# Article information:

Sensors | Free Full-Text | Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things
<https://www.mdpi.com/1424-8220/20/6/1793>

# Article summary:

1. IoT devices are vulnerable to illegal access, posing significant threats to personal and property safety.

2. Access control is an effective solution to address this issue.

3. The proposed Capability-Based Access Control (CapBAC) scheme, using Ethereum smart contract technology, achieves more fine-grained and flexible capability delegation while ensuring consistency between delegation information and stored tokens.

# 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:

该文章提出了一种基于智能合约的分布式和可信任的能力访问控制（CapBAC）方案，以解决物联网系统中非法访问资源的问题。然而，该文章存在以下几个问题：

1. 偏袒：该文章只关注了非法访问资源的问题，而没有考虑到可能存在滥用权限或者误操作等其他安全风险。因此，该文章在呈现问题时存在偏袒。

2. 片面报道：该文章只介绍了作者提出的方案，并未对其他已有方案进行充分比较和评估。因此，读者无法全面了解不同方案之间的优缺点。

3. 缺失考虑点：该文章并未考虑到智能合约本身存在漏洞或者被攻击的风险。如果智能合约受到攻击或者出现漏洞，则可能导致整个系统遭受损失。

4. 所提出主张缺乏证据支持：该文章声称作者提出的方案在灵活性、粒度和一致性方面优于其他已有方案，但并未给出充分证据来支持这些主张。

5. 未探索反驳：该文章并未探索可能存在的反驳观点或者质疑，并且没有平等地呈现双方观点。因此，读者无法全面理解不同观点之间的争议和分歧。

6. 宣传内容：该文章过于强调作者提出的方案的优势，并且没有充分说明其局限性和潜在风险。因此，读者可能会对该方案产生过高期望，并忽略其潜在局限性和风险。

# Topics for further research:

* Other security risks in IoT systems
* Comparison and evaluation of existing access control solutions
* Risks and vulnerabilities of smart contracts
* Evidence supporting the superiority of the proposed solution
* Exploration of opposing viewpoints and controversies
* Limitations and potential risks of the proposed solution

# Report location:

<https://www.fullpicture.app/item/28012e4d3604d96d53efb7ee883c6677>