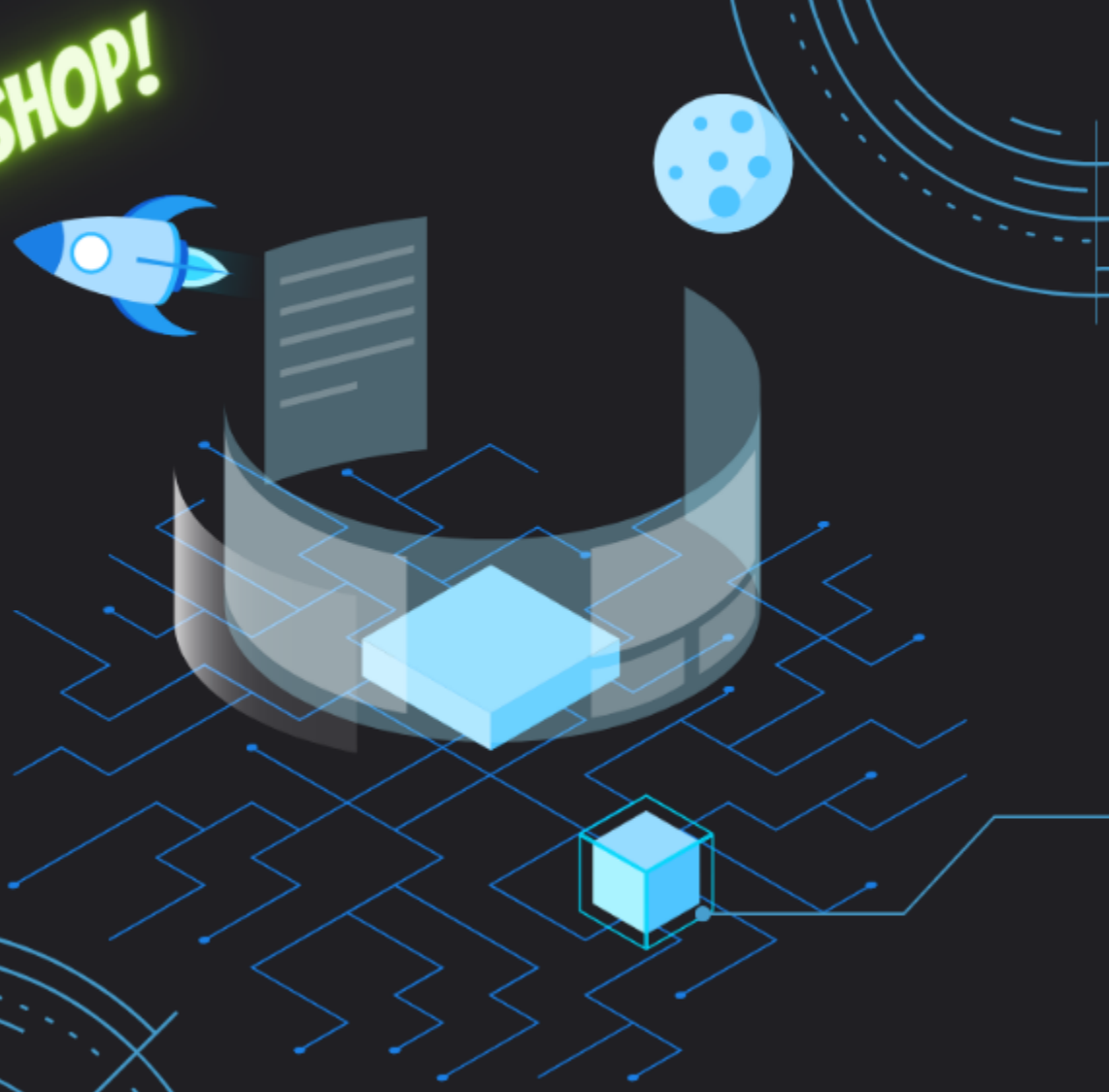
ZK SHANGHAI
零知识证明工作坊

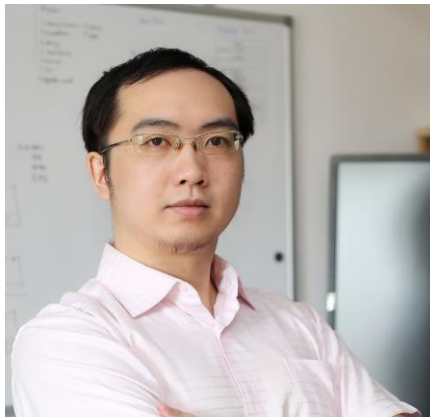


初识零知识

现代零知识密码学

Hosted by SutuLabs & Kepler42B-ZK Planet

个人介绍



梁爽

区块链 架构师

上海交大 计算机博士生
（正在办理休学创业）

微信：icerdesign
微博：@wizicer
Github: @wizicer
Twitter: @icerdesign
LinkedIn: www.linkedin.com/in/icerdesign

1999年	• 正式开始学习写程序
2009年	• 在新媒传信（飞信）做高性能服务器程序架构及开发
2012年	• 在Honeywell工业控制部门做PLC、RTU上位机组态软件架构及开发
2017年	• 接触区块链，并开始创业开发区块链数据库
2020年	• 入学上海交大攻读博士学位，研究零知识证明数据库
2022年	• 获Chia全球开发大赛第一名，并开始Pawket钱包的开发
2023年	• 获得零知识链Mina的项目资助

为什么我们对现代 ZK 感兴趣?

论点

我预计 **ZK-SNARK** 将在未来 **10** 到 **20** 年内渗透到主流世界，从而成为一场重大革命。

vitalik.eth ✓
@VitalikButerin

Replying to @tarunchitra

I expect ZK-SNARKs to be a significant revolution as they permeate the mainstream world over the next 10-20 years.

5:40 PM · Sep 1, 2021 · Twitter Web App

537 Retweets **198** Quote Tweets **2,732** Likes

论点

- ZK密码学（特别是 SNARK、STARK 等可用于任意计算的 ZKP）比人们想象的更重要和普遍。
- ZK密码学比人们意识到的更容易使用，新进入者可以迅速开始做出真正的贡献。
- ZK密码学是一类有趣且具有挑战性的问题，知识的广度可以增加创新性解决问题的可能性。

这门课程是关于什么的?

ZK的“全栈”

- 现代ZK密码学的理论基础
  - 重点是建立直觉，而不是严格的数学严谨性。
- 现代ZK工具栈，以及如何使用它们
  - 基于 F_p 而不是 {0, 1}的二进制计算机，基于$F_p[x]$ 而不是数组。
  - 我们将主要使用 circom + snarkjs 技术栈。
- ZK的应用程序，及其设计模式
  - 这些应用程序通常是去中心化的应用程序（“dapps”），原因我们稍后会讲到。

- ▶ 第一课【4月8日周六】 ZK引言
- ▶ 第二课【4月22日周六】 Circom 1
- ▶ 第三课【4月29日周六】 数学基础构件
- ▶ 第四课【5月7日周日】 Circom 2
- ▶ 第五课【5月13日周六】 承诺方案
- ▶ 第六课【5月20日周六】 高效密码运算算法
- ▶ 第七课【5月27日周六】 算术化
- ▶ 第八课【6月3日周六】 PLONK和多项式恒等式
- ▶ 第九课【6月10日周六】 证明系统栈；递归和组合
- ▶ 第十课【6月17日周六】 应用ZK结构 1
- ▶ 第十一课【6月24日周六】 应用ZK结构 2
- ▶ 第十二课【7月1日周六】 应用演示

- 现代ZK密码学的理论基础
  - 重点是建立直觉，而不是严格的数学严谨性。

- ▸ 第一课【4月8日周六】 ZK引言
- ▸ 第二课【4月22日周六】 Circom 1
- ▸ 第三课【4月29日周六】 数学基础构件
- ▸ 第四课【5月7日周日】 Circom 2
- ▸ 第五课【5月13日周六】 承诺方案
- ▸ 第六课【5月20日周六】 高效密码运算算法
- ▸ 第七课【5月27日周六】 算术化
- ▸ 第八课【6月3日周六】 PLONK和多项式恒等式
- ▸ 第九课【6月10日周六】 证明系统栈；递归和组合
- ▸ 第十课【6月17日周六】 应用ZK结构 1
- ▸ 第十一课【6月24日周六】 应用ZK结构 2
- ▸ 第十二课【7月1日周六】 应用演示

- 现代ZK工具栈，以及如何使用它们
  - 基于 F_p 而不是 {0, 1}的二进制计算机，基于$F_p[x]$ 而不是数组。
  - 我们将主要使用 circom + snarkjs 技术栈。

课程项目

我们强烈鼓励大家参与项目实践，以巩固对零知识证明的理解。课程工作人员将在课程期间为有兴趣构建 ZK 项目的学生提供指导。

你可以从以下角度找到一些项目的灵感：

- 零知识证明的全栈应用程序，例如匿名投票应用程序、点对点/去中心化游戏、混币器等。
- 有用的ZK原语库，例如 ZK友好加密方案的ZK电路。
- 实现零知识证明系统或一些关键组件，并包含一系列教程或文章。
- 文档或教材，例如解释 ZK 证明系统的一系列博客文章或教程。

有兴趣的学生可以在课程的第二次课程后陆续提交项目提案。项目演示将安排在最后一周。

- ▶ 第一课【4月8日周六】 ZK引言
- ▶ 第二课【4月22日周六】 Circom 1
- ▶ 第三课【4月29日周六】 数学基础构件
- ▶ 第四课【5月7日周日】 Circom 2
- ▶ 第五课【5月13日周六】 承诺方案
- ▶ 第六课【5月20日周六】 高效密码运算算法
- ▶ 第七课【5月27日周六】 算术化
- ▶ 第八课【6月3日周六】 PLONK和多项式恒等式
- ▶ 第九课【6月10日周六】 证明系统栈；递归和组合
- ▶ 第十课【6月17日周六】 应用ZK结构 1
- ▶ 第十一课【6月24日周六】 应用ZK结构 2
- ▶ 第十二课【7月1日周六】 应用演示

- ZK的应用程序，及其设计模式
  - 这些应用程序通常是去中心化的应用程序（“dapps”），原因我们稍后会讲到。

课程项目

我们强烈鼓励大家参与项目实践，以巩固对零知识证明的理解。课程工作人员将在课程期间为有兴趣构建 ZK 项目的学生提供指导。

你可以从以下角度找到一些项目的灵感：

- 零知识证明的全栈应用程序，例如匿名投票应用程序、点对点/去中心化游戏、混币器等。
- 有用的ZK原语库，例如 ZK友好加密方案的ZK电路。
- 实现零知识证明系统或一些关键组件，并包含一系列教程或文章。
- 文档或教材，例如解释 ZK 证明系统的一系列博客文章或教程。

有兴趣的学生可以在课程的第二次课程后陆续提交项目提案。项目演示将安排在最后一周。

课程安排

- 每周六 下午 14:00~16:00 上课，16:00~17:00 答疑
  - 除了第二次和第四次课程时间有调整，见课程表
  - 地点：上海市杨浦区国康路100号上海国际设计中心22楼多功能厅
- 问题沟通主要在Github Discussion中进行
  - 有意义的提问回答会记录到课程网站上
  - 指出课程错误或提出改进意见可以进入到课程网站的光荣榜
- 课程资源都可以从主页上下载: zkshanghai.xyz
  - 部分课程活动将进行录制，回放将可供下载
  - 幻灯片、讲义和补充材料都托管在这里

课程安排——编程实践

- 作业提交方法
- 答疑时间——讨论项目
- 课程项目
  - 构建 ZK app
  - 构建 开发者工具
  - 实现ZK原语库
  - 文档或教材
- 可选作业
- Hackathon

课程项目

我们强烈鼓励大家参与项目实践，以巩固对零知识证明的理解。课程工作人员将在课程期间为有兴趣构建 ZK 项目的学生提供指导。

你可以从以下角度找到一些项目的灵感：

- 零知识证明的全栈应用程序，例如匿名投票应用程序、点对点/去中心化游戏、混币器等。
- 有用的ZK原语库，例如 ZK友好加密方案的ZK电路。
- 实现零知识证明系统或一些关键组件，并包含一系列教程或文章。
- 文档或教材，例如解释 ZK 证明系统的一系列博客文章或教程。

有兴趣的学生可以在课程的第二次课程后陆续提交项目提案。项目演示将安排在最后一周。

前置课程

- 初等数论和群论
- 基本密码原语
- 基本代数概念，尤其是多项式

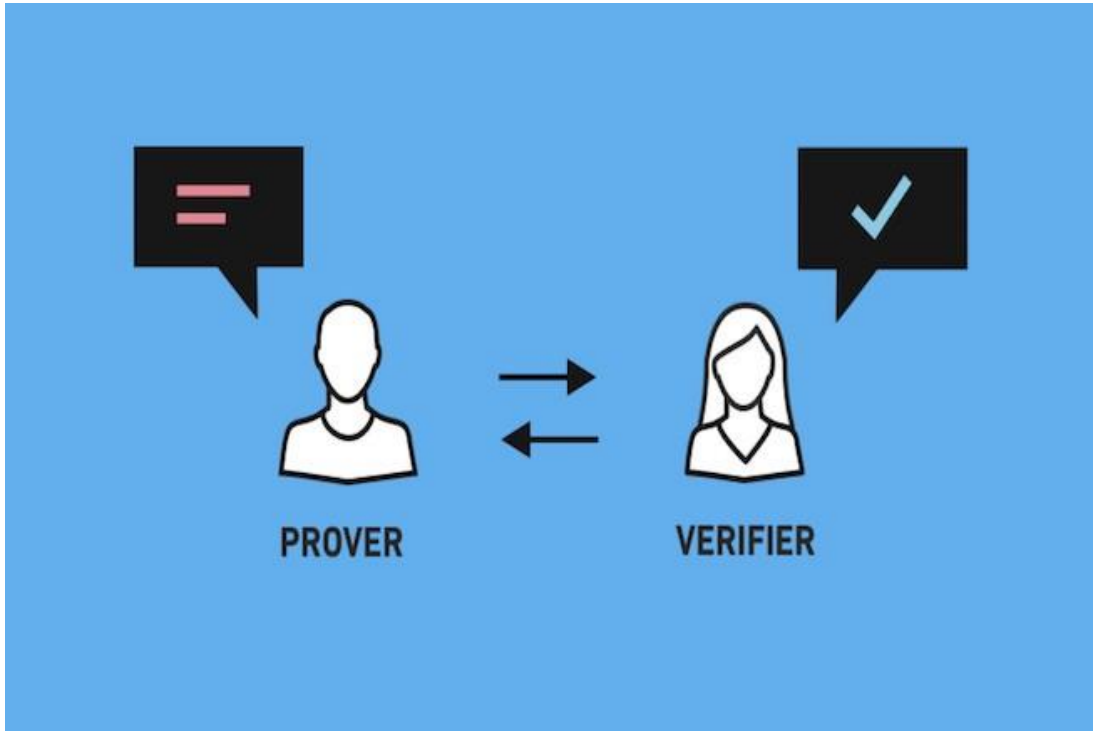
什么是零知识协议?

零知识证明/协议

- 零知识证明让我向你证明我知道一个事实，而不用告诉你事实本身是什么。
- 我知道以太坊账户对应的私钥，但我不会告诉你我的私钥是什么！
- 我知道一种用 3 种颜色填充地图的方法，这样相邻的两个区域的颜色就不会相同，但我不会告诉你颜色！
- 我知道一个数字 x 使得 SHA256(x) = 0x77af...，但我不会告诉你 x！

零知识证明/协议

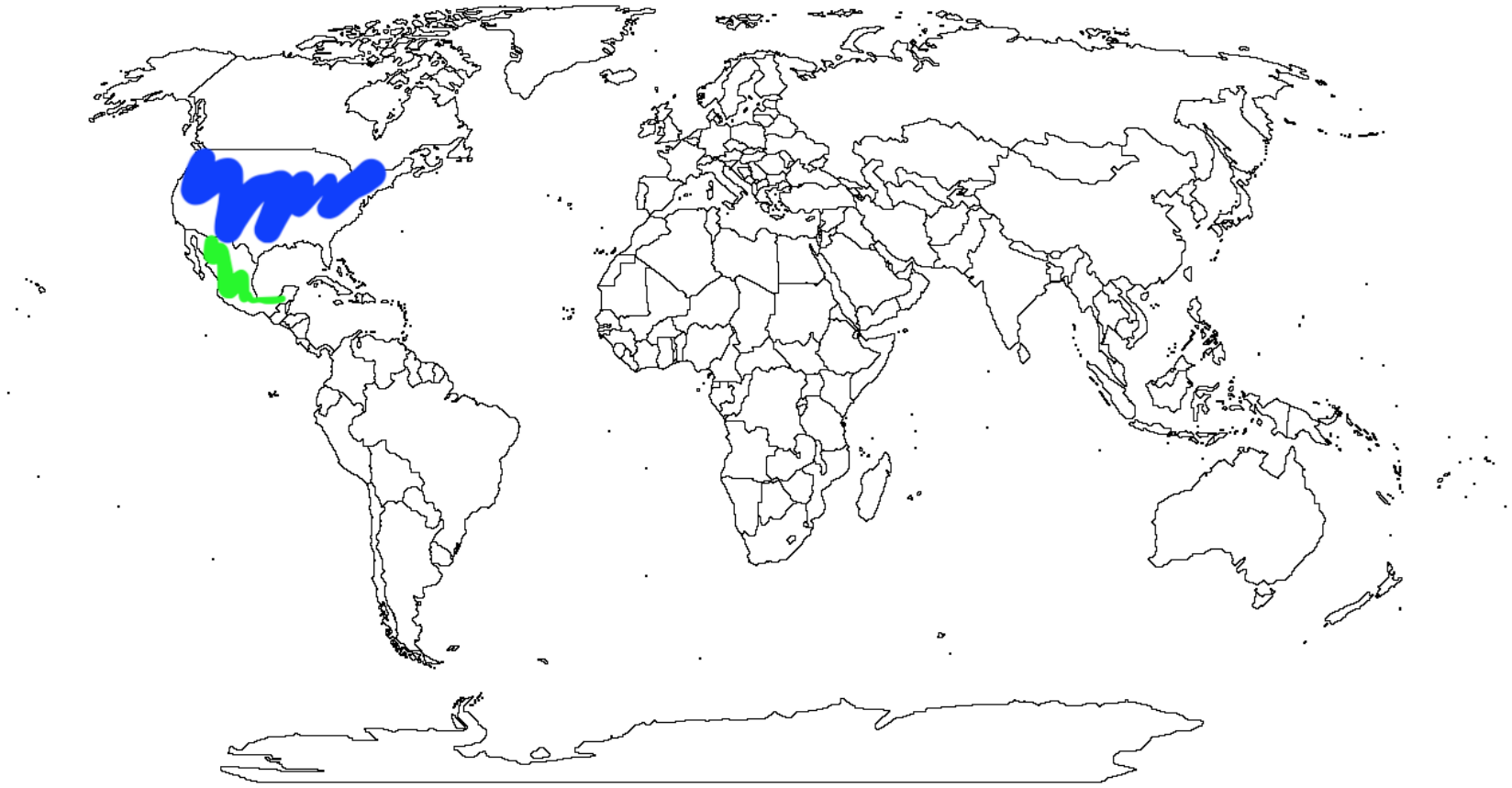
- 场景：证明者想说服验证者他们知道一些事情，而不透露具体信息。
- 验证者：向证明者提出问题或挑战，并检查响应。
- 证明者：回应验证者的问题或挑战。



示例：地图三色问题的 ZK 协议

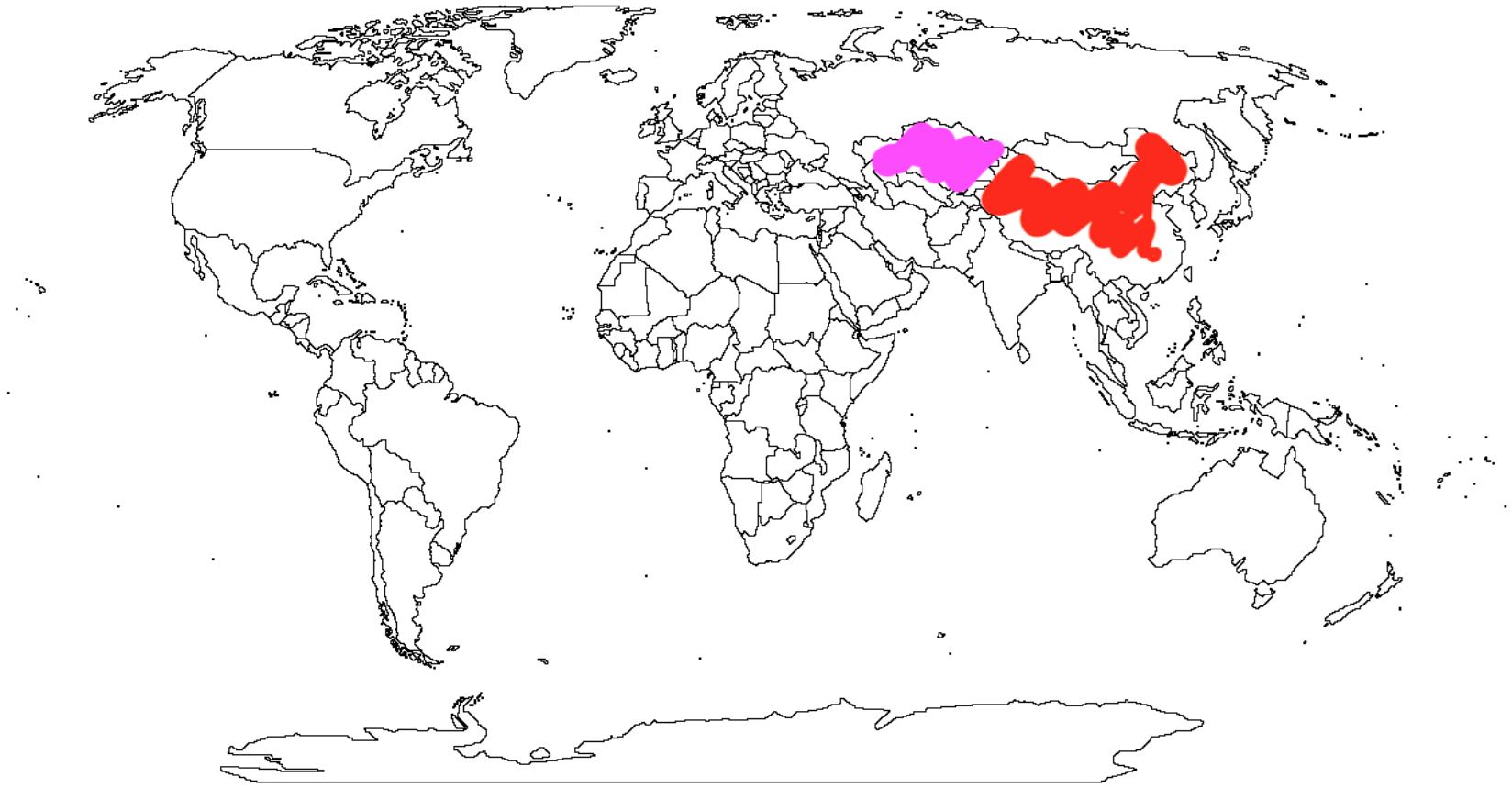
示例：地图三色问题

示例：地图三色问题



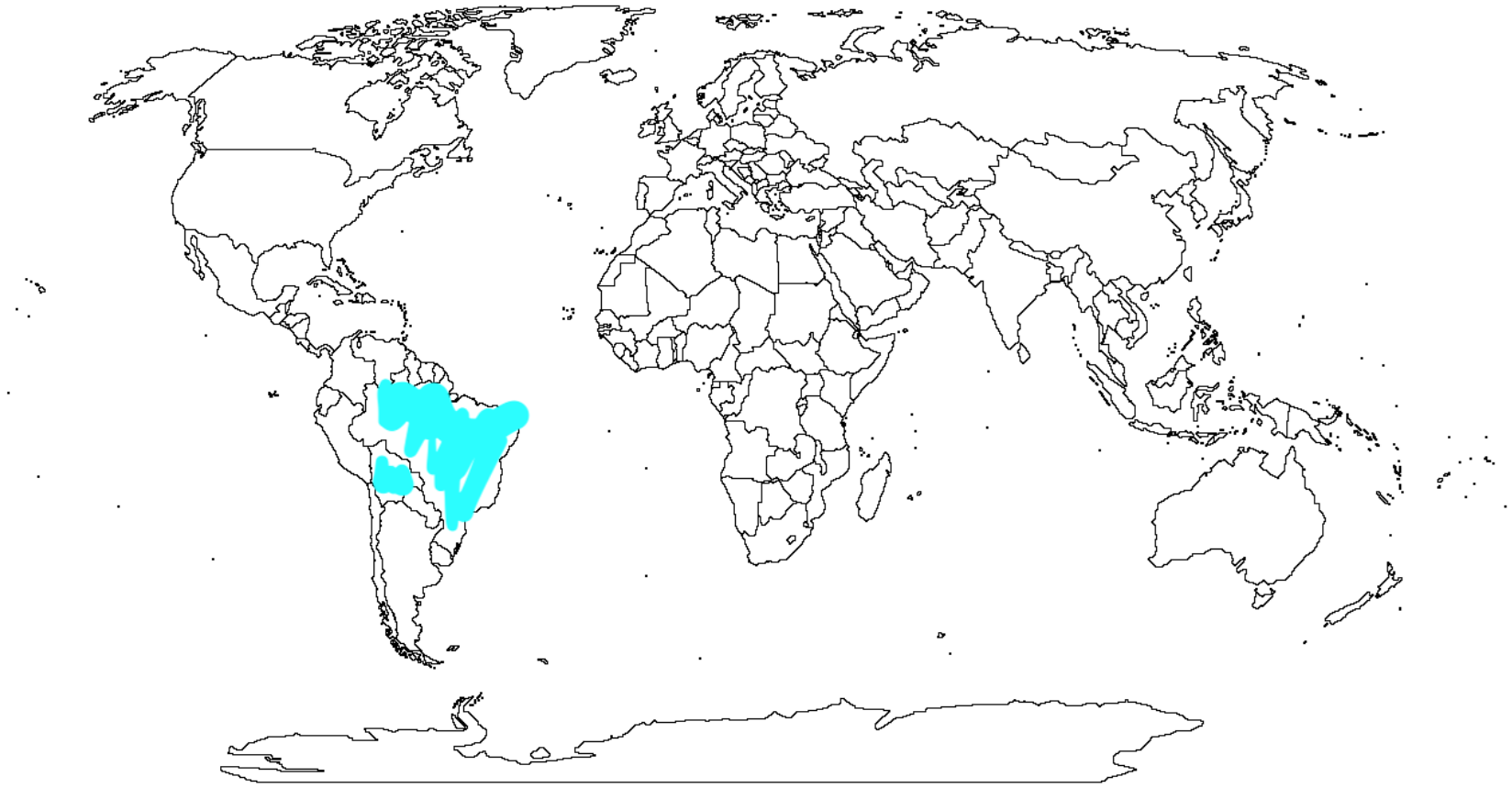
示例：地图三色问题

示例：地图三色问题



示例：地图三色问题

示例：地图三色问题



示例：地图三色问题

- https://zkshanghai.xyz/interactive/graph.html

零知识证明/协议的三个属性

零知识
Zero Knowledge

- 证明者的回答不会透露具体信息。

完备性
Completeness

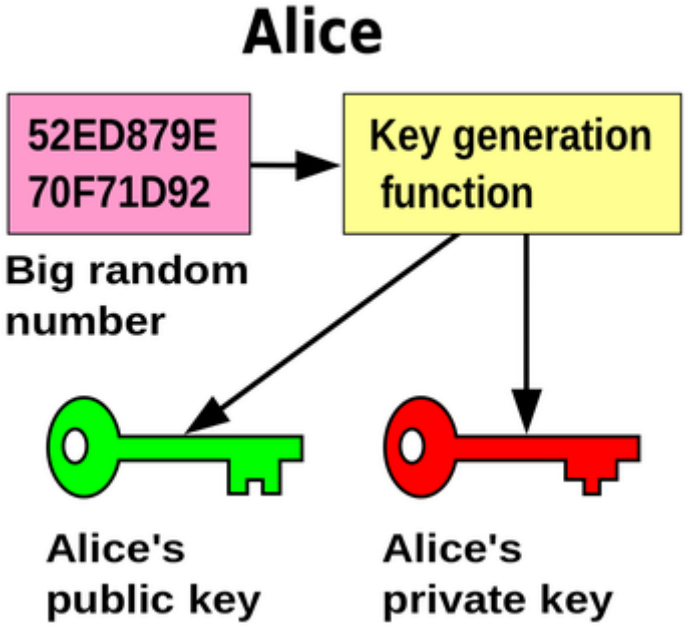
- 如果证明者知道具体信息，他们总能做出令人满意的回答。

可靠性
Soundness

- 如果证明者不知道具体信息，他们最终会被发现。

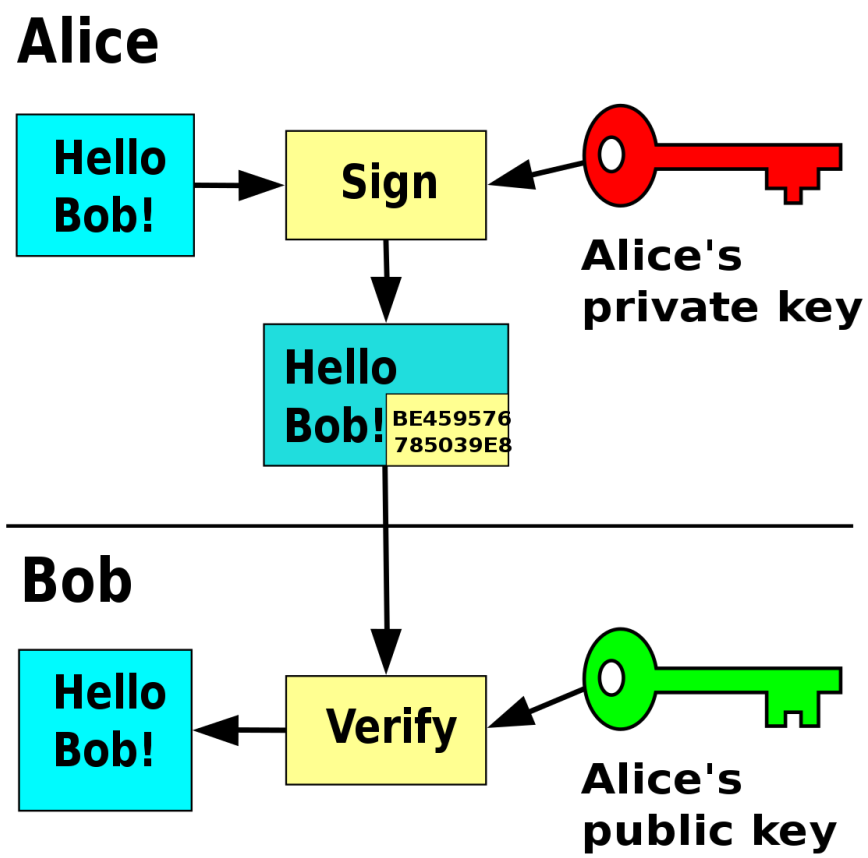
示例 2：数字签名

- 在以太坊中，所有交易都使用公钥进行签名。
- 每个公共帐户都与一个秘密的私钥相关联。
- 除非你知道该帐户的私钥，否则不能从帐户中发送资金。



示例 2：数字签名

- 每笔交易都附有"签名"。
- 签名（本质上）是一个零知识证明，证明你知道与你发送资金的公钥相对应的私钥。



ZKP 并不新鲜！

- 数字签名方案已经存在了几十年。
- 几十年来，针对特定问题的零知识协议也广为人知。
  - 地图三色
  - 图同构
  - 离散对数
  - 哈希原像

ZKP 并不新鲜！

- 对于上述每个问题，研究人员都必须提出一个特殊用途/特定的 ZK 协议。
- 圣杯：“这是一个输出 y 和一个任意函数 f。 我知道一个秘密值 x 使得 f(x) = y”
- 这样做的技术将使我们能够在完全隐私的情况下验证任意计算（例如，货币或数字所有权转移）

示例：匿名投票

- 设置：五个拥有已知公钥/私钥的人，进行投票
  - {sk1, pk1}, {sk2, pk2}, {sk3, pk3}, {sk4, pk4}, {sk5, pk5}
- 除了我的投票，我还会附上一个证明：
- 我知道某个秘密私钥 sk，例如：
  - pubkeygen(sk) = pk
  - (pk - pk1)(pk - pk2)(pk - pk3)(pk - pk4)(pk - pk5) = 0
- 这够了吗？

示例：匿名投票

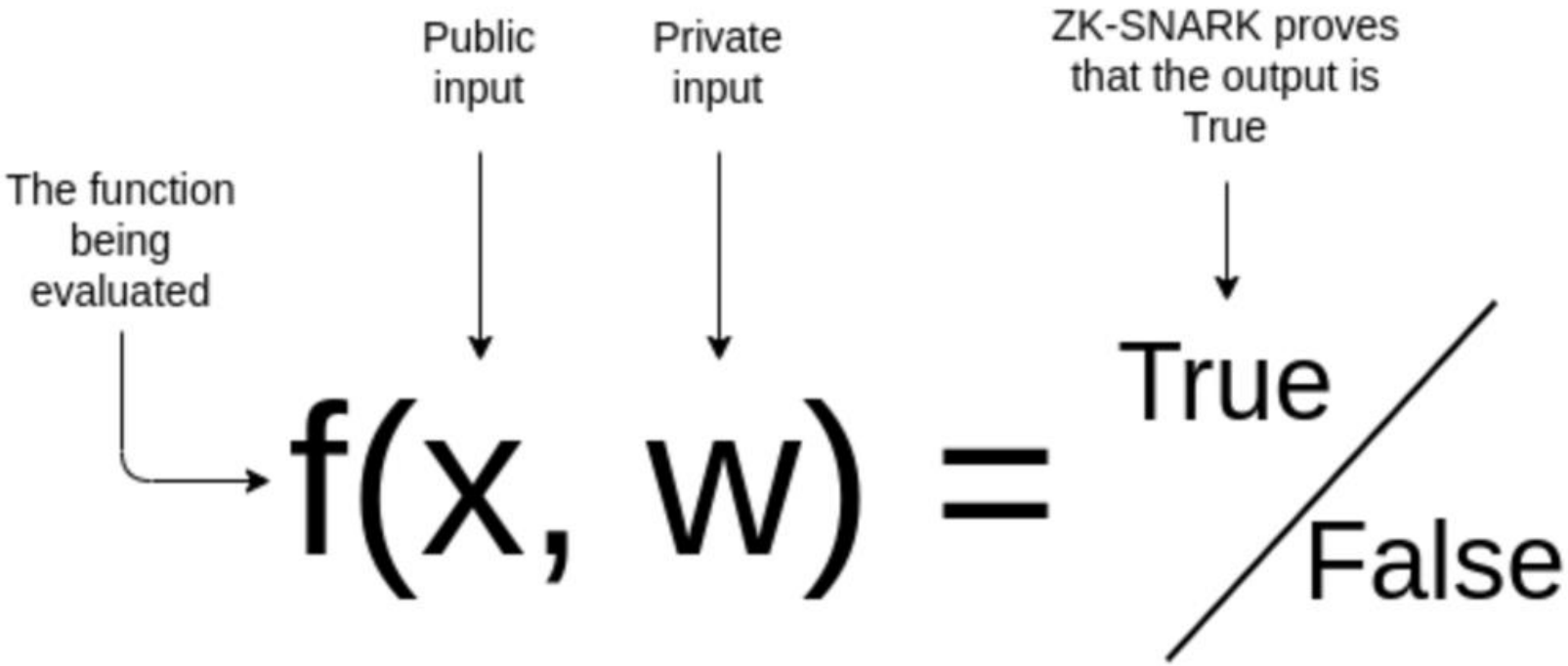
- 设置：五个拥有已知公钥/私钥的人，进行投票
  - {sk1, pk1}, {sk2, pk2}, {sk3, pk3}, {sk4, pk4}, {sk5, pk5}
- 除了我的投票，我还会附上一个证明：
- 对于公开的 nf，我知道某个秘密私钥 sk，例如：
  - pubkeygen(sk) = pk
  - (pk - pk1)(pk - pk2)(pk - pk3)(pk - pk4)(pk - pk5) = 0
  - hash(sk) = nf

zkSNARKs

什么是 zkSNARK?

- 一种新的密码学工具，可以针对任何问题高效地生成零知识协议。
- 特性：
  - zk 零知识：隐藏输入
  - Succinct 简洁：生成可以快速验证的简短证明
  - Noninteractive 非交互式：不需要来回交互
  - ARgument of Knowledge 知识论证：证明你知道输入

什么是 zkSNARK?


Public input
Private input
ZK-SNARK proves that the output is True
The function being evaluated
f(x, w) =
True
False

什么是 zkSNARK?

- 高层次的想法：
  - 将问题（图同构、离散对数等）转换为您要隐藏其输入的函数。
- 将该函数转换为等效的“R1CS”（或其他）方程组
  - 算术电路：一堆在素数域元素中的 + 和 * 操作
  - 简化：形式为 $x_i + x_j = x_k$ 或 $x_i * x_j = x_k$ 的方程
- 为 R1CS 的可满足性生成 ZKP

zkSNARK 属性

- 一种新的密码学工具，可以针对任何问题高效地生成零知识协议。
- 特性：
  - zk：隐藏输入
  - Succinct 简洁：生成可以快速验证的简短证明
  - Noninteractive 非交互式：不需要来回交互
  - ARgument of Knowledge 知识论证：证明你知道输入

zkSNARKs

- 函数输入：x1，x2，x3，x4
- OUT = f(x) = (x1 + x2) * x3 - x4

- zkSNARK：我知道一些秘密（x1，x2，x3，x4），以及这个函数的计算结果 OUT。利用“签名”可以证明存在这样的秘密，但不需要告诉你秘密是什么。

zkSNARKs 证明约束

- 函数输入：x1，x2，x3，x4
- y1 := x1 + x2
- y2 := y1 * x3
- OUT := y2 - x4

- SNARK 证明器输入：x1，x2，x3，x4，y1，y2，OUT
- SNARK 证明器输出：仅当满足以下约束时的可验证“签名”：
  - y1 == x1 + x2
  - y2 == y1 * x3
  - y2 == OUT + x4

zkSNARKs 证明约束

- 函数输入: 02, 04, 08, 05
- 06 := 02 + 04
- 48 := 06 * 08
- 043 := 48 - 05

- SNARK 证明器输入: 02, 04, 08, 05, 06, 48, 043
- SNARK 证明器输出: 仅当满足以下约束时的可验证"签名":
  - 06 == 02 + 04
  - 48 == 06 * 08
  - 48 == 043 + 05

zkSNARKs 证明约束

- 函数输入：x1，x2，x3，x4
- y1 := x1 + x2
- y2 := y1 * x3
- 043 := y2 - x4

- SNARK 证明器输入：x1，x2，x3，x4，y1，y2，043
- SNARK 证明器输出：仅当满足以下约束时的可验证“签名”：
  - y1 == x1 + x2
  - y2 == y1 * x3
  - y2 == 043 + x4

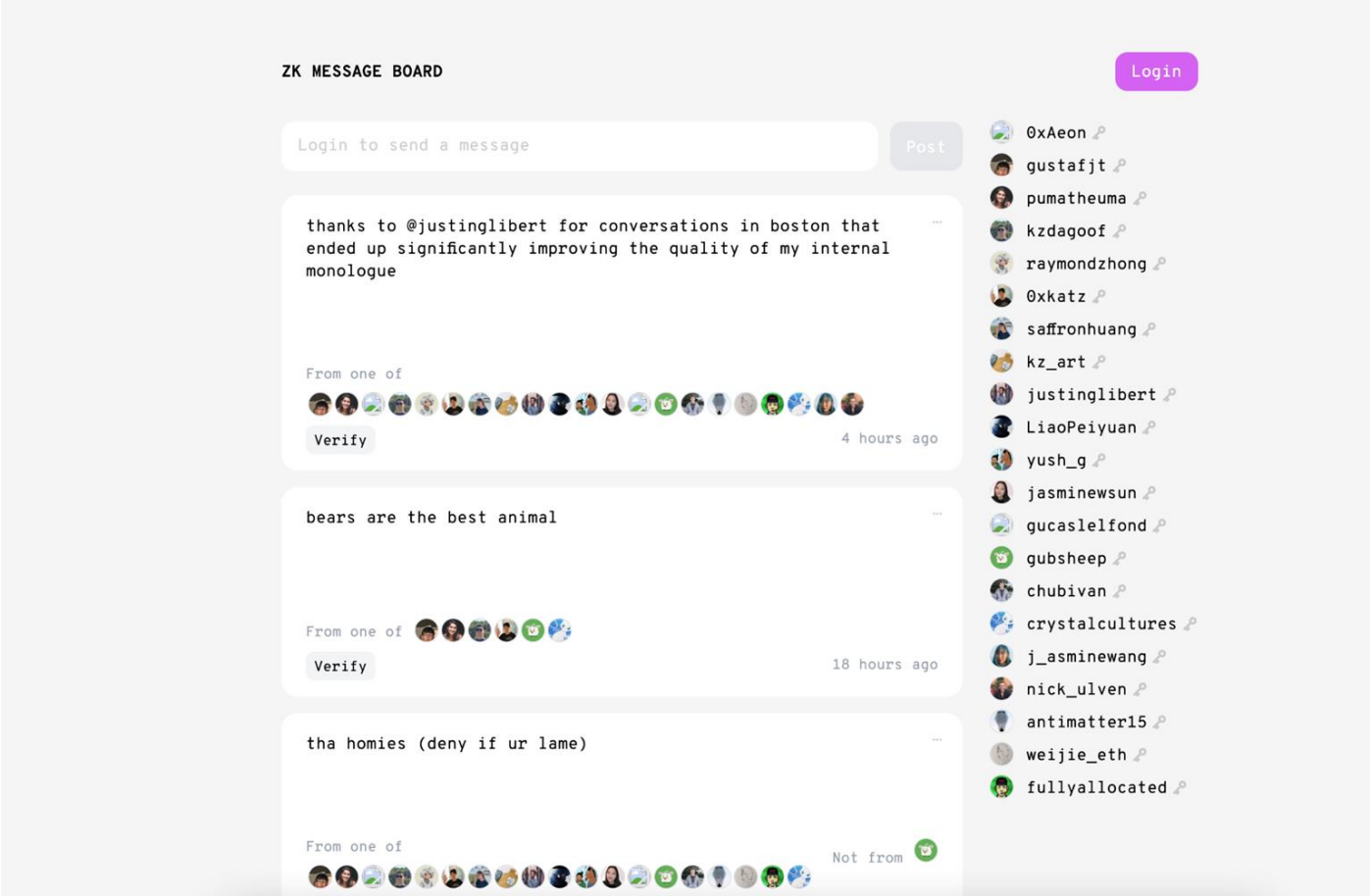
zkSNARKs 证明约束（只用 + 和 *）

- 函数输入： x1， x2， x3， x4
- y1 := x1 + x2
- y2 := y1 / x3
- OUT := y2 - x4

- SNARK 证明器输入： x1， x2， x3， x4， y1， y2， OUT
- SNARK 证明器输出：仅当满足以下约束时的可验证“签名”：
  - y1 == x1 + x2
  - y1 == y2 * x3
  - y2 == OUT + x4

ZKRepl demo #1

应用

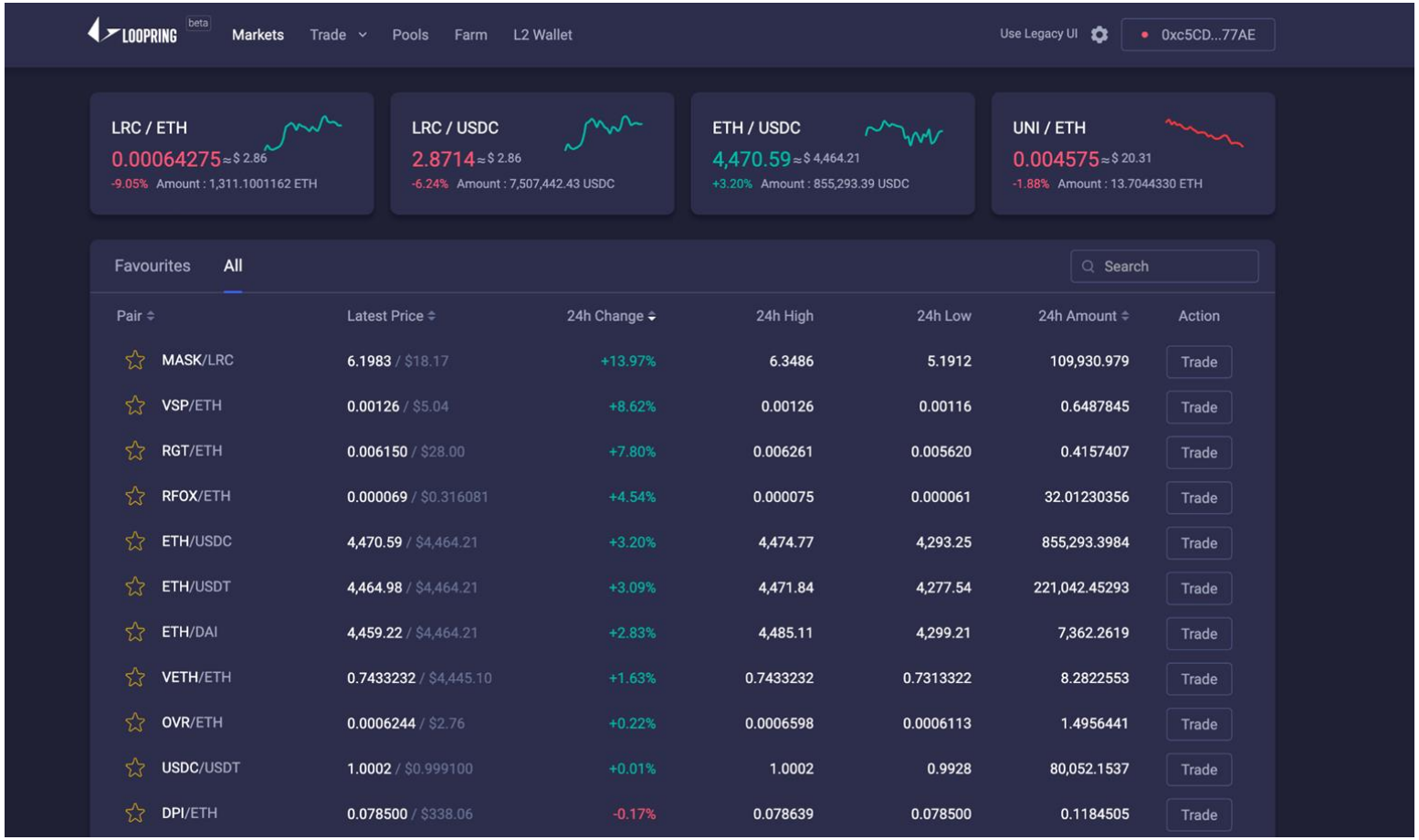

ZK MESSAGE BOARD
Login
Login to send a message
Post
thanks to @justinglibert for conversations in boston that ended up significantly improving the quality of my internal monologue
From one of
Verify
4 hours ago
bears are the best animal
From one of
Verify
18 hours ago
tha homies (deny if ur lame)
From one of
Not from
0xAeon
gustafjt
pumatheuma
kzdagoof
raymondzhong
0xkatz
saffronhuang
kz_art
justinglibert
LiaoPeiyuan
yush_g
jasminewsun
gucaslelfond
gubsheep
chubivan
crystalcultures
j_asminewang
nick_ulven
antimatter15
weijie_eth
fullyallocated

应用

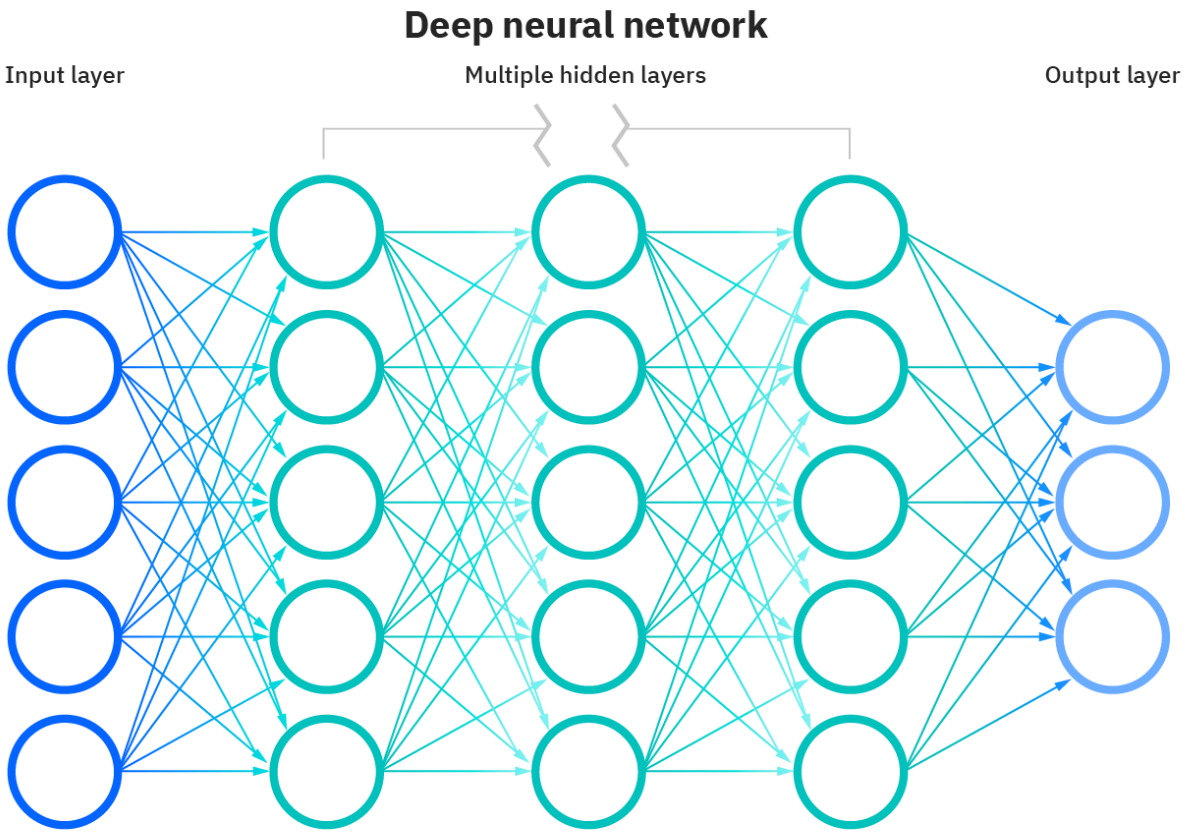
应用


tornado
CASH
Non-custodial anonymous transactions on Ethereum

应用


LOOPRING beta
Markets
Trade
Pools
Farm
L2 Wallet
Use Legacy UI
0xc5CD...77AE
LRC / ETH
0.00064275 ≈ $ 2.86
-9.05% Amount : 1,311.1001162 ETH
LRC / USDC
2.8714 ≈ $ 2.86
-6.24% Amount : 7,507,442.43 USDC
ETH / USDC
4,470.59 ≈ $ 4,464.21
+3.20% Amount : 855,293.39 USDC
UNI / ETH
0.004575 ≈ $ 20.31
-1.88% Amount : 13.7044330 ETH
Favourites
All
Search
Pair
Latest Price
24h Change
24h High
24h Low
24h Amount
Action
MASK/LRC 6.1983 / $18.17 +13.97% 6.3486 5.1912 109,930.979 Trade
VSP/ETH 0.00126 / $5.04 +8.62% 0.00126 0.00116 0.6487845 Trade
RGT/ETH 0.006150 / $28.00 +7.80% 0.006261 0.005620 0.4157407 Trade
RFOX/ETH 0.000069 / $0.316081 +4.54% 0.000075 0.000061 32.01230356 Trade
ETH/USDC 4,470.59 / $4,464.21 +3.20% 4,474.77 4,293.25 855,293.3984 Trade
ETH/USDT 4,464.98 / $4,464.21 +3.09% 4,471.84 4,277.54 221,042.45293 Trade
ETH/DAI 4,459.22 / $4,464.21 +2.83% 4,485.11 4,299.21 7,362.2619 Trade
VETH/ETH 0.7433232 / $4,445.10 +1.63% 0.7433232 0.7313322 8.2822553 Trade
OVR/ETH 0.0006244 / $2.76 +0.22% 0.0006598 0.0006113 1.4956441 Trade
USDC/USDT 1.0002 / $0.999100 +0.01% 1.0002 0.9928 80,052.1537 Trade
DPI/ETH 0.078500 / $338.06 -0.17% 0.078639 0.078500 0.1184505 Trade

应用


Deep neural network
Input layer
Multiple hidden layers
Output layer