropriate level of protection against malicious activity. Nevertheless, project growth does not always incentivize developers to raise testing standards, which can ultimately result in significant losses.

Having identified the underlying causes of "reactivation" vulnerabilities in protocols, it is appropriate to examine a practical example of the realization of this threat. It should be noted that the case below focuses on a scenario in which a protocol vulnerability was exploited to facilitate the theft of cryptocurrency. However, given that tokenized assets are built on similar or analogous blockchain infrastructures, this example remains relevant for the analysis of risks in tokenized asset systems (World Economic Forum, 2025).

Let us consider the case of the *2016 attack on the DAO*, which led to a split within the Ethereum community and the emergence of Ethereum Classic (ethereum.org, n.d.). This article does not aim to examine the entire context of the DAO breach; rather, it focuses specifically on the aspects related to the exploitation of the "reactivation" vulnerability, the causes of its occurrence, and the consequences of it. A DAO is a form of organizational structure designed to codify governance rules and decision-making processes within smart contracts, thereby eliminating the need for traditional documentation and centralized management. Its objective is to establish a system of decentralized control and automated governance (Siegel, 2023). The operational mechanism of a DAO involves:

- the founders develop a smart contract (protocol) that will govern the organization;
- this is followed by a fundraising period (also referred to as "funding"), during which participants contribute capital to the DAO by purchasing tokens that confer ownership rights or voting power in the operation of the project;
- after the funding period ends, the DAO begins operating;
- people who have invested funds receive the right to make proposals regarding the use of DAO resources (Siegel, 2023).

Understanding how the DAO works is necessary to clearly understand how the protocol breach occurred and its consequences.

In the selected case, the discussion concerns a specific organization developed by the German startup Slock.it, which enabled individuals to share physical assets (e.g., a car) through a decentralized platform conceptually similar to Airbnb, utilizing "smart locks." The founders initiated a fundraising campaign to support the project's development; this funding phase lasted 28 days, beginning on April 30, 2016. As a result, more than $150 million was raised from over 11,000 investors. It is noteworthy that, even during the funding phase, concerns were raised by some participants regarding imperfections in the protocol's code and its susceptibility to attacks. This constitutes a clear indication of one of the previously identified causes of "reactivation" vulnerabilities – namely, *flawed protocol logic*. Furthermore, given that such vulnerabilities were identified not only by the project's developers but also by external observers, it can be inferred that the level of testing conducted during the early stages was insufficient. The issue had already been detected during the fundraising phase, that is, after the completion of the development and testing of the protocol's core logic (Siegel, 2023). Finally, the substantial volume of funds raised served as a strong incentive for an attacker to exploit the identified vulnerability within the protocol.

Following the completion of the fundraising phase, discussions started regarding whether the identified vulnerabilities should be addressed prior to the full operational launch of the DAO. In particular, Stephan Tual, one of the creators of the DAO, announced on June 12, 2016, that a "recursive call bug" (another term for "reactivation") had been identified in the software. Nevertheless, he asserted that "DAO funds are not at risk." However, on June 18, 2016 – immediately after the conclusion of the fundraising phase – while developers were still attempting to mitigate the protocol's vulnerabilities, attackers had already succeeded in extracting approximately 3.6 million Ether, which at that time was valued at around $60 million. This was achieved precisely through the exploitation of the aforementioned vulnerability, the operational mechanism of which has been described earlier (Siegel, 2023).

The outcome of the attack on the DAO was the temporary loss of investor funds. The majority of these funds were eventually recovered as a result of implementing a hard fork initiated by the Ethereum Foundation in 2016. However, this decision led to a division within the Ethereum community and the emergence of Ethereum Classic, as not all network participants agreed with the execution of a hard fork. A portion of the community maintained that the blockchain should remain immutable, even in cases involving significant attacks. It is important to emphasize that modifying any block within a blockchain requires the consensus of more than 50% of participants responsible for validating and adding new blocks. Consequently, it would be imprudent to assume that every instance of a protocol attack can be mitigated through rewriting blockchain history.

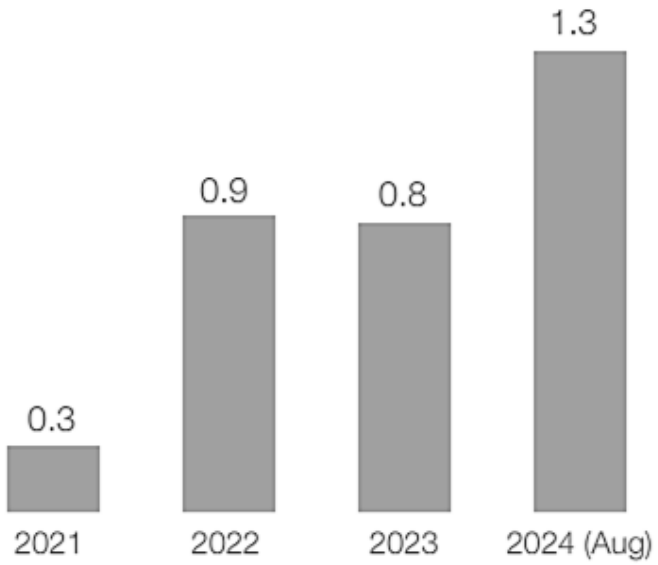
The relevance of this case for the domain of tokenized assets lies in the fact that, although the example examined does not directly involve an attack on tokenized assets, the analysis of the underlying cause that enabled the exploit, as well as its consequences, provides valuable insights for preventing similar incidents in this field. This is particularly important given that certain tokenized

https://doi.org/10.17721/apmv.2026.167.1.178-185
equities are built on the Ethereum blockchain (xStocks, n.d.), which implies a potential risk of companies replicating similar design flaws when developing their own protocols. Accordingly, the set of recommendations presented at the conclusion of this study has been formulated with the aim of reducing the likelihood of such vulnerabilities and ensuring more secure implementation of tokenized asset systems.

Given the increasing momentum in the issuance of tokenized assets – particularly tokenized bonds, as illustrated in Figure 1 – it is essential for issuers to understand the cybersecurity threat posed by "reactivation" in order to ensure the secure operation of tokenized securities within the framework of international finance.

Figure 1

Global bond issuance in blockchain systems, billion euros



Note. (World Economic Forum, 2025)

An illustrative example of how an issuer of tokenized assets may encounter a similar situation can be outlined as follows. Company "A," based in Ukraine, decides to issue tokenized shares instead of pursuing a traditional initial public offering, with the aim of expanding its pool of potential investors. However, without adequately analysing the case of the DAO, the company develops a protocol that contains a comparable flaw in its logic. As a result, investors from multiple jurisdictions incur financial losses following a "reactivation" attack. As noted previously, it would be unrealistic to assume that a majority of blockchain nodes would agree to implement another hard fork to compensate affected investors. In such a scenario, investors' funds would not be recovered, while the company's financing prospects and reputation would be severely compromised. Moreover, widespread publicity surrounding the incident could foster scepticism regarding the reliability of tokenized assets, potentially slowing the development of the sector and disrupting international investment processes. Considering that the outcome of the DAO attack was a division within the Ethereum community – which, at the time in 2016, was significantly smaller than it is today – the recurrence of similar attacks affecting issuers with a substantially larger base of stakeholders could generate even greater controversy and reduce the predictability of potential resolution mechanisms. An alternative to a hard fork is the implementation of a soft fork – effectively isolating the wallet to which the stolen assets were transferred (Siegel, 2023). However, in such a case, investors would still be unable to recover their invested funds.

Based on the results of the analysis, a list of recommendations was formed, which is presented in Table 1 below.

Table 1

Recommendations for preventing the "reactivation" vulnerability for tokenized assets

Cause of occurrence	Prevention recommendations
Imperfect protocol logic.	Ensure the correct design of protocol logic at the development stage, in which any modification of the contract balance occurs prior to any possibility of external "reactivation", in accordance with the Checks-Effects-Interactions principle.
Absence of dedicated safeguards against "reactivation" attacks and the use of increasingly sophisticated techniques by attackers to circumvent established security mechanisms.	Implement multilayered security mechanisms, such as restrictions on repeated function calls and additional contract state validations. It is also essential to ensure the regular updating of security systems in order to address emerging attack vectors.
Code "bugs" that occur during protocol updates.	Implement rigorous update management procedures, including testing contracts within isolated environments, as well as employing staged deployment mechanisms for updates.
Insufficient testing of protocols.	Ensure comprehensive testing, including the use of automated analysis tools and the engagement of independent auditors to assess protocol's security prior to deployment.

The recommendations outlined above provide guidance on measures that can help mitigate the risk of "reactivation" vulnerabilities in tokenized assets within the context of international finance. By addressing identified causes, these measures contribute to enhancing the security, stability, and reliable integration of tokenized assets into the global financial system.

Discussion and Conclusions. To sum up, the causes underlying the emergence of threats related to "reactivation" in tokenized assets include the following:

- imperfect protocol logic
- absence of dedicated safeguards against "reactivation" attacks and the use of increasingly sophisticated techniques by attackers to circumvent established security mechanisms
- code "bugs" that occur during protocol updates
- insufficient testing of protocols

The aforementioned factors may give rise to "reactivation" vulnerability either independently or in combination. The article examines the example of the attack on the DAO, the causes of which included flawed protocol logic, an insufficient level of testing, and the significant attractiveness of the exploit for hackers seeking substantial financial gain. The outcome of the attack was the theft of cryptocurrency, followed by its subsequent restitution to rightful owners through the implementation of a hard fork – effectively a rewriting of the blockchain's transaction history. The importance of analysing this event for issuers of tokenized assets lies in the fact that such assets may be deployed on similar or analogous blockchain infrastructures, thereby increasing the likelihood of replicating comparable vulnerabilities.

Ensuring an adequate level of cybersecurity in protocol design constitutes a necessary precondition for the integration of tokenized assets into the global financial system. The set of recommendations developed and presented in the "Results" section is aimed at mitigating the risk of "reactivation" vulnerability affecting tokenized assets in international markets, thereby supporting their secure operation within the sphere of global finance. Failure to adhere to these recommendations (and, accordingly, to address identified risks) may result in capital losses, disruptions to international investment processes, and a deceleration in the digitalization of the global financial system.

Funding: *no external funding.*

Conflict of Interest: *the authors declare no conflict of interest regarding the publication of this article.*

Data Availability Statement: *not applicable*

References:

https://doi.org/10.17721/apmv.2026.167.1.178-185

Bank for International Settlements, & Committee on Payments and Market Infrastructures. (2024, October). *Tokenisation in the context of money and other assets: Concepts and implications for central banks*. https://www.bis.org/cpmi/publ/d225.pdf

Britannica, T. Editors, & Hemmendinger, D. (2026, February 13). Control structures. In *Computer programming language*. Encyclopaedia Britannica. https://www.britannica.com/technology/computer-programming-language/Control-structures

CertiK. (2022, April 30). *Fei Protocol incident analysis*. Medium. https://certik.medium.com/fei-protocol-incident-analysis-8527440696cc

Chainlink. (2026, February 11). *What is a liquidity pool? DeFi markets explained*. https://chain.link/article/what-is-liquidity-pool

Ethereum Foundation. (2016, July 20). *Hard fork completed*. *Ethereum Foundation Blog*. https://blog.ethereum.org/2016/07/20/hard-fork-completed

Ethereum.org. (n.d.). *Smart contract security*. https://ethereum.org/developers/docs/smart-contracts/security/#reentrancy

LlamaRisk. (2023, August 2). *Curve pool reentrancy exploit postmortem July 30th, 2023*. HackMD. https://hackmd.io/@LlamaRisk/BJzSKHNjn

Nervos Network. (2025, November 7). *What is a reentrancy attack and how does it work?* https://www.nervos.org/knowledge-base/what_is_a_reentrancy_attack_(explainCKBot)

OpenZeppelin. (2020, October 6). *The state of smart contract upgrades*. https://www.openzeppelin.com/news/the-state-of-smart-contract-upgrades

REKT. (2022, May 1). *Fei Rari - REKT 2*. https://rekt.news/fei-rari-rekt

Siegel, D. (2023, January 13). *Understanding the DAO attack*. CoinDesk. https://www.coindesk.com/learn/understanding-the-dao-attack

Solidity Authors. (n.d.). *Security considerations*. *Solidity documentation*. https://docs.soliditylang.org/en/latest/security-considerations.html#re-entrancy

Vyperlang Team. (2023, August 5). *Vyper nonreentrancy lock vulnerability technical post-mortem report*. HackMD. https://hackmd.io/@vyperlang/HJUgNMhs2

World Economic Forum. (2025, May 23). *Asset tokenization in financial markets: The next generation of value exchange* [Insight report]. https://reports.weforum.org/docs/WEF_Asset_Tokenization_in_Financial_Markets_2025.pdf

XStocks. (n.d.). *Products*. https://xstocks.fi/products

Received: 02.04.26 / Revised: 17.04.26 / Accepted: 04.05.26 / Published: 30.06.26