NFT 市场

Piyush Batra阿尔伯塔大学
计算机科学系
pbatra2@ualberta.ca

Gagan RajSingh阿尔伯塔
大学计算机科学系
grsingh@ualberta.ca

Ritik Gandhi阿尔伯塔大学
计算机科学系
rgandhi1@ualberta.ca

arXiv:2304.10632v1 [cs.MM] 20 Apr 2023

摘要——**在日益数字化的世界中，如何安全地管理和交易数字资产已成为亟待解决的问题。本项目旨在应对这一挑战，开发一种利用区块链技术和深度学习模型的去中心化应用（dApp），以实现安全、高效的数字资产管理，重点关注非同质化代币。该去中心化应用具备安全的钱包连接、NFT 图像生成、铸造、市场和个人资料管理等功能。其后端基于 Goerli 测试网，采用 Solidity 编写智能合约；同时，使用 IPFS 实现去中心化存储，并使用 ReactJS/EtherJS 进行前端开发。此外，项目集成了 OpenAI API，可根据用户输入生成独特的 NFT 图像。本项目展示了区块链技术和深度学习模型在开发用于安全、去中心化数字资产管理的去中心化应用中的实际应用。总体而言，本项目为区块链数字资产安全管理解决方案的持续研究作出了贡献，同时凸显了区块链和深度学习技术改变数字资产管理与交易方式的潜力。**

I. 引言

区块链技术为数字资产的管理和交易创造了新的可能性，其中非同质化代币（NFT）是这项技术最引人注目的应用之一。然而，确保 NFT 的安全性仍是一项重大挑战，尤其是在保护用户私钥方面。本项目旨在通过开发一个名为 NFT Marketplace[2] 的去中心化应用（dApp），解决这些挑战，为 NFT 管理提供一个安全且用户友好的平台。

本项目旨在解决有关非同质化代币（NFT）安全管理与交易的若干基本问题。用户如何安全地将加密货币钱包连接到去中心化应用（dApp），从而在不暴露其私钥的情况下与 NFT 进行交互？如何利用深度学习模型生成独特的 NFT，并将其上传至去中心化存储？如何在基于区块链的市场上安全、透明地交易 NFT？以及用户如何以简单直观的方式管理和查看自己的 NFT 收藏品？

为了解答这些问题，我们设计并实现了 NFT 市场。该平台支持用户安全地将钱包连接到去中心化应用，使用深度学习模型创建独特的非同质化代币，并管理其 NFT 收藏品。我们使用以 Solidity 编写的智能合约 [1]，以确保区块链上的资产转移安全且透明，并采用了 Goerli 测试网 [3]。此外，我们还使用了 OpenAI API [4] 根据用户输入生成独特的 NFT 图像，然后将其上传到 IPFS 上的去中心化存储 [9]。

在本报告的后续章节中，我们将介绍去中心化应用（dApp）的设计与实现，并展示对该 dApp 的性能、可用性进行测试和评估的结果，同时讨论我们所采用方法的局限性，以及该领域未来研究与开发的方向。此外，我们还将从非同质化代币生成和铸造过程中 API 调用所需时间的角度，展示对该 dApp 进行性能评估的结果。我们还将详细介绍为评估该 dApp 的用户友好程度而开展的可用性研究。

II. 设计与实现

我们的 NFT 市场去中心化应用的开发过程包含几个关键阶段，包括设计用户界面、在区块链上实现智能合约、集成第三方 API，以及开展测试和评估。本节将详细介绍每个阶段，包括所使用的工具和技术、遇到的挑战以及制定的解决方案。此外，我们还将介绍用于安全连接用户钱包、利用深度学习模型生成独特非同质化代币、在区块链上铸造非同质化代币、开发用于交易非同质化代币的市场，以及创建用于管理 NFT 收藏品的用户档案的方法。通过全面介绍我们的开发过程，我们旨在为构建便于用户管理和交易区块链上数字资产的安全、易用的去中心化应用提供参考和最佳实践。

A. 钱包连接

钱包连接功能是 NFT 市场去中心化应用的关键组成部分，它使用户能够将加密货币钱包安全地连接到该去中心化应用，而无需暴露私钥。此功能通过使用 MetaMask [11], 来实现。MetaMask 是一款热门的浏览器扩展程序，可充当用户的浏览器与其加密货币钱包之间的桥梁。

当用户访问 NFT 市场去中心化应用时，系统会提示其通过 MetaMask 连接钱包。连接成功后，用户即可使用该去中心化应用的各项功能，例如生成和铸造非同质化代币，而无需手动输入私钥。这消除了密钥盗窃或对用户数字资产进行未授权访问的风险。

为了实现与 NFT 市场去中心化应用的安全、便捷交互，我们使用了 React.js [6] 和 Ether.js[7]。Ether.js 是一个用于与基于以太坊的网络交互的热门库。借助该库，我们能够通过 MetaMask 浏览器扩展程序将去中心化应用连接到用户的加密货币钱包。Ether.js 库提供了简单直观的 API，用于从区块链发送和接收数据，让我们能够轻松地将去中心化应用集成到以太坊 [5] 网络中。

B. 非同质化代币生成

非同质化代币生成是我们应用程序的一个关键功能，它涉及使用深度学习模型，根据用户输入创建独一无二的 NFT 图像。为了实现这一功能，我们使用了 OpenAI API [4], , 该 API 提供了对预训练 DALL·E 模型的访问，该模型能够根据文本提示生成图像。

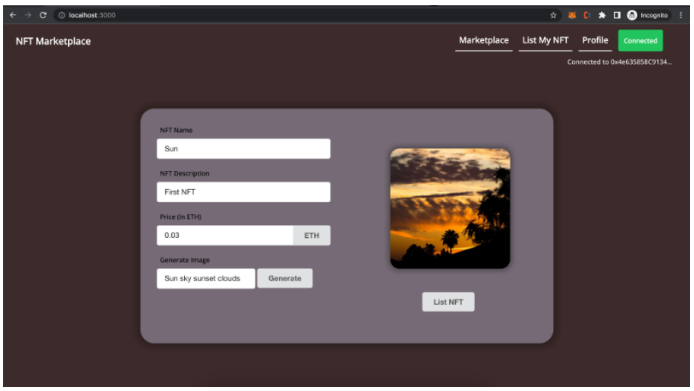

图 1. 非同质化代币生成页面

要生成非同质化代币，用户需要输入一组描述该非同质化代币所需特征的种子词或短语。这些输入会通过我们的后端 Express[8]服务器传递，该服务器与 OpenAI API 通信，并使用 DALL·E 模型生成独特图像。该模型基于庞大的图像和文本提示数据集进行训练，因此能够根据用户输入生成高质量、多样化的非同质化代币图像。深度学习模型的使用还有助于创作个性化且独一无二、难以轻易复制的非同质化代币。

区块链技术与深度学习在 NFT 生成过程中的结合，能够创造出具有价值且独具特色的数字资产。通过充分利用这些技术的强大能力，NFT 市场去中心化应用为用户提供了一种独特且令人兴奋的方式，使他们能够创建、拥有和交易非同质化代币。

C. 非同质化代币铸造

非同质化代币铸造功能使用户能够在区块链上创建和出售独特的数字资产。为实现此功能，我们结合使用了 OpenAI API、IPFS 和以太坊 [5] 区块链。

要铸造 NFT，用户首先使用 OpenAI API 生成图像。图像生成后，用户点击“上架 NFT”按钮，启动铸造流程。此时，系统会创建一个 JSON 对象，其中包含 NFT 的名称、描述、价格以及 OpenAI API 提供的图像 URL。随后，系统会使用 Pinata API 的 pinJSONToIPFS 方法将此 JSON 文件固定到 IPFS 上 [10]. 该方法会返回一个 IPFS 哈希值，作为 NFT 的元数据 URI。

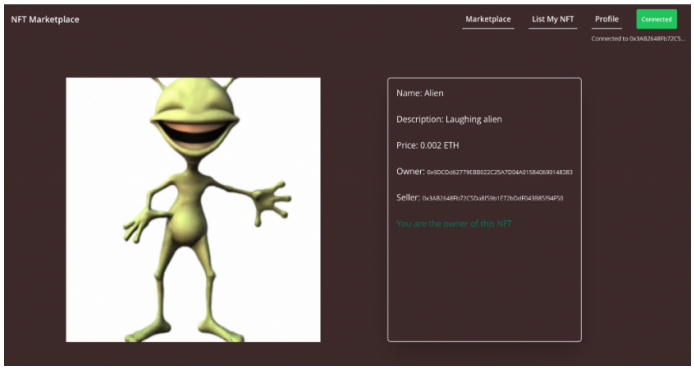

图 2. NFT 描述页面

随后调用智能合约中的 mint 函数，在以太坊区块链上创建一个新代币，并将其 URI 设置为 Pinata API 返回的 IPFS 哈希。智能合约还会指定代币的特征，例如名称、符号以及现存代币的总数。函数执行后，NFT 即正式铸造完成，并可在市场中查看。存储在 IPFS 上的元数据 URI 允许任何人查看 NFT 的名称、描述、价格和图片。区块链上的代币 ID 可确保 NFT 独一无二，并可在用户之间转移。

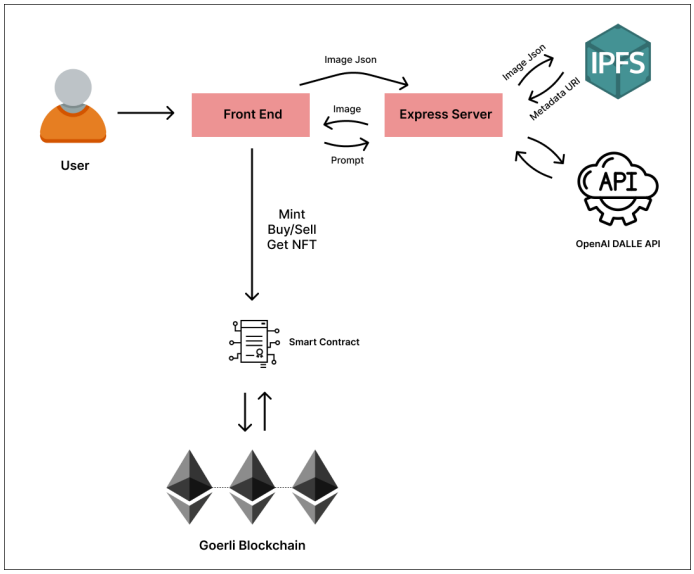

图 3. 我们应用程序的工作流程

通过将 NFT 代币与 IPFS 哈希值关联，我们确保 NFT 的元数据具有去中心化和防篡改的特性。此外，在以太坊区块链上使用智能合约，使用户能够安全、透明地进行转移。

其非同质化代币的所有权，因为所有权信息都不可篡改地存储在区块链上。

D. 市场

该应用的市场功能使用户能够浏览和购买其他用户创建的非同质化代币。该功能构建于以太坊区块链之上，利用 Goerli 测试网[3]，，并允许用户与负责非同质化代币创建、存储和转移的智能合约进行交互。

市场会显示存储在合约中的所有可用非同质化代币，用户可以浏览这些代币并查看其相关元数据，例如名称、描述和价格。元数据存储在 IPFS 上，从而确保去中心化并防止篡改。

要购买非同质化代币，用户需点击所需非同质化代币对应的“购买”按钮，从而调用智能合约的 buyToken 函数。该函数会将非同质化代币的所有权转移给用户，并更新智能合约的存储以反映新的所有权。随后，交易会记录在区块链上，为此次转移提供不可篡改的记录。

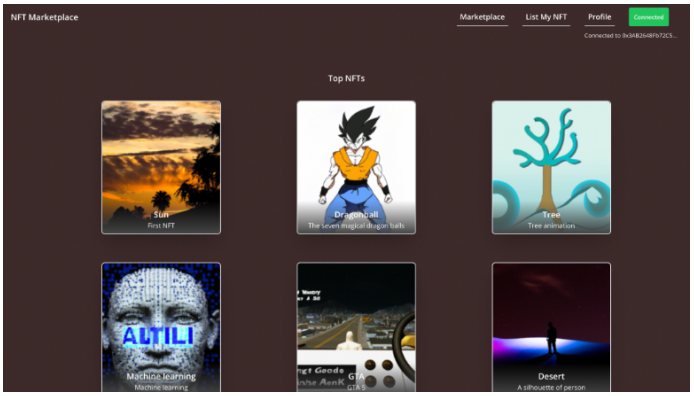

图 4. NFT 市场页面

该去中心化应用采用了用户友好的界面，其中包含清晰的操作说明和直观的按钮，方便用户浏览、购买和出售非同质化代币。区块链技术和 IPFS 的使用确保了非同质化代币交易及其元数据的安全性与完整性，为用户提供流畅的使用体验。

E. 用户个人资料

用户个人资料页面是 NFT 市场去中心化应用的关键组成部分，为用户提供其账户中 NFT 所有权和价值的概览。以太坊区块链的智能合约功能集成到了去中心化应用的界面中，以实现此功能。

当用户访问其 UserProfile 页面时，去中心化应用会检索与用户账户相关的数据。这些数据包括用户的钱包地址、拥有的非同质化代币总数，以及用户持有的非同质化代币的总价值。去中心化应用会在 UserProfile 页面上以用户友好的格式显示这些信息。该页面还会显示所有

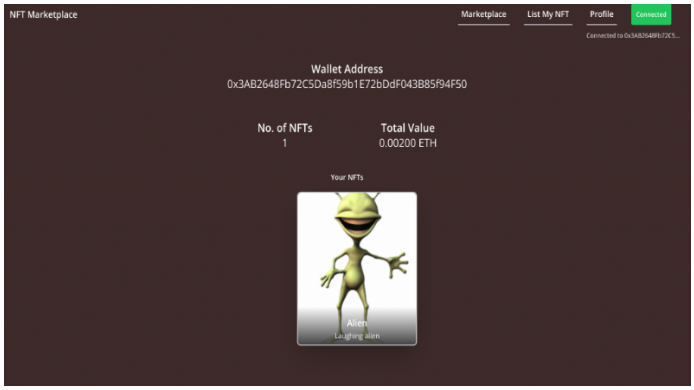

图 5. 用户个人资料页面

用户拥有的非同质化代币。去中心化应用通过查询以太坊区块链的智能合约，获取用户拥有的非同质化代币列表，并使用与每个代币 ID 关联的元数据 URI 从 IPFS 获取非同质化代币的元数据。这些信息以美观且易于浏览的形式呈现。

将智能合约集成到用户个人资料页面后，用户便能在区块链上安全、透明地查看其 NFT 所有权和价值。

F. 团队协作与贡献

我们的项目是全体三位团队成员共同协作完成的。我们根据每位成员的优势和专业领域，为其分配了不同的任务。我们采用敏捷方法，确保每项任务都能在规定时间内完成。

下表展示了分配给每位团队成员的任务明细：

Task	**分配给**
定义需求	All
非同质化代币生成架构	Gagan、Piyush
Web 应用的客户端部分	Gagan、Ritik
将 Web 应用与 web3.js 库集成	Piyush、Ritik
实现铸造流程	Gagan、Piyush
将生成的对象连接到区块链	Piyush、Ritik
测试并部署合约	Gagan、Ritik
测试 Web 应用并开展可用性研究	Gagan、Piyush

表 I
团队合作

III. 项目状态

该项目已实现预期功能，可在以太坊区块链上生成并铸造非同质化代币。项目范围中规定的所有要求均已顺利达成，团队成功交付了一款功能完备的 Web 应用，允许用户生成并铸造自己的非同质化代币。

在整个项目过程中，团队遇到了若干技术难题，主要是 Web 应用与 web3.js 库的集成问题，导致项目进度有所延迟。不过，团队通过向在线社区求助并利用相关资源，最终克服了这些问题。

总而言之，尽管遇到了一些小挫折，项目仍实现了预期目标并顺利完成。团队积累了开发基于区块链的 Web 应用程序的宝贵经验，所学知识也可应用于未来与区块链技术相关的项目。

IV. 结果

本节将介绍我们项目的性能和可用性研究结果。性能测试包括测量使用 OpenAI API 生成非同质化代币图像，以及在 Goerli 测试网上通过智能合约交易铸造非同质化代币所需的时间 [3]。在可用性研究中，我们对校园内的十位用户进行了调查，以评估市场的易用性、清晰度和视觉吸引力，以及购买流程和整体用户体验。我们以条形图的形式展示可用性研究结果，以呈现参与者的反馈。

A. 性能评估

性能测试包括使用 OpenAI 的 DALL·E 模型生成非同质化代币图像，以及在 Goerli 测试网上通过智能合约交易铸造非同质化代币 [3]。我们绘制了两张图表来直观呈现性能测试结果。图表的 x 轴表示发出的不同请求，y 轴表示每个请求所花费的时间。

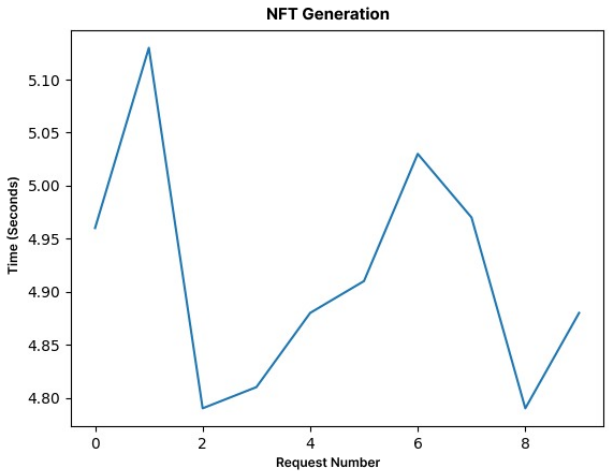

图 6. 非同质化代币生成性能

在图像生成方面，结果显示生成一张图像平均耗时约 4.9 秒，最长耗时为 5.15 秒。

在铸造方面，铸造一枚 NFT 的平均耗时约为 16.9 秒，最长耗时为 17.05 秒。结果表明，NFT 市场原型的性能尚可，但仍有改进空间，尤其是铸造流程，其耗时比图像生成流程更长。造成这一延迟的因素之一是使用了 Goerli 测试网 [3]，其速度不如以太坊主网。

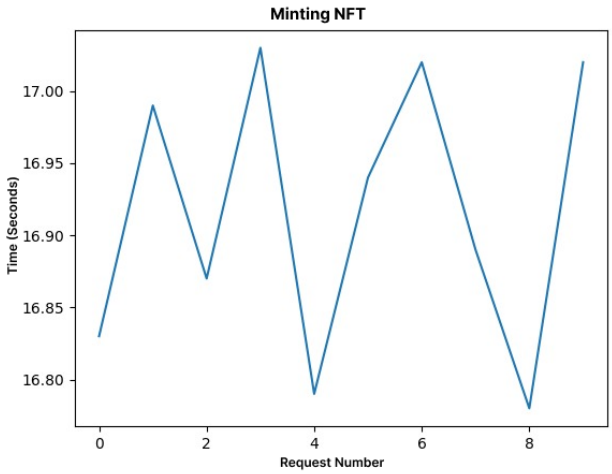

图 7. 非同质化代币铸造性能

B. 可用性研究

我们邀请了校园内的 10 名用户进行可用性研究，请他们评价使用该市场的体验。在 1 到 5 分的量表中，5 名用户认为该市场易于浏览和使用，其余 5 名用户则认为它非常易于使用。

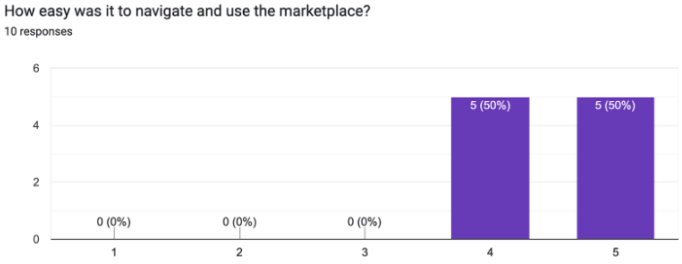

图 8. 可用性研究 Q1 结果

同样，6 位用户认为图像生成流程清晰且易于使用，另有 4 位用户认为非常易用。

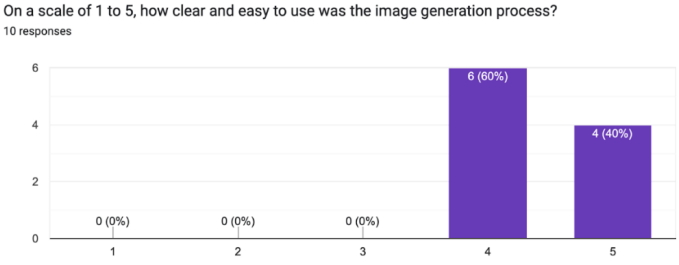

图 9. 可用性研究第 2 题结果

在铸造 NFT 方面，5 位用户认为非常简单，4 位用户认为简单，1 位用户认为略有困难。

在 NFT 市场的视觉吸引力方面，4 位用户认为其非常有吸引力，3 位用户认为其比较有吸引力，另有 3 位用户认为其比较缺乏吸引力。

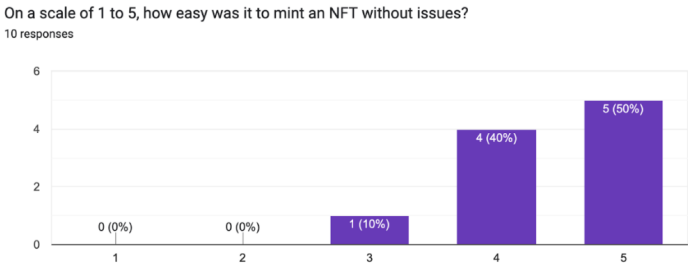

图 10. 可用性研究 Q3 结果

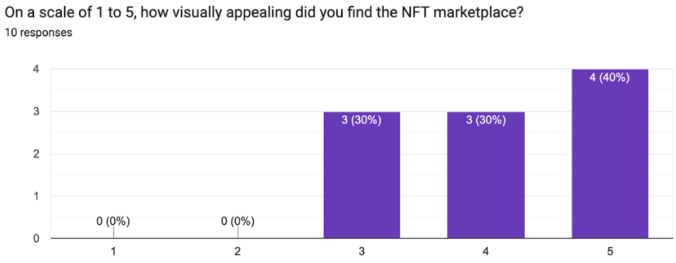

图 11. 可用性研究第四季度结果

在寻找要购买的非同质化代币时，5 位用户认为非常容易，2 位用户认为比较容易，1 位用户认为比较困难。对于 7 位用户而言，购买流程简单易用，另有 3 位用户认为购买流程非常简单。在整体体验方面，6 位用户评价为良好，3 位用户评价为非常好。另有 1 位用户提出了一项改进建议，指出 MetaMask 钱包无法动态更新地址。

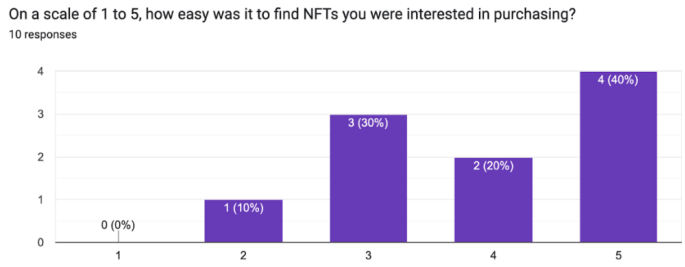

图 12. 可用性研究 Q5 结果

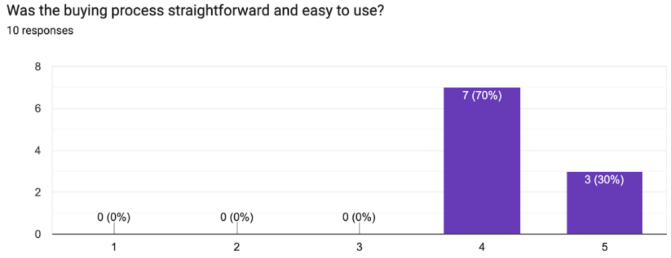

图 13. 可用性研究 Q6 结果

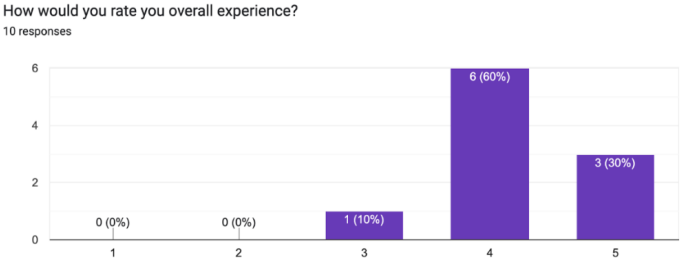

图 14. 可用性研究 Q7 结果

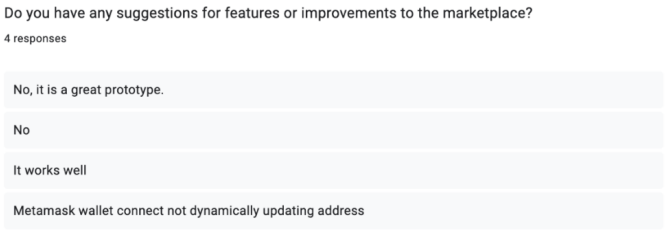

图 15. 可用性研究 Q8 的结果

根据我们的性能和可用性评估，我们发现，所提出的方法能够有效地在区块链上生成和铸造非同质化代币（NFTs）。我们的去中心化应用（dApp）具有良好的用户友好性，能够满足不同区块链应用经验水平的用户的使用需求。然而，需要注意的是，仍需开展更多测试，以评估该方法在不同使用场景和不同用户群体中的可用性。此外，还需要进一步测试，以评估该方法在不同网络条件和使用场景下的可扩展性和稳健性。

V. 局限性与未来工作

尽管 NFT 市场去中心化应用通过区块链技术和深度学习模型提供了一种创新的数字资产安全管理方法，但在未来的应用迭代版本中，仍有若干局限性需要解决。

首先，目前非同质化代币生成过程仅限于使用 OpenAI API，而该 API 存在若干限制，例如最大图像分辨率以及每月允许的 API 请求次数。未来的工作可以包括开发定制的深度学习模型，使其更适合非同质化代币的生成，并能够处理更多种类的输入类型。

其次，该应用目前部署在 Goerli 测试网上，这是一个用于基于以太坊的网络的测试环境。虽然这使我们能够在安全且可控的环境中测试该应用，但也限制了去中心化应用的可扩展性及其在现实世界中的适用性。未来的工作可以考虑将去中心化应用部署到主网上，以实现真实非同质化代币的交易。

第三，尽管该应用目前支持非同质化代币（NFT）的铸造和交易，但尚未支持 NFT 的转售功能。这是 NFT 市场的一项重要功能，

未来的工作可以包括开发一种机制，以确保非同质化代币（NFTs）的安全、透明转售。

最后，还可以进一步改进去中心化应用的用户界面，以提升用户体验并让更广泛的受众能够使用该平台。这可以包括采用更先进的设计与可用性原则，以及加入社交分享和社区建设工具等更多功能。

结论

总而言之，NFT 市场去中心化应用的开发展现了区块链技术和深度学习模型在打造安全、透明且易于使用的平台方面的潜力，这些平台可用于管理和交易数字资产。我们的去中心化应用解决了非同质化代币管理中的若干根本性挑战，包括安全的钱包连接、利用深度学习生成非同质化代币、在区块链上铸造非同质化代币，以及用于交易非同质化代币的市场。OpenAI API 与以太坊网络的集成，使我们能够生成个性化且独一无二、不易被复制的非同质化代币，从而创造出有价值且独特的数字资产。我们开展的可用性研究表明，我们的去中心化应用易于使用和操作。未来在该领域的研究与开发方向可能包括提升非同质化代币市场的可扩展性、探索非同质化代币生成的新方法，以及应对数字资产管理与交易中可能出现的安全问题。总体而言，我们的 NFT 市场应用代表着非同质化代币管理与交易去中心化应用的发展迈出了重要一步。

参考文献

[1] “Solidity — Solidity 0.8.19 文档”，Soliditylang.org，2023年。https://docs.soliditylang.org/en/v0 09, 2023 8 19. . /index.html（访问日期：2023年4月9日）。[2] “去中心化应用简介 — ethereum.org”，ethereum.org，2021年。https://ethereum.org/en/developers/docs/dapps/（访问日期：2023年4月9日）。[3] Goerli 测试网，“Goerli 测试网”，Goerli.net，2022年。https://goerli.net/（访问日期：2023年4月9日）。[4] “OpenAI API”，Openai.com，2023年。https://platform.openai.com/docs/（访问日期：2023年4月9日）。[5] “以太坊开发者资源 — ethereum.org”，ethereum.org，2023年。https://ethereum.org/en/developers/（访问日期：2023年4月9日）。[6] “入门指南 – React”，Reactjs.org，2021年。https://legacy.reactjs.org/docs/getting-started.html（访问日期：2023年4月9日）。[7] “文档”，Ethers.org，2023年。https://docs.ethers.org/v5/（访问日期：2023年4月9日）。[8] “Express - Node.js Web 应用程序框架”，Expressjs.com，2017年。https://expressjs.com/（访问日期：2023年4月9日）。[9] “IPFS 文档 — IPFS 文档中心”，Ipfs.tech，2023年。https://docs.ipfs.tech/（访问日期：2023年4月9日）。[10] “Pinata API - Pinata 文档”，Pinata.cloud，2023年。https://docs.pinata.cloud/pinata-api（访问日期：2023年4月9日）。[11] “面向去中心化金融、Web3 去中心化应用和非同质化代币的加密钱包 — MetaMask”，Metamask.io，2023年。https://metamask.io/（访问日期：2023年4月9日）。