# Article information:

基于区块链的多关键词模糊搜索加密方案 - 中国知网
[https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C45S0n9fL2suRadTyEVl2pW9UrhTDCdPD67HXaPEY-Wrd9oce5HdgoCkLLFiYPRtf243t\_Xd8HVoLWI-elCUjUV0=NZKPT](https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C45S0n9fL2suRadTyEVl2pW9UrhTDCdPD67HXaPEY-Wrd9oce5HdgoCkLLFiYPRtf243t_Xd8HVoLWI-elCUjUV0&uniplatform=NZKPT)

# Article summary:

1. 提出了基于区块链的多关键词模糊搜索加密方案，解决了一对多数据密文共享中的多关键词模糊匹配和用户公平性问题。

2. 引入了R-HashMap索引结构，使用双重编码函数和位置敏感哈希函数建立安全索引，并使用K最近邻算法加密索引，实现多关键词模糊搜索。

3. 结合以太坊区块链技术和可搜索加密方案，避免恶意服务器篡改数据，并使用智能合约作为可信第三方进行检索，保护用户隐私和数据安全。

# 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:

作为一篇学术论文，该文章提出了基于区块链的多关键词模糊搜索加密方案。然而，在阅读文章时，我们可以发现一些潜在的偏见和缺失的考虑点。

首先，该文章没有充分探讨区块链技术可能存在的风险和局限性。尽管区块链技术可以确保数据不被篡改，但它并不能完全保证数据的安全性。例如，在以太坊网络中，智能合约代码可能存在漏洞或错误，这可能导致黑客攻击或数据泄露。此外，由于区块链技术本身的限制，其处理速度较慢，并且需要大量的计算资源和能源消耗。

其次，该文章没有平等地呈现双方。作者只关注了用户隐私和数据安全问题，并没有考虑云服务器提供商可能面临的挑战和困境。例如，在实施可搜索加密方案时，云服务器提供商需要承担更高的计算成本和存储成本，并且需要采取额外的安全措施来保护用户数据。

此外，该文章也存在一些片面报道和缺失考虑点。例如，在介绍R-HashMap索引结构时，作者声称使用双重编码函数和位置敏感哈希函数可以构建安全索引。然而，作者并没有详细说明这些函数的具体实现方式和安全性能。此外，在介绍可搜索加密方案时，作者只关注了时间开销和准确性，并没有考虑其他因素，如空间开销、通信成本等。

最后，该文章提出的主张缺乏充分的证据支持。尽管作者声称通过安全证明分析可以满足自适应选择关键词的语义安全性，并保护用户隐私和数据安全，但作者并没有提供详细的证据来支持这些主张。此外，在与其他方案进行实验比较时，作者只关注了时间开销和准确性，并没有考虑其他因素。

总之，该文章提出了一个有趣的研究方向，但存在一些潜在偏见、片面报道、缺失考虑点和未探索反驳等问题。为了更好地评估该方案的有效性和可行性，需要进一步深入研究区块链技术可能存在的风险和局限性，并平等地呈现双方的利益和挑战。

# Topics for further research:

* Limitations and risks of blockchain technology
* Challenges and dilemmas faced by cloud service providers
* Implementation details and security performance of encoding and hashing functions
* Other factors to consider in searchable encryption schemes
* such as space and communication costs
* Evidence supporting the claims of semantic security and privacy protection
* Comparison with other schemes beyond time complexity and accuracy

# Report location:

<https://www.fullpicture.app/item/ca4c507a82d3f91fa7dee9855b6ae853>