

ASSESSMENT OF THE RISKS OF USING SMART CONTRACTS IN CRYPTOCURRENCY TRANSACTIONS ON DOMESTIC CAPITAL MARKETS

OLEKSII MOSTOVENKO¹, VOLODYMYR TSAP², VOLODYMYR BORKOVYCH³,
NATALIIA RUDYK⁴, VIACHESLAV NYKONENKO⁵

¹Candidate of Economic Sciences, Associate Professor, Department of Economic Theory of Accounting and Taxation, Construction Faculty, Kyiv National University of Construction and Architecture, Ukraine

²Candidate of Economic Sciences, Associate Professor, Finance, Accounting and Taxation Department, Faculty of Economics and Business, Dmytro Motornyi Tavria State Agrotechnological University, Ukraine

³PhD Student, Finance, Accounting and Taxation Department, Faculty of Economics and Business, Dmytro Motornyi Tavria State Agrotechnological University, Ukraine

⁴Candidate of Economic Sciences, Associate Professor, Department of Finance named after Victor Fedosov, Faculty of Finance, Kyiv National Economic University named after Vadym Hetman, Ukraine

⁵PhD student, Department of International Economic Relations, Business and Tourism, Faculty of Law and International Relations, State University "Kyiv Aviation Institute", Ukraine

E-mail: ¹omostovenko@gmail.com, ²sosnaalexandru@gmail.com, ³volborkovych@gmail.com,
⁴natrudyk@gmail.com, ⁵nykonenkonik@gmail.com

ABSTRACT

The study's relevance is determined by the critical dependence of cryptocurrency market stability on the technical reliability of smart contracts and the increasing risks of financial losses due to their defects. *Aim: The aim of the study* is to formalize the ranking of technical vulnerabilities of smart contracts by their impact on the economic stability of domestic capital markets through systematization, simulation modelling, and quantitative assessment of financial indicators. *Methods:* The research used the following *techniques:* vulnerability typing, simulation modelling, financial analytics, and comparative analysis. *Obtained results:* The study confirmed the critical impact of smart contract technical vulnerabilities on the financial stability of the markets, with peak VaR of up to -68.5% and liquidity deterioration of over -80% for reentrancy attack, delegatecall injection, and oracle manipulation. The risks were reduced by more than half after implementing multi-level optimisations, demonstrating the effectiveness of comprehensive mitigation to stabilise key financial indicators. *Academic novelty of the study:* *The academic novelty of the study* is the formalized classification of technical vulnerabilities of smart contracts and the first empirical assessment of their impact on the economic stability of capital markets based on comprehensive financial and economic metrics, which extends the theory of DeFi structural risks. *Prospects for future research:* *Prospects for further research* include the development of a pilot project for technical optimization of smart contracts with a focus on increasing resilience to logical and synchronization defects.

Keywords: *Economic Growth, Reentrancy, Delegatecall Injection, Oracle Manipulation, Integer Overflow, Front-Running, Dos Attacks*

1. INTRODUCTION

Current financial ecosystems are actively implementing blockchain infrastructure and smart contracts, which provide decentralized management of digital assets, automate the execution of transactions, and increase the transparency of transaction processes [1]. At the same time, the emergence of autonomous programmable contracts

creates a new risk paradigm that is significantly different from classic financial threats [2]. In particular, the specifics of the architecture of smart contracts imply technical vulnerabilities that can initiate financial failures through logical errors, state races, manipulation of the order of transactions, or compromise of external oracles [3].

These vulnerabilities become systemically important in the context of digitalization of capital

markets, as the interrelation of software defects, as well as financial and economic consequences can lead to large-scale prolonged crises. Increased asset volatility, deterioration of liquidity, growth in transaction costs and the risk of financial losses create the need for in-depth analysis of risk patterns and the search for effective mitigation strategies. This makes the study of technical risks of smart contracts as a key factor in the stability of domestic capital markets relevant.

The aim of the study is to formalize the ranking of technical vulnerabilities of smart contracts by the level of impact on the economic stability of domestic capital markets through their systematization, simulation modelling of activation scenarios, and quantitative assessment of financial and economic indicators to determine priority areas of technical mitigation.

Research objectives:

1. Typify technical vulnerabilities of smart contracts by risk classes and activation mechanisms.
2. Perform simulation modelling of vulnerability activation scenarios in Hardhat with case replications (DAO, Parity, etc.).
3. Perform financial analytics of key metrics (volatility, VaR, liquidity, Gas Fee Impact, failure rate).
4. Conduct comparative analysis to assess the effectiveness of optimization measures.

2. LITERATURE REVIEW

The results of assessing the risks of using smart contracts in cryptocurrency transactions in domestic capital markets are considered below. The authors [4] studied the risk profile of smart contracts in Smart Sukuk, emphasizing the reduction of operational costs and technical risks through the automation of tokenization. The authors focused on regulatory barriers and jurisdictional fragmentation, which caused legal uncertainty and affected the liquidity of domestic capital markets.

Other aspects of the studied vector are highlighted by the researchers [5], who analysed the systemic risks of DeFi protocols, emphasizing the vulnerabilities of smart contracts, liquidity shocks and regulatory arbitrage as threats to the stability of domestic markets. The authors identified stress testing, risk management models and real-time compliance as strategies to minimize financial contagion.

In turn, the author [6] analysed the legal risks of smart contracts and tokenized assets, emphasizing the fragmentation of regulatory regimes and the

challenges of arbitration settlement. The author noted the difficulty of integrating smart contracts with international arbitration caused by technical and jurisdictional conflicts. In contrast, the researchers [7] studied the synergy of blockchain and smart contracts, revealing the reduction of risks of fraud, money laundering, and data leakage through cryptographic protection. The authors emphasized the automation of compliance, reduction of costs and increased transparency as key factors in minimizing risks.

The author [8] disagrees with the benefits of blockchain, having examined the risks of integrating cryptocurrencies into the financial systems of Switzerland and El Salvador, focusing on the impact of regulatory regimes and technological architectures on domestic market stability. The author analysed the political and economic challenges associated with the implementation of smart contracts and tokenized assets, emphasizing the risks of legal fragmentation, liquidity, and interoperability in local cryptocurrency transactions. The researchers [9] share a similar view, having examined the risks of integrating cryptoassets into the financial system, emphasizing their high volatility and limited monetary functionality as factors of market instability. The authors analysed the threats of decentralized finance to regulatory control and outlined the risks of financial contagion, which increase the systemic vulnerability of domestic capital markets.

The author [10] adheres to a similarly cautious approach, examining the impact of smart contracts and blockchain on financial systems, focusing on the risks of volatility and cyberthreats. He analyses the role of AI and quantum technologies in scaling blockchains, and notes the threats of cryptographic compromise to domestic capital markets.

The author [11] drew ambiguous conclusions, having examined the legal aspects of smart contracts and the use of blockchain in FinTech, emphasizing its role in increasing transparency, asset verification, and reducing transaction costs. The author outlined the regulatory challenges of implementing smart contracts, which create legal uncertainty risks for domestic capital markets.

The researchers [12] identified regulatory issues and analysed the legal risks of smart contracts, revealing problems related to regulatory uncertainty, enforcement, and dispute resolution. The authors emphasized the challenges of encoding the parties' intentions, blockchain anonymity, and limited legal liability as key risk factors for domestic crypto transactions.

The authors [13] recognised the technological advantage of implementing smart contracts and investigated the implementation of zkAML, a zk-SNARK-based cryptographic framework for AML/CFT compliance that provides proof of regulatory compliance without disclosing PII. The authors demonstrated increased blockchain throughput (up to 324 TPS) and minimized latency, emphasizing the effectiveness of the zero-knowledge approach in reducing privacy risks and transaction costs in internal crypto transactions.

The reviewed studies confirm that smart contracts demonstrate significant technical advantages, including automation of obligation fulfilment, increased transaction transparency, cryptographic protection, and a reduction in the role of intermediaries, which contributes to the optimization of financial operations and increased efficiency of internal cryptocurrency transactions.

At the same time, the studies indicate significant risks associated with regulatory fragmentation, jurisdictional conflicts, asset volatility, legal uncertainty of smart contracts, and enforcement challenges, which necessitate the need for comprehensive risk management to ensure the stability of domestic capital markets. Accordingly, an appropriate direction of research is to assess the impact of risks of technical vulnerabilities of smart contracts on the economic stability of domestic capital markets.

3. METHODS AND MATERIALS

3.1. Research design

The procedure of the current study is illustrated in (**Error! Reference source not found.**).

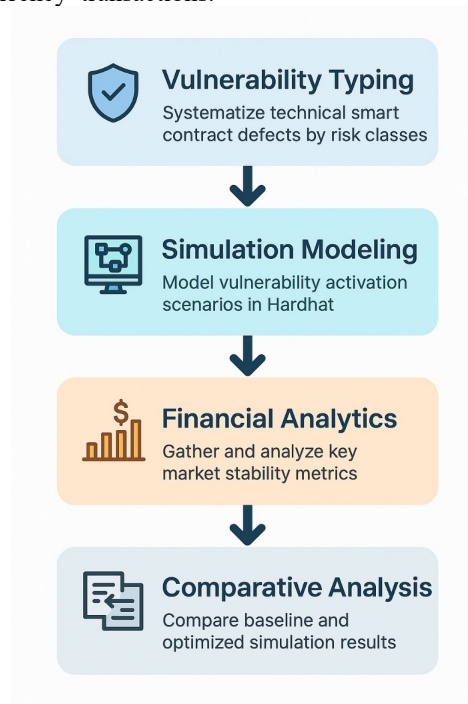


Figure 1: Research design

Source: created by the authors

3.2. Methods

The following methods were developed and used in the study:

1. Vulnerability typing. The risk classes systematised technical defects of smart contracts to classify the main mechanisms of their activation (Table 2).

2. Simulation modelling. Simulation of vulnerability activation scenarios was performed in the Hardhat environment with realistic case replications (DAO, Parity, etc.) to assess the impact on financial metrics.

3. Financial analytics. Key metrics (volatility, VaR, liquidity, Gas Fee Impact, failure rate) were

collected and analyzed to assess the economic stability of the market quantitatively.

4. Comparative analysis. The results of basic simulations and repeated modelling after implementing optimizations were compared to determine the effectiveness of mitigation measures. The methods used allowed for verifying risks and

developing optimisation strategies to increase the stability of smart contracts.

3.3. Sample

The sample of our study consists of currently known technical vulnerabilities of smart contracts – **Error! Reference source not found..**

Table 1: Technical Vulnerabilities of Smart Contracts: Activation Mechanisms, Techno-Economic Consequences

Item No.	Vulnerability	Brief description of mechanism	Activation cases (year)	Technical consequences	Economic consequences	Research references
1	Reentrancy attack	Incorrect contract state management allows the function to be called again before the first execution cycle is complete.	DAO hack (2016), Lendf.Me (2020)	Infinite execution loop, atomicity violation, complete balance compromise	Contract exploitation, massive loss of assets (~\$60 million DAO)	Ajibola, Adeniran & Taiwo (2025) [14]
2	Integer overflow/underflow	Arithmetic overflows because of lack of SafeMath.	BatchOverflow (2018), BeautyChain (2018)	Incorrect calculations, integer wraparound, accounting logic violation	Token depreciation, uncontrolled emission	Huang, Zeng & Shang (2024) [15]
3	Timestamp dependency	Dependency of business logic on manipulated environment parameters (block.timestamp).	FairWin (2019)	Vulnerability to attacks from miners (timestamp manipulation), fairness violation	Manipulation of results, losses of participants	Ghosh, Srivastava, Upadhyaya, Halder & Chandra (2025) [16]
4	DoS (Gas Limit)	Contract functions consume gas beyond the block gas limit, causing DoS.	GovernMental (2016)	Denial of service, blocking of critical functions	Asset stagnation, temporary inoperability of the protocol	De Lima Cabral, Antonino & Sampaio (2025) [17]
5	DoS with contract blocking	Blocking the contract logic through specially created conditions that provoke a failure.	King of Ether (2017)	Smart auction logic blocking, contract lockup	Transaction failure, economic losses to participants	Zhang et al. (2025) [18]
6	Front-running (Transaction Ordering Dependency)	The attacker executes the transaction before the victim, using the mempool and a higher gas fee.	Uniswap (2020+), MEV exploits	Transaction order violation (non-determinism), market manipulation	Trader losses, price distortion	Zhang, Wang, Li, Gu & Chen (2025) [19]
7	Lack of Randomness	Using predictable sources of randomness (blockhash, timestamp).	Fomo3D (2018)	Low entropy sources, predictable random outcomes	Bots' predicted profits, financial injustice	Puoti, Pittorino & Roveri (2024) [20]
8	Delegatecall injection	Abuse of the delegatecall function enables modifying the storage calling contract.	Parity Wallet Hack (2017)	Call context state change, full takeover attack	Frozen funds (~\$150 million ETH), loss of trust	Iuliano, Allocca, Cicalese & Di Nucci (2025) [21]
9	Unchecked external call failures	Calls to external contracts without proper error handling (Low-level call).	Rubixi (2016)	Silent failures, inconsistency of state	Transaction failures, funds freeze	Gou, Zhao, Wang, Zhang & Yang (2024) [22]

Item No.	Vulnerability	Brief description of mechanism	Activation cases (year)	Technical consequences	Economic consequences	Research references
10	Lack of emergency stop (Fail-safe)	Lack of an emergency mechanism to isolate or stop the contract during an attack.	Many cases (2016–2023)	Inability to respond promptly, protracted attacks	Escalation of losses, response delays	Tarhouni & Chaabane (2025) [23]
11	Oracle manipulation	Compromise of the oracle or use of unstable third-party data.	bZx (2020), Mango Markets (2022)	Poisoned data feeds, manipulation of price oracles	Over/undervaluation, financial losses over \$100 million	Gao, Wang, Wei, Liu, Goh & Lo (2025) [24]
12	Access Control Flaw	Lack of strict role validation (admin, owner), which allows exploitation of functions.	EasyFi (2021), Rubixi (2016)	Privilege escalation, unauthorized state change	Theft of funds (~\$80 million EasyFi), breach of trust	Wijesekara (2024) [25]
13	Storage collision	Data storage collision between proxy and logical contract because of incorrect memory alignment.	Known problems EIP-1967 (2020+)	Data corruption, unpredictable behaviour	Contract execution failures after upgrade	Ruaro et al. (2024) [26]
14	Block gas limit vulnerability	Bulk transactions exceed the maximum block size (block gas limit).	CryptoKitties (2017), DeFi	Partial execution failure, functional blocking of mass transactions	Freezing of transfers, losses caused by unavailability of services	de Lima Cabral, Antonino & Sampaio (2025) [17]

Source: created by the authors

3.4. Instruments

The following set of key financial and economic metrics is used to assess the impact of technical vulnerabilities in smart contracts on the economic sustainability of domestic capital markets:

1. *Asset Volatility* (σ) — a measure of the price fluctuations of tokens associated with smart contracts. High volatility indicates market instability, exacerbated by technical failures of contracts:

$$\sigma = \sqrt{\frac{1}{N-1} \sum_{t=1}^N (r_t - \bar{r})^2}, \quad (1)$$

where r_t — return in the period t ; $\bar{r}$ — average return.

Accordingly, the increase in the token volatility after its use:

$$\Delta\sigma = \sigma_{\text{post-event}} - \sigma_{\text{pre-event}}. \quad (2)$$

2. *Value at Risk (VaR)* — determination of the maximum expected loss at a level of confidence. Important for assessing potential losses because of smart contract risks:

$$VaR_\alpha = \mu - z_\alpha \times \sigma, \quad (3)$$

where μ — expected return; z_α — quantile of the normal distribution.

3. *Liquidity Ratio (LR)* — assessing the market liquidity of tokens managed by smart contracts. Contract failures can dramatically reduce liquidity (LR↓):

$$LR = \frac{V_t}{O_t}, \quad (4)$$

where V_t — trading volume for the period t ; O_t — average volume of open positions.

4. *Liquidity Coverage Ratio (LCR)* — analysis of the market's ability to withstand crisis scenarios (for example, mass exit of participants because of contract failures):

$$LCR = \frac{\text{High Quality Liquid Assets (HQLA)}}{\text{Net Cash Outflows over 30 days}}. \quad (5)$$

Accordingly, the decrease in the Liquidity Ratio at the time of an attack on smart contracts:

$$\Delta LR = LR_{\text{before}} - LR_{\text{after}}. \quad (6)$$

5. *Gas Fee Impact (GFI)* — measuring the share of transaction costs in the total volume of transactions, which increases during contract overload or DoS attacks:

$$GFI = \frac{\sum_{i=1}^N Gas_i \times GasPrice_i}{V_t} \quad (7)$$

6. *Risk-Adjusted Return (RAR)* – identifying the effectiveness of assets managed by smart contracts, taking into account their risk profile:

$$RAR = \frac{\bar{R} - R_f}{\sigma} \quad (8)$$

where $\bar{R}$ – average asset return; R_f – risk-free rate.

7. *Market Resilience Index (MRI)* – assessing the speed of liquidity recovery after risk events (e.g., realization of smart contract vulnerabilities):

$$MRI = \frac{\Delta V_t^{\text{post-shock}}}{\Delta V_t^{\text{pre-shock}}} \quad (9)$$

8. *Failure Rate (FR)* – measuring the proportion of failed transactions in the total volume - a key indicator of the technical reliability of contracts:

$$FR = \frac{F_{\text{failed tx}}}{F_{\text{total tx}}} \quad (10)$$

9. *Recovery Time (RT)* – measuring the time from the moment of attack to the full restoration of liquidity and stability:

$$RT = t_{\text{stabilization}} - t_{\text{attack}} \quad (11)$$

The defined metrics allow for a comprehensive combination of the technical state of smart contracts with macro- and microeconomic parameters, which forms a holistic picture of the impact on economic stability in domestic capital markets.

The Hardhat platform [27] is used as a simulation environment for modelling technical vulnerabilities of smart contracts and the corresponding economic consequences by calculating the above metrics. Hardhat is a framework for compiling, deploying, unit testing and debugging smart contracts in a virtual EVM environment. It integrates the Ethers.js and Waffle modules for low-level transactions, supports mainnet fork, gas consumption simulation, and automated fuzz tests. It provides granular control over the blockchain state, manipulation of chain parameters (block.timestamp, gasLimit), and call stack tracing for audits and security analysis of contracts.

Simulation of smart contract vulnerability in Hardhat included deployment of target contract and exploit contract, attack initialization via low-level calldata and EVM state manipulation (snapshots, reverts). The monitoring was performed by tracing transactions, logging gas consumption, tracking changes in storage and contract balance. Financial and economic metrics were measured by collecting data on failure rate, token price volatility (through integration with off-chain API), liquidity (transaction volume), gas fee impact and recovery time (RT), which enabled creating empirical risk profiles of smart contracts.

4. RESULTS

The known technical vulnerabilities of smart contracts (Table 1) were ranked by the level of impact on the economic stability of domestic capital markets through the investigation and systematization of the mechanisms of their activation — Table 2.

Table 2: Typing of Known Technical Vulnerabilities of Smart Contracts

Vulnerability class	Vulnerability Mechanism Class	Vulnerability Type	Vulnerability Mechanism Type
Logic & Synchronization Flaws	Atomicity Violation, State Race, Logic Blocking	Reentrancy	Race Condition / Improper State Synchronization
		DoS with contract blocking	Logic Blocking) / Execution Condition Abuse
		Lack of emergency stop (Fail-safe)	Fail-safe Deficiency / Lack of kill-switch
Arithmetic & Computation Flaws	Incorrect handling of numeric values, no range restrictions	Integer overflow/underflow	Integer Arithmetic Flaw / Lack of range checks
External Environment Dependency	Using uncontrolled blockchain parameters	Timestamp dependency	Environment Manipulation / External dependency
		Lack of Randomness	Weak Randomness / Lack of randomness
Transaction Manipulation	Using mempool and transaction ordering mechanism	Front-running (Transaction Ordering Dependency)	Transaction-Ordering Dependency / MEV use
Delegatecall & Proxy Flaws	Execution context change,	Delegatecall injection	Delegatecall Hijacking /

Vulnerability class	Vulnerability Mechanism Class	Vulnerability Type	Vulnerability Mechanism Type
	memory conflict		Changing the execution context
		Storage collision	Storage Collision / Memory Alignment Flaw in proxy patterns
Resource & DoS Vulnerabilities	Gas exhaustion, mass execution	DoS (Gas Limit)	Resource Exhaustion / Gas limit restrictions
		Block gas limit vulnerability	Block Gas Limit Bottleneck / Batch Processing Flaw
Oracle & External Data Attacks	Data compromise, price oracle manipulation	Oracle manipulation	Oracle Poisoning / Unreliable price feeds
Access & Privilege Flaws	Incorrect access rights validation	Access Control Flaw	Access Control Misconfiguration / Privileged escalation
Unhandled External Calls	Lack of proper error handling	Unchecked external call failures	Unhandled Exception / Low-level call failure

Source: created by the authors

The typing of technical vulnerabilities of smart contracts (Table 2) systematically classified key risk mechanisms — from race condition and arithmetic flaw to oracle poisoning and access misconfiguration, which comprehensively affect the economic stability of domestic capital markets. It was found that these vulnerabilities determined a multidirectional impact on key economic indicators, in particular market liquidity, asset volatility, failure rate and gas efficiency of contracts. The degree of

risk was assessed through a simulation of each vulnerability carried out in the Hardhat environment (realistic scenario modelling based on known cases was used (DAO, Parity, bZx, MEV, etc.) according to the algorithm (1) – (11)) with a targeted collection of financial and economic metrics, which provided empirical verification of their impact on the economic stability of domestic capital markets – Table 3.

Table 3: Results of Simulation of Known Vulnerabilities of Smart Contracts in the Hardhat Environment Characterized by Financial and Economic Metrics (1) – (11) with Ranking by the Level of Impact on the Economic Stability of Domestic Capital Markets (from the Most Destructive)

Item No.	Vulnerability	$\sigma\uparrow$ (%)	VaR (95%) (%)	LR $\downarrow$ (%)	LCR $\downarrow$ (%)	GFI $\uparrow$ (%)	RAR $\downarrow$ (%)	MRI (h)	FR (%)	RT (h)
1	Reentrancy attack	+75.4	-68.5	-82.3	-77.1	+24.7	-65.9	48	92.5	72
2	Delegatecall injection	+72.1	-65.3	-78.9	-74.5	+22.9	-63.8	52	89.4	69
3	Oracle manipulation	+68.7	-62.5	-81.2	-76.9	+16.3	-61.7	36	65.3	54
4	Access Control Flaw	+66.5	-60.9	-74.4	-70.2	+14.8	-59.1	44	87.0	65
5	Integer overflow/underflow	+52.3	-48.7	-60.2	-57.5	+21.1	-47.6	28	74.5	42
6	Front-running (Transaction Ordering Dependency)	+49.8	-46.2	-58.3	-54.7	+31.5	-45.0	18	63.8	30
7	Storage collision	+43.5	-39.8	-49.5	-45.2	+19.6	-38.2	22	52.1	34
8	Timestamp dependency	+28.4	-24.1	-35.8	-33.0	+12.5	-20.6	15	36.2	18
9	DoS with contract blocking	+21.7	-18.9	-45.1	-40.2	+44.2	-17.9	12	82.4	10
10	DoS (Gas Limit)	+19.3	-16.7	-41.7	-38.5	+47.5	-15.4	9	85.7	8
11	Lack of emergency stop (Fail-safe)	+24.5	-22.2	-37.3	-34.9	+28.4	-21.0	18	54.3	20
12	Lack of Randomness	+13.8	-11.5	-22.1	-18.6	+8.9	-10.4	6	27.8	7
13	Unchecked external call failures	+15.4	-13.2	-25.4	-21.3	+12.0	-12.6	10	33.7	12
14	Block gas limit vulnerability	+17.1	-14.8	-33.5	-29.7	+39.6	-14.0	8	78.5	9

The results of empirical simulation in Hardhat showed that such vulnerabilities as Lack of Randomness and Unchecked calls were the least influential for the economic stability of domestic markets were (VaR up to -13.2%, failure rate ~30%), while medium-risk categories, including DoS attacks and Timestamp dependency, caused an increase in volatility up to +28.4% and a significant increase in Gas Fee Impact (+47.5%). Integer overflow and Front-running turned out to be more critical (VaR ~ -48.7%, liquidity -58%), however,

the maximum destabilizing effect was recorded for reentrancy attacks, delegatecall injection, and oracle manipulation (VaR up to -68.5%, liquidity decline over 80%, failure rate >89%), which caused a prolonged market recovery (up to 72 hours) and demonstrated the systemic nature of these risks, which require priority mitigation.

The following the measures to reduce the risks of technical vulnerabilities of smart contracts in cryptocurrency transactions on domestic capital markets are considered – Table 4.

Table 4: Optimization Solutions to Eliminate Technical Vulnerabilities of Smart Contracts in Cryptocurrency Transactions on Domestic Capital Markets

Item No.	Vulnerability	Optimization solutions
1	Reentrancy attack	Implementation of the Checks-Effects-Interactions pattern; use of ReentrancyGuard to block repeated calls; transition to pull payments instead of direct transfer of funds; performance of static analysis (Slither, MythX) to detect recursive cycles; implementation of state machine design for clear synchronization of states.
2	Delegatecall injection	Use of strict access controls to limit delegatecall; compliance with EIP-1967/UUPS proxy standards for isolation of memory slots; formal verification of ABI compatibility; prohibition of delegatecall to external unverified addresses; implementation of failover mechanisms in case of inconsistency of logical contracts.
3	Oracle manipulation	Integration of decentralized oracles (Chainlink OCR); implementation of price deviation limits to limit sudden changes; multi-channel data confirmation (multi-source oracles); application of cryptographic evidence of data integrity (Merkle proofs); implementation of time-weighted average price (TWAP) models to smooth out manipulations.
4	Access Control Flaw	Use of RBAC (Role-Based Access Control); mandatory integration of Ownable/AccessControl libraries (OpenZeppelin); multi-level role validation via multi-sig authentication; audit of critical functions using Slither and Oyente; on-chain audit trail logging for transparency of administrator actions.
5	Integer overflow/underflow	Using SafeMath libraries (built into Solidity >=0.8); using formal verification of arithmetic expressions; boundary testing; auditing using Mythril and Securify to detect dangerous arithmetic patterns; checking all arithmetic calculations for compliance with expected ranges.
6	Front-running (Transaction Ordering Dependency)	Implementation of commit-reveal schemes for auctions/lotteries; use of pre-signature mechanisms; integration of Fair Sequencing Services; use of private transactions via Flashbots/MEV-Resistant protocols; provision of randomized delays to reduce predictability of transaction execution.
7	Storage collision	Adherence to proxy patterns (EIP-1967, UUPS) for strict organization of memory slots; use of gap variables for slot reservation; formal verification of the architecture via Slither storage analyser; testing of updates via proxy upgrade simulation; mandatory isolation of logic and data storage.
8	Timestamp dependency	Minimizing dependence of business logic on block.timestamp; use of block.number for greater stability; integration of time buffers for increased tolerance; auditing using MythX to detect manipulated parameters; use of off-chain time oracle for critical scenarios.
9	DoS with contract blocking	Limiting the size of input arrays through input validation; using loop protection (circuit breakers); implementing gas-efficient algorithms (unchecked loops); introducing timeout policies for long-running executions; using try-catch constructs to protect critical calls.
10	DoS (Gas Limit)	Optimization of functions through batch processing; implementation of off-chain processing for large amounts of data; breaking long processes into small transaction blocks; automatic cancellation of transactions approaching the gas limit threshold; use of proxy patterns to delegate features.
11	Lack of emergency stop	Circuit Breaker Pattern implementation; use of pausable modifiers for urgent contract termination; integration of multi-sig confirmation to activate emergency mode; implementation

Item No.	Vulnerability	Optimization solutions
	(Fail-safe)	of automatic triggers when abnormal events are detected (for example, abnormal volatility); constant audit of failover mechanisms.
12	Lack of Randomness	Using Chainlink VRF (Verifiable Random Function); implementing off-chain randomness generation with cryptographic verification; using commit-reveal schemes to improve entropy; auditing sources of randomness for low-entropy patterns; integrating entropy oracle fallback for critical cases.
13	Unchecked external call failures	Ensuring error propagation through require/assert checks; using try-catch blocks for low-level calls; implementing a fallback error handling mechanism; auditing using Slither (external calls check); introducing mandatory checks after each external call.
14	Block gas limit vulnerability	Limiting mass transactions by implementing hard limits; using off-chain aggregation to reduce on-chain load; introducing staggered execution; using dynamic gas management for adaptive control; auditing bulk transactions through gas consumption profiling.

Source: created by the authors

The proposed set of optimization solutions (Table 4) demonstrates a holistic multi-level risk reduction strategy that combines static and dynamic code analysis, the use of standards (EIP/UUPS), cryptographic protocols (VRF, Merkle proofs), protection against DoS attacks (loop breakers, gas optimization), as well as formal verification and

multi-channel orchestrations, which ensures increased stability of smart contracts in cryptocurrency transactions on domestic capital markets. The feasibility was empirically confirmed through a repeated simulation calculation of the specified metrics (1) – (11) in the Hardhat environment – Table 5.

Table 5: Results of Repeated Simulation of Known Vulnerabilities of Smart Contracts in the Hardhat Environment After the Implementation of Optimization Solutions

Item No.	Vulnerability	$\sigma\uparrow$ (%)	VaR (95%) (%)	LR $\downarrow$ (%)	LCR $\downarrow$ (%)	GFI $\uparrow$ (%)	RAR $\downarrow$ (%)	MRI (h)	FR (%)	RT (h)
1	Reentrancy attack	+28.9	-24.7	-31.2	-29.5	+10.3	-22.1	18	34.8	20
2	Delegatecall injection	+26.5	-22.4	-28.5	-26.1	+9.6	-20.8	20	30.1	18
3	Oracle manipulation	+24.2	-20.3	-30.7	-27.8	+7.9	-19.5	14	23.7	16
4	Access Control Flaw	+23.1	-19.8	-25.9	-24.0	+7.4	-18.3	16	29.4	17
5	Integer overflow/underflow	+15.7	-13.4	-15.9	-14.7	+6.8	-12.5	10	19.2	12
6	Front-running (Transaction Ordering Dependency)	+14.3	-12.6	-14.8	-13.9	+12.1	-11.2	7	16.7	9
7	Storage collision	+12.5	-10.8	-12.4	-11.3	+6.2	-9.6	8	14.2	10
8	Timestamp dependency	+8.7	-6.9	-8.5	-7.4	+3.8	-5.7	5	10.8	6
9	DoS with contract blocking	+6.9	-5.8	-10.2	-9.1	+16.2	-4.9	4	24.1	5
10	DoS (Gas Limit)	+6.1	-5.2	-8.9	-7.8	+17.5	-4.2	3	25.3	4
11	Lack of emergency stop (Fail-safe)	+7.5	-6.4	-9.5	-8.2	+10.8	-5.0	6	15.6	7
12	Lack of Randomness	+4.3	-3.7	-4.5	-3.8	+3.2	-2.9	2	6.8	3
13	Unchecked external call failures	+5.1	-4.2	-5.8	-4.9	+4.5	-3.6	3	8.4	4
14	Block gas limit vulnerability	+5.8	-5.0	-7.1	-6.2	+13.1	-4.0	3	20.3	4

Source: created by the authors based on simulations in Hardhat [27]

Comparative analysis of simulation results (Table 3 vs Table 5) showed a significant reduction in risk after the implementation of optimization solutions.

The most critical defects – Reentrancy Attack, Delegatecall Injection and Oracle Manipulation – demonstrated decreased asset volatility from

+75.4%, +72.1% and +68.7% to +28.9%, +26.5% and +24.2% respectively, and VaR decreased almost threefold (from -68.5% to -24.7% for reentrancy attack). Liquidity (LR) and coverage ratios (LCR) improved almost 2.5–3 times, and failure rate decreased from >90% to ~30%. The effect was even more noticeable for less risky vulnerabilities, such as Lack of Randomness and Unchecked External Call Failures — volatility fell below 5%, and market recovery was reduced to 2–4 hours. The reduction in Gas Fee Impact in DoS vulnerabilities was especially noticeable (for example, DoS (Gas Limit) from +47.5% to +17.5%). Overall, the optimization measures demonstrated high effectiveness, reducing the systemic vulnerability of smart contracts and improving all key financial and economic metrics, which is critically important for the stability of domestic capital markets.

5. DISCUSSION

Therefore, based on the results of the study, the following thesis is put forward for discussion: optimization measures have proven effective in reducing the risk of smart contracts, providing a more than twofold reduction in financial losses and recovery time, while logical and synchronization defects remain the most critical with high atomic instability and attacks due to a change in the execution context. The obtained conclusions will be compared with the specialized scientometric horizon.

Unlike the authors [28], which focused on reducing counterparty risks of derivatives, this study demonstrated the systemic impact of logical and synchronization defects of smart contracts on market stability. Both approaches recognize the benefits of decentralization, but modelling confirmed the key role of technical vulnerabilities in prolonged crisis effects.

The authors [29] focused on the technical analysis of key vulnerabilities in smart contracts (reentrancy attacks and arithmetic defects) with attack modelling and countermeasure evaluation. In contrast, this study comprehensively covers the impact of different classes of defects on financial and economic metrics, highlighting the critical role of logical and timing vulnerabilities in prolonged market destabilization.

The researcher [30] performed an in-depth audit of smart contracts with a focus on identifying and neutralizing defects at the code level (code-level vulnerability mitigation). Our study demonstrates that even with the implementation of formal verification and optimization methods, logical and

timing anomalies remain critical triggers of financial and economic destabilization in domestic capital markets.

The authors [31] proposed CrossGuard for dynamic control flow whitelisting in DeFi, which reduces technical risks. However, our study proves that even such mechanisms do not neutralize the prolonged destabilization caused by synchronization defects and systemic economic consequences.

The researchers [32] developed the concept of ICT/ICE as a decentralized insurance architecture to compensate for losses in crypto transactions with low on-chain costs. In comparison, the results of our study indicate that technical defects of smart contracts remain a fundamental source of systemic destabilization, which cannot be eliminated even by insurance protocols.

The authors [33] identified three drivers of the crypto market: the stability of exchange rates in the darknet, speculative strategies of newcomers, and the impact of the Central Bank Digital Currency (CBDC). Instead, our study focuses on technical defects in smart contracts as key triggers of prolonged financial destabilization, regardless of macroeconomic factors.

The author [34] revealed the impact of blockchain on the securities trading infrastructure through increased transparency and risk management. Our study, however, states that technical flaws in smart contracts are key triggers for financial destabilization in domestic markets.

The researcher [35] analysed the role of hype, speculative trading, and fraudulent schemes as key destabilizers of the crypto market, emphasizing the need for strict regulation. At the same time, our study provides that, regardless of behavioural factors, the technical vulnerabilities of smart contracts are fundamental triggers for market failures.

The authors [36] examined the integration of blockchain, ML, IoT, and AI to transform the insurance sector, outlining the prospects of smart contracts for automation and trust. Our study, however, proves that the technical defects of smart contracts are a key trigger for financial destabilization, regardless of the level of digitalization of the industry.

The scientist [37] optimized the financial platform through the integration of blockchain and Big Data, eliminating centralized risks and increasing efficiency. Our study found that technical vulnerabilities of smart contracts remain a critical source of financial destabilization even in the case of structural modernization.

Summarizing the results of the discussion analysis, it was found that despite significant researchers' attention to architectural improvements, risk management and increased transparency of smart contracts, technical defects — in particular logical, synchronization and context-dependent vulnerabilities — are still the main trigger for prolonged financial and economic destabilization of domestic capital markets. This emphasizes the key role of technical audit and formal verification in strategies to increase the resilience of blockchain ecosystems, regardless of the general trends in the development of digital financial infrastructures.

5.1. LIMITATION

The study is limited to using simulation data in the Hardhat environment, which does not fully reproduce the full range of real-world market scenarios and behavioural anomalies. The validity of the results can be increased by conducting full-scale experiments involving on-chain data and empirical financial measurements in dynamic environments.

5.2. RECOMMENDATIONS

It is recommended to develop a pilot project on technical optimization of smart contracts, focused on implementing comprehensive measures to increase resilience to logical and synchronization defects. Further scaling of this project involves integration into large financial ecosystems for empirical validation of effectiveness and stress testing in real conditions.

6. CONCLUSIONS

The study confirmed the systemic impact of technical vulnerabilities in smart contracts on the economic stability of domestic capital markets. The most destructive defects — reentrancy attack, delegatecall injection and oracle manipulation — caused peak asset volatility at +75.4%, +72.1% and +68.7% respectively, with a critical liquidity drawdown of over -80% and VaR of up to -68.5%. Arithmetic and computational defects (Integer overflow/underflow) demonstrated a VaR of -48.7% and a failure rate of 74.5%, while DoS attacks reached a maximum Gas Fee Impact of +47.5%, indicating excessive consumption of computing resources. Such vulnerabilities as Lack of Randomness and Unchecked calls, with a VaR of -11.5...-13.2% and a failure rate of ~30% were the least influential.

Implementation of a multi-level optimization strategy (static analysis, ReentrancyGuard, VRF,

TWAP, loop protection) resulted in decreased key risk indicators by more than half: VaR for reentrancy attack decreased from -68.5% to -24.7%, liquidity increased from -82.3% to -31.2%, and failure rate decreased to 34.8%. For less risky categories (DoS (Gas Limit), Block gas limit vulnerability), volatility dropped to +5.8%, and recovery time decreased to 3–4 hours. The results prove that complex optimization can radically reduce the systemic vulnerability of smart contracts and stabilize the financial and economic indicators of domestic capital markets.

Academic novelty. A formalized classification of technical vulnerabilities of smart contracts was carried out and their impact on the economic stability of capital markets was empirically studied for the first time using complex financial metrics, which extends the theory of DeFi structural risks.

Practical significance of the obtained results. The priority of mitigating critical defects (reentrancy attack, delegatecall, oracle manipulation) was substantiated and an applied framework of optimization solutions was proposed to increase the stability of smart contracts and reduce systemic risks.

REFERENCES

- [1] U. Nikonenko, T. Shtets, A. Kalinin, I. Dorosh, & L. Sokolik, „Assessing the Policy of Attracting Investments in the Main Sectors of the Economy in the Context of Introducing Aspects of Industry 4.0”, *International Journal of Sustainable Development and Planning*, Vol. 17, No. 2, 2022, pp. 497–505. doi:10.18280/ijdsdp.170214
- [2] O. S. Oliynyk, R. M. Shestopalov, V. O. Zarosylo, M. I. Stankovic, & S. G. Golubitsky, “Economic Security through Criminal Policies”, *Revista Científica General José María Córdova*, Vol. 20, No. 38, 2022, pp. 265–285. doi:10.21830/19006586.899
- [3] J. Crisostomo, F. Bacao, & V. Lobo, “Machine Learning Methods for Detecting Smart Contracts Vulnerabilities within Ethereum Blockchain – A Review”, *Expert Systems With Applications*, Vol. 268, 2025, 126353. doi:10.1016/j.eswa.2024.126353
- [4] A. Delle Foglie, I. C. Panetta, E. Boukrami, & G. Vento, “The Impact of the Blockchain Technology on the Global Sukuk Industry: Smart Contracts and Asset Tokenisation”, *Technology Analysis & Strategic Management*, 2025, pp. 1–15. doi:10.1080/09537325.2021.1939000

- [5] U. Obiageli Ogbuonyalu, K. Abiodun, S. Dzamefe, E. N. Vera, A. Oyinlola, & I. Emmanuel, "Integrating Decentralized Finance Protocols with Systemic Risk Frameworks for Enhanced Capital Markets Stability and Regulatory Oversight", *International Journal of Innovative Science and Research Technology*, Vol. 10, No. 4, 2025, pp. 762–777. doi:10.38124/ijisrt/25apr1165
- [6] R. Walters, "Smart Contracts and International Commercial Arbitration", In: *Routledge handbook on transnational commercial law* (pp. 390–414). London: Routledge, 2025. doi:10.4324/9781003394822-25
- [7] O. Sopitan, K. S. Adetola, A. W. Morenikeji, J. A. Shonubi, & E. Uzoma, "Blockchain and Smart Contracts for Financial Transparency and Risk Mitigation in Banking and Business Transactions", *International Journal of Blockchains and Cryptocurrencies*, Vol. 1, No. 2, 2024, pp. 1–24. doi:10.34218/ijbc_01_02_001
- [8] G. Meneghelli, "The Political Impact of Cryptocurrencies on Emerging Markets", *SSRN 5182572*, 2025, URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5182572/ (date of access: 06.06.2025)
- [9] H. Joebges, H. Herr, & C. Kellermann, "Crypto Assets As a Threat to Financial Market Stability", *Eurasian Economic Review*, 2025, pp. 1-15. doi:10.1007/s40822-025-00311-4
- [10] S. Ramesh, "Cryptocurrencies", In: *The political economy of contemporary human civilisation*, Vol. II (pp. 93–140), Cham: Springer Nature Switzerland, 2025. doi:10.1007/978-3-031-84185-9_4
- [11] G. Amone, "Legal Aspects of Smart Contracts and Application of Blockchain Technology in Fintech", *Fintech for ESG and the Circular Economy*, 2025, pp. 173-191. doi: 10.1002/9781394234035.ch9
- [12] Ali Bukhtiar, Hafiz Abdul Rehman Saleem, Asif Iqbal, Muhammad Sohaib Younas & Atif Hassan, "Blockchain and Cryptocurrency (Legal Challenges in Implementing Smart Contracts)", *Research Journal of Psychology*, Vol. 3, No. 1, 2025, pp. 704–712. doi:10.59075/rjs.v3i1.101
- [13] D. Oh, S. Han, J. Kim, H. Oh, J. Chung, J. Lee, & T. wan Kim, "zkAML: Zero-Knowledge Anti Money Laundering in Smart Contracts with Whitelist Approach", *Cryptology ePrint Archive*, 2025.
- [14] T. E. Ajibola, O. T. Adeniran, & P. Taiwo, "SmartPattern: A Machine Learning Framework for Detecting Reentrancy Vulnerabilities in Blockchain Smart Contracts", *2025 59th annual conference on information sciences and systems (CISS)*, John Hopkins University (USA), March 19-21, 2025, pp. 1–6. doi:10.1109/ciss64860.2025.10944738
- [15] Q. Huang, Z. Zeng, & Y. Shang, (2024). "An Empirical Study of Integer Overflow Detection and False Positive Analysis in Smart Contracts", *BDIOT 2024: 2024 8th international conference on big data and internet of things*, ACM (USA), September 14-16, 2024, pp. 247-251. doi:10.1145/3697355.3697396
- [16] K. Ghosh, & S. Rai, "Changing Landscape in Insurance Sector", In *Sustainable business ecosystems and social perspectives* (p. 249–276), Hershey: IGI Global, 2025. doi:10.4018/979-8-3693-8437-4.ch012
- [17] D. R. de Lima Cabral, P. Antonino, & A. Sampaio, "Demystification and Near-perfect Estimation of Minimum Gas Limit and Gas Used for Ethereum Smart Contracts", *arXiv preprint arXiv:2501.04483*, 2025. doi: 10.48550/arXiv.2501.04483
- [18] J. Zhang, J. Chen, Y. Shen, T. Zhang, Y. Wang, T. Chen, Z. Chen, "When Crypto Fails: Demystifying Cryptographic Defects in Ethereum Smart Contracts", *IEEE Transactions on Software Engineering*, Vol. 99, 2025, pp. 1–17. doi:10.1109/tse.2025.3551776
- [19] Y. Zhang, G. Wang, P. Li, W. Gu, & H. Chen, "FRACE: Front-Running Attack Classification on Ethereum Using Ensemble Learning", *The Computer Journal*, 2025, pp. 1-15. doi:10.1093/comjnl/bxaf027
- [20] F. Puoti, F. Pittorino, & M. Roveri, "Quantifying Cryptocurrency Unpredictability: A Comprehensive Study of Complexity and Forecasting", *AIMLSystems 2024: The 4th international conference on AI-ML systems*, ACM (USA), October 8-11, 2024, pp. 1–8. doi:10.1145/3703412.3703420
- [21] G. Iuliano, L. Allocca, M. Cicalese, & D. Di Nucci, "Automated Vulnerability Injection in Solidity Smart Contracts: A Mutation-Based Approach for Benchmark Development", *arXiv preprint arXiv:2504.15948* 2025. doi: 10.48550/arXiv.2504.15948
- [22] N. Gou, X. Zhao, S. Wang, H. Zhang, & J. Yang, "FlawCheck: Detecting Smart Contract Vulnerabilities Based on Symbolic

- Execution”, *Security and Privacy*, Vol. 8, No. 2, 2024, p. 447. doi:10.1002/spy2.477
- [23] M. Tarhouni, & F. Chaabane, „An Advanced Secure Medical File-Sharing System Based on IPFS and Blockchain Technology”, In: *Using blockchain technology in healthcare settings* (pp. 190–205), Boca Raton: CRC Press, 2025. doi:10.1201/9781003483113-10
- [24] B. Gao, Y. Wang, Q. Wei, Y. Liu, R. S. M. Goh, & D. Lo, “Airaclex: Automated Detection of Price Oracle Manipulations via Ilm-driven Knowledge Mining and Prompt Generation”, *arXiv preprint arXiv:2502.06348*, 2025. doi: 10.48550/arXiv.2502.06348
- [25] P. A. D. S. N. Wijesekara, „A Literature Review on Access Control in Networking Employing Blockchain”, *Indonesian Journal of Computer Science*, Vol. 13, No. 1, 2024, pp. 734-768. doi:10.33022/ijcs.v13i1.3764
- [26] N. Ruaro, F. Gritti, R. McLaughlin, I. Grishchenko, C. Kruegel, & G. Vigna, “Not Your Type! Detecting Storage Collision Vulnerabilities in Ethereum Smart Contracts”, In: *Network and distributed system security symposium* (pp. 46-64), Reston, VA: Internet Society, 2024. doi:10.14722/ndss.2024.24713
- [27] Hardhat | Ethereum development environment for professionals by Nomic Foundation, 2025. URL: <https://hardhat.org/> (date of access: 06.06.2025).
- [28] H. Wang, J. Liu, & J. Zhao, “Blockchain Smart Contracts for Decentralized Matching of Counterparties and Automatic Settlement of Financial Derivatives”, *Blockchain: Research and Applications*, 2025, 100300. doi:10.1016/j.bcr.2025.100300
- [29] Y. Ding, H. Peng, & X. Li, “A Comprehensive Study of Exploitable Patterns in Smart Contracts: From Vulnerability to Defense”, *arXiv preprint arXiv:2504.21480*, 2025. doi:10.48550/arXiv.2504.21480
- [30] B. Zhao, “Towards A Secure Blockchain Ecosystem: Current Vulnerabilities and Future Directions in Smart Contract Security”, *ITM Web of Conferences*, Vol. 73, 2025, 03014. doi:10.1051/itmconf/20257303014
- [31] Z. Chen, S. M. Beillahi, P. Barahimi, C. Minwalla, H. Du, A. Veneris, & F. Long, “Secure Smart Contract with Control Flow Integrity”, *arXiv preprint arXiv:2504.05509*, 2025. doi:10.48550/arXiv.2504.05509
- [32] A. Abadi, A. Sarencheh, H. Skeoch, & T. Zacharias, „ICT: Insured Cryptocurrency Transactions”, *Cryptology ePrint Archive*, 2025. <https://eprint.iacr.org/2025/088>
- [33] A. Faccia, & A. Salman, “Cryptocurrencies and Cbdc: Investigating Stable Conversion Rates, Criminal Activity, and Regulatory Implications”, In: *Advances in science, technology & innovation* (pp. 31–45), Cham: Springer Nature Switzerland, 2025. doi:10.1007/978-3-031-81739-7_4
- [34] J. Wang, “Innovation and Application of Blockchain Technology in Securities Trading”, *Highlights in Business, Economics and Management*, Vol. 49, 2025, pp. 166-173. doi:10.54097/dp0ksy32
- [35] D. Krause, “The Dangers of Cryptocurrency Hype and Deregulation: Why Oversight Matters in the Digital Asset Economy”, *SSRN 5136389*, 2025, URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5136389 (date of access: 06.06.2025).
- [36] K. Ghosh, & S. Rai, “Changing Landscape in Insurance Sector”, In *Sustainable business ecosystems and social perspectives* (p. 249–276), Hershey: IGI Global, 2025. doi:10.4018/979-8-3693-8437-4.ch012
- [37] X. Zhou, “Blockchain+big Data: Smart Contract Design for Decentralized Financial Sharing Platform”, *Edelweiss Applied Science and Technology*, Vol. 9, No. 4, 2025, pp. 1942–1961. doi:10.55214/25768484.v9i4.6430