# Article information:

Semantic Understanding of Smart Contracts: Executable Operational Semantics of Solidity | IEEE Conference Publication | IEEE Xplore  
<https://ieeexplore.ieee.org/abstract/document/9152785>

# Article summary:

1. Solidity is a Turing-complete programming language used to develop smart contracts on the Ethereum blockchain, but developing correct and secure smart contracts is challenging due to the decentralized nature of the blockchain and potential vulnerabilities.

2. Existing works focus on analyzing and verifying smart contracts at the EVM bytecode level or through intermediate languages, but it is important to formally define the semantics of Solidity for programmers who write and reason about smart contracts at the source code level.

3. The proposed formal semantics for Solidity provides a specification for semantic-level security properties and defines correct and secure high-level execution behaviors of smart contracts to assist developers in writing secure contracts and reasoning about compiler bugs.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

该文章主要介绍了Solidity语言的可执行操作语义，以及为什么理解和形式化定义Solidity的语义是重要和必要的。文章指出，由于智能合约的去中心化计算特性，编写正确和安全的智能合约具有挑战性，并且存在漏洞可能会导致巨大的财务损失。因此，对智能合约进行验证和安全分析至关重要。

然而，该文章存在一些潜在偏见和不足之处。首先，文章没有探讨Solidity语言本身可能存在的缺陷或风险。其次，文章没有提到已经发生过的智能合约攻击事件，并未充分强调智能合约安全问题的紧迫性。此外，文章只涉及到了现有研究中关于EVM字节码或中间语言的验证方法，并未探讨其他可能存在的验证方法。

另外，该文章也存在宣传内容和偏袒之嫌。例如，在介绍Smart Contracts时，作者只强调了其优点而忽略了其缺点；在介绍现有研究时，作者只列举了与自己观点相符合的研究而忽略了其他可能存在的研究。

总之，虽然该文章提供了对Solidity语言的可执行操作语义的形式化定义，但其存在一些潜在偏见和不足之处，需要更全面和客观地探讨智能合约安全问题及其验证方法。

# Topics for further research:

* Solidity语言的缺陷或风险
* 已发生的智能合约攻击事件
* 其他可能存在的验证方法
* Smart Contracts的缺点
* 与自己观点不符合的研究
* 更全面和客观的探讨智能合约安全问题及其验证方法

# Report location:

<https://www.fullpicture.app/item/6545d3a6bbaa7caefb8ec781c214ee5d>