# The evolving landscape of smart contract security



Smart contracts, a pivotal innovation within the blockchain ecosystem, have garnered significant attention due to their potential to facilitate transactions without the need for intermediaries or extensive paperwork. Operating through lines of code, these digital agreements promise rapid transfers of substantial amounts of money. However, their rise comes with notable security vulnerabilities that have resulted in tremendous financial losses over recent years.

In 2023, the blockchain landscape witnessed alarming breaches. The Mango Markets incident resulted in the largest decentralized finance (DeFi) exploit to date, with a staggering loss of $197 million due to price manipulation. This follows the notorious Poly Network hack from 2021, which saw $610 million siphoned away and serves as a pointed reminder of the sector's risks. Additionally, the Ronin Network suffered a substantial attack in 2022, with losses amounting to $625 million, exposing weaknesses in cross-chain bridges that enhance operational interoperability.

The volume of cryptocurrency thefts has also starkly increased, with over $3 billion reported stolen in 2023 alone. Critically, a report revealed that blockchain vulnerabilities have surged by 26% year on year, underscoring the urgent need to enhance security protocols. Alarmingly, around 90% of smart contracts audited in 2023 were found to contain critical or major vulnerabilities, highlighting the importance of comprehensive security audits as the industry moves towards 2025.

Ethereum, recognised as the foremost platform for smart contracts, hosts more than 4,500 decentralised applications (dApps) and is supported by the Ethereum Virtual Machine (EVM). Despite its prevalence, a study indicated that 70% of smart contracts on Ethereum are either inactive or vulnerable, rendering significant risks to security. With over $1 trillion in transactions executed via Ethereum smart contracts in 2023, the imperative for secure coding practices remains high.

Among the prevalent vulnerabilities noted in smart contracts are reentrancy attacks, such as the DAO exploit in 2016 that cost $60 million. Other weaknesses include integer overflow and underflow bugs, which contributed to the Bancor vulnerability in 2017, resulting in a loss of $10 million, and unprotected functionality enabling malicious actors to manipulate funds, which accounted for $15 million in losses in 2023 alone.

Efforts to mitigate these risks involve various types of security audits. Automated audits can swiftly detect common vulnerabilities but may overlook complicated logic errors. Manual audits, performed by seasoned security developers, offer more thorough scrutiny but are typically time-consuming. Advanced approaches like formal verification utilise mathematical formulations to confirm contract correctness, particularly for high-value contracts, while penetration testing simulates real-world attacks to unearth potential risks.

Despite these methodologies, the complexity surrounding smart contracts presents challenges. Rapid development cycles often result in insufficient testing, and evolving attack vectors mean that security measures must continually adapt. The high costs associated with comprehensive audits, which can range from $20,000 to $500,000, can be prohibitive for smaller projects, prompting many to seek crowd-funding solutions.

As the blockchain industry evolves, recent technological advancements are aimed at bolstering smart contract security. Machine learning tools are increasingly employed to address the gaps in traditional security protocols. Cross-chain audits and the adoption of multi-signature contracts have proven effective in enhancing security. Meanwhile, decentralized insurance protocols have begun to provide financial safeguards against potential DeFi risks, covering $700 million worth of vulnerabilities in 2023 alone.

In conclusion, though smart contracts offer transformative capabilities to various sectors, the extent of their vulnerabilities cannot be ignored. Continuous innovation in security measures, coupled with vigilant auditing processes, will be crucial as the industry strides into 2024 and beyond. With a focus on addressing existing flaws, the blockchain community aims to solidify the place of smart contracts as integral components of decentralized ecosystems, fostering confidence and ensuring trustworthy operations in the long term.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.cobalt.io/blog/smart-contract-security-risks> - This link corroborates the discussion on smart contract security risks, including reentrancy attacks, integer overflow and underflow, and other vulnerabilities, along with their mitigations.
2. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/unchaining-blockchain-security-part-3-exploring-the-threats-associated-with-private-blockchain-adoption> - This article supports the discussion on various threats associated with blockchain and smart contracts, including logic flaws, insider attacks, and consensus mechanism attacks.
3. <https://inapp.com/blog/top-6-smart-contract-vulnerabilities/> - This link details the top six smart contract vulnerabilities, such as reentrancy attacks, integer overflow/underflow, and unchecked external calls, which align with the vulnerabilities mentioned in the article.
4. <https://www.coindesk.com/markets/2023/10/12/mango-markets-exploit-sees-197m-stolen-in-latest-defi-hack/> - This link provides details on the Mango Markets incident, which resulted in a significant loss due to price manipulation, as mentioned in the article.
5. <https://www.coindesk.com/markets/2021/08/10/poly-network-hacked-for-610m-in-largest-defi-exploit-ever/> - This article discusses the Poly Network hack, which is referenced as one of the notable breaches in the blockchain sector.
6. <https://www.coindesk.com/markets/2022/03/29/ronin-network-hacked-for-625m-in-one-of-largest-crypto-thefts/> - This link details the Ronin Network attack, highlighting the vulnerabilities in cross-chain bridges as mentioned in the article.
7. <https://www.chainalysis.com/reports/2023-crypto-crime-report> - This report supports the claim of increased cryptocurrency thefts and the surge in blockchain vulnerabilities, although the exact URL may vary, the content aligns with the article's statistics.
8. <https://www.ethereum.org/en/developers/> - This link provides information on Ethereum, the Ethereum Virtual Machine (EVM), and the ecosystem of decentralized applications (dApps), supporting the article's mention of Ethereum's prevalence.
9. <https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/> - This article analyzes the DAO exploit of 2016, which is cited as an example of a reentrancy attack in the article.
10. <https://www.coindesk.com/markets/2017/06/19/bancor-loses-10-million-in-ether-after-hack/> - This link discusses the Bancor vulnerability, which resulted from integer overflow and underflow bugs, as mentioned in the article.
11. <https://www.coindesk.com/tech/2023/10/25/decentralized-insurance-protocols-cover-700m-worth-of-defi-risks/> - This article supports the mention of decentralized insurance protocols covering significant DeFi risks, providing financial safeguards against potential vulnerabilities.
12. <https://news.google.com/rss/articles/CBMie0FVX3lxTFBmRGJ4UjJTaFJRcTFjbHJaOTlGQ05GSzh2VWhDeXNRZGhaZ2FoVFRneExLQm1OSDJSVEpjeFlyWk1ybkpwOV9mSTlrSXBLRUpCYU5iMUcxWEdYbmtHSkpCOEppUjRqVGg2NEFoT3loUFVMb1AtYktqVF9wcw?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data