

企业开源治理的实践与案例

刘天栋 - 开源社发起人、理事
我不是律师

下一代
软件开发
SOFTWARE
DEVELOPMENT

议程

1. 开源社简介
2. 开放与开源
3. 开源治理的实践
4. 选择许可证



开源社是由支持开源的企业、社区及个人，依“贡献、共识、共治”原则，所组织的 **纯公益、草根开源联盟**，旨在共创健康可持续发展的开源生态体系，并推动中国开源社区成为全球开源软件的积极参与及贡献者。

56家单位 (2014.10-2017.04)

- ✓ 社区，企业，媒体，协会，高校，政府
- ✓ 软件，硬件，服务，外包
- ✓ 操作系统，数据库，云计算，开放数据，大数据，物联网

7位理事会理事+秘书处



64位开源大使遍布全国



开源治理

- ✓ [开源许可证介绍](#)，[开源许可证选择器](#)，
开源流程指导文档，法律委员会...

国际桥梁

- ✓ Apache Software Foundation, AllSeen Alliance, GNOME Foundation, Linux Foundation, Node.JS Foundation, Open Source Initiative (OSI), Open Innovation Networks (OIN)...

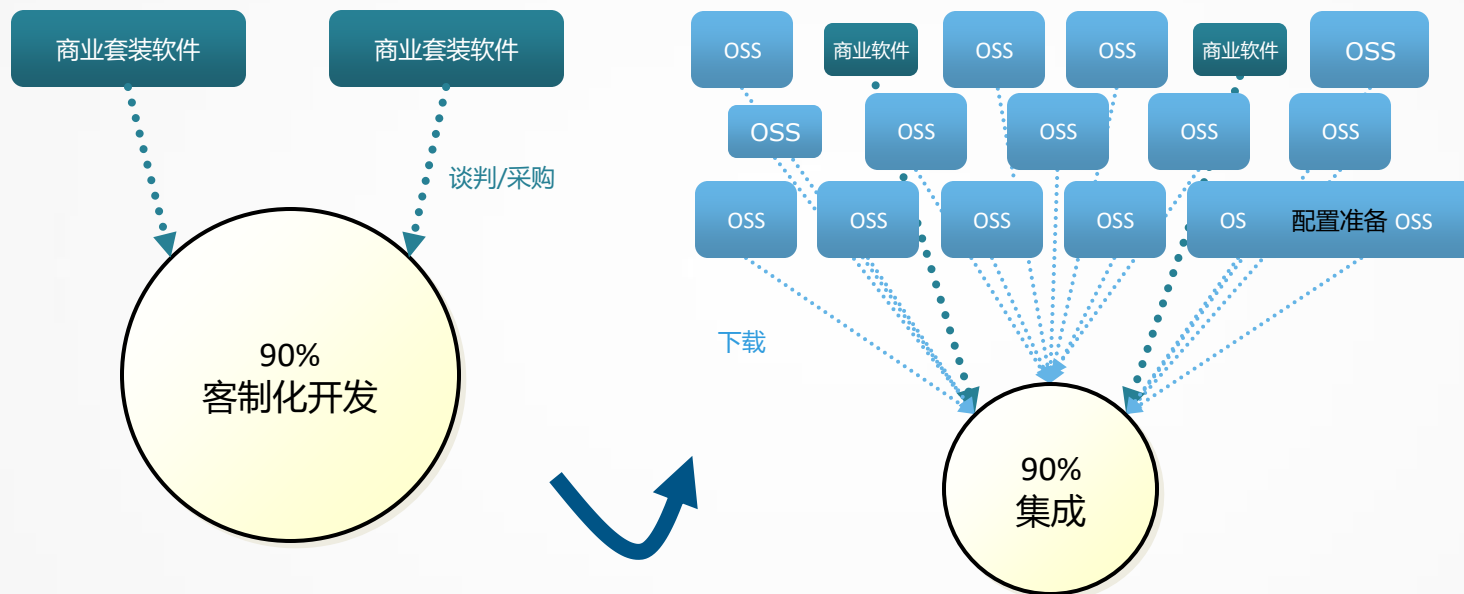
社区建设与服务

- ✓ 开放黑客松，开源生态系统报告，社区活动推广/支持...



议程

1. 开源社简介
2. 开放与开源
3. 开源治理的实践
4. 选择许可证



78%公司使用开源
63%公司参与开源

■ 吸引人的利益

- 更快的部署及实施
- 更低的开发及维护成本

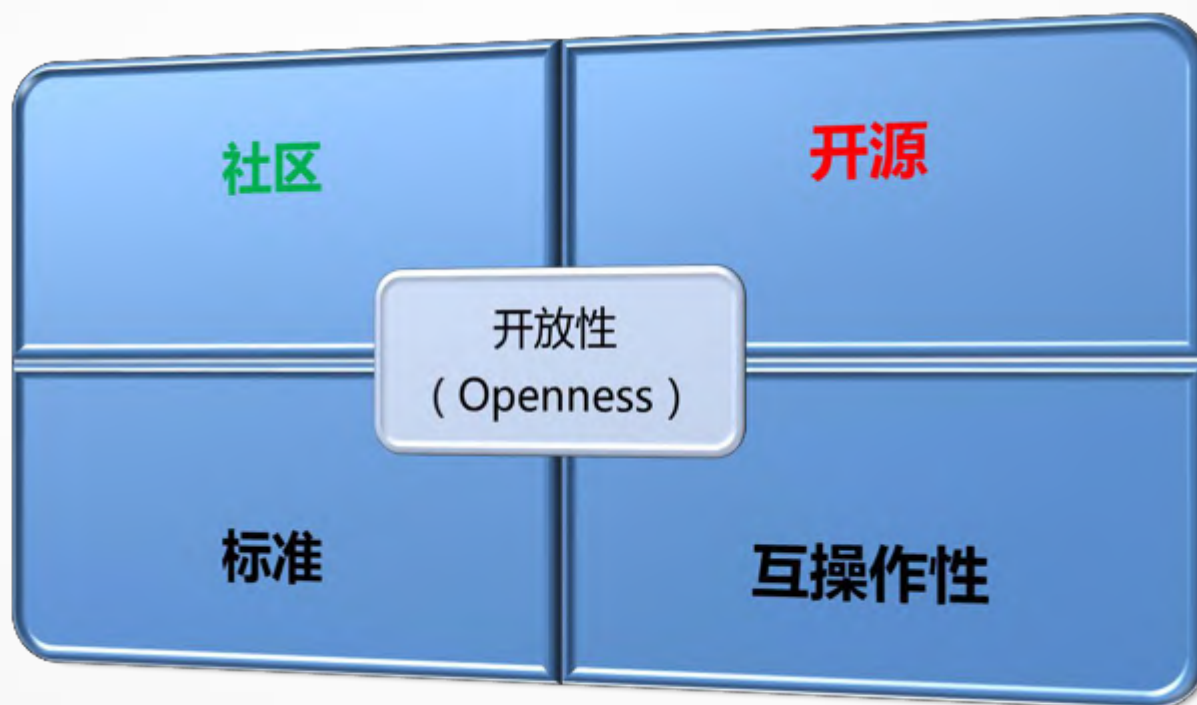
■ 但是。。。增加软件项目的复杂性

- 更多代码来源，许可证，兼容性问题
- 自助式更新

云里雾里的选择？



开放的真义



玻璃天花板？

最成功的开源项目的规模及治理模式

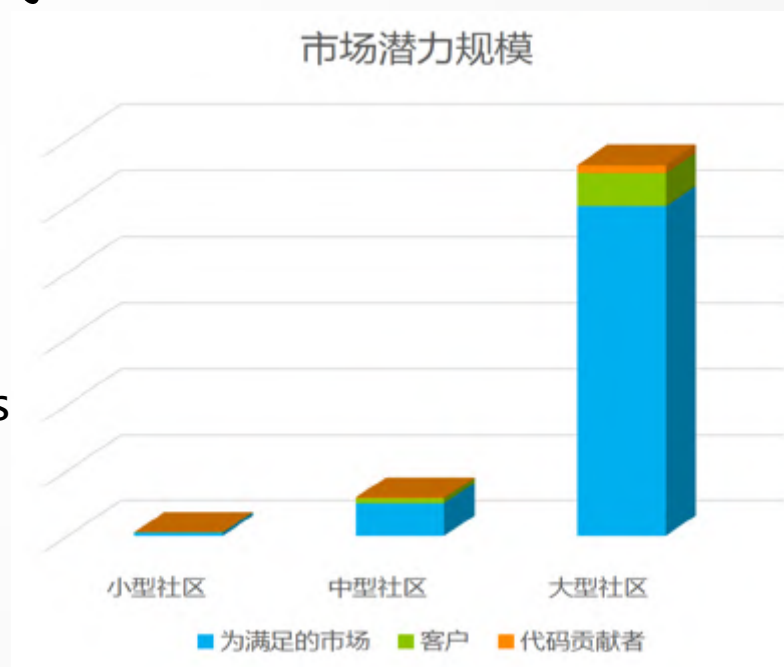
非盈利基金会助力社区及业务增长

■ 规模 X 10

- Linux, KDE, Apache, Eclipse, Perl+CPAN, Mozilla+Addons, Gnome, Drupal, GNU

■ 回报 X 5

- 单一厂商如 MySQL, Qt, OpenOffice, JBoss
 - <200开发者，日均代码提交<100次
- 9大基金会项目
 - >1000开发者，日均代码提交>100次



Henrik Ingo, 2010

议程

1. 开源社简介
2. 开放与开源
3. 开源治理的实践
4. 选择许可证

- 开源治理是社会/社交框架
OSS Governance is a Social Framework
 - 开源许可证是法律框架
OSS License is a Legal Framework
- Ross Gardler, President, ASF

行业巨头

- Google: <https://developers.google.com/open-source/>
- Intel: <https://01.org/>
- Microsoft: <https://microsoft.com/opensource>
- Samsung: <http://commit101.org/>

新兴公司

- Box: <http://opensource.box.com/>
- Dropbox: <https://opensource.dropbox.com/>
- Facebook: <https://code.facebook.com/opensource>
- GitHub: <http://todogroup.org/blog/why-we-run-an-open-source-program-github>
- Twitter: <http://todogroup.org/blog/why-we-run-an-open-source-program-twitter/>



推荐：每家公司都应设立开源项目部门(OSPO) – 李建盛, 2017-03-15, 开源之道

企业开源治理的要素

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

问题#1

你的企业对于使用开源软件抱持的态度（ 1-5 ）

- 1 – 不允许使用任何开源软件
- 2 – 仅限于如果没有其他解决方案存在
- 3 – 如果开源软件优于其他解决方案
- 4 – 开源软件和专有软件解决方案一视同仁
- 5 – 如有开源解决方案时优先考虑

开源策略

- 组织意图及目标
- 清晰的商业表达
- 发展策略的价值

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告



2017

Twitter的开源之旅

2006-2015

- 开源自第一天起
- 4000员工
- 3亿+ 活跃用户
- 5亿+ 推特/天
- 80%为移动用户

开源办公室 (OSO)

- 速度及最少的官僚
- 让开源流程令人愉快
- 有效率地保护公司
- 为关键项目建立社区
- 培训/文化至为关键
- 我们为工程师服务



Bootstrap项目

- 聪明地选择许可证
- 由Apache License 2.0转换到MIT
- 一开始就要选对许可证 (更宽容-Permissive)
- 项目成败难以预料
- 务必确保工程师有时间管理开源项目 (社区)
- 确保项目有一个以上的项目主要负责人或交给社区管理

贡献带来影响力

Mesos项目

- 与高校/学术界密切合作
 - UC Berkeley AMPLab
- 与开源基金会密切合作
 - 获取更佳实践
 - 培养协作, 加速成长

TWEMCACHE项目

- 尽量避免分叉 (Fork)
- 别让上游/主干感到意外

社区不会凭空诞生

Parquet项目

- 在开源之前, 先在内部分享代码以测量未来潜力
- 与协作伙伴携手发布势头
 - 2012夏: Twitter与Cloudera合并Parquet计划
 - 2013三月: 宣布开源
 - 2013七月: 发布1.0版; 获得来自5个不同组织的18个贡献
 - 2014五月: 进入阿帕奇孵化器; 40+ 贡献者
 - 2015五月: 项目毕业成为阿帕奇顶级项目; 60+ 贡献者

开源项目办公室成为核心

开源政策

详述规则（重点要素）

- 法务政策
- 获取政策
- 使用政策
- 支持政策
- 管理政策
- 伙伴政策
- 贡献及发布政策

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

领导支持

- 转化争议
- 预算/资源
- 以身作则

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

利害关系人认可

- 确保遵循流程
- 最佳途径
 - 高层决心（如软件开发）
 - 理解开源软件策略
 - 参与到政策及流程
 - 快速批准关键活动
 - 参与定期检讨

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

问题#2

你的企业用何种技术追踪开源软件的使用
(可复选)

- 1 – 没有用任何正式的软件库存系统
- 2 – 每个项目自行报告
- 3 – 所有项目自行报告
- 4 – 人工审计已经自行报告的软件项目
- 5 – 自动化代码扫描工具

- 咨询，软件或硬件解决方案
- 优化管理
 - 咨询顾问
 - 代码库的评估
 - 软件扫描工具
 - 批准、追踪及管理工具
 - 技术支持及保障

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

资源库

- 原因-了解企业现状
- 时机-建立库存清单；定期检查更新
- 内涵-按部就班，逐步拓展
- 选项一：自行报告（耗时耗力，不准确）
- 选项二：扫描系统或应用 (如OSS Discovery)

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

- 调研：

- [Ohloh](#): 社区数据
- [Osalt](#): 开源替代方案
- [Ostatic](#): 开源软件发现、评估、协作网站
- [OpenLogic](#): 专业第三方厂商
- 开源项目主页

- 认证：自主/第三方

- 社区健壮度，采用度，法务考量，技术支持等
- 企业架构师的评估及推荐

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

- 一般代码资源库
 - Soureforge.net, Google Code, java.net, freshmeat等
 - 确认由正式来源取得代码
 - 小心未经审查的镜像（或Maven资源库）
- 内部资源库
 - 自行维护内部资源库
- 在线咨询服务厂商（如：[OLEX](#)）
 - 可信赖的代码来源
 - 已认证的软件
 - 审核过的代码

运营开源政策

- 需要做什么？
 - 利用技术手段以强力执行开源政策
- 所需能力？
 - 依据开源政策允许/避免代码下载
 - 追踪下载情形
 - 要求在下载时宣告使用理由
 - 要求在下载时先取得批准

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

请求与批准

- 原因? 例外处理原则
- 时机? 下载前, 开发前, 投产前, 或发布前
- 参与者? 申请人及批准者
- 途径?
 - 人工处理或自动化系统 (自行开发或第三方)
 - 流程及规则自动化, 评论及反馈追踪, 可客制化

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

审计

- 原因? 政策, 许可证, 内部智慧财产权
- 时机?
 - 应用生命周期: 开发/组建, 测试, 模拟上线, 投产
 - 定期审计+不定期抽检
- 对象?
 - 使用中的开源项目及许可证
 - 选项: 开源软件抄袭 (如果对外发行)
- 手段?
 - 信息比较: 政策, 使用者的宣告/请求, 代码扫描
 - 找出违规并矫正修复

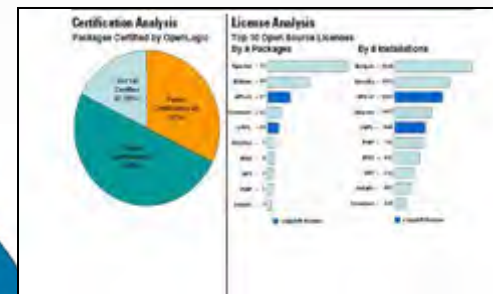
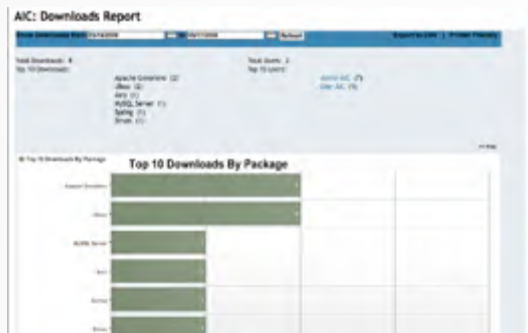
1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

报告

- 开源软件库存及更新定期报告
- 开源软件下载及用户宣告
- 请求及批准的状况
- 政策合规及违规状况
- 应用 “物料及许可证清单”

1. 开源策略
2. 开源政策
3. 领导支持
4. 利害关系人认可
5. 资金
6. 资源库
7. 配置/准备
8. 请求与批准
9. 审计
10. 报告

资源库



批准

政策



Sample screenshot from OpenLogic

Google是如何做开源的

<https://opensource.google.com/docs/>

- Google发布一款新的开源项目[遵循那些流程](#)
- 如何为其它开源项目[提交补丁](#)
- Google是如何[管理引入第三方的开源项目以及如何使用](#)
- Google 为何仅仅使用[某些特定的许可协议的项目](#)
- 为什么Google需要将所有接受到的补丁都是[遵循许可协议](#)

TODO Group

Google在2014年协助组建的众多商业公司组成论坛，讨论参与开源的最佳实践和协作。

推荐：杜玉杰-
开源协议可以有
什么样的商业打
法，GitChat

议程

1. 开源社简介
2. 开放与开源
3. 开源治理的实践
4. 选择许可证

- 开源治理是社会/社交框架
OSS Governance is a Social Framework
- 开源许可证是法律框架
OSS License is a Legal Framework

- Ross Gardler, President, ASF

分辨开源软件与其他

- Freeware (免费软件)
 - 免费使用
 - 限制用途、不给源码
- Shareware (共享软件)
 - 通常免费使用，有限制 (时间或功能)
 - 通常另有商业版本可以购买
 - 限制用途、不给源码
- Public Domain (公共领域，公共财)
 - 著作权期间结束、抛弃著作权
 - 没有权利

开源软件的定义

<http://www.kaiyuanshe.cn/govern/1.html>

- ✓ OSI 核准的每项许可协议都符合开源定义的条件。该定义包含10项标准。其中最重要的是软件可以自由再发行，直接访问源代码，以及允许对软件与演绎作品进行修改并在相同的许可条件下发行。

1.可以自由再发行 Free
Redistribution

2.直接访问源代码 Source Code

3.衍生作品 Derived Works

4.作者源代码的一致性 Integrity
of The Author's Source Code

5.许可证的分发 Distribution of
License

6.不歧视任何个人或团体 No Discrimination Against Persons
or Groups

7. 不歧视任何特定用途 No Discrimination Against Fields of
Endeavor

8. 许可证不得限于某个特定产品 License Must Not Be Specific
to a Product

9. 许可证不得限制其他软件 License Must Not Restrict Other
Software

10. 许可证必须保持技术中立 License Must Be Technology-
Neutral

主流的开源许可证

1. [Apache License 2.0](#)
2. [BSD 3-Clause "New" or "Revised" license \(BSD-3-Clause\)](#)
3. [BSD 2-Clause "Simplified" or "FreeBSD" license \(BSD-2-Clause\)](#)
4. [GNU General Public License \(GPL\)](#)
5. [GNU Library or "Lesser" General Public License \(LGPL\)](#)
6. [Mozilla Public License 2.0 \(MPL-2.0\)](#)
7. [MIT license](#)
8. [Eclipse Public License \(EPL-1.0\)](#)
9. [Common Development and Distribution License \(CDDL-1.0\)](#)

<http://www.kaiyuanshe.org/article/> (中文版)

<https://opensource.org/licenses/category> (英文版)

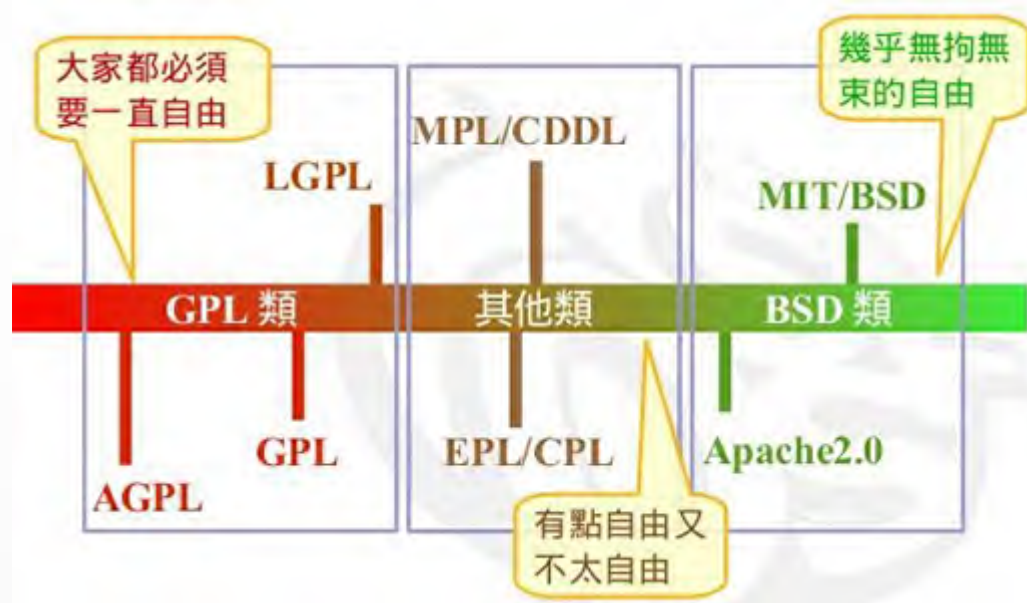
选择开源许可证

我该选择哪一种许可证？

- 跟着我喜爱的开源社区？
- 你会生气吗？
- 为你老板省律师费？知名/通用

著作权/著佐权 (Copyleft)？

- 你想强制他人贡献回馈吗
- 专利保护？
- 允许转为商业用途？



选择开源许可证

<http://www.ruanyifeng.com/blog/Cc-By-3.0/>
2011.5.2



选择开源许可证

开源社 kaiyuanshe

主页 资讯 论坛 成员 资源 关于

搜索

开源许可证分辨器

该工具旨在帮助用户理解他们自己对于自由和开源软件许可协议的偏好。用户必须自己阅读这些许可协议。在将许可协议适用于您的财产之前，阅读并完全理解您选择的许可协议是非常重要的。支撑该工具运行的许可类型分类，会不可避免地有些缩减。因此，不能也切不可将该工具的输出信息视为法律意见。

切记：必须阅读并理解您选择的许可协议。

筛选条件

1

您想将结果限定为开放源代码促进会（OSI）所描述的“流行并广泛使用，或拥有广泛社群”的许可协议吗？
这将以牺牲一些更冷门但或许有用的特征为代价来确保该许可协议成为“主流”协议。

请选择

下一步

筛选结果

Academic Free License 3.0	评分 100
Adaptive Public License	评分 100
Affero GNU Public License	评分 100
Apache License 2.0	评分 100
Artistic License 2.0	评分 100
Attribution Assurance Licenses	评分 100

Choose an open source license

Which of the following best describes your situation?



I want it simple and permissive.

The **MIT License** is a permissive license that is short and to the point. It lets people do anything they want with your code as long as they provide attribution back to you and don't hold you liable.

jQuery, **.NET Core**, and **Rails** use the MIT License.



I'm concerned about patents.

The **Apache License 2.0** is a permissive license similar to the MIT License, but also provides an express grant of patent rights from contributors to users.

Android, **Apache**, and **Swift** use the Apache License 2.0.



I care about sharing about improvements.

The **GNU GPLv3** is a copyleft license that requires anyone who distributes your code or a derivative work to make the source available under the same terms, and also provides an express grant of patent rights from contributors to users.

Blash, **GIMP**, and **Privacy Badger** use the GNU GPLv3.

What if none of these work for me?

My project isn't software.

There are licenses for that.

I want more choices.

More licenses are available.

I don't want to choose a license.

You don't have to.

<http://www.kaiyuanshe.org/license-tool.html>

<http://choosealicense.com/>

非软件的许可证

<http://creativecommons.org/choose/>

文档、
视频、
图片、
多媒体等

许可协议要点

本网页其他显示框的内容将根据你在下面的选择自动更新。

允许您的作品的衍生作品被分享吗？

☒ 是 ☐ 不

☐ 是的，只要他人以相同方式共享

允许对您的作品进行商业性使用吗？

☒ 是 ☐ 不

你选择的许可协议

署名 4.0 国际

这是一个“自由文化协议”！



更多署名信息

这部分是可选的，如果填写，将在我们建议的HTML代码中增加计算机可读的元数据。

作品标题

作品署名

作品网址

源作品网址

获取更多许可的网址

作品形式

协议标识

把作品放到网上



本作品采用知识共享署名 4.0 国际许可协议进行许可。

复制以下代码到你的网站，让访问者知道你采用的协议。

```
<a rel="license"
href="http://creativecommons.org/licenses/by/4.0/"></a><br />本作品采用<a rel="license"
href="http://creativecommons.org/licenses/by/4.0/"
```

☒ 普通图标 ☐ 紧凑图标

加入我们，加入开源社！

- ✓ 关注开源社公众号
- ✓ 登陆开源社官网
www.kaiyuanshe.org
- ✓ 申请成为[开源社成员](#)
(单位/个人)
- ✓ 申请加入[开源大使](#)
- ✓ 关注[GitChat](#)开源治理
系列文章：庄表伟，
杜玉杰，刘天栋，李
建盛。。。

