

教育经历

2021.09-2025.06 香港中文大学 (深圳) 本科

电子信息工程--计算机工程分支 GPA 3.7+ 专业前 10%

实习经历

Schema AI (web3 面向海外市场) 产品助理 2024.3.1-2024.5.31

- 此产品的功能是将标注后的数据打包成 NFT 资产, 用于 AI 训练者付费使用。以下是我负责的部分:
- 提出数据隐私权保护的技术方案: 利用同态加密 BGV 方案进行 AI 模型的训练, 既保证了数据可以参与运算, 又让数据窃取者需要花费巨大的算力才能破解 (当前最好的计算机需要几千年才能破解)
- 提出数据所有权的跨国认证方案: 将 NFT 资产部署在以太坊区块链, 由于去中心的特性, 任何有以太坊全节点运行的国家都可以所有权互认, 篡改所有权的成本至少需要 $32 \times 8000 \times 3000 \times 6$ 美元 (46 亿美元)
- 负责设计代币发行循环: 了解 web3 早期项目盈利模式, 让治理代币与 NFT 铸造和 AI 训练挂钩, 具备具体价值标的, 从一级市场的代币需求设计来减缓二级市场的冲击, 预计 ICO 超越同赛道“空气币”项目的百万美元融资。
- 撰写技术白皮书: 与产品经理进行几十次沟通, 调研同赛道 10 多款竞品, 在 GPT4 辅助下写出 17 个板块共计 2 万字左右的英文产品介绍; GPT4 辅助下翻阅 100 多篇 AI 和区块链相关英文学术论文, 筛选出 7 个可用的前沿技术。
- 丰富的 GPT 实战经验: 利用 GPT4 设计公司名称, 从上百个候选中选择既有科技感又顺应海外文化; 计划利用 Fine-tuning 技术大幅度减少撰写产品白皮书的提示轮数, 高效与不同文化背景的 KOL 沟通并达成宣发合作等。

研究经历

深圳北理莫斯科大学人工智能实验室 研究助理 2023.12.15-2024.5.31

为了解决个人难以训练大模型, 开展“基于区块链激励机制的去中心化大模型训练”的研究

- 负责设计去中心化 AI 协作训练协议: 类比特币去中心化记账系统, 将一次 AI 模型训练抽象为一次交易, 矿工负责在 PoW 共识机制下测试训练后的模型是否有性能的提升, 其他节点负责验证矿工的结论, 完全同步后获得治理代币奖励。应用如下:
- 商业模式的创新: 改善 AI 模型难以用 web2 免费使用+后向广告变现的商业模式, 转变为 web3 激励使用+代币发行变现 (ICO), 提高用户积极性。
- 提高 AI 模型的性价比: 由于用合理的激励机制汇聚了闲散算力训练 AI 模型, 让开源 AI 社区更加丰富, 同时由于减少了数据收集的成本, 也会比闭源模型花费更加低的成本。

香港中文大学 (深圳) PASS Lab 物理与系统安全实验室 研究助理 2023.10.15-2023.12.15

为了将通信开销降低 33%和增强对内存入侵的防御, 将 RFFI 融合在基于 PUF 的安全通信及密钥交换协议中。

- 负责设计安全通信协议使得 PUF 产生的硬件指纹用来加密 RFFI 的射频特征, 使得外界无法自由篡改用于身份验证的射频特征, 并且完成对称密钥交换。可以减少身份验证过程中的通信次数。应用如下:
- 由于区块链中加密资产完全受私钥支配, 普通用户难以保证私钥完全不泄露, 所以大多将私钥存储在硬件钱包里, 减少与互联网的接触。PUF 可以用于加密硬件钱包中的私钥, PUF 产生的硬件指纹通常不存储在内存中, 从而实现比现有硬件钱包更高的安全性。2024 年硬件钱包市场规模将达 4.7 亿美元, 预计未来 5 年复合年增长率 31.94%。(来自 Mordor Intelligence)
- 可用于防止黑客入侵智能家居的联网器件如家用摄像头, 通过将硬件指纹用于安全通信加密来防止他人破解。

项目经历

超市数据库管理系统开发 大作业组长 2024.3.1-5.15

- 负责在选课前就招募优秀组员, 组员之间的问题沟通以及项目进度管理, 选题确定等。成功在截止日期前 3 天完成项目并且获得 A 级评分。
- 负责审查和修改组员完成的 ER 图以及 SQL 代码, 并在 GPT4 的辅助下成功完成符合课程要求的 40+ 条增删查改的 SQL 语句。
- 利用 GPT4 生成 JavaScript 代码来对接 SQL server 和前端 Vue3, 利用 Postman 来 debug GPT4 生成的代码。
- 负责将代码从 github 下载、整合, 并编写到 latex 文档的附录, 将组员写好的 latex 文档转换成 pdf 文件交到课程网站。
- 帮助负责前端和基于 llama index 开发的 LLM 智能查询的组员录制 demo 视频, 并嵌入到 PPT 中配合课堂展示。