web3黑客松隐私赛道

痛点💊

在开放透明的区块链世界中，**链上记录“永久公开、不可删除”**，这既是技术特性，也是隐私风险源。

特殊风险包括：

- **人肉搜索**：钱包地址、交易记录可被公开追踪，配合链下社交信息易被锁定身份
- **社群针对与暴力**：DAO 或社区治理记录暴露价值倾向，引发针对性攻击
- **网络钓鱼**：NFT、POAP、链上身份被恶意定位或制造造成资产损失的社交陷阱
- **隐私威胁**：在政治敏感或社会不安全地区，公开的链上行为可能带来线下风险

这使得女性用户、少数族裔、LGBTQ+ 群体、记者、活动人士等**在链上的“生存成本”更高**。

场景	痛点	风险后果
钱包地址暴露	链上交易全部可查、可溯源	资产规模、消费习惯暴露，被诈骗或跟踪、精准钓鱼攻击
链上身份与社交绑定	NFT、POAP、ENS 与现实身份关联	匿名性丧失，用户画像化，**暴露社群关系**、被人肉、骚扰、钓鱼
DAO 治理透明化过度	投票记录公开	政治立场、观点被攻击
链上内容永久存储	敏感信息上链无法删除	心理伤害、法律风险
身份验证	线上社交中遭遇女性身份伪造	信任威胁、信息泄露、隐私泄露
弱势群体求助信息隐私	弱势群体链上活动记录公开	失去匿名援助安全感

隐私赛道赛题设计🎯

一、赛道目标

- 鼓励开发者构建**易用、可验证**的隐私保护工具
- 帮助大众应对 **信息泄露、链上可追溯性、数据滥用** 等问题
- 推动 **零知识证明（ZKP）、去中心化身份（DID）** 等技术落地到实际应用场景

二、题目方向（任选或自由创新）

什么是web3世界的隐私？大致有三个方向：资产/身份/行为

web3的隐私保护就是别让 谁的钱包有钱、谁是钱包主人、在web3的行为轨迹、链下身份这些信息泄露。

题目名称	现实痛点	技术关键词	目标产出示例
链上隐私转账工具	公链转账记录完全公开，容易被溯源、跟踪	零知识证明、隐私支付、混币	一个基于 ZKP 的轻量化隐私交易合约
NFT 匿名转让	NFT 收藏品交易暴露钱包历史和身份	Ring signature、Stealth Address	一个可匿名赠送/交易 NFT 的 DApp
匿名治理			匿名投票与提案工具
Web3 聊天加密插件	线上沟通监听和审查	端到端加密、密钥协商、临时会话密钥	钱包验证的加密聊天的插件
防链上画像浏览器	链上交易+社交数据结合后易被画像	交易混淆、链上行为伪装	一键生成随机化、混淆化交易模式的工具
用户友好型零知识身份登录	ZK 应用门槛高，普通人难以使用	ZK proof、DID、无密码登录	易用的 ZK 身份认证入口
私钥泄露监控工具	私钥泄露导致的钱包、资金损失		帮助用户监控私钥泄露情况，提供预警提示等服务降低风险
身份属性验证工具	存在伪装成女性加入全女社区扰乱秩序的破坏分子	zkp	帮助社区验证用户女性身份但不暴露其隐私信息的验证方式

三、参赛要求

1. 必备要求

- 必须是可运行的 MVP（最小可行产品），可以是原型或 Demo
- 前端可交互，后端逻辑可验证（智能合约 ）
- 必须在作品说明中阐述**隐私保护机制**（原理 + 设计图）
- 数据、代码需开源（可采用 GPL / MIT / Apache 2.0 等开源协议）

2. 技术要求

- 支持的技术栈不限
- 至少使用 **一种隐私增强技术**（如 ZKP、MPC、Ring Signature、Stealth Address、Commit-Reveal 等）

3. 评审维度（总分 10 分）

维度	权重	说明
创新性	3	是否提出新的隐私保护思路或应用场景
技术实现	3	隐私技术的正确性、完整度、可验证性
易用性	2	普通用户是否能低门槛使用；非技术背景用户可快速上手
社会价值	1	是否能切中大众的隐私痛点；对弱势群体隐私保护的创新性；技术与人性化结合程度
展示效果	1	演示清晰、有说服力

四、加分项

- 兼容性 跨链、钱包、移动端等
- 在 Demo Day 上进行 **链上实测演示**
- 对非技术用户的隐私教育
- 设置**隐私社会影响奖金**

参考资料

隐私赛道黑客松案例📅

赛事 / 组织	亮点	技术支持	时间	站点
Privacy4Web3 Hackathon（P4W3）（Oasis Network）	专注隐私支付、ZK 身份验证、隐私社交	Oasis Privacy Layer（OPL）和 Sapphire 的隐私协议；Oasis 的 ROFL（Runtime Off-Chain Logic）框架 ；使用 Oasis 的 Sapphire 和 ROFL 框架开发隐私应用	2023 年起；每年3个月；报名开启 2025 年 9 月 19 日	https://oasis.net/hackathon ；Privacy4Web3 HackathonOasis ForumDoraHacks
ETHDam 2024：隐私专场	围绕隐私保护和安全性挑战，开发创新	隐私与安全主题演讲；以太坊隐私协议、零知识证明、去中心化身份（DID）等技术研讨会；面向私密合约的工作坊；Secret Network/Aztec/Polygon ID/**Aleo/Findora等多个知名项目和组织的支持**	2024 年 荷兰线下活动 由 CryptoCanal 赞助	https://www.youtube.com/watch?v=dKlrTbypmo0

赛事 / 组织	亮点	技术支持	时间	站点
Aztec	以太坊的 **隐私 Layer2 网络**	专注于 **以太坊隐私层** 的区块链协议，主要通过 **零知识证明（ZKP）** 为以太坊交易和智能合约提供**端到端加密与隐私保护；开发语言 Noir**		借助 ETHGlobal 平台开展
Polygon ID	聚焦在 **去中心化身份（DID）** 与 **零知识证明（ZKP）** 技术的创新应用	**Polygon ID** 是 Polygon 推出的 **Web3 去中心化身份系统；**基于 **W3C DID 标准** 与 **可验证凭证（VC）；**使用 **zk-SNARK** 实现隐私保护；Polygon ID SDK、zk-SNARK 库（circom/snarkjs）、Polygon zkEVM	通常为线上或混合形式，持续 2-4 周	通过**ETHGlobal** 和 **Decentralized Identity Foundation (DIF) Hackathon**合作平台
Semaphore	面向匿名发声、反跟踪应用	Semaphore是一种基于零知识证明（ZKP）的**匿名信号广播协议**, **Semaphore JS/Go 库**（官方 SDK）	2024 Q3–Q4	ETHIndia 黑客松中举办 Semaphore & Bandada 工作坊
Geeks Without Bounds Hackathon	针对弱势群体与人道主义援助隐私保护	Secure Messaging, Privacy Wallet 数据加密、匿名通信等隐私保护技术	2010；2012 “EveryoneHacks”黑客松 特别关注女性和其他代表性不足群体的参与；2**016 年** 在印度 Ranchi 举办了“黑客松对抗性别暴力”活动	失效https://en.wikipedia.org/wiki/Geeks_Without_Bour
Aleo Privacy Virtual Hackathon	围绕 Aleo 平台与其支持的零知识证明技术，鼓励使用 Aleo zk-circuit 构建隐私保护类应用	Aleo 的专有编程语言 Leo；Aleo 测试网或主网	2025 年 5 月	https://aleoprivatehackathon.devpost.com/ ； https://aleo.org/

赛事 / 组织	亮点	技术支持	时间	站点
ETHSanFrancisco Hackathon		Findora 提供隐私 ：使用 Privacy Routing SDK 构建链上私密转账；使用 ZK-DID SDK 实现选择性数据披露（如年龄、成绩、信用分证明）	2022 年	由 ETHGlobal 主办 https://docs.findora.org/developers/resources/events/san-francisco-2022
HackSecret 5	主题聚焦机密 AI dApps（Confidential AI dApps）	**Secret AI SDK可**用于构建保护用户数据的 AI 代理；**Autonomys Agent Framework**：支持构建具有永久链上记忆的 AI 代理，确保社交机器人不受审查或操控；**SecretPath / Axelar / IBC**：实现跨链隐私 dApp 的构建	2025 年 2 月 1 日至 3 日	ETHDenver Hacker House **主办方**：Secret Network https://dorahacks.io/hackathon/hacksecret5/detail
Rebuild Ownership 2.0：Internet Privacy	强调赋予用户对个人数据的控制权，构建去中心化的互联网隐私架构；关注网络隐私倡议，以 Web3 技术应对 Web2 的数据滥用问题	去中心化身份（DID）、分布式存储（dStorage）、零知识证明（ZKP）、多方计算（MPC）、同态加密（FHE）得到了以下项目和组织的支持：**Fhenix**：提供去中心化身份和隐私计算的技术支持。 **PSE（TLSNotary）**：提供去中心化存储和隐私保护的技术支持。 **Linera**：提供去中心化计算和隐私保护的技术支持。	2023 年；**主办方**：DataverseOS	https://rebuild-ownership-internet-privacy.devfolio.co/
W3PN_Hacks（Berlin Blockchain Week）	强调实用隐私（Practical Privacy），鼓励开发者构建符合赛博朋克精神的隐私保护工具。	得到了多个隐私技术项目和组织的支持，包括：**Jensei**：提供黑客松策划包，帮助参与者构思和实现隐私应用。**Pagency Framework**：由Mykola提供，用于隐私用例的构思和设计。**Privacy Academy**：由Peter Farbey维护，提供隐私技术的教育资源。**Privacy Use-Cases Generator**：一个工具，帮助开发者实验潜在的隐私用例，由Vitalik Buterin等隐私专家协助	2025 年 6 月	https://lu.ma/wero3jvo https://hackathon.web3privacy.info/ https://www.youtube.com/watch?v=97madHNGXtk

赛事 / 组织	亮点	技术支持	时间	站点
Digital Identity Hackathon — Encode Club	推动数字身份领域的创新，特别是在 Web3 社交、账户抽象和可扩展性方面	**Onyx by J.P. Morgan**：提供数字身份 SDK 和 API，支持可验证凭证的签发和交换。Biconomy、Visa、Lens Protocol、zkSync、Magic 等提供技术支持和指导	2023 年	由 Encode Club 主办、J.P. Morgan 的 Onyx 部门赞助的 黑客松https://www.encode.club/digital-identity-hackat

借鉴要点：

赛事主办方需要提供的资源清单

（1）技术资源

每个赛事会**指定一个技术栈或协议**作为核心（方便选手切入）

- 指定可用的隐私框架 / 工具（如 Aztec、Semaphore、Polygon ID）
- 主办方通常会提前**准备教程 & SDK**，降低参赛门槛。比如提供开发文档、代码示例、视频教程
- 提供测试网络和 API Key
- 技术答疑渠道（Discord / Telegram）

（2）参赛支持

- 赛题方向说明（最好给具体痛点和应用场景）
- 团队组建平台（让技术与非技术选手能组队）
- 办赛平台（DoraHacks、DevPost、Gitcoin）

（3）评审与奖金

会设置**奖项细分**：最佳隐私支付、最佳隐私社交、最佳隐私身份等

- 评审标准（创新性、隐私保护效果、可落地性）
- 奖金结构（总奖金 + 各赛道奖金）
- 评审团（技术专家 + 隐私领域研究者 + 行业从业者）

（4）宣传与生态对接

- 合作社区（ETHGlobal、Filecoin Orbit、Women in Blockchain）
- 媒体曝光（推特、微信、Discord 群）
- 赛后孵化（加速器、投资机构）

信息收集

技术资源🔨

主流隐私技术框架和工具分类

框架 / 协议	核心技术	优势	典型应用	
zk-SNARKs	椭圆曲线密码学，简洁证明	证明体积小、验证快	Zcash、Aztec	一种“零知识证明”，能在不透露数据的情况下证明知道这个数据
zk-STARKs	基于哈希，无需可信设置	安全假设简单，可扩展性好	StarkNet、Risc0	
Bulletproofs	范围证明	无需可信设置，适合保密交易	Monero	
Halo2	递归证明	可无限复用证明，降低成本	zkSync、Mina	
Risc0	zk-STARK + RISC-V	通用计算证明，支持 Web2/AI	ZKML、隐私计算	基于 zk-STARKs 与 RISC-V 架构的通用可验证计算平台，拥有高性能与透明性优势，是目前 ZKP 实践中一个框架
MACI	ZK 投票系统	防买票、防串通	Gitcoin Grants	一种防串票的匿名投票系统
Polygon ID	zk-SNARKs + DID	选择性披露，易集成	身份验证、KYC	
Semaphore	ZK 信号广播	群体匿名认证	匿名发布、投票	匿名发声工具，可验证你是群体中的一员
FHE	全同态加密	加密状态下计算	医疗/金融隐私计算	
Stealth Address	隐藏收款地址	防骚扰、一次性收款		每次收款生成一个新地址，别人不能轻易追踪你
Midnight 链		内建隐私层，编程友好性高	隐私应用链搭建	隐私优先的公链，支持通过零知识加密实现“可编程隐私”能力，为 Web3 开发者提供更灵活的隐私工具
去中心化身份（DID）	用户自主身份控制	通过 ZKP 实现无需泄露个人数据的验证（如年龄、居住地等）		
MPC	**多方安全计算**			多个人一起算一个结果，但没人知道对方的数据
Verifiable Credentials	**可验证凭证**			数字版的“证明文件”，可选择性公开部分信息

隐私技术应用场景分类

分类	应用示例	说明	技术
隐私支付与转账	Aztec, Tornado Cash, Zcash,COTI Privacy Layer	加密转账、交易混淆、隐藏交易金额、参与方、交易时间等信息	zk-SNARKs、zk-STARKs、Stealth Address、MPC
隐私身份	Polygon ID, Iden3, Civic, Lit Protocol、SpruceID	ZK 身份验证、选择性披露、证明某一属性（如年龄、资质、女性、创业者、社区成员)而不泄露其他信息	ZK Credentials、Verifiable Credentials
隐私治理	MACI（Minimum Anti-Collusion Infrastructure）, Snapshot + ZK, Vocdoni	匿名投票、防串票、提案内容加密、**群私密治理工具**	Blind Signature、ZK Voting
匿名通信	Status, Matrix, XMTPSession,Waku（Status.im）	去中心化加密聊天，端到端加密、去中心化消息路由	MLS（Message Layer Security）、Double Ratchet
数据保护	FHE.org, Partisia, Secret Network	加密状态下计算	
匿名社交	Lens Protocol + ZK, CyberConnect	去中心化社交隐私插件	
隐私开发工具	Circom, Noir, snark.js, Halo2	ZK 电路与应用开发	
隐私 NFT 与数字资产	Secret NFTs、Aztec Connect	匿名铸造、匿名转让、持仓不可公开追踪	Commit-Reveal、ZK Merkle Proofs
隐私 DeFi	Railgun、Findora	隐藏流动性提供、借贷、衍生品交易细节	Confidential Transactions、FHE（全同态加密）
跨链隐私桥	Axelar + ZK、Secret Network IBC	在多链环境中保持资产流动隐私	ZK Bridges、TEE（可信执行环境）

分类	应用示例	说明	技术
反跟踪隐私钱包		混淆交易记录，防止资产与身份绑定	Stealth Address、ZK Mixer、交易伪装
私密援助与资金资助	匿名加密捐助通道	保护捐助人和受助人的身份与金额	Confidential Transactions、MPC
防骚扰链上社交插件	NFT 黑名单插件	拦截、过滤带有冒犯内容的链上资产	内容哈希屏蔽、链上黑名单

资源📖

- **“Awesome ZKP” 资源库**：matter-labs 的开源项目整合了多种 ZKP 类型（SNARKs、STARKs、Bulletproofs 等）、教程与工具，仍是开发者的重要参考资源
- **Web3Privacy Now 项目**：构建了一个覆盖 500+ 隐私增强项目与服务的数据库，还包括选题灵感生成（PEDApps framework）、市场地图、评分平台等资源，可为赛题定位提供决策支持 https://explorer.web3privacy.info/ https://github.com/web3privacy/web3privacy

技术资源包

- **基础组件**
  - 测试网接入：Sapphire（Oasis）、Shielded Pool（Aztec）、Aleo测试网
  - 开发套件：Noir语言示例库、Semaphore JS模板、Polygon ID Widget
- **降门槛工具**
  - 可视化ZK电路编辑器（如Circom Studio）
  - 一键部署脚本（如Hardhat隐私插件）

▼ 技术栈选择

具体根据赛事举办时间、面向的参与对象技术水平综合考虑

开发友好性排序：

等级	技术 / 协议	特点	适合对象	举例赛事
入门级	Polygon ID SDK、Semaphore SDK	提供高层 API，文档完善，样例多	初中级开发者、快速出 Demo	Polygon ID Hackathon、Semaphore Hackathon
中级	MACI、Aztec Noir、Oasis Sapphire、Secret Network SDK	有一定门槛，需要理解合约编译与隐私运行环境	有智能合约经验的开发者	Aztec Hackathon、Oasis Privacy4Web3
进阶	Aleo Leo、Risc0 zkVM、Halo2	高灵活性，但需要深入理解 ZK 电路	专项ZK黑客松 /密码学开发者/研究院合作赛事	Aleo Privacy Hackathon、ZPrize
专家级	自定义 zk-SNARK/STARK 电路、FHE、MPC 框架	几乎无上手封装，需要数学与密码学背景	专业研究员、核心协议开发者、学术性竞赛	ZK Hack、ETHPrivacy Tracks

基础设施依赖：（按部署/运行所需条件）

类别	技术 / 协议	依赖要素	注意事项
链上合约型	Aztec、Oasis Sapphire、Secret Network、Polygon zkEVM	EVM 兼容链 / 专用测试网	需提供 faucet、合约部署工具、测试账户
链下计算型	FHE（Zama、TFHE）、MPC（Lit Protocol、Phala）	Off-chain 计算节点或容器环境	需提供部署文档、计算资源（云服务或本地运行）
混合架构（链上 + 链下）	Risc0、Aleo、MACI、Semaphore	链上验证合约 + 链下 ZK 证明生成服务	需确保验证 gas 成本可控
身份/凭证类	Polygon ID、Veramo、Spruce DIDKit	去中心化身份网络（Polygon、Ceramic 等）	需提前发放验证节点 API key 或本地验证工具

类别	技术 / 协议	依赖要素	注意事项
存储与隐私数据	IPFS + Filecoin、Sia、Arweave + ZK 加密层	分布式存储网络	注意加密层设计，避免明文存储

依赖清单

技术栈	真实依赖组件	部署复杂度	本地测试方案
Aztec Noir	• **Aztec Sandbox**（本地节点） • **Noirup** 工具链 • PXE（Private eXecution Environment）	⭐⭐⭐⭐(需Docker+链同步)	`aztec-sandbox -d`（官方Docker镜像）
Oasis Sapphire	• **Oasis ParaTime**• **Web3 Gateway** • Confidential EVM（隐私执行环境）	⭐⭐⭐(RPC公开可用)	测试网直接接入（无需本地节点）
Secret Network	• **SecretJS**• **TEE验证模块**• **IBC中继器**（跨链需求）	⭐⭐⭐⭐(依赖SGX环境)	`secretd testnet`（限Linux+SGX）
Risc0 zkVM	• **zkVM Host**（Rust）• **Bonsai证明服务**• **Groth16验证合约**	⭐⭐(纯软件栈)	`cargo run --release`（无硬件依赖）

参赛支持🙋

赞助商合作方式

社区/组织	可能的合作角色	合作理由
Encode Club	教育支持/教育内容合作	Web3 教育生态成熟
DoraHacks (Privacy4Web3)	隐私主题合作伙伴；可邀请作为赞助或冠名合作方。https://dorahacks.io/	具隐私赛道经验。举办专注隐私保护的 Hackathon（Privacy4Web3）
Geeks Without Bounds	社会价值赞助方 但是最近没有新的动态	曾举行以性别暴力（Gender-Based Violence）为主题的 Hackathon
HackerNest	社区宣传 &扩散支持	非盈利全球科技社区，以“Tech Socials”和社会责任导向的黑客松著称
Calyx Institute	隐私教育 &资助；是开展隐私教育赛道或社区宣传的潜在合作机构。	隐私权方向的社会资源；致力于提升公众隐私与数字安全意识，支持相关项目并参与多个网络隐私会议与黑客活动
ETHGlobal 系列	大赛赞助或专项协作	主流平台资源丰富；曾与隐私协议相关企业（如 Oasis Protocol、Aztec、Tusima zkBridge）合作举办高奖金 Hackathon
Bybit / DMCC x DWF Labs	区域性赛道支持；可拓展为区域性赛道参与方，结合地区性别与安全议题	曾资助中东最大 Web3 黑客松，包括 ZKP、数字身份等主题
Filecoin Orbit**/ IPFS 社区**	技术社区支持；可聚焦隐私存储、保护用户内容的赛题，使赛事兼具技术性与社会价值。	推广去中心化存储、Web3 工具
Consensus / CoinDesk	可以作为传播平台，并邀请其设置“隐私 + 女性/弱势群体”专项	市场号召力强；Web3 大型主流会议平台

联合主办 https://docs.web3privacy.info/projects/women-in-privacy/