



不止于代码，构建开源项目的 安全基础设施与开放社区治理



周鹏飞

微软 Azure 产品经理
CNCF project maintainer



[@FeynmanZhou](https://twitter.com/FeynmanZhou)



目 录

开源软件的基础设施与供应链安全

01

软件供应链安全的案例与挑战

02

业内开源云原生安全方案与框架

03

构建端到端供应链安全与 Demo

04

开源项目中的开放社区治理

05

参考链接

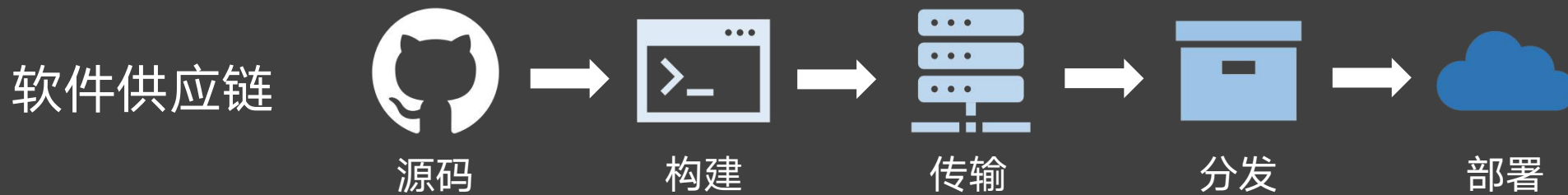
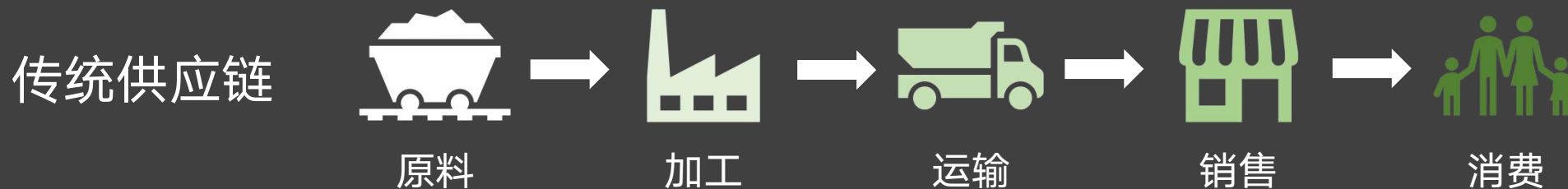
06

第一部分

开源软件的基础设施 与供应链安全



传统供应链 v.s. 软件供应链

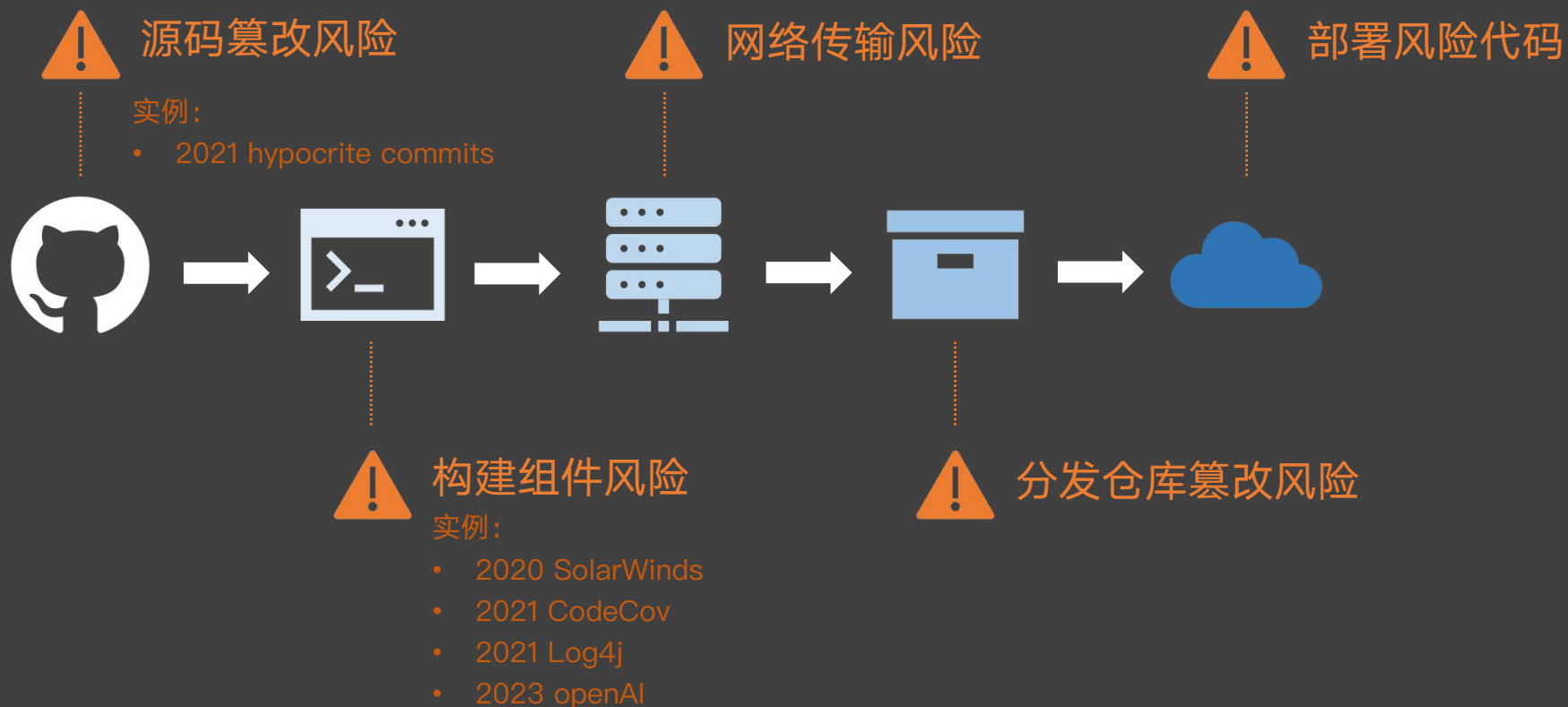


第二部分

软件供应链安全的案例与挑战




软件供应链安全的案例与挑战



软件供应链安全的案例与挑战


Key findings from EO

- Maintaining trusted supply chains by ensuring the integrity of delivery and distribution
- Securing development environments with strong access controls
- Using automated code scanning to find and remediate vulnerabilities in software
- Keeping accurate and up-to-date data on the provenance (i.e. origin) of software components



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

 [BRIEFING ROOM](#) [PRESIDENTIAL ACTIONS](#)

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal

第三部分

业内开源云原生安全 方案与框架



软件供应链安全框架

软件供应链消费框架 (S2C2F)



来源: <https://openssf.org/>





























软件制品的供应链级别 (SLSA)



(OpenSSF 基金会)

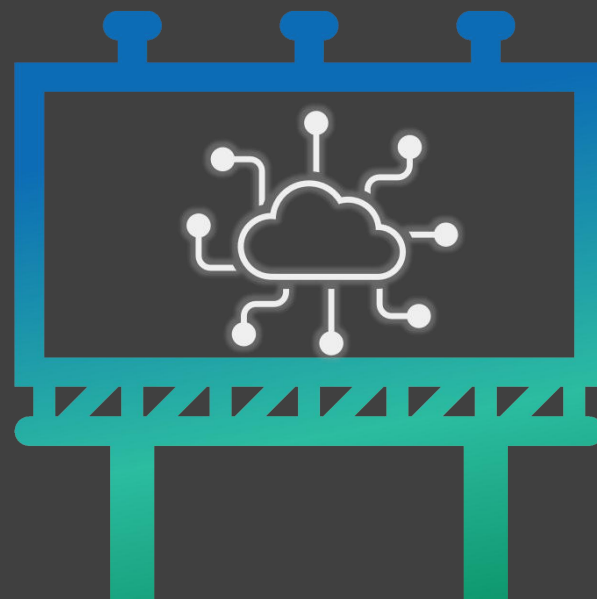
传统供应链 v.s. 软件供应链

Security & Compliance

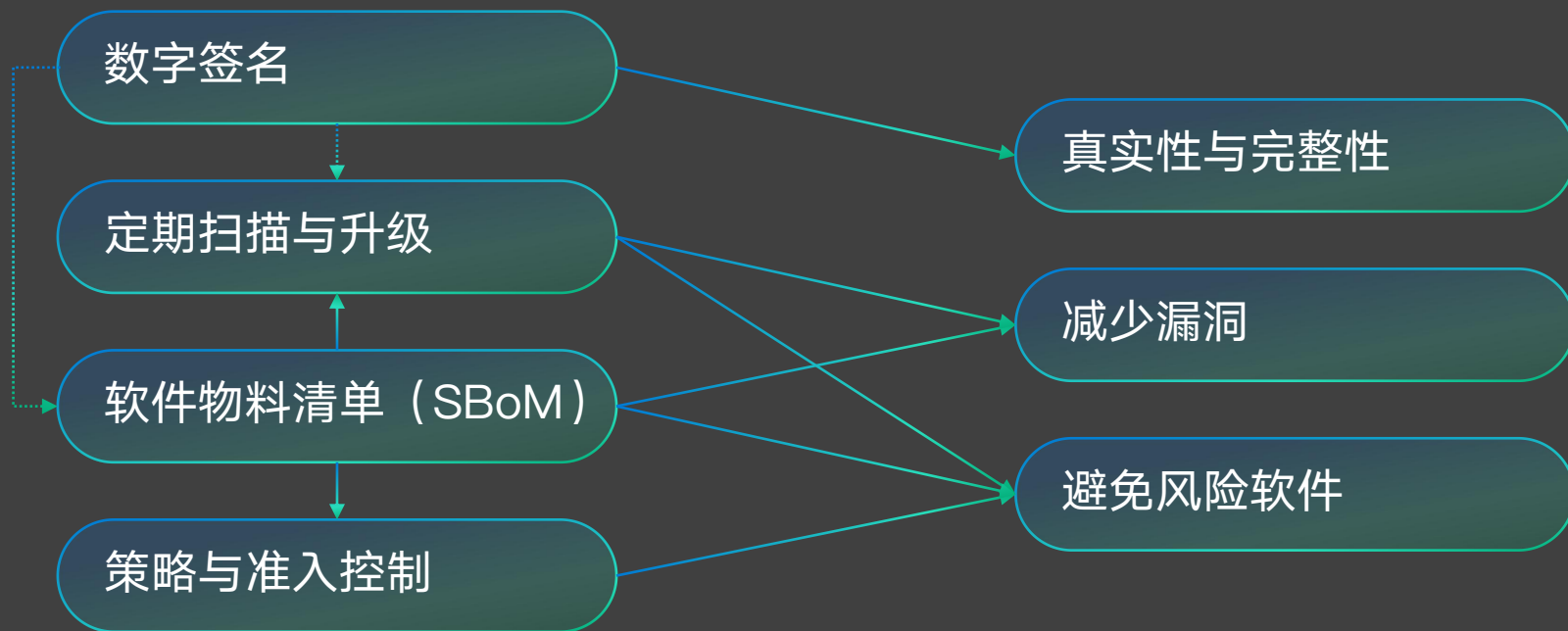
 Open Policy Agent CNCF Graduated	 TUF CNCF Graduated	 CERT MANAGER CNCF Incubating	 falco CNCF Incubating	 in-toto CNCF Incubating	 Kyverno CNCF Incubating	 Notary CNCF Incubating	 AIRLÖCK							
														
														
														
														
														

云原生安全开源项目

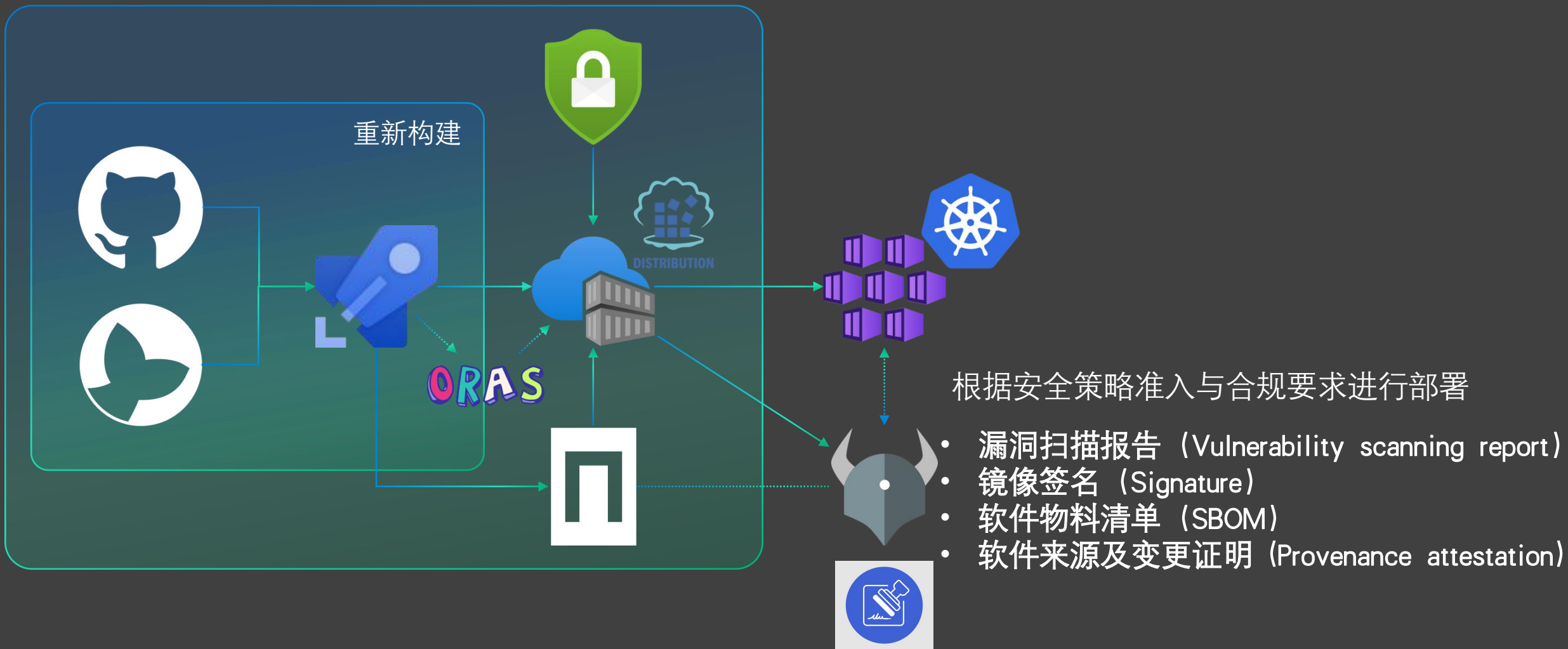
- 容器镜像及制品签名
 - Notation (Notary)
 - Cosign
- 容器镜像及制品分发管理
 - ORAS, regctl, skopeo
- 软件物料清单生成
 - Microsoft sbom-tool
 - Syft / Docker SBOM
- 软件来源及变更证明
 - in-toto attestation
- 容器镜像安全漏洞扫描与分析
 - Trivy, Synk, Clair
- 开放策略代理 (OPA)



引入数字签名技术提升镜像分发安全与一致性



引入数字签名技术提升镜像分发安全与一致性



Notary – 镜像签名与验证



JUSTIN CORMACK

Jan 27 2020

One of the most productive meetings I had KubeCon in San Diego last November was a meeting with Docker, Amazon and Microsoft to plan a collaboration around a new version of the CNCF project Notary. We held the Notary v2 kickoff meeting a few weeks later in Seattle in the Amazon offices.

Emphasising that this is a cross-industry collaboration, we had eighteen people in the room (with more dialed in) from Amazon, Microsoft, Docker, IBM, Google, Red Hat, Sylabs and JFrog. This represented all the container registry providers and developers, other than the VMware Harbor developers who could unfortunately not make it in person. Unfortunately, we forgot to take a picture of everyone!



Steve Lasker

@SteveLasker · Follow



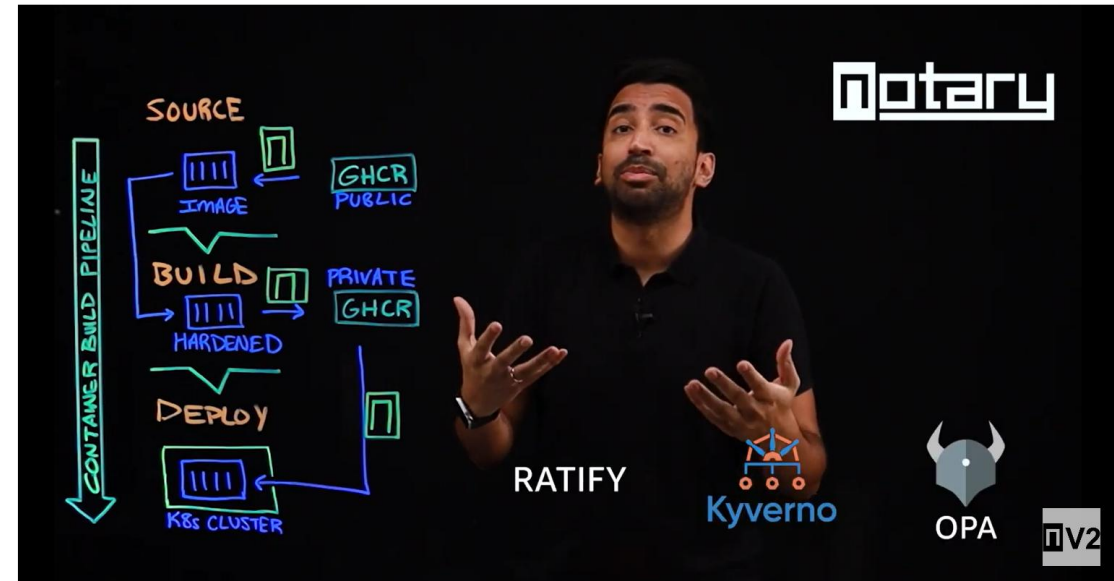
@awscloud, @GCPcloud, @Azure, @Docker, @RedHat, @jfrog collaborating on @CloudNativeFdn Notary v2 - touring the amazon spheres. Who would have thought...



- Notary was originally started at Docker to provide a general signing
- CNCF Incubating project
- Redesigning Notary in a Multi-registry world
- Amazon, Microsoft, Docker are developing the next generation of Notary project
- Integrating and move signatures across registries
- Improving usability and balance security

Standards-based spec and tooling for securing software supply chains

Signing and verifying artifacts. Safeguarding the software delivery security from development to deployment.

[Get started](#)[Try it ↗](#)

Contributed by the community, in collaboration with



Notation CLI Command Sets

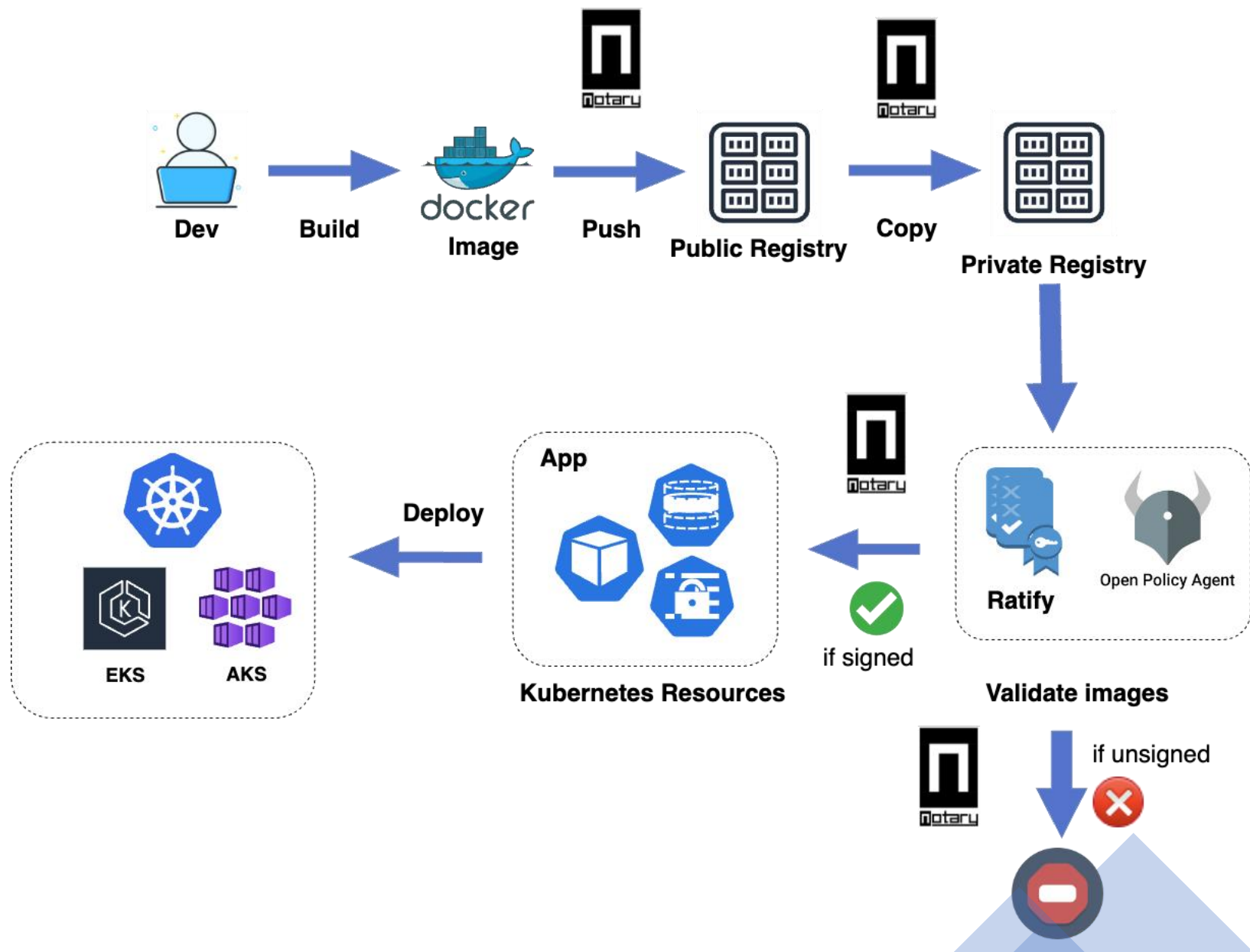
```
notation certificate: Manage certificates in trust store
notation key:        Manage keys used for signing
notation list:       List signatures of the signed artifact
notation login:      Log in to the registry
notation logout:     Log out from the registry
notation plugin:     Manage plugins
notation sign:       Sign artifacts
notation verify:     Verify OCI artifacts
notation version:    Show the notation version information
```


第四部分

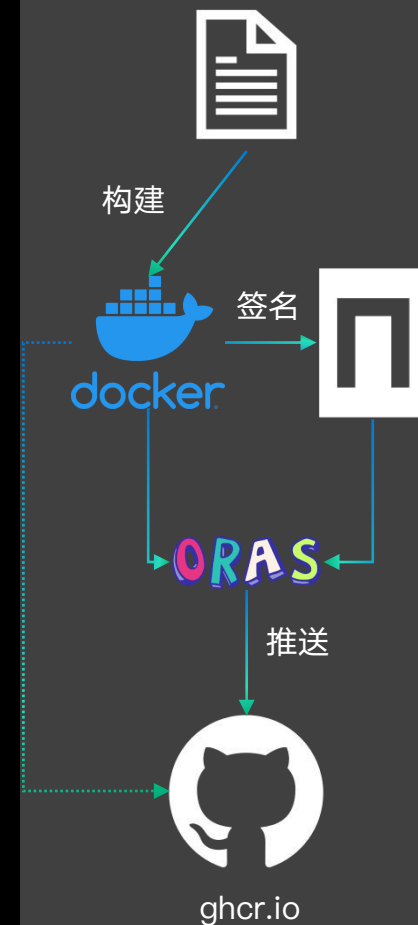
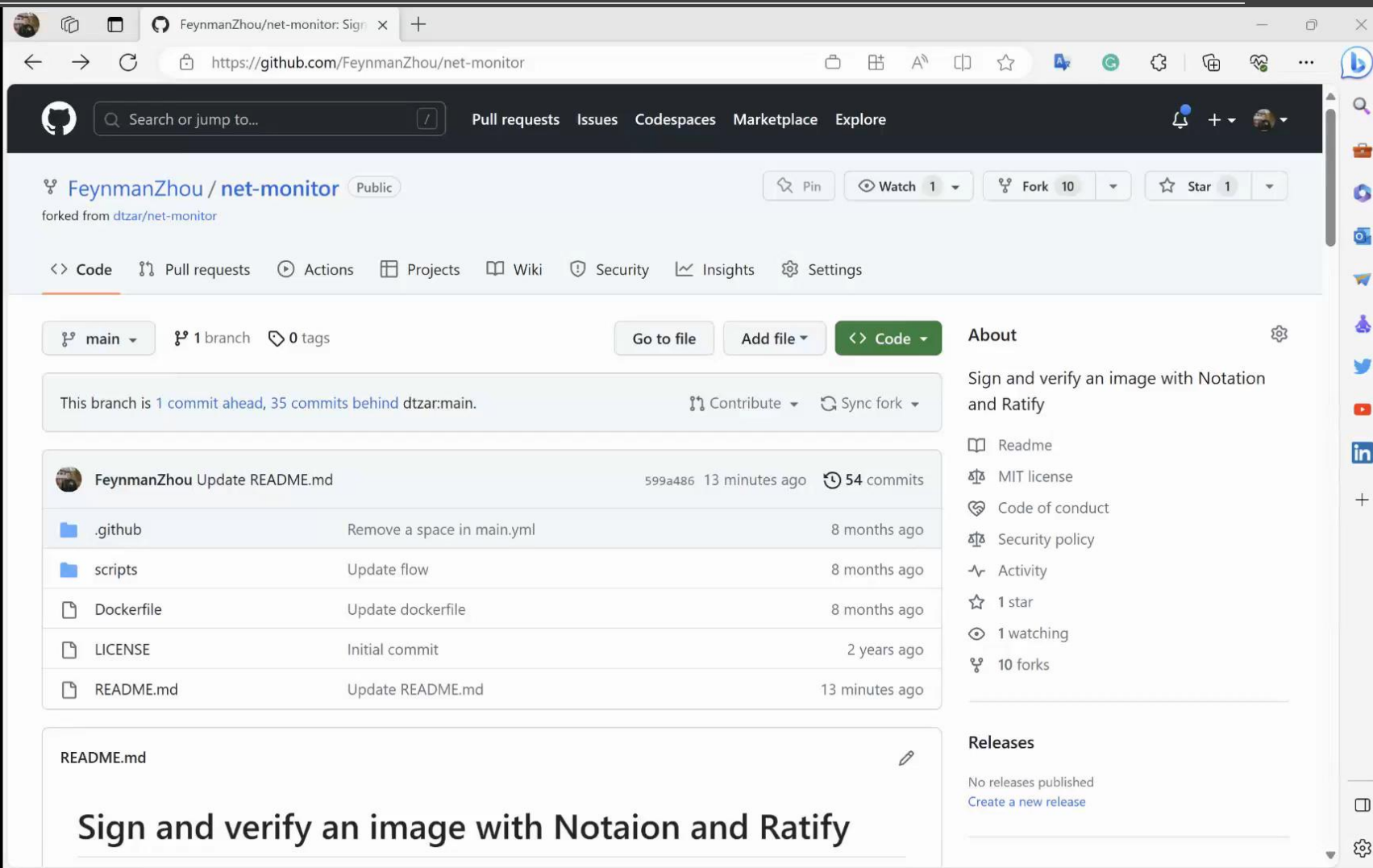
构建端到端供应链安全 + Demo



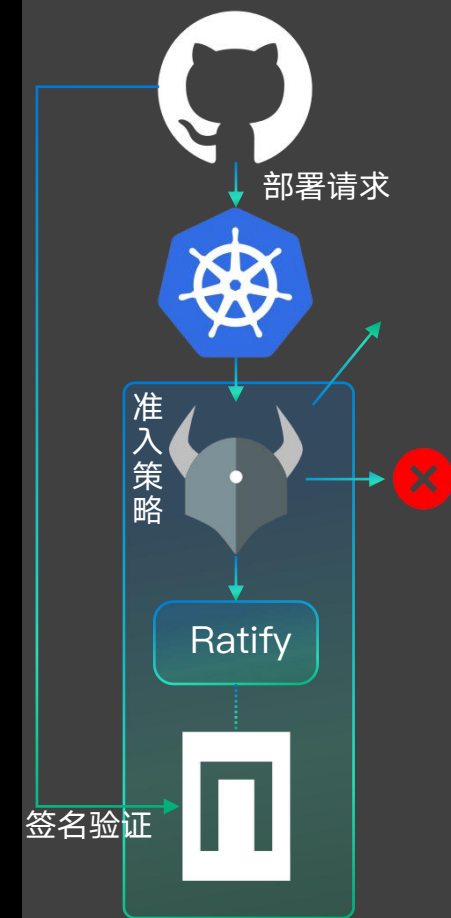
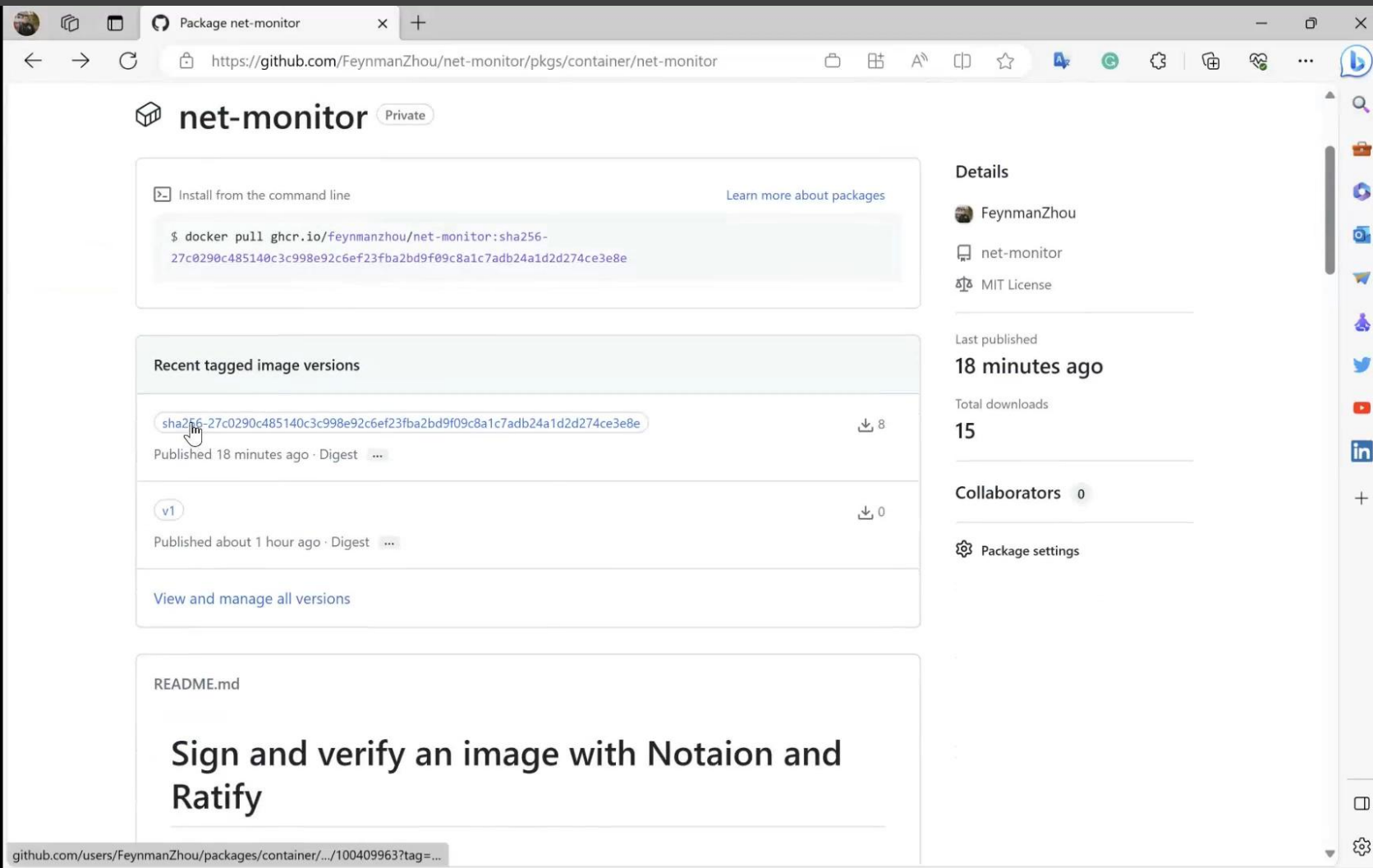
为开源基础设施构建端到端的供应链安全



Demo: 镜像签名, 并推送到 GHCR 镜像仓库



Demo: 验证签名, 对部署到 K8s 加入准入策略



应用到 CI/CD: 如 GitHub Actions

🏠 Summary

Jobs

✔ SSC image build to remote registry

Run details

🕒 Usage

📄 Workflow file

SSC image build to remote registry

succeeded 24 days ago in 57s

🔍 Search logs



- > ✔ Set up Docker Buildx 4s
- > ✔ Install oras 0s
- > ✔ Docker build and push net-monitor image 6s
- ⊘ Azure Login 0s
- ⊘ Setup Notation with azure-kv plugin 0s
- > ✔ Setup Notation with local temp key 6s
- > ✔ Notation sign image 5s
- > ✔ Install and Generate SBOM 5s
- > ✔ Oras Attach SBOM 0s
- > ✔ Notation sign SBOM 2s
- > ✔ Install trivy and generate vuln scan 4s
- > ✔ Oras attach vuln scan 0s
- > ✔ Notation sign vuln scan 2s
- ⊘ Login to ACR 0s
- ⊘ Copy local image and all artifacts to remote registry 0s

第五部分

开源项目中的开放 社区治理



Notary 项目社区治理的故事

cncf / toc Public

Edit

<> Code Issues 73 Pull requests 48 Actions Projects 2 Security Insights

Health of the Notary V2 project #981

Open JustinCappos opened this issue on Dec 15, 2022 · 80 comments



JustinCappos commented on Dec 15, 2022 · edited

Contributor

As I understand it, the TOC is starting to review projects with a consideration to reassess their level in the CNCF or even to remove them altogether. I wanted to bring the Notary V2 project to the TOC's attention as a project that is misplaced and worthy of review.

First of all, the original Notary V1 project was added by the CNCF and was voted in both because it had a strong security foundation and a substantial user base.

Strangely, the Notary V2 project has none of the original Notary project members, none of the lines of code from Notary V1, and none of the security design. It is effectively a completely different project that has taken the same name in order to preserve the incubating status in the CNCF. Even worse, it is at incubation level and making use of CNCF resources / marketing / reputation, yet has had no security reviews, etc.

I would kindly suggest that the TOC consider either removing Notary V2 from the CNCF or asking it to reapply to the CNCF.

Notary V1 (the original) likely could also plausibly be archived or reviewed at some point, but this is of less urgency as it did actually receive due diligence at some point.

I know I raised the same concern back in July 2021, but after talking with others in the community I thought it was worth raising again. As transparency is an important part of open source foundations and projects, after raising this issue a week ago to the TOC privately, I am now making this request public.

I am including below the 2021 email where this issue was raised to the TOC. I will note that at time we were hoping for governance changes that would enable us to participate and prevent the project from making repeated, obvious security errors. Now, while to the project's credit, its [website](#) does not claim the project has or provides any security properties, its use of the Notary name and



Notary 项目社区治理的故事

面临的挑战：

- 核心贡献者主要来自 AWS、微软 Azure，贡献者多元性，既合作又竞争
- 社区贡献路径、沟通与决策流程不够公开透明，社区治理流程缺少文档化
- 社区活跃度不够高，PR 审核速度较慢
- 竞争对手的“舆论攻击”
- 安全威胁模型（Threat Model）未定义清晰
- 用户少，用户体验不友好，学习与体验门槛高
- 网站体验不友好，文档内容滞后
- . . .



开放社区治理解决的问题

人（参与者的角色）

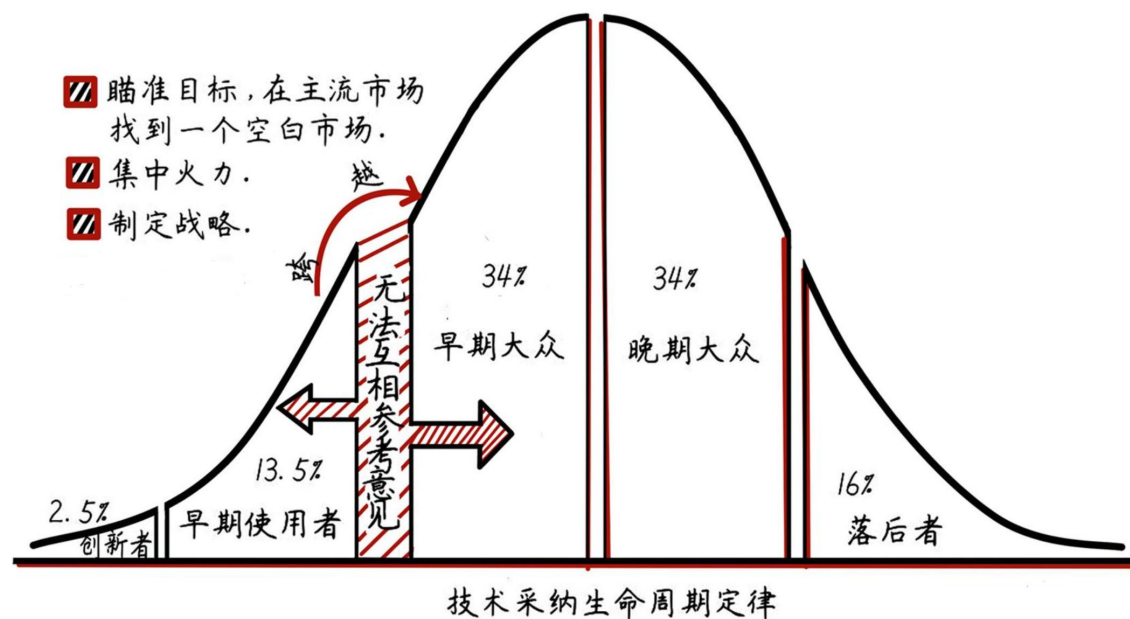
- 项目贡献者可以扮演哪些角色？
- 什么资格使某位成员能够在项目中扮演特定的角色？
- 每个角色都有哪些职责、特权和权威形式？
- 哪些项目资源是由执行某些角色的人负责或拥有的？

流程（开放协作的标准）

- 代码和文档以什么样的标准被合并到项目中？
- 代码如何发布？以及如何做版本管理？
- 有哪些规则管理项目中的沟通？
- 贡献者什么时候会晋升，以及怎样晋升？
- 项目中的各种决策（例如产品版本规划、技术路线、资源分配）是如何做出的？
- 如果开源项目有选举，它们是如何进行的？

用户与贡献者增长

- 在线 Demo 环境与快速入门教程，10分钟快速上手
- 向导式设计的网站、用户文档、视频教程
- 了解早期用户与大众用户的行为和诉求
 - 用户问卷 hotjar
 - 网站监测 Google Analytics
 - 开源社区活跃度 ossinsight.io
 - CNCF DevStats



认识技术采纳生命周期上的鸿沟, 集中力量, 攻克跨越

用户与贡献者增长

- **Mentorship:** LFX Mentorship、开源之夏、Google Summer of Code
- 定期的公开社区例会
- 开放 Roadmap
- 定期的管理与分类 issue、PR，如开放 good-first issue
- 简洁而清晰的社区治理文档
- 社区组织架构与贡献者发展路线

参考链接

- Notary: <https://notaryproject.dev>
- ORAS: <https://oras.land>
- Ratify: <https://github.com/deislabs/ratify>
- CNCF Maintainer Guide: <https://contribute.cncf.io/>
- OpenSSF: [OpenSSF Expands Supply Chain Integrity Efforts with S2C2F — Open Source Security Foundation](#)

与我联系

- 邮箱: feynmanzhou@microsoft.com
- [Twitter: @FeynmanZhou](#)
- GitHub: FeynmanZhou
- 微信: 493200090

谢谢聆听!

