开源讲座

汇报人：庄表伟

时间：2024.08

目录

CONTENTS

01

缘由篇

最简单的开源定义

开源=以开放式协作的方式生产数字公共产品

技术问题

- 开源基础设施

法律问题

- 开源授权协议与知识产权

管理问题

- 如何运营开源社区

经济问题

- 开源的经济效益从何而来

商业问题

- 通过开源如何获取商业利益

教育问题

- 通过开源如何培养人才

个人为何使用开源?

- 好奇心：尝试新技术，我想看看，这个技术是怎么跑起来的?
- 自学：把软件下载回来，打开代码就能学习
- 需求：我需要一个解决XX问题的软件，到社区里去找一找吧

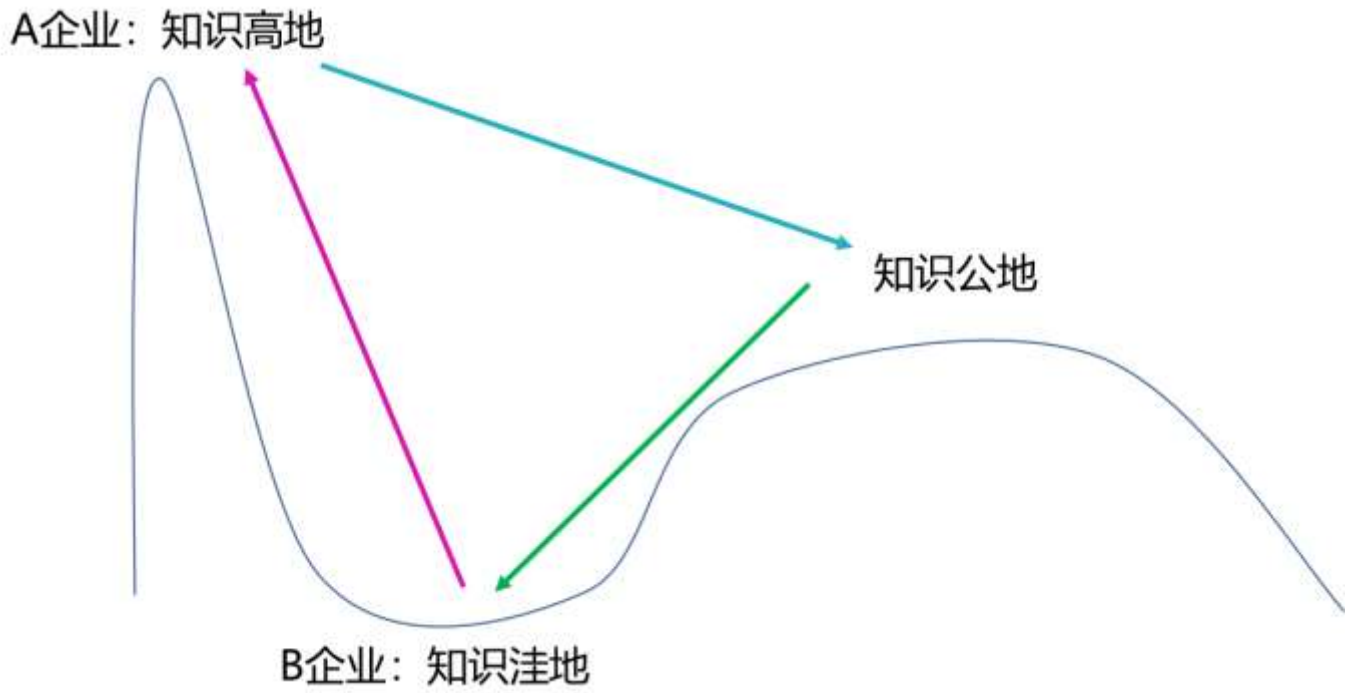
个人为何贡献开源?

- 解决了自己的问题，顺手放到社区里去
- 智商炫富：看看，我的这个代码多厉害
- 礼物文化：为社区贡献最多的人，获得最高的社会地位
  - 崇拜的目光
  - 求职、升职、加薪都更加顺利
  - 也许还能创业
- 教学相长：在社区里分享与交流，我成长得更快

企业为何使用开源?

- A企业与B企业，生产同类产品，假设开发一个产品的复杂度，都是100人年。
- A企业的产品中，包含80%的开源成分，B企业的产品中，包含90%的开源成分。
- 合理推论：A企业的开发人员，大约20人，B企业的开发人员，大约10人。
- B企业的经营成本，大约只有A企业的50%。
- 越是善于使用开源的企业，竞争力越强

企业为何贡献开源?



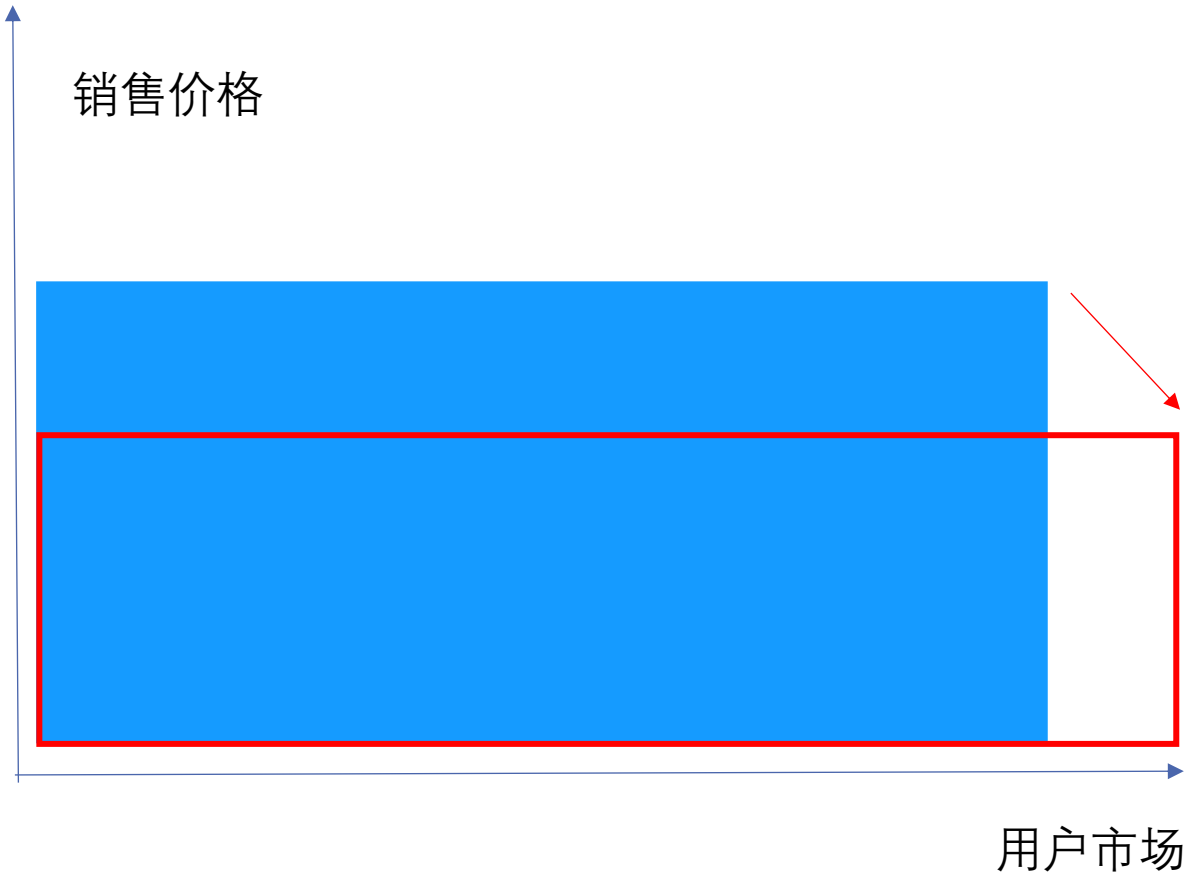
-> 贡献开源

-> 使用开源

-> 购买服务

企业的开源战略，背后的逻辑是什么？

- 公地的价值 ↑，用户市场 ↑
- 知识落差 ↑，销售价格 ↑
- 当一个企业对外开源，会带来两个结果
  - 公地的价值 ↑，知识落差 ↓
- 当一个企业，积极贡献开源时，可能会带来另外两个结果
  - 提升自己在市场份额中的占比
  - 培养自己潜在的竞争对手



企业对外开源的策略选择

- 在市场成长的早期阶段
  - 尽可能多的对外开源，培育市场对“我”的品牌认知与忠诚度
- 在市场成长的中期阶段
  - 有选择性的对外开源，保持节奏
  - 我开源的部分，是否能够获得来自开源社区的更多助力？
  - 选择填平哪一段知识落差？竞争对手具有优势的那一段
- 在市场进入衰退期以后
  - 减少投入，吃尽红利再走

开源的公益属性：政府支持开源的理由之一

- 数字公共产品，就是：以数字形式凝聚的人类知识
  - 分为两大类：能够被机器直接运用的知识，以及需要通过人类阅读才能应用的知识。
  - 前者包括：代码、数据、AI系统
  - 后者包括：文档、标准
- 一个开源项目的价值
  - 用户数量 × 节约的单位时间 = 总的节约时间
- 开源生态的整体价值
  - 作为数字公共产品为全世界节约的时间

开源的创新属性：政府支持开源的理由之二

在知识公地中诞生的创新，不可或缺

- 在专业机构中诞生的创新
  - 基础性创新
  - 突破性创新
- 在企业中诞生的创新（围绕商业场景）
  - 基础、突破
  - 改进、填补
- 在社区中诞生的创新
  - 改进型创新
  - 填补型创新

02

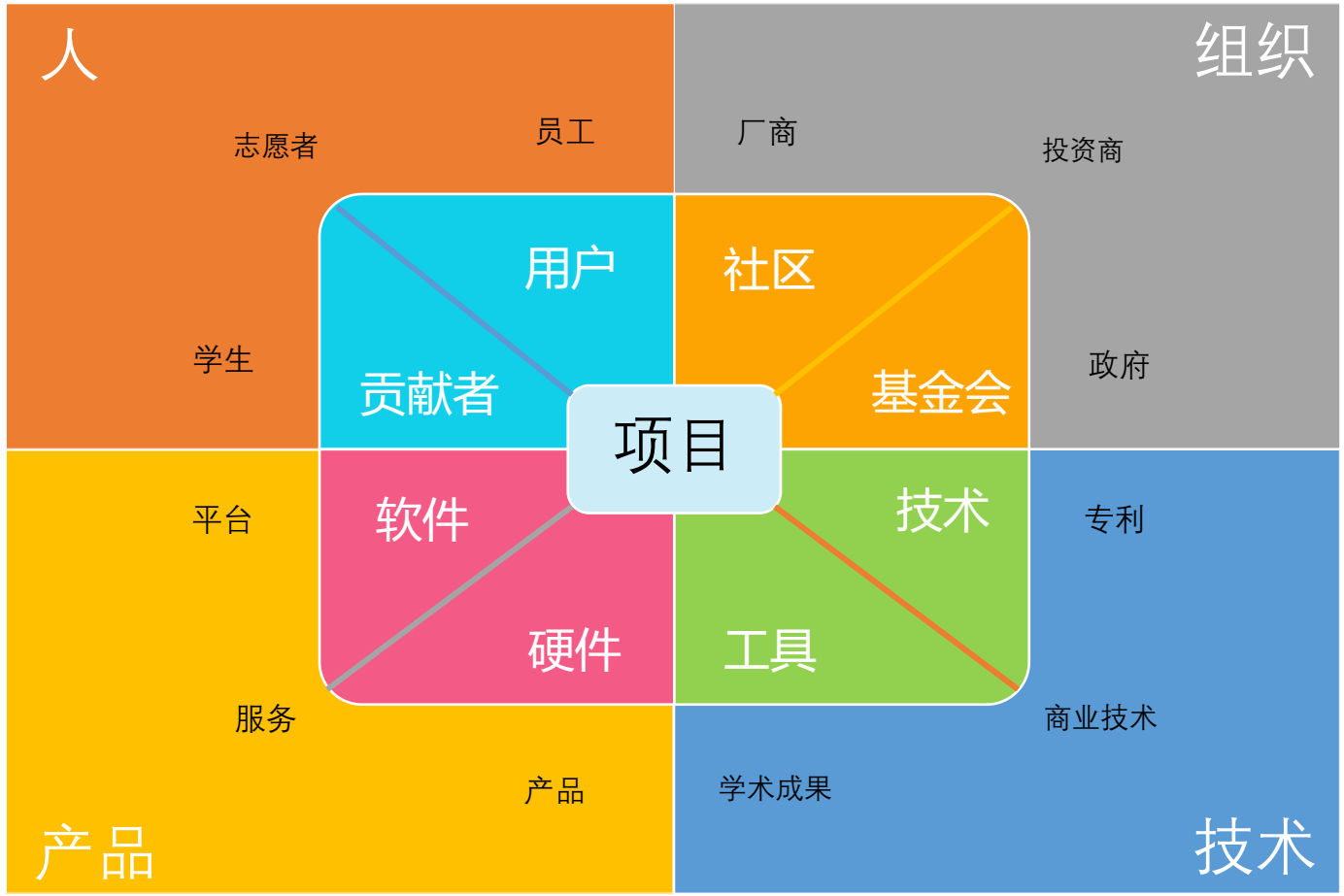
生态篇

开源软件的供应链是如何形成的?

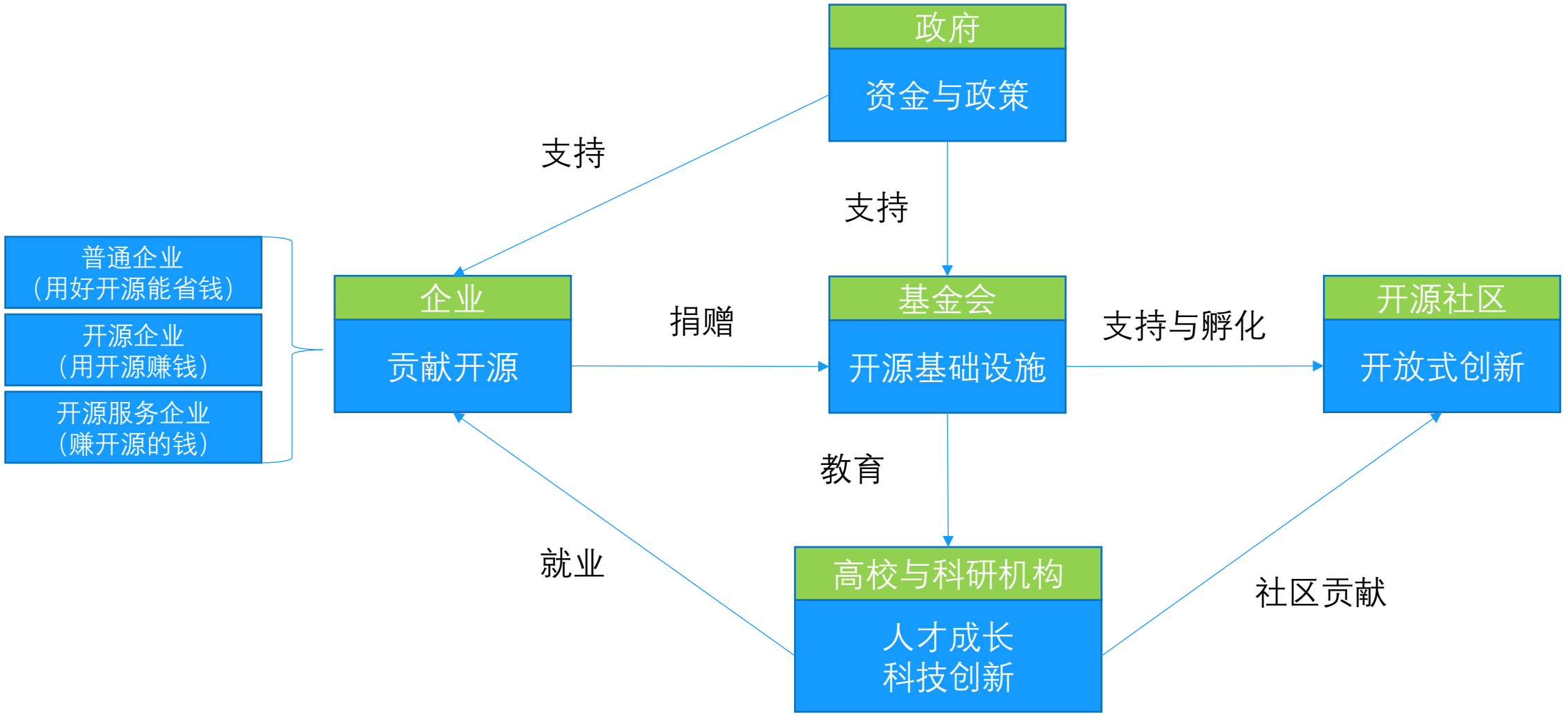
开源生态是如何繁荣起来的?

- 从数字公共产品，到数字知识工地
- 从黑客文化，到礼物文化
- 围绕开源基金会形成的行业联盟

开源生态中的众多角色


人
志愿者
员工
学生
组织
厂商
投资商
政府
用户
社区
贡献者
基金会
项目
软件
技术
硬件
工具
平台
专利
服务
商业技术
产品
学术成果
产品
技术

开源基金会的生态位


政府
资金与政策
支持
支持
普通企业
（用好开源能省钱）
开源企业
（用开源赚钱）
开源服务企业
（赚开源的钱）
企业
贡献开源
捐赠
基金会
开源基础设施
支持与孵化
开源社区
开放式创新
教育
就业
高校与科研机构
人才成长
科技创新
社区贡献

03

供应链篇

供应链、软件供应链与开源软件供应链

- 供应链
  - 原本是一个制造业中的概念
  - A零件+B零件+C零件，组合在一起，生产制造出D组件
  - D组件+E组件+F组件，加工组合，生产制造出G产品
  - 如果C零件缺货，或者无法供应，就会导致D组件无法被生成，也进而影响到了G产品
- 软件供应链
  - 制造业中的零件、组件、产品等概念，被平移到软件中的组件、库、包、产品等概念
  - 因为软件代码的复制，成本为零。制造业中的断供，被偷换概念成：不被允许继续使用
- 开源软件供应链
  - 与商业销售的软件不同，开源软件与组件，通常不会被阻止下载，断供的概念需要进一步发挥想象，才能从制造业平移过来

开源生态（供应链）出了什么问题?

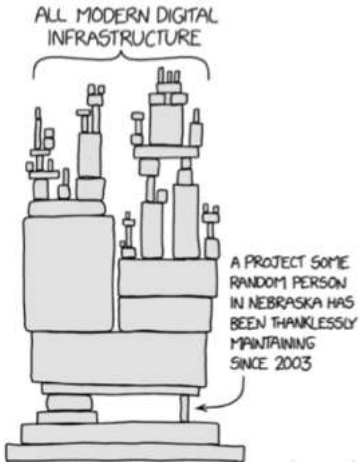
礼物文化的问题

只有少数大牛，
才会受到足够的关注。
绝大多数开发者，
其实并无人知晓!

Linus眼球定律的问题

随着软件的数量越来越多
眼球不够用了。

开源生态脆弱性的根源



如何理解断供?

- 别人不让我们用了
- 软件没人维护了
- 出了安全漏洞，我们不知道
- 我们自己改了软件，搞不定了

开源软件的供应链风险分类

技术风险

- 代码Bug
- 无法下载
- 安全漏洞
- 人为投毒

法务风险

- 未遵循License义务，导致诉讼风险
- 修改License：闭源
- 修改License：排除特定用户

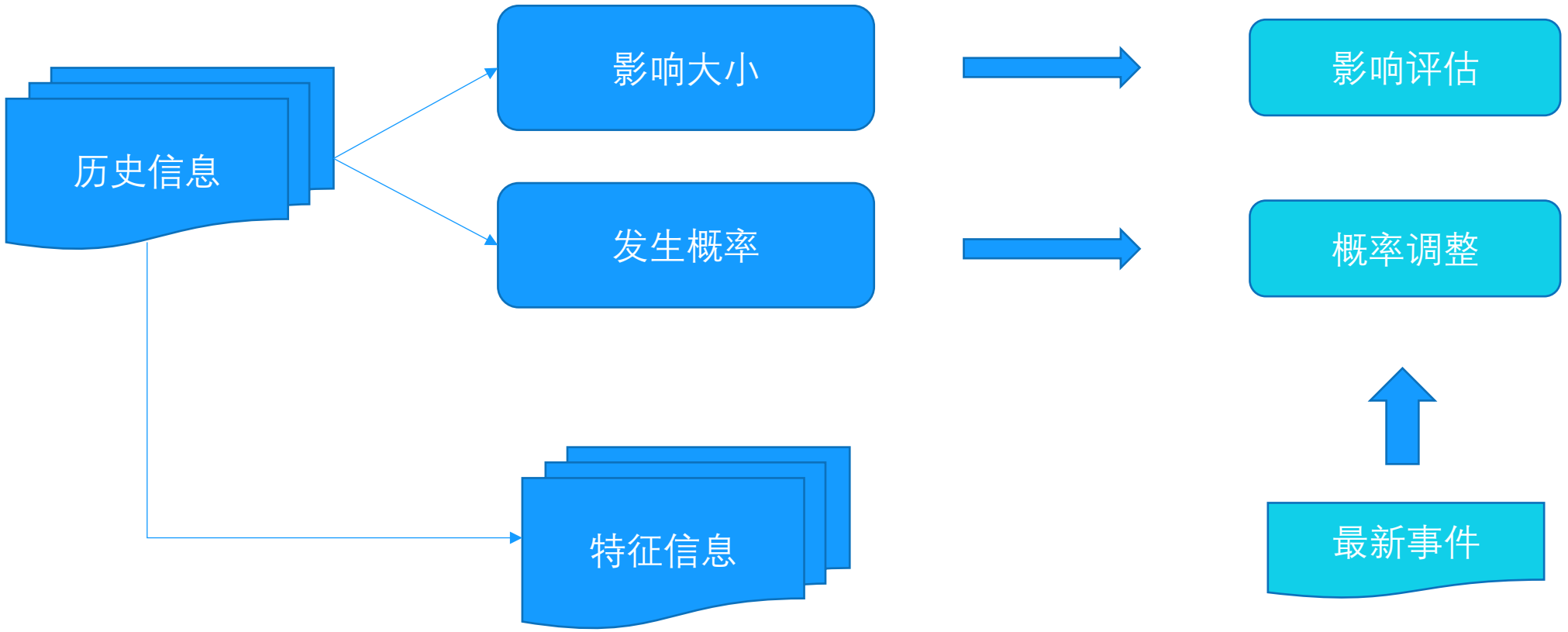
生态风险

- 社区/个人不再维护
- 贡献被上游拒绝
- 依赖服务不再提供

政策风险

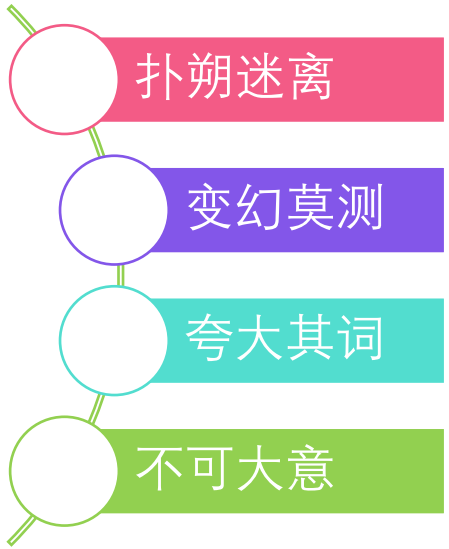
- 平台限制使用
- 出口管制

如何评估风险大小?



以政策风险为例

- 1996年成立，瓦森纳安排全称为“关于常规武器和两用物品及技术出口的瓦森纳安排”
- 2013年12月，出口限制技术清单进行了修订，增加包括基于互联网的监视系统，被出口管制的新技术包括“渗透软件”（旨在破坏计算机或网络保护措施以提取数据或信息的软件）以及IP网络监视系统
- 2019年，谷歌限制华为使用安卓服务（GMS）。业界开始讨论，开源是否也会受到限制?
  - 2019年5月22日，Apache回应，参与开源不受美国出口管理条约限制
  - 2020年7月8日，Linux基金会发布了一份中英文版的《了解开源科技和美国出口管制》的白皮书。其中提到，开源技术不受制于《美国出口管制条例》（EAR）
- 2019年5月19日，全球最大的技术专业组织（IEEE）宣布暂时禁止华为担任旗下期刊编辑或同行评议审稿人
  - 2019年6月13日，IEEE发布合规性声明，声称在向商务部咨询后宣布解除对华为的管制，华为员工可以正常参与期刊编辑与同行评议工作。
- 2021年10月21日：突发！美国政府将禁止向中国和俄罗斯出口黑客工具
- 2022年6月4日：美商务部新规：未经审批禁止向中国分享安全漏洞，微软反对无效



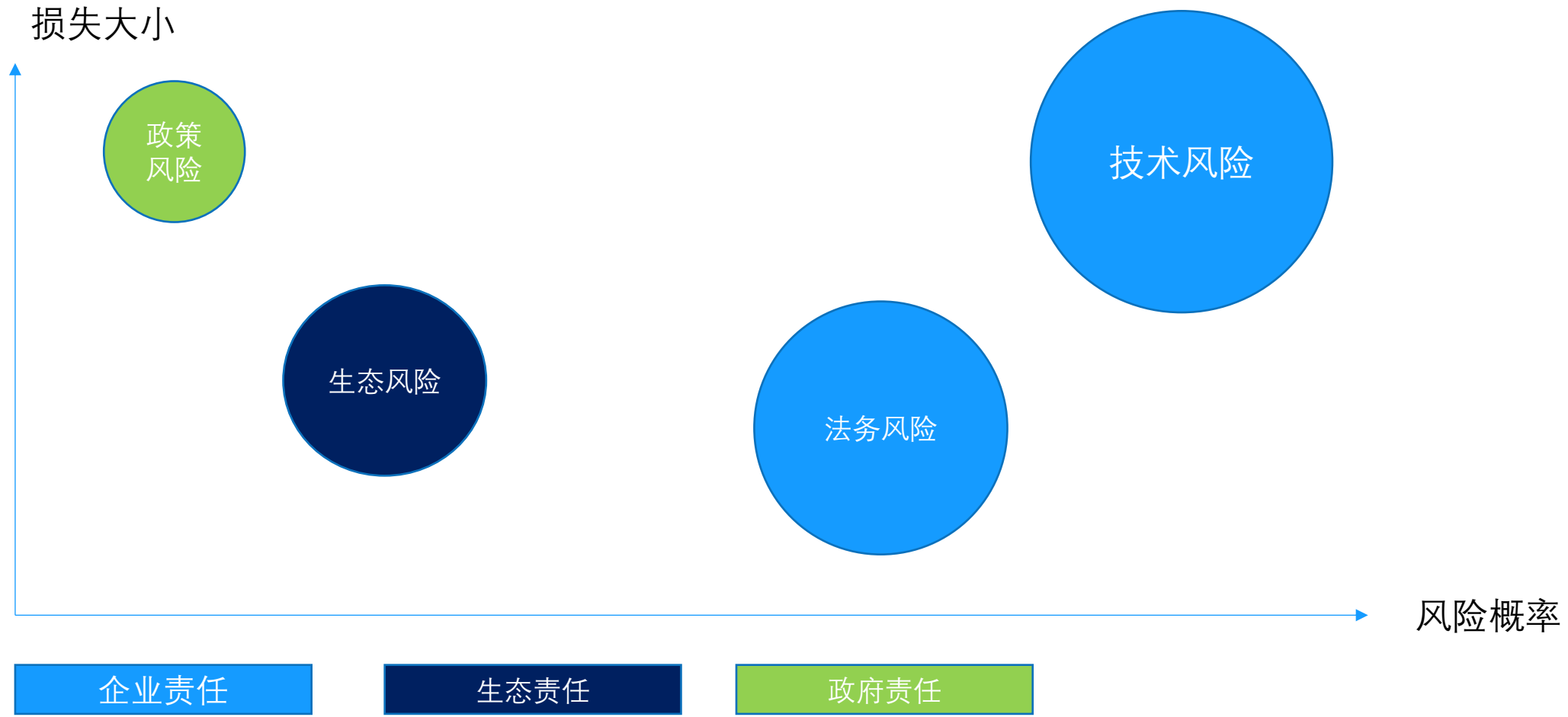
对于政策风险的初步判断

- 目前始终没有真正涉及开源软件供应链
- 周边有很多小动作
  - 限制个人
  - 限制贡献
  - 限制加密软件、黑客工具
  - 限制（商业）漏洞披露
- 不能掉以轻心
- 结论：概率很低很低，影响很大很大

开源生态风险

- 2016年3月：Azer匹夫之怒撼全网
  - 把自己的273个js模块，在npm上全给删了
  - 一个叫left-pad的模块，好几个大型 npm 软件包使用了它
  - 例如：Babel，一个 JavaScript 转译器，每周下载 1100 万次
- 2018年11月：Dominic转手他人放后门
  - event-stream，每月有几千万的下载量
  - 轻率转手，被植入偷窃数字货币的后门
- 2022年1月：Marak大发脾气改乱码
  - faker.js和colors.js，运行时输出乱码
  - 遭遇火灾，求助无果
- 2023年2月14日：Denis情人节绝望哭诉
  - core-js 库的维护者
  - 2020 年末，他因骑摩托车与两名行人相撞，并导致其中一人死亡，但是拿不出8万美元赔偿
  - 最后入狱，判刑18个月（实际关了10个月）
  - 到2023年5月1日，每月收入达到了 $ 6K+

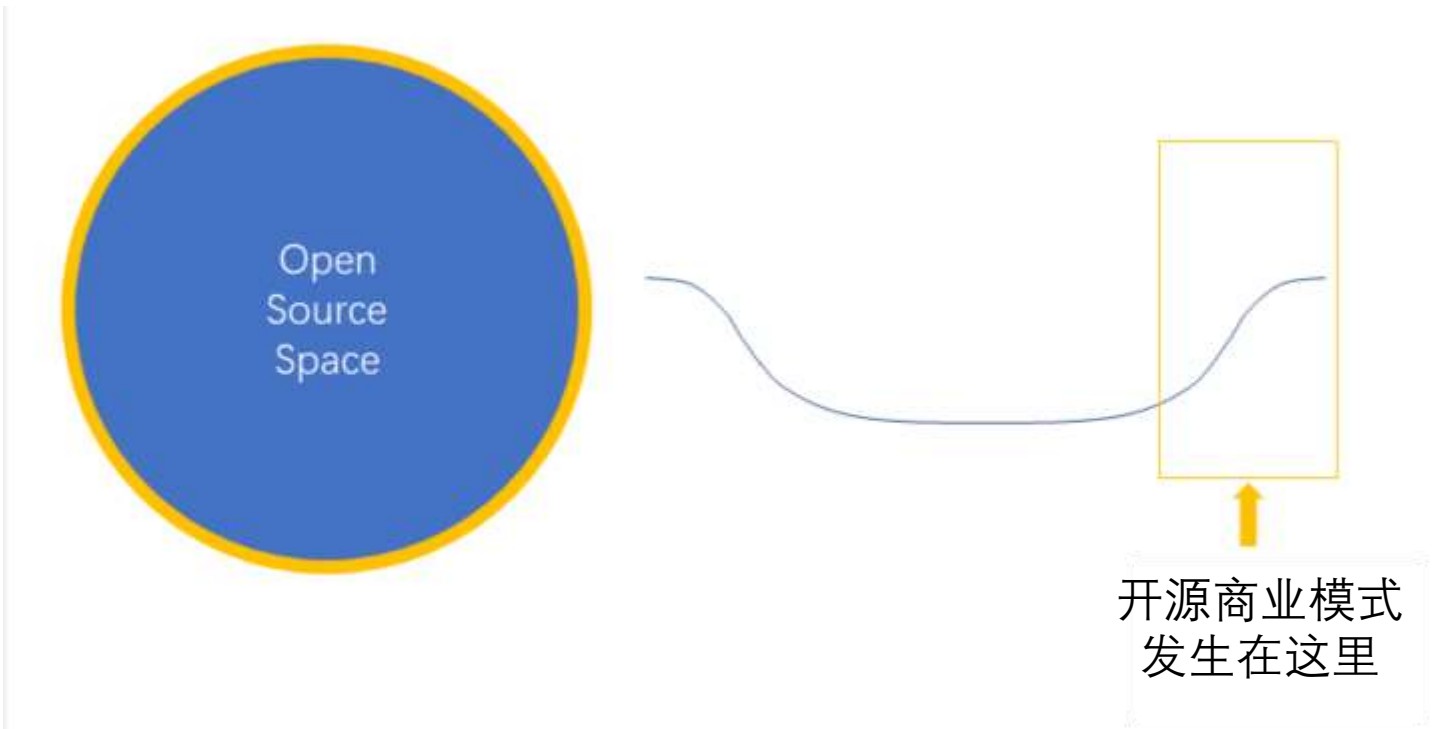
开源软件的断供风险分类



04

商业篇

开源生态中的商业模式

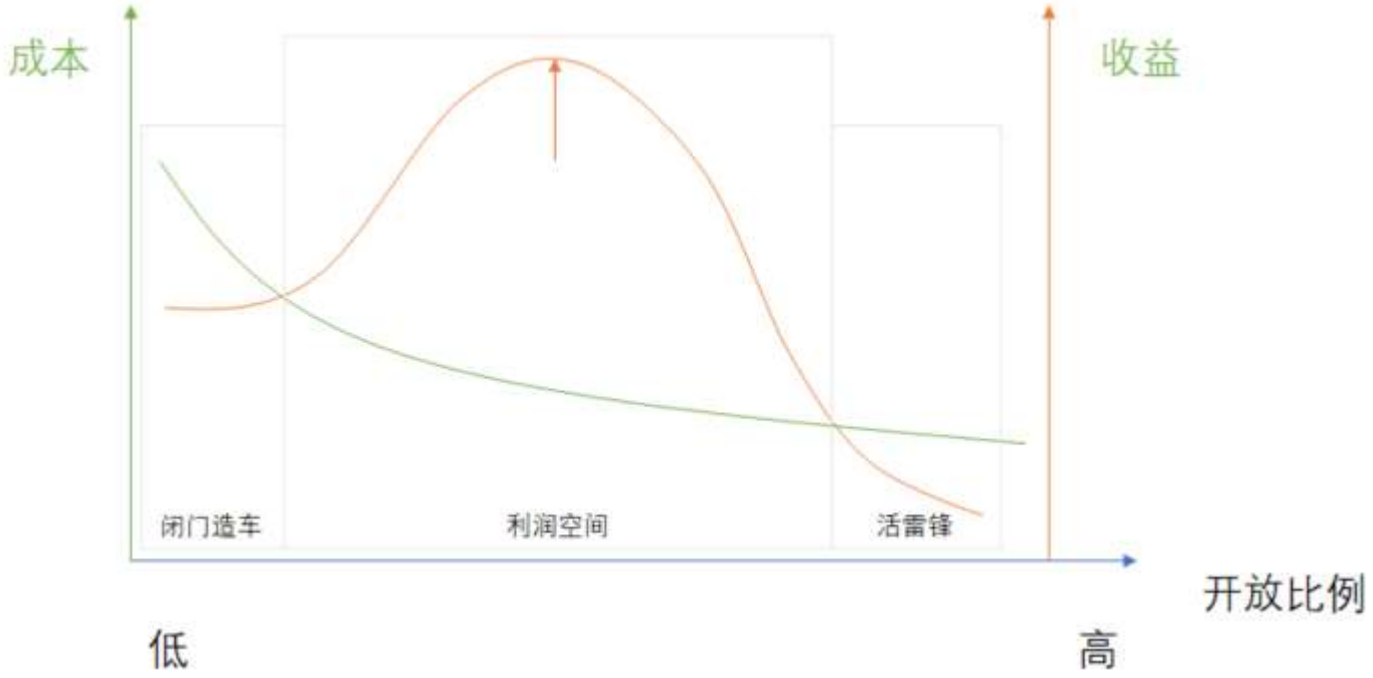


开源空间（Open Source Space）是一个边界封闭，内部开放的空间。现实世界的约束，商业规则的约束，就是这个开源空间的边界。

我们可以这么设想，在开源空间之中，Bit流动的阻力为0。也就是说，在这个空间范围内，是赚不到钱的。这也就是为什么我们会觉得：开源商业模式是一个伪命题的原因。

但是，在这个空间的边界，我们可以设计一个合理的斜坡，从完全开放到完全封闭，从完全免费到各种收费策略。本质上就是利用封闭与开放之间的落差赚钱。

开源商业模式为啥步履维艰?



- 闭门造车：在现在这个时代，还想所有的代码都自己从0开始写的公司，是不可能有利润的，软件都卖不出去
- 利润空间：随着开放程度的提高，成本降低，收益提高（因为开放性，使得获客成本，支撑成本，交易成本都不断下降）
- 活雷锋：太过于开放，以至于用户根本无需付费，就能用得很好了

从商业上来说，我们应该追求的，就是橘黄色箭头，指向的那个利润最高点!

开源商业的各种形态

	普通企业（用好开源能省钱）	开源企业（用开源赚钱）	开源服务企业（赚开源的钱）
特点	主要以传统商业模式运营，并非专注于开源软件领域。	将开源软件作为核心业务模式，通过提供服务或产品来获取收益。	专注于提供与开源软件相关的工具与服务，例如：托管、开发、测试、扫描、支持、培训等。
开源利用方式	选择合适的开源软件来降低IT成本、提高效率和灵活性。	积极开发和维护自己的开源项目，并围绕其构建商业生态系统。	深度理解和掌握多个开源项目的特性，并根据客户需求提供定制化解决方案。
例子	很多中小企业使用免费的办公软件如LibreOffice，或者搭建基于Apache服务器的网站等。	Red Hat、MongoDB、MySQL等公司都以开源软件为基础，发展出成功的商业模式。	Github是全球最大的开源代码托管平台，Synopsys提供SCA等相关工具。
经营水平	是否有能力选用，或者采购性价比最高的（开源）软件。	是否能够设计出足够合理的商业模式，以获取最大利益。	在免费服务与收费服务之间，获取平衡。
风险	是否能够识别供应商的能力，包括开源供应链的保障能力。	过犹不及，都可能导致经营陷入困境。	遭遇来自开源替代产品的竞争。

05

人才篇

关于计算机/软件/开源教育的两个疑问

擅长自学的学生与始终懵懂的学生，区别何在？

为什么很多开发者，常年996，苦不堪言？

不同的学生，区别何在?

有些学生，似乎天生就喜欢计算机，从小就开始玩（电脑、游戏、手机、编程）

有些学生，只是听说“IT是一个不错的行当”，就在大学志愿的填报时，选择了相关专业

当前我们缺少哪些开源人才

会写代码的程序员

- 但是这远远不够

写出优秀技术文档的Tech Writer

- 现在凤毛麟角

产品经理、设计师

- 为什么很多开源软件，都那么难用、难看？

开源社区运营

- 仅仅照搬普通的社区运营经验，也是不行的

开源法务工作者

- 现在倒是有越来越的律师朋友，开始对开源感兴趣了

开源布道师

- 那些能用自己的热情，点燃他人的人

开源教育者

- 谈开源教育，有多少擅长教育的老师呢？

开源研究者

- 现在严重缺乏，能够从经济学、社会学、人类学、法学、伦理学、管理学等诸多领域，对开源进行研究的人

开源需要什么样的人才?

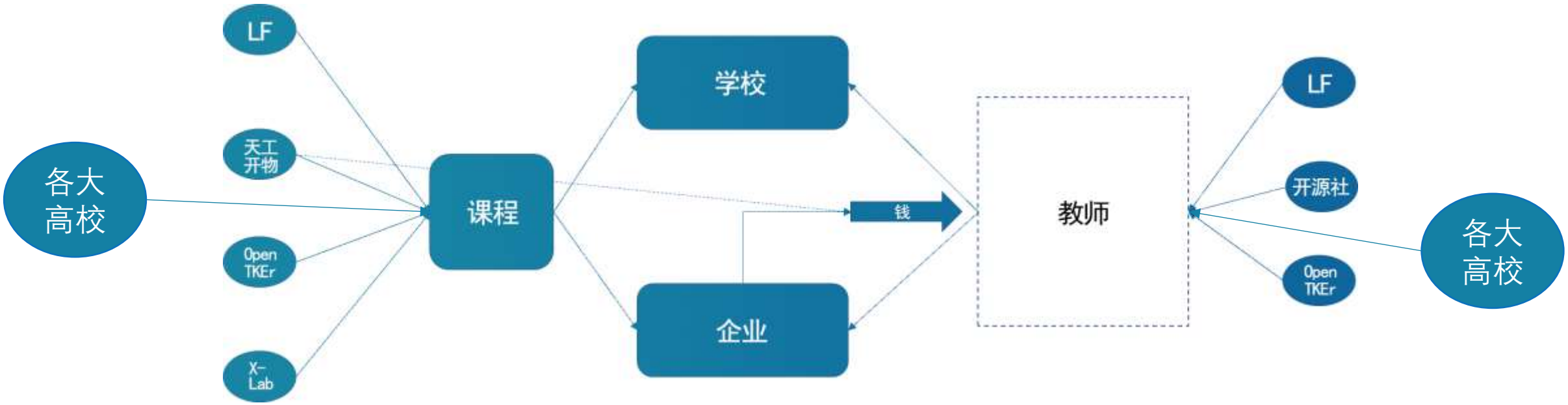
开源教育方法论

在数字的世界中学习

在开放的环境中学习

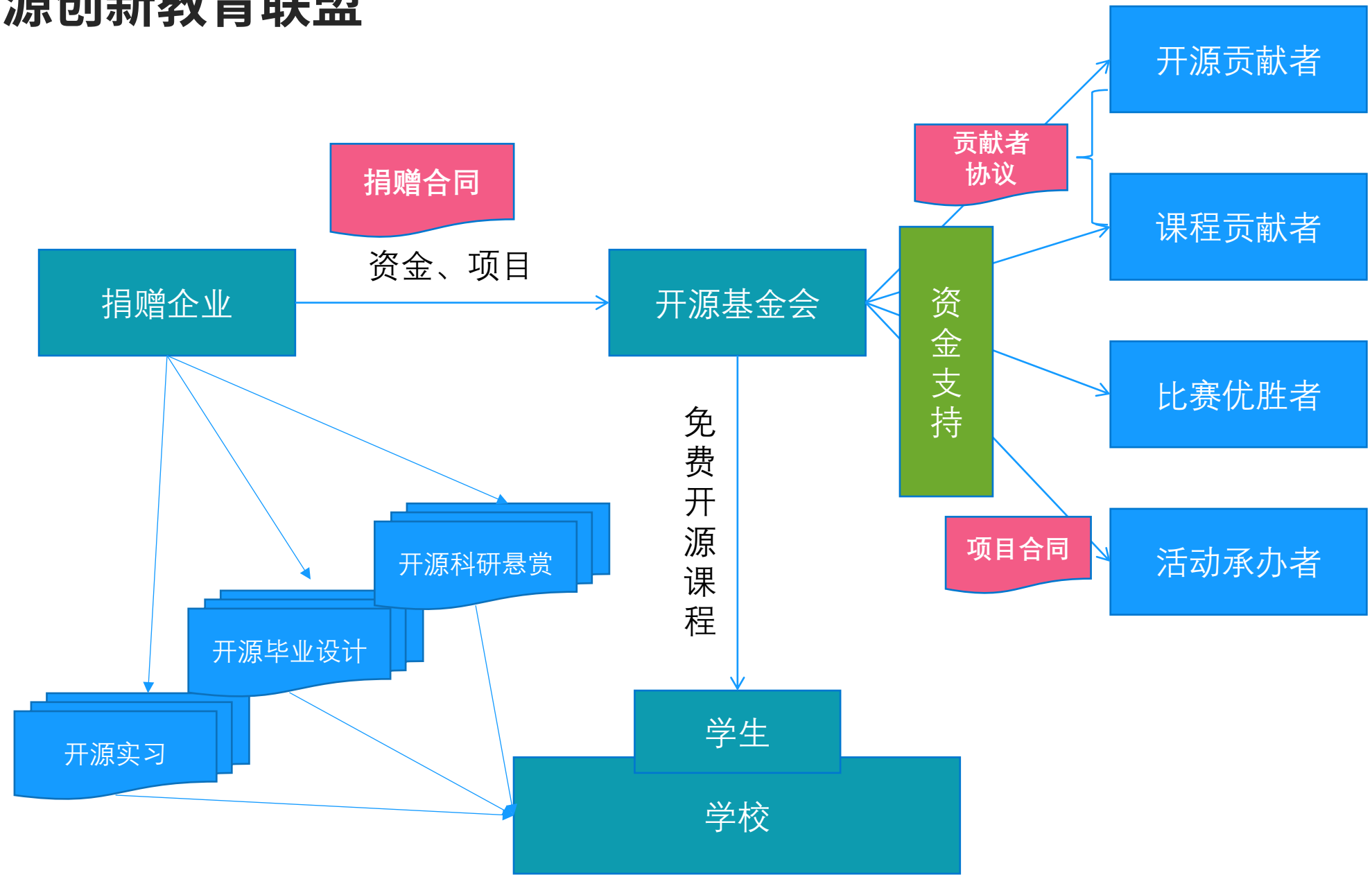
在实践与实战中学习

开源创新教育联盟



授课对象	授课内容	授课时长	费用	证书
高校学生	开源101	20周		高校学分
高校学生	开源创新与数字治理	20周		高校学分
企业员工	开源治理师培训	3天		Linux基金会、OpenChain、天工开物开源基金会、上海开源信息技术协会
企业员工	开源社区运营师培训	3天		Linux基金会、天工开物开源基金会、上海开源信息技术协会、开源社
企业管理者	开源管理与战略研讨班	3天		Linux基金会

开源创新教育联盟


捐赠合同
资金、项目
捐赠企业
开源基金会
贡献者
协议
开源贡献者
课程贡献者
资金支持
比赛优胜者
项目合同
活动承办者
免费开源课程
开源科研悬赏
开源毕业设计
开源实习
学生
学校

开源创新教育项目

开源毕业设计

- 高校、企业：双向选择
- 双导师制度
- 新颖性、实用性、难度适中、适当激励

开源实习

- 基金会牵头：与企业、学生签约
- 基于OpenRank的激励资金池
- 为期半年，自由参与，颁发实习证书

开源科研悬赏

- 企业出题，出奖金
- 基金会监督并组织
- 高校研究团队自由申请

06

政策篇

美国的开源产业政策

- 出台支持开源发展的政府政策
  - 早在 2002 年，美国智库就开始对开源软件的政府政策问题进行研究，并发布关于开源软件的政府政策报告，对包括政府采购和专利等在内的政策议题进行探讨，为政府政策提供支持。此后，欧美国家政府开始有意识地出台相关政策推动开源发展。据欧盟委员会“开源观测”项目 2020 年发布的分析报告，欧盟成员国（包括英国）过去 20 年来共出台了不少于 75 份政策文件（如政府计划、战略文件等）和 25 份法律文件（如议会决议、法律、法规等）以推动开源发展；其中，有 25 份政策文件和 6 份法律文件专门针对开源软件而制定，其他文件则是在其数字化议题中提到了开源。欧美国家政府促进开源发展的政策主要包括：推动政府软件开源和公共数据开放、引导业界关注开源风险等。
- 推动政府软件和财政资助项目成果软件开源
  - 2016 年 8 月，美国政府发布“联邦源代码政策”，要求联邦机构每年必须将不少于 20% 的新开发源代码以开源形式公开发布，并且要求开源至少 3 年。2019 年，英国出台的《数字服务标准》及此后更新的《服务标准》中要求，政府部门应选择合适的许可证开源所有新的代码。2020 年 10 月，欧盟委员会批准了《开源战略 2020-2023》特别强调软件解决方案和专业知识的共享和重用，以及在信息技术和其他战略领域增加开源的使用，秉持开放、转型、共享、贡献、安全等原则提高欧洲数字化建设和公共服务能力。2021 年，法国发布的《国家开放科学计划（2021—2024 年）》要求，公共资金资助的研究数据、算法和源代码应通过开放许可进行传播共享。

美国的开源产业政策

- 推动政府公共数据开放
  - 2016 年，法国《数字共和国法案》要求开放公共研究数据。2019 年 1 月，美国国会通过了《开放政府数据法案》，将开放数据作为美国法典的一部分。美国成为继法国、和德国之后，将开放政府公共数据从政府政策上升为国家法律的国家。在这些国家，政府公共数据应以机器可读的格式，在不损害隐私或安全的前提下，默认向公众开放。
- 引导产业关注开源风险
  - 早在 2004 年，美国联邦金融机构审查委员会发布的《开源软件风险管理指引》要求，金融机构在采用开源软件时参照该指引加强风险管理。此外，英国政府发布了《开放代码的安全注意事项指南》；欧盟发起过开源软件审计项目改善关键开源软件的安全性。
  - 2022 年，美国白宫与开源组织、科技巨头共同推动 1.5 亿美元开源软件保护计划。Linux 基金会和 OpenSSF 已经为 1.5 亿美元确定了 10 个投资流，将在两年内分摊。

英国的开源产业政策

- 英国在 2004 年首次发布开源产业政策，并于 2009 年 2 月进行了更新，开源非营利组织 OpenUK 于 2021 年 2 月在 2021 年欧盟开源政策峰会发布了其三阶段报告，报告指出开源技术为英国贡献了高达 430 亿英镑（602.2 亿美元）的经济增长，这表明英国在开源开发方面领先于欧洲。并表示，英国仍是开源技术的领导者，其国内预计有 12.6 万名贡献者参与了创建、开发和维护开源的工作；这一数字将近欧盟 26 万名开源开发者中的一半。
- 事实上早在 2012 年 11 月，英国政府内部就已经就采用开源技术发出了 Open Standards Principles 的指引，但这次却更进一步，将采用开源技术常规化。这次在政府服务设计手册中的 When to use open source 中，就明文指出政府必须在作业系统、网路软体、网页伺服器、资料库和程式语言方面，逐步以开源技术技术取代专属或闭源的技术。
- 2016 年为英国政府开发的新代码现在已经开源了。在 2017 年，已经越来越多的国家，组织和公司采用开源软件。现在，英国政府也宣布采用开源公司办公套件，那就是基于 LibreOffice 的“GovOffice”。协作办公套件 GovOffice 支持超过 100 种格式，包括 Microsoft Office 和 Google Docs。GovOffice 是基于最流行的办公软件 LibreOffice，也将支持从移动设备直接跳转到 Web 浏览器打开和编辑文档。这个措施将会覆盖所有的 Govt 机构，甚至是政府机构代表。

德国的开源产业政策

- 自 2001 年德国慕尼黑决定推动 LiMux 计划，2005 年正式启动了相关迁移工作，但是，2017 年 11 月，慕尼黑城市委员会（Munich City Council）正式决定到 2020 前回归微软的 Windows 系统，这意味着德国开源运动遭受重大挫折，甚至于可以说是失败了。
- 慕尼黑启动的LiMux既包括操作系统，还涉及到了大量的应用软件。操作系统主要推出LiMux，它是Linux的一个发行版本，包括了Ubuntu、LibreOffice和WollMux等套件；应用软件主要涉及到OpenOffice，后来切换到LibreOffice。
- 只是非常可惜，这种技术上的独立运动，在慕尼黑的开源计划中，并没有足够的群众基础。德国是一个重视产业政策的国家，强大的政府希望推动具有自主知识产权的开源运动，借此挑战微软等“霸权”，只是事与愿违，该运动并没有得到除了跟LiMux项目利益相关者之外的支持，甚至于一些德国IT企业，例如SAP等也没有深入参与该计划。
- 总体来讲，德国开源产业还处于个人主义阶段（缺乏群众基础），没有进入到成熟商业模式运行阶段。

中国的开源政策

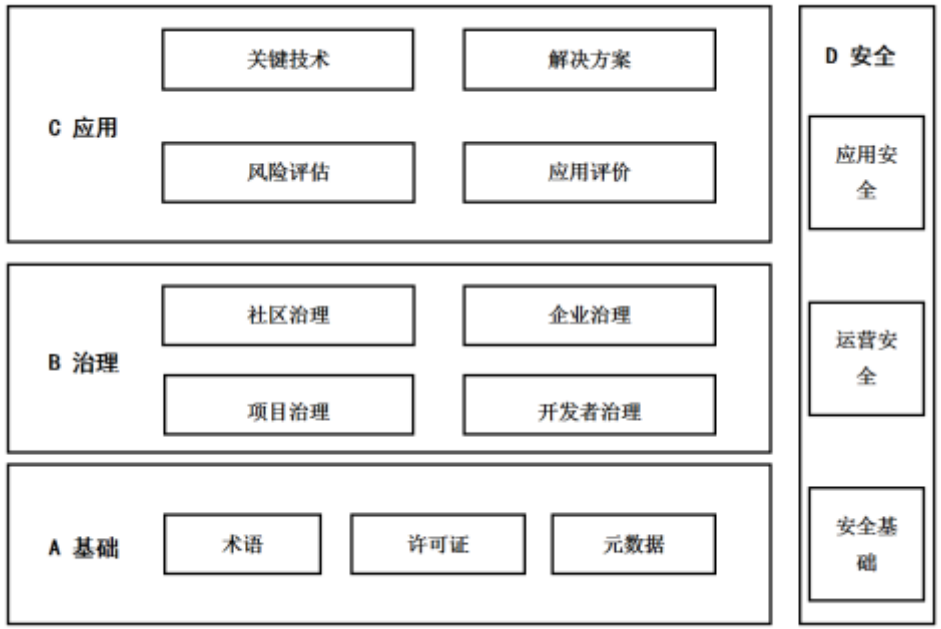
- 2019 年，华经情报网在《2018 年中国开源软件行业发展现状，开源软件整体发展形势向好》文章中，对国内开源政策做了详细说明，以下是部分段落的节选。
  - 2017 年，我国政府对开源的认识进一步提升，对开源软件发展的政策支持力度在不断加强。《信息产业发展指南》明确提出："支持企业联合高校、科研机构等建设重点领域产学研用联盟，积极参与和组建开源社区"，"支持开源、开放的开发模式"，重点推进云操作系统等基础软件产品的研发和应用。《软件和信息技术服务业发展规划（2016－2020 年）》中提到："发挥开源社区对创新的支撑促进作用，强化开源技术成果在创新中的应用，构建有利于创新的开放式、协作化、国际化开源生态"，"支持建设创客空间、开源社区等新型众创空间"，要实施软件"铸魂"工程，重点"构筑开源开放的技术产品创新和应用生态"。

中国的开源规划

- 2021 年 3 月 12 日，新华社受权全文播发《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》，「开源」首次被明确列入国民经济和社会发展五年规划纲要，相关内容摘录如下：
  - 聚焦高端芯片、操作系统、人工智能关键算法、传感器等关键领域，加快推进基础理论、基础算法、装备材料等研发突破与迭代应用。加强通用处理器、云计算系统和软件核心技术一体化研发。加快布局量子计算、量子通信、神经芯片、DNA 存储等前沿技术，加强信息科学与生命科学、材料等基础学科的交叉创新，**支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。**

中国的开源标准

信通院：可信开源标准体系



标准院：开源标准体系

开源政策的误区

- 基于错误的供应链想象
  - 将开源生态，想象成一串供应链，其中一环断掉，就会整个断供。
  - 误判开源代码托管平台，在开源生态中的定位与价值
  - 误判开源供应链的韧性，假设美国议员一个提案，就能够断掉一个国家的开源软件使用许可（事实上到现在，俄罗斯都还没有被开源断供）
  - 混淆软件断供与开源供应链断供
- 基于错误的科技创新想象
  - 在开源社区，主要诞生的创新是：改进型与填补型的。而基础型创新与突破型创新，主要还是会在专业研究机构与企业（围绕商业场景）中诞生。
  - 要求科研攻关团队，在获得成果之后开源，是正确的做法，但是要注意2点：
    - 【有限开源】科研成果的开源范围，应该事先有所规划
    - 【真开源】开源之后的社区，应该确保其社区活跃度

开源政策的出发点

- 从开源生态总体价值的角度出发
  - 扩大数字公共产品的数量、质量、用户量，提供各类企业与组织对于开源的利用水平，降低本国、本地区的IT综合成本
  - 普及开源供应链安全的正确知识，鼓励企业与各种机构设立OSPO，对接开源社区与开源基金会，提高自身的开源治理水平
- 从注重开源供应链安全的角度出发
  - 从政府、国央企开始，对供应商提出要求，提供完整、准确的SBOM
  - 注重供应商的开源安全、研发能力。
    - 【限制】设立某种资质认证机制
    - 【鼓励】为符合资质的企业，建立倾斜扶持政策

开源政策的出发点

- 从开源商业模式的逻辑出发
  - 企业在开源贡献之后，能够得到License、专利等知识产权保护。企业对于知识落差的预期能够实现，不至于被非法侵权，导致“开源反受其害”。
  - 基于开源的企业，为开源提供服务的企业，能在一个更加健康的市场环境中生存。
- 从开源人才培养的角度出发
  - 支持更加综合性的开源人才培育计划，例如《开源微专业》的设立
  - 在现有的论文KPI体系之外，建设基于开源贡献的教/学激励机制
  - 作为新技术不断发生的土壤，直接扎根土壤学习的效果，要比“总结梳理知识、编写教材、年度授课”的机制更加及时、高效。需要支持在高校推广立足开源社区的教学模式
- 从建立全球影响力的角度出发
  - 如何通过开源，输出技术，在全球范围建立技术影响力？
  - 如何帮助那些愿意接受我们帮助的国家（一带一路国家?），以“开源共建、协作赋能”的方式，建立并巩固自身的数字主权？

开源政策建议

- 建设数字公共产品这个“知识公地”，帮助企业更好的使用开源
- 注重开源供应链安全
- 健全围绕开源的知识产权保护体系
- 鼓励开源教育创新
- 积极参与全球开源贡献

谢谢大家

汇报人：庄表伟

时间：2024.08