

## 个人简介

我是香港科技大学二年级 MPhil 的学生, 研究方向是区块链, 密码学及他们的相交领域。我是 ALPACAS 研究小组的成员, 该小组由我的导师 [Prof. Amir K. Goharshady](#) 带领。在我的本科, 我的专业是计算机工程, 并有许多 AI 及数据相关的项目和实习。

- 编程语言: C++ · Python · Solidity · JavaScript · HTML · MySQL.
- 技术栈: 算法 · 数据结构 · 以太坊 · 区块链 · zkSNARK · 智能合约 · 密码系统 · AI · 共识机制 · 承诺方案
- 语言: 普通话 (母语) · 广东话 (母语) · 英文 (雅思 7.5 分)

## 教育经历

### 计算机科学硕士 (香港科技大学)

香港 09/2023 - 至今

- 研究方向: 以太坊, 智能合约开发, 区块链, 密码学, 算法
- 助教经历: 1. 计算机科学离散数学工具荣誉课程。2. 计算机组织

### 计算机工程学士 (香港科技大学)

香港 09/2019 - 06/2023

- 辅修: 大数据科学
- 奖项: 1. Prof. Samuel Chanson 最佳毕业项目奖, 2. 行业赞助最佳毕业项目奖, 3. 工程学院院长奖学金

## 论文 (作者按姓氏排序)

### Fast and Gas-efficient Private Sealed-bid Auctions

[PODC 2025](#)

J. Ballweg, A. K. Goharshady, Z. Lin

### Improved Gas Optimization of Smart Contracts

[FSEN 2025](#)

T. Barakbayeva, S. Farokhnia, A. K. Goharshady, P. Li, Z. Lin

### Blind Vote: Economical and Secret Blockchain-based Voting

[IEEE Blockchain 2024](#)

A.K. Goharshady, Z. Lin

## 实习经历

### 研究助理, (香港科技大学)

香港 07/2023 - 07/2023

为智能停车场开发空位检测系统, 并为 OrangePi Mini 计算机和 Jetson Orin NX 板等边缘设备设置环境。将一个老年人跌倒检测系统集成到了网络应用程序中, 实时显示提取的人体姿态, 并在检测到跌倒时发出警报。

### AI 及数据工程实习生, (Baronford & Associates)

香港 07/2022 - 09/2022

开发了 MERN (MongoDB、Express、React Node.js) 栈 Webapp, 支持基本的 CRUD 功能。对患者数据集进行探索性数据分析, 并建立了预测患者健康参数的随机森林回归模型, 并利用 GridSearchCV 自动超参数调整优化模型。使用 SDV 中的 SMOTE、RandomOversampler 和 GaussianCopula 对患者数据集进行数据扩增。最终合成数据的分布相似度大于 95%, 双变量相关性差异小于 0.5。

## 项目经历

### 以太坊智能合约 Gas 优化,

09/2024 - 02/2025

将 Syrup2.0 Gas 优化工具用作黑盒, 结合动态编程方法加以改进。最终结果使 Syrup2.0 的优化效果进一步翻倍, 并在测试中使链上智能合约的气体使用量降低了 11.23%。

### 基于区块链及盲签名的电子投票系统,

09/2023 - 01/2024

使用盲签名技术, relayer structure, 在区块链 (以太坊) 上设计并实现了一个投票系统。该协议实现了不可追踪的匿名性以及可验证性、透明性等其他特性, 并在 Gas 成本方面比其他现有区块链电子投票系统节省了至少 40%。

### 以太坊三方随机数生成,

02/2023 - 05/2023

该协议利用 Goldwasser-Micali 密码系统对随机数进行同态加密, 并利用 RSA 和承诺方案, 以确保安全性和隐私性。最终设计并实现了一个去中心化协议, 可在区块链上实现真正的随机数生成。

### 鱼眼摄像头实时车位检测系统,

08/2022 - 05/2023

通过使用 yolo 模型和训练卷积神经网络, 利用鱼眼摄像头和计算机视觉技术为智能停车场建立了空位检测系统。该系统识别空置车位的准确率达到 92.8%。荣获最佳 FYP 奖。