ETHPanda LXDAO

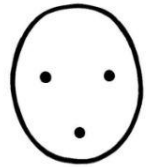
Web3 实习计划（分享会）

Web3 运行原理

时 1月13日 (周二)

间 8-9PM (UTC+8)

嘉 宾



Bruce

@brucexu_eth

Co-initiator @LXDAO_Official & @ETHPanda_Org

特别支持 南塘 DAO OGBC SCALINGX Kite AI DataDance SpoonOS ethereum foundation dev growth OneKey NODIT 合作伙伴 reactive PLUTOS CAPITAL

Web3 实习计划

ETHPanda LXDAO

Web3 运行原理：从钱包到出块，从应用到协议

- 目标：从原理出发理解 Web3 怎么“跑起来”
- 方式：边操作边讲解（钱包 → 交易 → 出块 → 合约）
- 不止技术：讨论 Web3 的特性与价值（去中心化 / 无许可 / 抗审查 / 隐私等）

1.11 - 2.8

Web3 实习计划

ETHPanda LXDAO

Outline

钱包、私钥和个人主权

交易与签名

区块链网络运行

智能合约

区块链协议如何升级

Web3 关键特性回顾

1.11 - 2.8

Web3 实习计划

ETHPanda LXDAO

钱包、私钥和个人主权

1.11 - 2.8

私钥、助记词、地址：三者关系

ETHPanda LXDAO

私钥（Private Key）：你的“终极签名印章”，谁拥有谁就能控制资产

助记词（Seed Phrase）：私钥的可读备份（通过派生路径可生成多个账户）

地址（Address）：公钥截取后的字符串，公开收款号（不是隐私信息，但可能被关联分析）

实战演示：

- https://vanity-eth.tk/**（请勿真实使用）私钥导入**
- **私钥到地址的转换流程** https://gemini.google.com/share/95120a5b2063

私钥的安全性建议

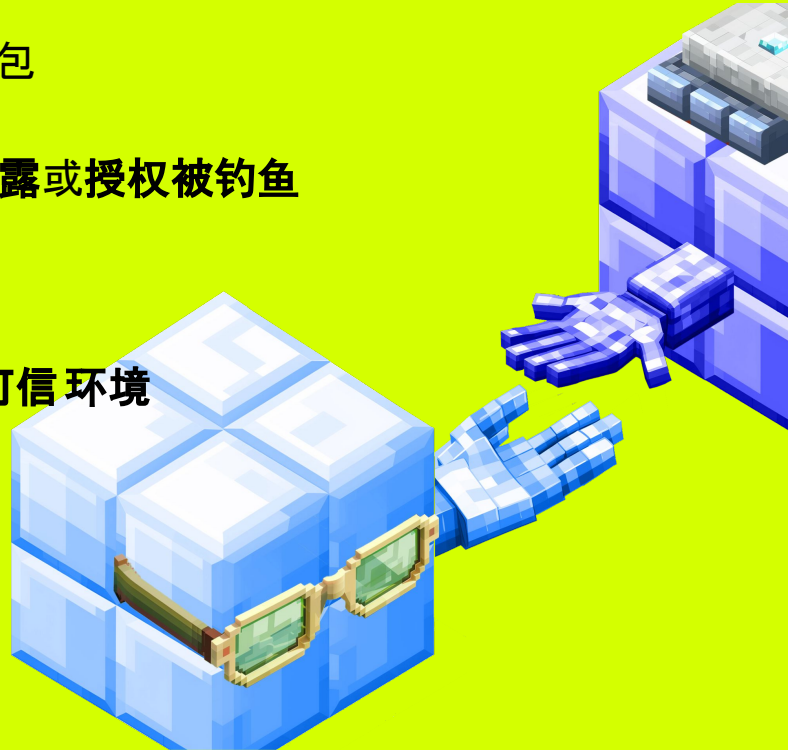
ETHPanda LXDAO

私钥很安全 —— 除非你自己泄漏了

- 私钥是不可重置的密码(丢了就是永远丢)，只能换钱包
- 区块链不认识你是谁，只认识“谁能签名”
- 大部分资产被盗，不是链被攻破，而是**私钥/助记词泄露**或**授权被钓鱼**

安全原则(强制记住)

- 助记词/私钥:**不截图、不网盘、不发人、不复制到不可信环境**
- 剪贴板是高风险区(很多恶意软件会读剪贴板)
- 任何人一旦拿到私钥/助记词 = 拿到资产控制权



私钥的社会学意义：个人主权的起点

ETHPanda LXDAO

- 任何人都可以随机创建私钥 → 立刻拥有一个无需许可的账户与资产权利
- 对比传统金融：开银行账户需要身份、审批、地域、制度

背后原因：

- 这是密码学提供的“可验证的个人主权”
- 你不需要别人“给你账号”，你自己就能生成“权利入口”

Web3 实习计划

1.11 - 2.8

ETHPanda LXDAO

交易与签名

交易是什么

ETHPanda LXDAO

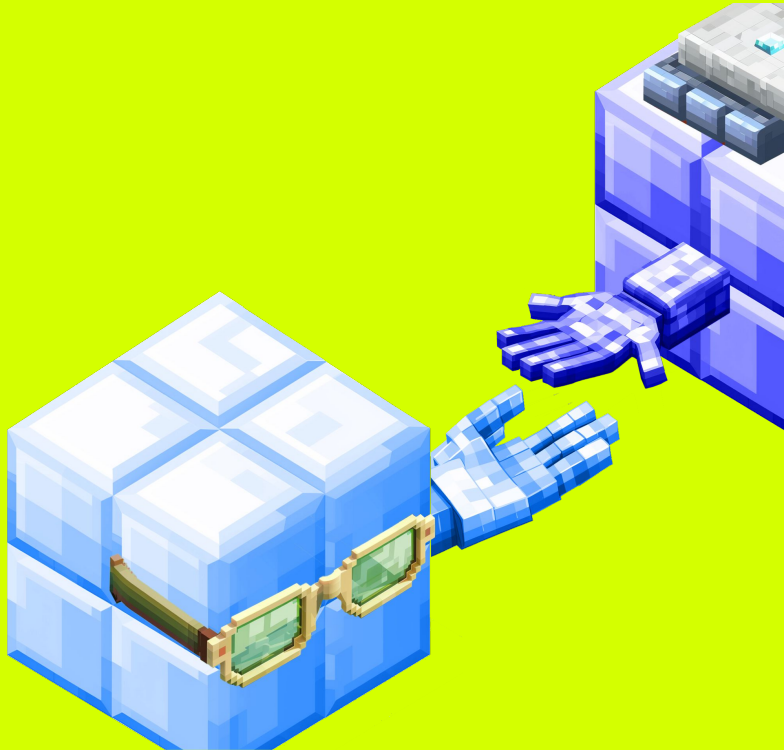
交易（Transaction or tx）= 你要做的事 + 手续费 + 防重放序号

- 你要做的事：比如转账、调用合约 mint、投票等
- 手续费（Gas Fee）：为网络资源付费（并提供激励）
- 防重放序号（Nonce）：避免同一笔交易被重复执行

钱包在做什么：

- 组装交易内容
- 用私钥签名（生成数字签名，证明是你授权）
- 广播到区块链网络

实操：发送一笔测试网交易



数字签名是什么?

ETHPanda LXDAO

数字签名的核心:

- 你用私钥签名一段消息(Message / Transaction)
- 任何人都可以用你的地址验签(Verify)
- 但任何人都无法伪造你的签名(除非拿到私钥)

工作流程: https://gemini.google.com/share/54a1d1ee8263

Gas Fee 是什么?

ETHPanda LXDAO

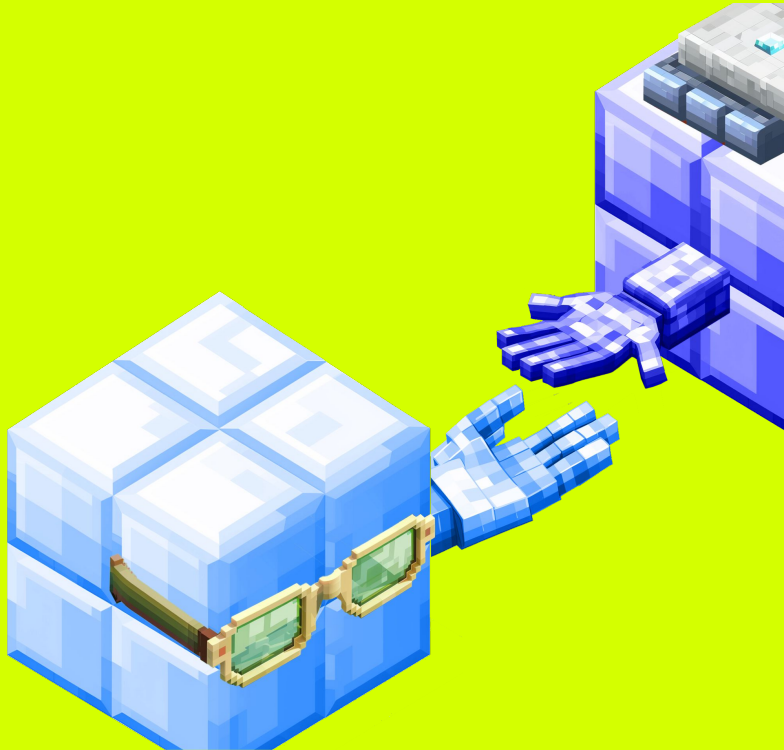
Gas Fee 的三层作用:

- 防垃圾交易淹没网络(提高作恶成本)
- 激励打包者/验证者提供算力与带宽
- 形成经济闭环:资源使用者付费 → 网络可持续运转

经济学视角:

- Gas 是去中心化网络的激励机制之一
- 没有激励,网络很难长期稳定运行

实操:查看一笔交易(Tx)信息
测试网:https://sepolia.etherscan.io/
主网:https://etherscan.io/



Web3 实习计划

ETHPanda LXDAO

区块链网络运行

1.11 - 2.8

从一笔交易到出块

ETHPanda LXDAO

交易的完整生命周期： https://txcity.io/v/eth-btc

- Wallet（签名）
- RPC/Node（传播）
- Mempool（排队）
- Builder/Validator（挑选）https://beaconcha.in/block/24224597#votes
- Block（落盘）https://beaconcha.in/block/24224597
- Explorer（可查）https://etherscan.io/

为什么“不可篡改需要时间”

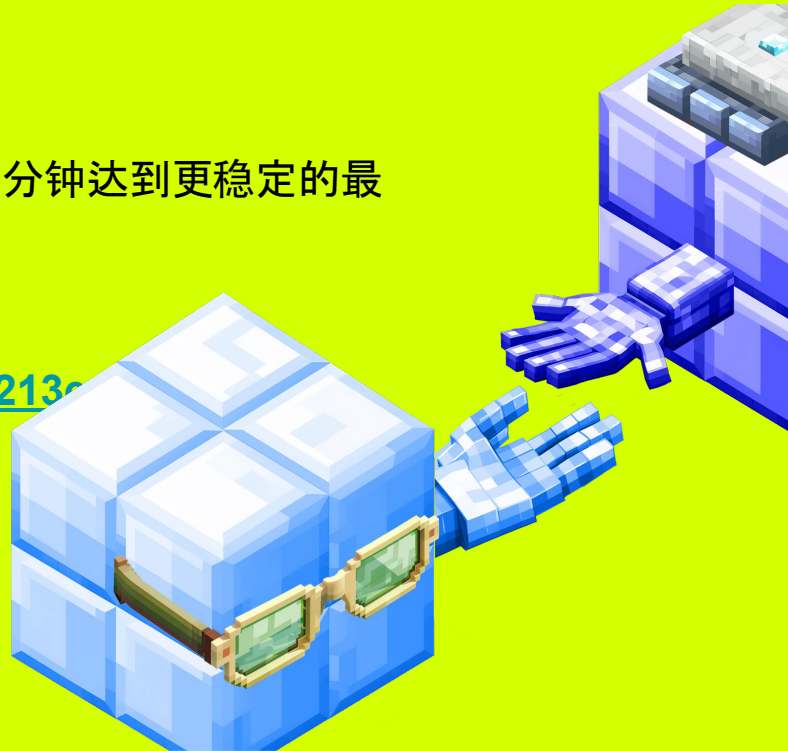
ETHPanda LXDAO

为什么要等确认？

- 区块像账本新一页，会引用上一页指纹（hash）
- 区块越往后叠，历史被推翻的成本越高
- PoS 下存在“最终确认（finality）”：通常需要约 12–13 分钟达到更稳定的最终状态

实操：查看 Block 信息

https://etherscan.io/block/0xb36a9426b3646ddf3d64213c
bcc65f85e4db7b7ba1cc9995ffc62



共识机制：PoW vs PoS

ETHPanda LXDAO

挑战：匿名且互不信任的全球节点，如何认可同一本账？

PoW（工作量证明）BTC

- 算力竞争写账（耗能）
- 像“解一道很难但答案很好验的题”：谁先解出谁记账，全网快速验算

PoS（权益证明）ETH

- 质押 + 随机选人写账（更节能）
- 像“押保证金参加抽签当记账员”：押得多/信誉好概率更高；作恶会被罚没押金

钱包、RPC、节点、网络：如何链接

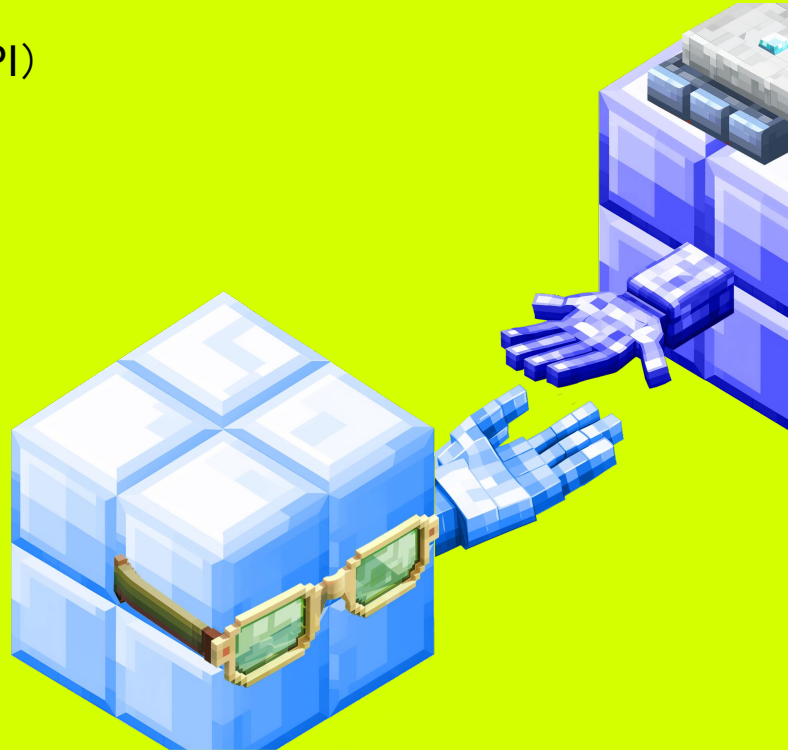
ETHPanda LXDAO

关键关系：

- 钱包通常不直连全网：它连一个 RPC（访问节点的 API）
- RPC 背后是节点（或节点集群）
- 所以：RPC 往往是“中心化入口风险点”

实操：看钱包的 RPC 设置

- 打开钱包网络设置 → 查看 RPC URL / Chain ID
- 用 Chainlist 查看/添加网络：https://chainlist.org/



Web3 实习计划

1.11 - 2.8

ETHPanda LXDAO

智能合约

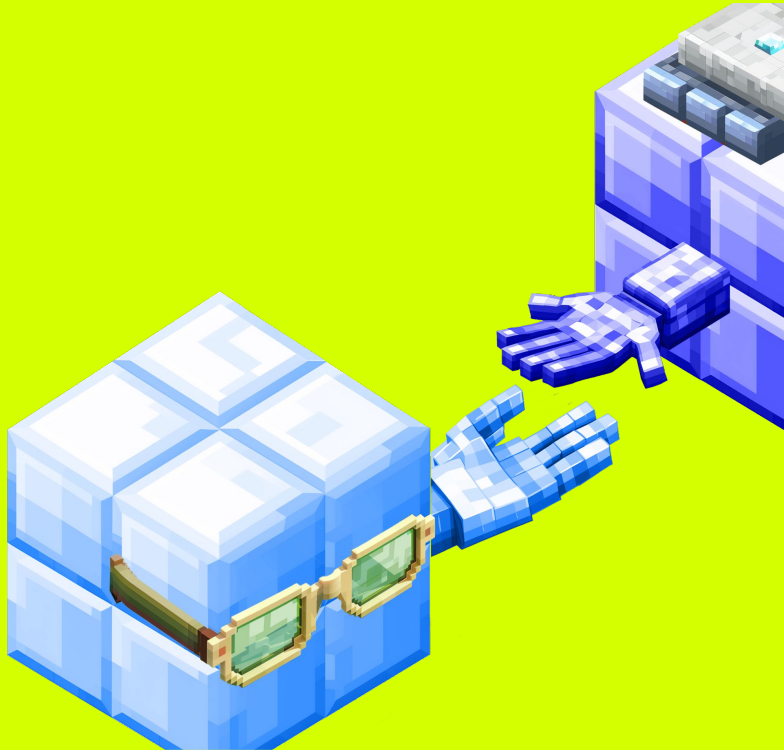
智能合约的本质

ETHPanda LXDAO

智能合约 = 区块链账本里的“可执行代码”。

- 在 EVM（虚拟机）里运行
- 交易触发执行 → 改变链上状态
- 写进区块链：具备“难以篡改、可追溯”的特性

实操：查看 https://nft.myfirst.io/ 的合约



智能合约的社会学意义

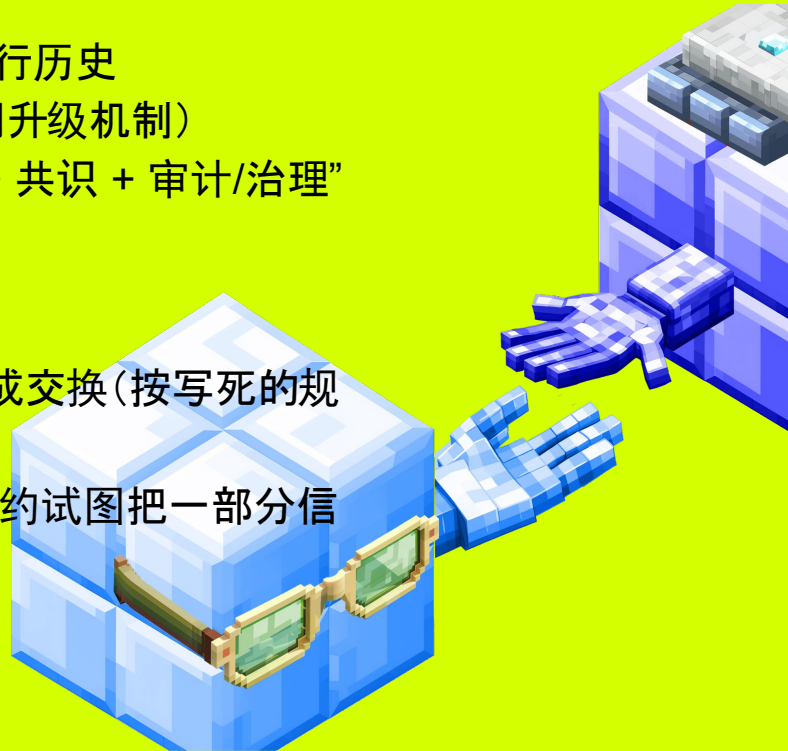
ETHPanda LXDAO

Code is law：

- **规则可验证、按代码执行：**任何人都能检查规则与执行历史
- **部署后难以更改：**减少“临时改规则”的空间（除非使用升级机制）
- **减少中介与摩擦：**把“信任人/机构”压缩为“信任代码 + 共识 + 审计/治理”

例子（交换的最小模型）：

- A 把 NFT 存入合约 -> B 转账进合约 -> 合约自动完成交换（按写死的规则执行）
- 传统世界往往要信任中介、律师、法院与流程；智能合约试图把一部分信任成本变成可验证的程序规则。



实操：Mint https://nft.myfirst.io/ 的 NFT

Web3 实习计划

ETHPanda LXDAO

区块链协议如何升级

1.11 - 2.8

以太坊如何“改规则”

ETHPanda LXDAO

EIP 的基本路径：

- 先讨论（Magicians 论坛）→ 再形成文档（EIPs）→ 再进入升级（每年 1-2 次）
- 每次升级都是一次硬分叉 https://eips.ethereum.org/EIPS/eip-7607
- 关键点：不是某公司拍板，是社区协作推进

相关入口：

- EIP 列表：https://eips.ethereum.org/
- EIP 论坛：https://ethereum-magicians.org/

节点客户端多样性

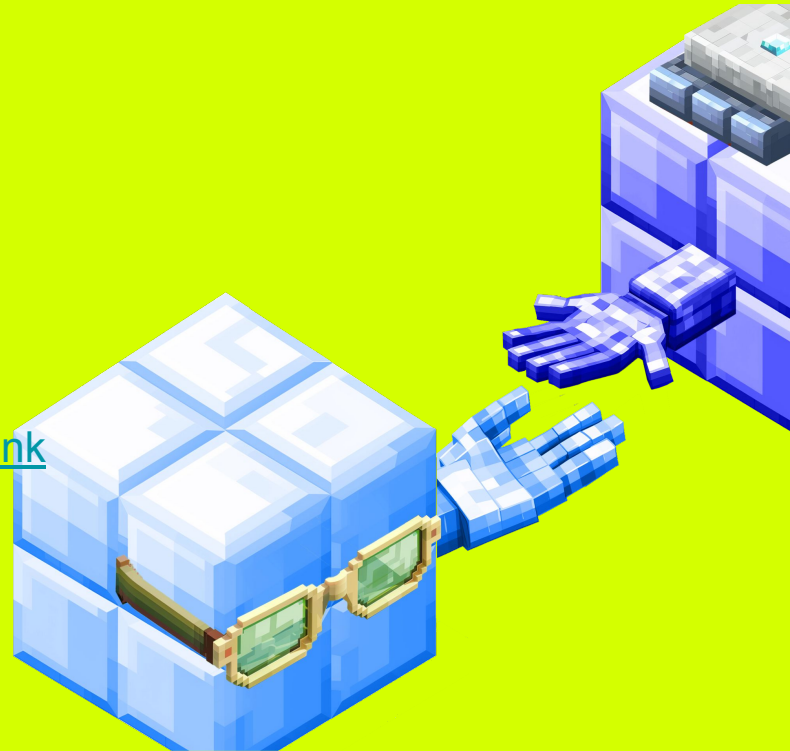
ETHPanda LXDAO

节点软件不止一种：执行层客户端 + 共识层客户端

- 多样性越高：越不怕单一软件 bug / 分叉风险
- 去中心化不仅是“节点多”，还包括“实现多样”
- 以太坊自上线期，从未有过宕机

实操：看主网节点/验证者分布数据

- 节点软件占比：https://ethernodes.org/
- Rated Network Explorer 查看 Validators（验证者）Link
- Etherscan Node Tracker（节点服务器）
  https://etherscan.io/nodetracker



Web3 关键特性回顾

Web3 关键特性

ETHPanda LXDAO

去中心化

- 钱包创建：高度去中心化（人人可生成钥匙）
- 交易广播：可能中心化（RPC 入口、前端入口）
- 网络运行：节点越分散越安全
- 客户端越多样越稳（减少单点软件风险）

- **无许可**：任何人都可以读/写网络（写入需要 gas）
- **抗审查**：节点全球分布、入口可替换（钱包/前端/RPC 都可换）
- **开放开源**：客户端开源、交易记录公开可查询（透明可审计）
- **隐私（现状与演进）**
  - 现状：公开账本 + 伪匿名（地址不等于身份）
  - 风险：可通过关联分析追踪行为图谱
  - 演进：隐私方案仍在发展（例如 ZK、隐私链/隐私层等）

总结

ETHPanda LXDAO

Web3 是跨学科的领域

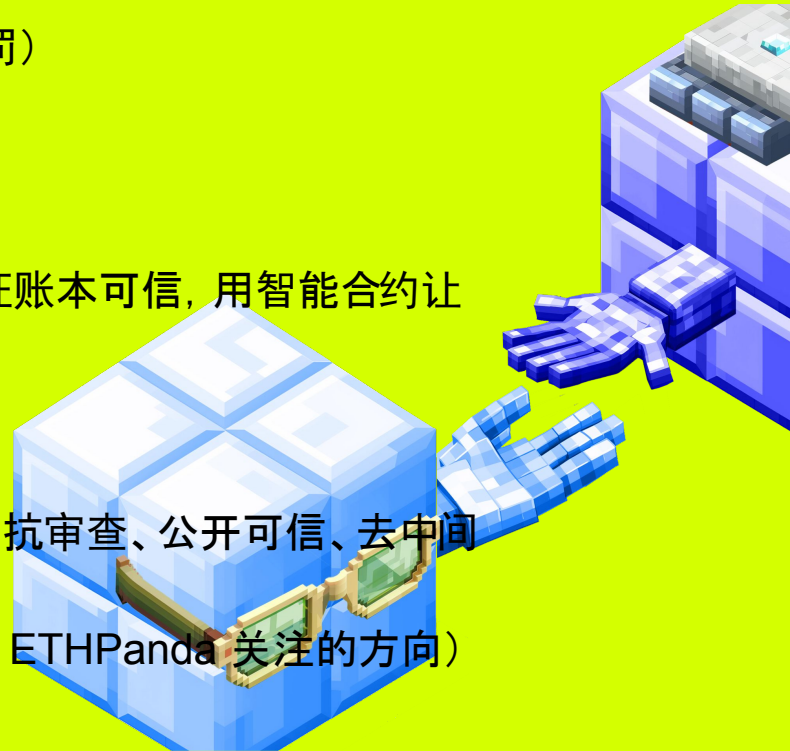
- 社会学：去中心化治理与共识形成
- 经济学：激励设计保证安全与可持续（Gas、质押、惩罚）
- 密码学：签名、哈希、ZK 提供可信基础

技术层面一句话：

- Web3 就是：用私钥签名证明你是谁，用共识网络保证账本可信，用智能合约让规则自动执行。

技术之外：

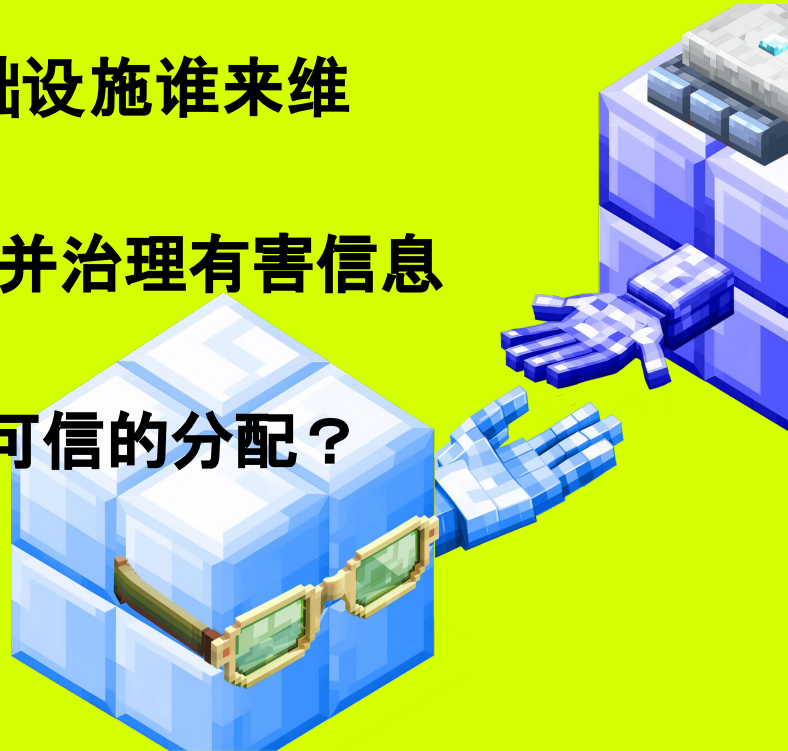
- 权力的重新分配：数字资产与权利自我控制、无许可、抗审查、公开可信、去中间商
- 这些是构建未来数字世界的重要基础（也是 LXDAO / ETHPanda 关注的方向）



留给大家的思考（新的挑战）

ETHPanda LXDAO

- 资产自托管:如何提高安全性、降低管理私 钥的复杂度？
- 没有中心化机构/税收时，公共基 础设施谁来维护？如果有税收，又如何分配？
- 没有审查且隐私很强时，如何界定并治理有害信息/黑产？
- 去中心化 协作下，如何 实现公平、可信的分配？



Web3 实习计划

1.11 - 2.8

ETHPanda LXDAO

Q&A

WX: brucexu-eth
X: @brucexu_eth
TG: @brucexu_eth

https://web3career.build/