# Article information:

ExGen: Cross-platform, Automated Exploit Generation for Smart Contract Vulnerabilities | IEEE Journals & Magazine | IEEE Xplore
<https://ieeexplore.ieee.org/abstract/document/9674230>

# Article summary:

1. Smart contracts are prone to vulnerabilities, which can lead to severe consequences such as massive token and coin losses.

2. ExGen is a cross-platform framework that generates multiple transactions as exploits for vulnerable smart contracts by translating them to an intermediate representation, generating symbolic attack contracts with transactions in a partial order, and concretizing all the symbols to verify exploitability on a private chain.

3. ExGen successfully exploits 89.9% of Ethereum and 96.9% of EOS vulnerabilities, including 24 zero-day vulnerable contracts on EOS, and generates exploits for vulnerabilities that require multiple transactions using Partially-ordered Transactional Set (PTS).

# Article rating:

Appears strongly imbalanced: The article is written in a biased or one-sided way, and the information it provides is not trustworthy enough to be considered a reliable source. You should consult other sources to find reliable information on the presented issues.

# Article analysis:

该文章是一篇关于智能合约漏洞自动化利用的研究论文，介绍了一个跨平台的框架ExGen，可以生成多个交易作为对给定智能合约的攻击。然而，该文章存在以下问题：

1. 偏袒：该文章只介绍了ExGen的优点和成功率，并没有探讨其可能存在的风险和局限性。例如，如果黑客使用类似的工具来攻击智能合约，会对区块链安全造成什么影响？是否有必要加强监管和审计？

2. 片面报道：该文章只提到了静态分析和符号执行等方法来检测漏洞，并没有探讨其他方法如动态分析、模糊测试等在智能合约安全中的应用。

3. 缺失考虑点：该文章没有考虑到智能合约漏洞利用可能会导致用户资产损失、信任危机等问题。同时，也没有探讨如何解决这些问题。

4. 宣传内容：该文章过于宣传ExGen的成功率和优势，并未提供足够证据支持其主张。同时，也没有探讨其他类似工具与ExGen之间的差异和优劣。

5. 未探索反驳：该文章并未探讨其他学者对于智能合约漏洞利用的研究成果和观点，缺乏对于该领域的全面了解。

综上所述，该文章存在一定的偏见和片面性，并未全面考虑智能合约安全问题的各个方面。在今后的研究中，需要更加注重平衡双方观点、探讨可能存在的风险和局限性、提供足够证据支持主张等方面。

# Topics for further research:

* Risks and limitations of ExGen
* Other methods for detecting smart contract vulnerabilities
* Consequences of smart contract exploitation for users and trust
* Comparison of ExGen with other similar tools
* Alternative research and viewpoints on smart contract exploitation
* Need for balanced and evidence-based analysis of smart contract security issues

# Report location:

<https://www.fullpicture.app/item/ffb505031c1bb2d8f3f5c4f49557407f>