OKX 高校访谈 ｜冯煜：用户不足是本周期中行业的最大瓶颈

冯煜是加州大学圣芭芭拉分校的助理教授，2018年于德克萨斯大学奥斯汀分校（UT Austin）获得计算机科学博士学位。研究领域涵盖区块链安全、编程语言与形式化验证。目前担任Nubit的创始人兼CEO。



自2011年起从事形式化验证研究，专注于各类软件系统的安全性，从浏览器到手机应用都有涉猎。攻读博士学位期间深入研究了分布式系统与安全协议，逐渐意识到区块链技术在构建安全且去中心化系统中的巨大潜力。因虚拟货币资产管理也使其成为黑客频繁攻击的目标，才决心投身Web3领域，致力于通过学术研究与实践应用，推动区块链生态系统的安全和高效发展。

我们希望通过访谈全球高校背景的创业者，透过他们的视角来观察 Web3行业发展，同时挖掘其在Web3行业的发展经历，为高校学子进入Web3就业、创业提供参考。本期我们特别邀请冯煜教授成为《OKX 高校访谈》的分享嘉宾。

《OKX 高校访谈》系列是 OKX 特别出品的专题栏目，由 OKX官方社区大使 Mercy（@Mercy\_okx）主持，旨在挖掘全球高校人士的行业视角，为在Web3创业以及寻找就业朋友们提供参考。

1、首先，请简单做个自我介绍。

我是冯煜，加州大学圣芭芭拉分校的助理教授，2018年在德克萨斯大学奥斯汀分校（UT Austin）获得计算机科学博士学位。我的研究领域涵盖区块链安全、编程语言与形式化验证。我同时担任Nubit的创始人兼CEO。

自2011年起，我便从事形式化验证研究，专注于各类软件系统的安全性，从浏览器到手机应用都有涉猎。攻读博士学位期间，我深入研究了分布式系统与安全协议，逐渐意识到区块链技术在构建安全且去中心化系统中的巨大潜力。然而，随着区块链领域的蓬勃发展，虚拟货币资产管理也使其成为黑客频繁攻击的目标。正因如此，我决心投身Web3领域，致力于通过学术研究与实践应用，推动区块链生态系统的安全和高效发展。

我清晰地记得2018年刚加入UCSB时，以太坊价格仅为80美元。系主任曾善意提醒我：“小冯啊，这以太坊要归零了，你还研究这干嘛？”我非常喜欢美国学术界的一点，就是可以对系主任和院长的建议保持自己的判断（当然并不提倡固执己见）。当时的我对技术充满热情，但对币价毫无概念，甚至没有交易所账号。

接下来的三年里，我与实验室的博士生们在区块链智能合约、零知识证明安全领域取得了一些成果。2022年，在前同事 Shumo（Manta 联合创始人）的介绍下，我结识了 Polychain 的 Luke。当时 Luke 提到：“DeFi Summer 的确精彩，但随之而来的频繁黑客事件让投资人头疼，不如你来创立一家 startup？”我当时回答道：“我既不懂开公司的流程，也没有资金啊……”他却说：“我们支持你！”就这样，我创立了 Veridise，正式踏上了 Web3 的创业之路。

创业初期，币圈各方好友给予了我极大的支持，使我得以在蹒跚中前行。同时，依托以太坊基金会和 0xparc 的支持，我们开展了多项零知识电路安全的研究和产品开发，并审计了几个领先的 ZK 项目。然而，事与愿违，由于管理理念不一致，今年初我决定退出 Veridise。那一刻心情复杂，感觉像放弃了自己一手带大的孩子，未能悉心守护。尤其遗憾的是，眼看着公司错失良机，未能实现我的理想愿景，也辜负了那些无条件信任我的投资人。

经过几周调整后，我与博士生共同成立了Nubit，目标是为比特币生态开发数据层和执行层的基础设施，并结合我们在安全领域的专长。让我意外且感动的是，Veridise的投资人在得知我新创办的Nubit项目后，几乎全都主动表示支持。尽管我在Veridise未能实现当初的承诺，他们依然信任我的品格，这份信任成为Nubit迅速成长的重要推动力。在dao5的Tekin、Polychain的Luke等老朋友的全力支持下，Nubit在短短五个月内迅速发展，完成了三轮融资，成为比特币生态的一股新生力量。

2、您眼中的Web3行业现状是怎样的？行业未来的发展驱动力将会是什么?

我认为，当前的Web3行业面临的挑战与机遇并存。尽管市场经历了多轮周期性波动，但基础设施和生态系统不断成熟。然而，近期对基础设施项目，尤其是以太坊生态的批评声音有所增加。从某种程度上来说，的确，整个Web3行业在过去几年投入了大量的人力和财力用于基础建设。在这一轮周期中，从基础设施项目到整个行业，都遇到了大规模应用的瓶颈——用户不足。然而，舆论似乎走向了另一个极端，质疑技术的作用，转而炒作meme文化等现象。当然，部分项目方确实高举技术旗帜，却未能落实实质性成果，这导致了投资者和用户对高估值基础设施项目的敬而远之。

此时，我认为我们需要保持清醒的认知。古语有云：“以史为鉴，可以知兴替。”我记得20多年前，家里的小平房第一次通过电话拨号连接互联网时，打开浏览器看到的是充斥着广告的小窗口，点击后更会弹出无数窗口，最终只能强行关机。当时的互联网基础设施已经存在，但它究竟能为普通人的生活带来什么变化，谁都没有把握。今天，传统互联网已深刻改变了我们的生活。我想表达的是，我们需要以开放、包容和辩证的态度来看待这个行业的发展，给创业者更多时间，或许几年后，Web3的Google、Facebook、Twitter就会出现。

当然，我并非试图推卸行业目前的问题。Web3行业确实面临一些亟待解决的挑战，如安全性、可扩展性和用户体验。安全性尤为关键，区块链系统和智能合约的漏洞可能带来严重的经济损失。有些OG认为当前黑客事件减少是因为审计公司的功劳，但事实上，上个周期的黑客事件频发，正是因为DeFi Summer时期百花齐放，创新与漏洞并存。而这轮周期，许多项目只在做质押等简单业务，黑客都无从下手（尽管仍有如bedrock hack这样的事件）。这也是我持续专注于区块链安全与形式化验证领域的原因，致力于提升整个生态的安全与可靠性。

展望未来，我认为行业的发展驱动力主要体现在以下几个方面：

1.技术创新：在学术界，AI技术已经在短短几年内渗透到多个领域，AI+区块链也成为本轮周期的热门话题。然而，至今尚未出现AI与区块链的杀手级应用，部分项目方借AI之名，行meme之实。但我相信，AI+区块链的应用终将落地。

2.安全保障：通过智能合约的审计与形式化验证等手段，提升系统的安全性与可靠性。

3.用户体验：通过简化区块链应用的架构，降低用户和开发者的使用门槛，推动真正的大规模应用。

4.监管合规：明确的监管框架有助于提升行业的信任度，促进其健康发展。

5.跨链互操作性：实现不同区块链之间的互通，打破数据孤岛，增强整个生态系统的协同效应。

3、高校的学生们选择进入Web3行业的比例是怎样的？您如何看待Web3行业当前的人才现状？

对于全球，甚至北美高校的整体趋势我不敢妄加评判（很可能也是上升趋势）。但就我在加州大学圣塔芭芭拉分校（UCSB）的观察而言，选择进入Web3行业的学生人数正在逐渐增加。尽管我没有具体的统计数据，但可以明显感受到学生们对区块链技术和去中心化应用的兴趣正在不断上升，这种趋势与比特币价格的涨势相呼应。

举几个简单的例子，UCSB计算机系拥有全美最顶尖的安全实验室之一，由两位安全领域殿堂级人物Chris和Giovanni领衔的Shellphish战队，常年在全球和美国军方的各大CTF竞赛中名列前茅。有趣的是，在我刚入职时，这两位教授对区块链并不看好，认为它是为洗钱和毒品交易服务的基础设施，没必要关注它的安全问题。当时我引用了中国的一句古话：“水能载舟，亦能覆舟”。如今，这两位教授的实验室中，超过50%的博士生正在从事区块链安全研究。我认为，面对新兴事物和技术，必须保持开放包容的学术态度。技术本身是一把双刃剑，本无所谓正邪。

关于Web3行业的当前人才现状，我认为这一领域正处于快速发展阶段，专业人才的需求非常旺盛。然而，由于区块链和Web3技术相对新兴，具备深厚知识和实践经验的人才仍然较为稀缺，导致行业内人才供不应求。为了应对这一局面，我们正在努力提供相关课程和研究机会，以满足学生们的需求。例如，2019年我在UCSB开设了第一门区块链课程，当时只有15名学生。经过几年学校和系里对区块链和Web3技术的研究和教学投入，目前每门课程的学生人数基本稳定在100人以上。虽然这一增长速度不及虚拟货币的涨跌幅度，但这也算是一个良好的开端。

总体而言，正如前面所提到的，整个Web3行业发展迅猛，基础设施和人才储备（无论是管理层还是技术研发）相较于传统的Web2行业仍显薄弱。这给Web3项目方带来了巨大的挑战。例如，在Nubit，我们更倾向于从传统的Web2大厂（如Google、字节跳动、阿里巴巴、腾讯）招募一些职业素养较高但缺乏区块链背景的工程师和管理人员，而不是短期速成的Web3从业者。毕竟任何行业，万变不离其宗。

为了解决这一问题，我们需要持续从教育和培训入手。一方面，高校和研究机构应加大对区块链和Web3技术的研究与教学投入，培养更多专业人才；另一方面，企业也可以通过实习项目和培训计划，帮助新人更快适应行业需求。总体来看，随着Web3行业的不断成熟，对人才的需求将持续增长。我对未来充满信心，坚信通过各方的共同努力，人才短缺的问题将逐步得到缓解，从而推动整个行业的健康发展。

4、对于即将进入Web3行业的年轻一代，您有哪些建议供其参考学习吗？

根据我这些年在科研和创业中的多重经历，我想提出几点建议供大家参考：

a. 夯实技术基础：虽然短期内通过炒币获利的快感十分刺激，但对于年轻的创业者，尤其是技术研发人员，扎实掌握计算机科学的核心知识至关重要，特别是对区块链技术、分布式系统和密码学的深入理解。保持对行业最新发展的敏锐度，定期阅读相关的学术论文、技术博客和新闻报道，参与行业会议、研讨会和黑客松活动，这些都能帮助你紧跟前沿技术与趋势。重视实践：理论固然重要，但实践经验同样不可或缺。参与开源项目、开发去中心化应用（DApp）或在测试网部署智能合约，都是提升实际技能的有效途径。

b. 强化安全意识：Web3领域的安全问题尤为突出。学习安全编码实践，了解常见漏洞及防范措施，这能帮助你在开发过程中避免重大错误。作为从事十几年安全研究并创立了Web3审计公司的我深知，绝大多数黑客并不比常人聪明，而是许多安全事件超过80%的漏洞都源于从业人员对基本安全机制的疏忽。因此，提高Web3的安全水平，不仅仅依赖于开发更强大的安全工具，更需要全行业人员普及安全意识。

c. 创业如做人：Web3初创公司面临的风险普遍高于传统领域，许多投资最终化为泡影。因此，作为年轻的创始人，当你拿到风险投资时，务必保持清醒，因为你透支的其实是投资人对你的信任。得势时，切勿自满，行业变化之快、风险之多往往在一念之间；失势时，不必妄自菲薄。两年前那些炙手可热的项目，许多也曾和你一样默默无闻，四处寻找投资。尊重你的同行、合伙人和每一位为你辛勤工作的员工，切勿为短期利益牺牲长远蓝图。

d. 保持饥饿感与创新精神：Web3技术日新月异，保持学习的热情和能力尤为重要。并非鼓励盲目追逐新技术，而是对任何新事物和技术始终怀有饥渴之心，这能帮助你在项目陷入困境时迅速作出反应。我最喜欢Web3的地方是，它是一个充满机遇的领域，鼓励创新与创业。不论你听到的技术多么不正统，在这个行业里都能找到它的应用场景。如果你有独特的想法，尝试付诸实践，或许能带来意想不到的收获。

e. 注重用户体验：相比Web2，Web3项目在用户体验和黏性上还有很大差距。关掉手机或电脑后，人们可以完全不接触Web3，但离开Uber、微信或亚马逊等传统Web2服务，生活会受到影响。年轻创业者在开发技术解决方案时，切勿为了技术炫耀而忽视用户体验。成功的产品不仅需要强大的技术支撑，还需要易用并能满足用户需求。走出办公室，与潜在客户多交流，加速产品迭代，及时找到产品的PMF（产品市场契合点）。

f. 遵守道德和法规：了解并遵守相关的法律法规和道德准则，确保你的工作推动行业健康发展。

最后，最重要的是保持对这个领域的热情与好奇心。

5、未来5-10年Web3领域最有可能产生重大变革将是什么？

我认为未来五到十年，Web3领域可能会经历以下几项重大变革：

一是大规模应用与主流化：随着技术的逐步成熟和用户体验的提升，Web3应用有望被更广泛的用户群体接受。去中心化金融（DeFi）、稳定币等领域将从小众走向主流，影响力将扩展至更多行业。同时，传统Web2应用也将逐步向去中心化方向扩展，Web2与Web3之间的界限将日渐模糊，最终趋于融合。

二是跨链互操作性与链抽象：不同区块链之间的互联互通将逐步实现，跨链技术的发展将打破各条链的孤立状态，使资产与数据能够在不同网络中自由流动，提升整个生态系统的协同效应。正如微信小程序的平台生态一样，区块链基础设施的抽象层将进一步完善，使传统Web2开发者能更快地开发出复杂的去中心化应用。

三是人工智能渗透与安全标准化：人工智能将在区块链行业的技术领域逐步渗透，提升系统性能、安全性和应用层的多样性。同时，Web3安全将从目前的“乱枪打鸟”阶段逐步走向标准化，对各细分领域的安全机制进行规范，从而增强用户对Web3应用的信任，并推动其更广泛的采用。

四是监管与合规框架的建立：各国政府及国际组织可能会出台更加明确的监管政策，为Web3行业提供法律保障。这将有助于消除不确定性，吸引更多的机构投资者与传统企业进入该领域。回顾互联网发展的历史，二十年前，人们不敢轻易将银行卡信息交给在线服务；而今天，连上一代人也已离不开微信支付等在线支付方式。

五是高校人才与创业团队的关键角色：正如哈佛孕育了Facebook，斯坦福孕育了Google，伯克利孵化了OpenAI，北美高校在Web2领域扮演了重要角色。展望未来，区块链领域的高校人才和创业团队也将在Web3的变革中发挥至关重要的作用。回顾区块链十余年的发展史，我将其分为三个阶段：

•2009年比特币诞生至2021年：这一阶段是区块链创业团队的“草莽时代”，无论是割韭菜者还是认真做项目的团队，都是在争分夺秒地站稳脚跟，基础设施则相对薄弱。2017年我刚开始研究智能合约安全时，曾与Solidity开发主管交流，提到该语言设计的问题，并建议他们在编译时引入中间语言（IR）层，以优化生成的EVM字节码。当时他的回应是：“That’s a genius idea! We will do that in the next version”（即今天的YUL）。这让我感到基础设计的疏忽竟如此显著。

•2021年DeFi夏季至2023年：这一阶段是百花齐放的时期，各类创新层出不穷。与此同时，北美高校的教授和科研团队逐步入场，我在编程语言和形式化验证领域的同行大多创立了各自的区块链公司。

•2023年至今：行业逐步趋于稳定，北美涌现的区块链初创公司中，创始人或顾问没有高校背景的，几乎难以引起投资人的关注。

尽管高校背景的创业团队有时会面临市场应变能力不足、执行力较差等问题，但正如诚信是西方国家的立国之本，高校背景的创业团队往往能够为Web3领域提供最为稀缺的两大要素：底线与创新。底线不难理解，这类团队受到学校和政府的严格监管，任何违规行为都可能面临严厉追究；而创新则是北美高校的强项。这并非因为教授和学生水平更高，而是高校环境相对纯粹，没有复杂的领导关系或外界干扰，能够专注于科研创新，营造出一种通宵达旦、初生牛犊不怕虎的科研氛围。

总的来说，高校人才与创业团队将在未来Web3变革中扮演创新引擎与实践推动者的角色。他们的研究和实践将有助于克服当前的技术与应用障碍，加速Web3的普及与成熟，推动整个行业迈向一个更加开放、去中心化和可信的未来。

风险提示及免责声明

本文章仅供参考。本文仅代表作者观点，不代表 OKX 立场。本文无意提供 (i) 投资建议或投资推荐； (ii) 购买、出售或持有数字资产的要约或招揽； (iii)财务、会计、法律或税务建议。我们不保证该等信息的准确性、完整性或有用性。持有的数字资产（包括稳定币和 NFTs）涉及高风险，可能会大幅波动。您应该根据您的财务状况仔细考虑交易或持有数字资产是否适合您。有关您的具体情况，请咨询您的法律/税务/投资专业人士。请您自行负责了解和遵守当地的有关适用法律和法规。