Truth Protocol 白皮书

Signer

摘要：余弦（慢雾创始人）在《区块链黑暗森林自救手册》中说过：“被黑是 100% 普适现象，绝无例外！”Web2用户进入Web3中除了有较高的钱包使用门槛，还有极大的被黑风险。为了让Web2用户更好地进入Web3，也为了保护当下Web3用户的网站访问安全，我们开发一个名为 Signer 的危险网站提醒插件。该插件基于一套名为 Truth Protocol 的链上协议，该协议致力于激励所有人参与危险网站的标记，以此降低危险网站库的维护成本及中心化共识非议。这些危险网站数据将会存储在 Scroll 链上，Signer 插件也将实时同步这些链上信息，在用户访问这些危险网站时给予最及时的提醒。除了服务于危险网站标记，Truth Protocol 还将有效应用于金融领域，构造出一种链上的去中心化的具有保险属性的 CDS（Credit Default Swap）。我们相信未来还将有更多的基于 Truth Protocol 的 DeFi 创新协议，这些带动下一轮的 DeFi 繁荣！

1. 背景

在Web3的圈子的里钱包被盗的事情几乎每天都在上演，据慢雾区块链被黑事件档案库（Hacked.slowmist.io）和 Elliptic 的数据统计，截止 2023 年 1 月，NFT 被盗的知名安全事件有几百起，攻击者偷走了价值近 2 亿美元的 NFT。其中就包括 2023 年 1 月28 日，Azuki 的Twitter 账号被黑，导致其粉丝连接到钓鱼链接，超122 枚NFT 被盗，损失超过 78 万美元。之所以一个钓鱼网站能够不断地让用户上当，**主要原因是因为信息不共享，以及缺少能够提醒用户的工具。**

据慢雾团队统计：**区块链行业被钓鱼攻击主要分布在“域名、签名”两点，其中 90% 的钓鱼都跟虚假域名有关。**

如果用户打开一个钓鱼页面，相关的插件、浏览器就能直接提示风险，这样就没有了后面骗签名的步骤，可以把风险阻断在第一步。因此，我们希望能够做一个安全检测插件来在用户访问网站的时候提醒用户该网站的安全性，以此来避免用户之后可能造成的损失。

目前也有一些安全团队已经开发了相关的插件工具，有些工具已经产生了很明显的效果，例如PeckShieldAlert等。但是这些插件平台的发展都面临着一些挑战：

a. 危险网站地址库**运维挑战大，成本高**；
b. 受去中心化共识的影响，钓鱼网站、黑名单库等需要中心化的运维支撑，**会产生共识侧的非议**；
c. 受商业化倾向影响，服务夹层虽能优化体验却**难以商业变现**。

以上这些是为什么目前没有一款安全插件得到真正的大面积普及的主要原因。为此，我们希望通过Web3的去中心化方式及代币经济模型来解决这些问题。我们设计的插件名为 Signer，协议名为

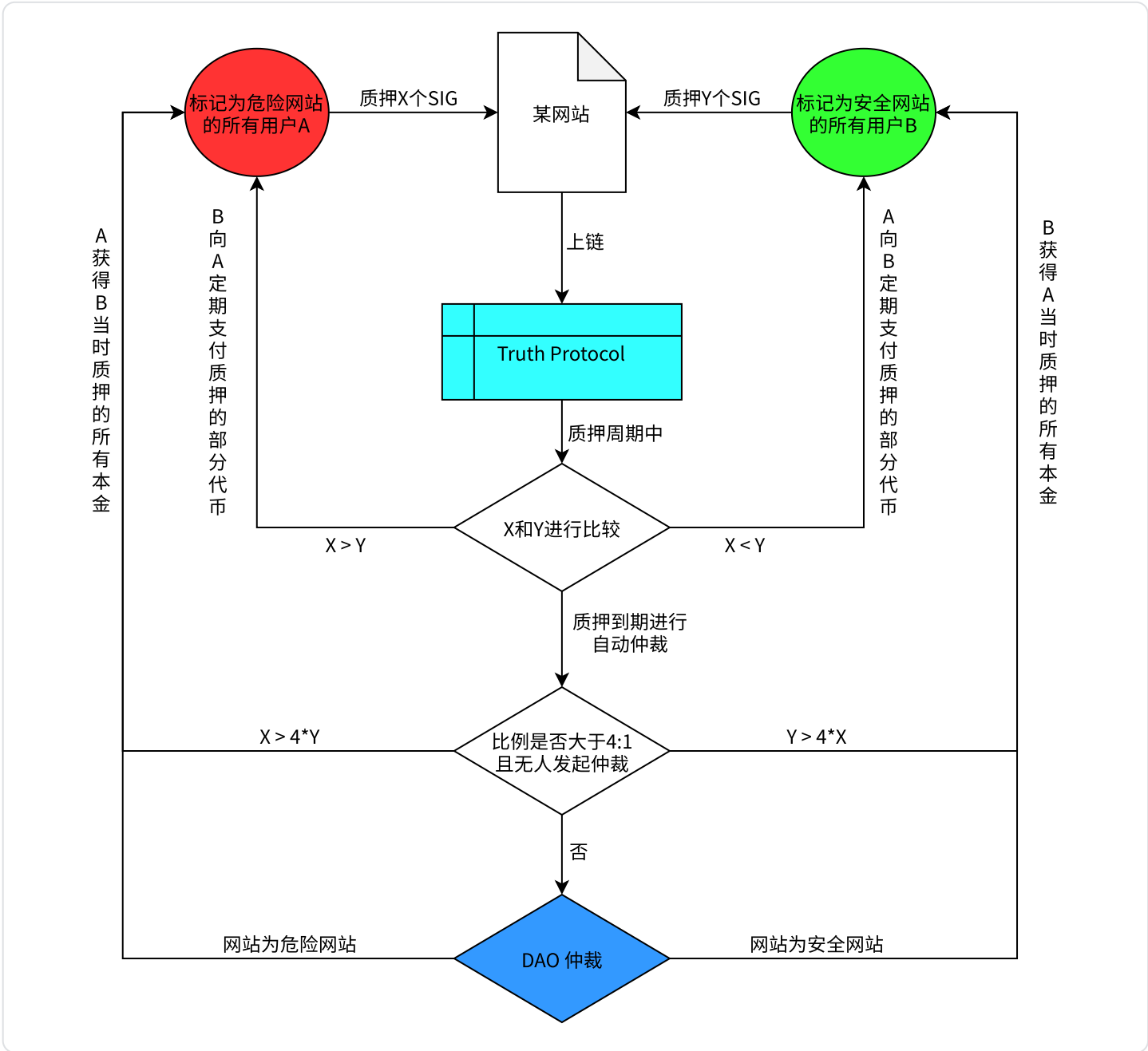
Truth Protocol。

2. 解决信息不对称

为了解决钓鱼网站信息得不到传播的问题，我们将通过区块链的形式来记录被用户标记的钓鱼网站信息。由于区块链的公开性，用户将可以非常容易地获取到被他人标记的钓鱼网站信息，激励用户会去主动标记我们的钓鱼网站的方式可以详见第3部分的经济模型激励。我们也会同步开发一个钓鱼网站监测插件及信息展示网站，用户仅需使用我们的插件就可以检测其当前网站的安全性，并通过我们的信息展示网站来更好地评估该网站及其他网站的安全性。

3. 经济模型激励

3.1 质押奖惩流程



为了让用户能够更加主动地参与到这个标记系统当中，并且减少错误标记，我们将通过上图的代币经济模型来实现。

a. 具体而言，用户在进行网站标记的时候首先需要选择标记为安全网站还是危险网站；
b. 然后在该方向质押一定的SIG代币，并选择质押期限，完成该操作后用户标记的网站及质押信息将会上链；
c. 之后根据 Truth Protocol，若用户质押的方向属于代币较少的一方，则需要向多方不间断地支付质押代币的一部分，直至质押结束或有人中途发起仲裁；
d. 当质押周期结束，该网站将进入自动仲裁，若某一方的质押代币数量高于另一方的4倍，且在该自动仲裁期无人发起 DAO 仲裁，则质押代币多的一方可以获得质押代币少的一方的当时质押的所有代币；
e. 若有人发起 DAO 仲裁或者比例不满足阈值，则进入 DAO 仲裁阶段，这个阶段将会有各方参与投票仲裁，具体详情可参见第4部分仲裁。

以下是收益及惩罚分配计算方法介绍。

3.2 基本质押收益：

对于某些在社会中具有强烈一致共识的网站，其网站质押的一方可能没有人与其进行对赌，但是这部分人也是为协议做出了贡献的人，因此 Truth Protocol 协议会给所有参与质押的用户分配一定的“基本质押收益”。这部分资金来源于 DAO 国库，其利率水平的调节依赖于 DAO 的投票决策。

3.3 劣势质押损耗

在某个网站的质押周期内，SIG 质押数量更少的一方需要向更多的一方不断支付部分质押当中的 SIG 代币，这部分损耗我们记为“劣势质押损耗”，在 6.2 的 CDS 保险案例中即为“保费”。该支付费用的计算公式如下：

$$\sum amountA > amountB : ((nowUserAmount) \times (\frac{\Delta t}{remainTimes})$$

即当一边大于另外一边的时候，以最小的连续时间间隔（在合约实现上是以用户trade时间间隔进行计算）计算剩下的应该支付的保费比例，直到最后一刻少的一方支付全部的保费到另一方，并且该过程在时间上各个位置等价——在金融上，一段时间内时间的衰减和演变往往是线性的，这也是我们选择此方法的原因。

SIG 质押数量多的一方将可以根据所占时间份额和资金份额等比例获得这部分收益，并且可以在质押期的任何时刻主动提取这部分收益。注意，在某个网站的质押周期内，这个“劣势质押损耗”可能会因为双方质押金额的改变发生反转，在 Truth Protocol 的系统当中，该损耗的计算在区块层面是连续的，因此可以很好地保障质押双方的权益。

3.4 代币分配

35%：DAO 国库，定期作为基本质押收益释放，五年内缓慢释放到所有参与网站质押的 SIG 持有者手中；

25%：空投给具有社会安全公信力的组织或个人；

20%：MMF（Market Making Found），即一个为了让经济模型更叫有效的市场调节基金，MMD 中的资金将会根据风险评估算法自动到所有的池子中与用户进行对赌；

20%：各期投资者和团队。

4. 仲裁

4.1 自动仲裁

自动仲裁，即由智能合约自动完成裁决。进入自动仲裁需要满足两个条件：一个是质押池比例是否大于4:1，另一个是之前是否有人主动发起 DAO 仲裁。当进入自动仲裁后，质押池还将进入三天的锁定期，这个时间窗口是留给用户发起 DAO 仲裁的。若无人发起 DAO 仲裁，则自动仲裁的结果将为最终状态。反之，则进入 DAO 仲裁阶段。

在质押池进入自动仲裁期的最后阶段，风险事件的可预测性将大大增加，用户在此时参与质押可以更稳健地获得收益。这个风险收益比将会吸引大量的用户或组织进行参与，这将使得一个被大众共识的网站其标记比例在这段时间会快速地超过4:1，进而在周期结束时直接完成自动仲裁，而不会进入 DAO 仲裁。

4.2 DAO 仲裁

所谓的 DAO 仲裁，就是让持有未参与质押的 SIG 的人，可以参与仲裁投票，DAO 仲裁组即由这些人组成。一个 SIG 记为一票，参与投票数量需要大于 1w 仲裁结果方为有效，否则该质押池将在进入仲裁后的 3 天后直接进入下一个周期。若投票数量满足条件，仲裁结果将依据“多数原则”决定。为了让这个结果更具有社会共识性，我们将在代币发行初期对世界范围内的可信组织和个人空投 SIG 代币。

进入 DAO 仲裁的情况有两种：一种是有人主动发起 DAO 仲裁；另一种是在协议到期不满足自动仲裁条件。

在前一种情况下，按照目前的构想，任何人在任何时间都可以对某个网站的安全性评判主动发起 DAO 仲裁，但是主动发起 DAO 仲裁的人需要质押该网站当前总质押量的 50% SIG 代币，并标记该网站是否为安全网站。若仲裁结果有效，并且符合发起仲裁人的标记，则其将获得输的一方金额的 20%，仲裁组获得输的一方的 10%，赢的一方获得剩下的 70%。若仲裁结果无效，则该发起仲裁者的质押 SIG 将自动放入其标记的一方进入下一周期等待仲裁。

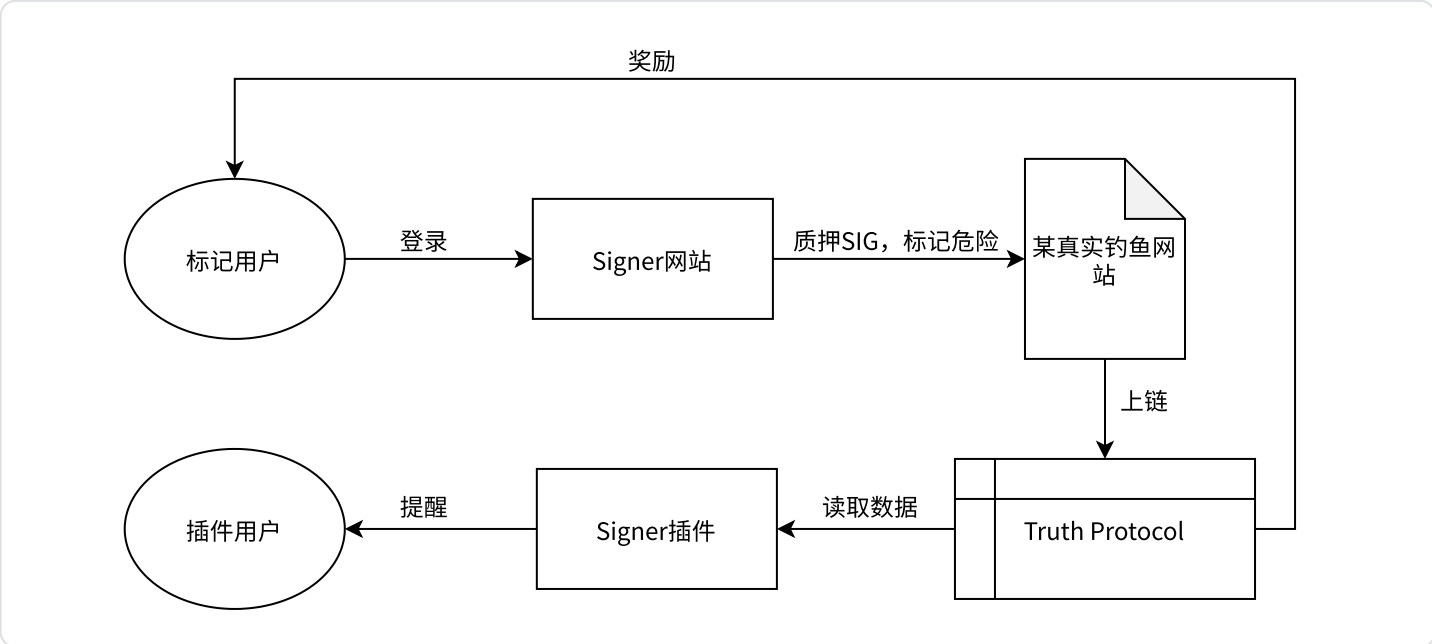
在第二种情况下，DAO 仲裁组会根据当前池子是否能够产生足够的仲裁收益来决定是否参与仲裁投票，若投票结果有效则仲裁组可以获得输的一方金额的 30%，反之则进入下一周期等待仲裁。

5. MMF（Market-Making Found）

这是一个由 DAO 控制的用来调节 Truth Protocol 有效性的一个以 SIG 为主的基金。由于项目早期可能缺少用户参与，因此协议的有效性不一定会得到体现。例如仅有的几个用户质押某个实际为钓鱼网站为安全网站，此时由于用户不足的情况导致其很难有对赌方。为此，DAO 会自己设计一套网站安全评分算法，并根据该算法利用MMF参与网站质押，尤其是被用户质押过的网站，以此来保证协议在早期阶段的有效性。除此之外，MMF 还会在每个网站质押期到期前参与网站质押，因为越接近到期，质押时的胜率越高。MMF 的这个行为将会使得大部分的网站质押在自动仲裁期就会结果，减少进入 DAO 仲裁的情况，以更大程度实现去中心化，避免协议纠纷。MMF 产生的收益和亏损都归属于 MMF，但 MMF 最多维持 20% 的代币持有量，多余的代币将会定期进行销毁。

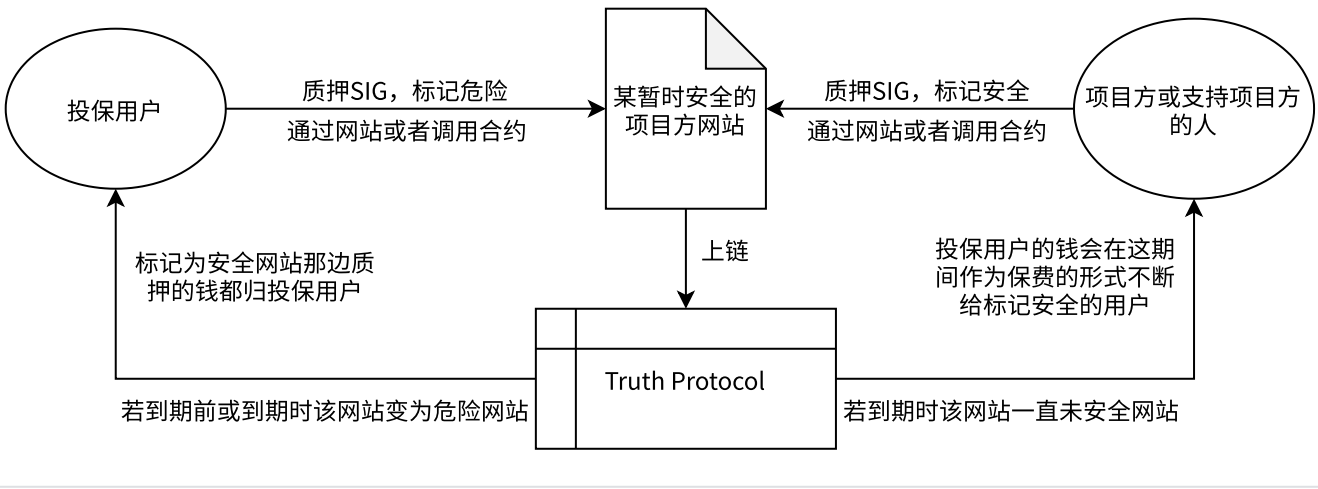
6. 协议的应用及拓展

6.1 钓鱼网站标记案例



在本案例中，想要标记网站的用户可以登录Signer网站，然后质押SIG代币来标记该网站为钓鱼网站，用户的质押行为和数据将上链，并进入 Truth Protocol，协议将根据第 3 部分的经济模型给予用户奖励。我们的 Signer 浏览器插件将会从 Truth Protocol 协议中读取各种网站的质押数据，这些数据将会提供给插件的使用用户，实时提醒他们所访问网站的安全性，并展示该网站的质押相关信息。

6.2 CDS 保险案例



在本案例中，此时某个项目方暂时是一个好的项目方，但是某些用户认为这个项目方未来一段时间可能出事，或者因为自己在这个项目上有一定的投资，想要对冲一下这个风险，他可以通过 Signer 网站来标记该项目方的网站为危险网站，项目方或者支持项目方的人为了避免用户对平台产生负面影响就会主动地去质押 SIG 来标记其为安全网站，并且会比标记危险的那一方质押数量更多，对于项目方来说这个比例越高越好。因此，在这样机制下，质押为危险那一方的用户本质实现了一个投保行为，因为一旦之后该项目方出现问题，其质押的代币将会归投保用户所有，反之，投保用户只需要付出其质押的少量代币，这就实现了一个具有保险属性的 CDS（Credit Default Swap）。CDS的工作原理是违约保护购买者向提供者支付保费，提供者向购买者提供违约保护。当违约事件发生时，购买者将得到违约票面总额作为补偿，而若没有发生违约事件，提供者将全额赚取保费。

7. 数据格式

```
struct poolTrade {
    address trade_address;
    uint256 trade_timestamp;
    uint256 amount;
    uint256 trust_score;
    uint256 other_score;
    bool isUpvote;
}

//存储外部的池子信息
struct poolState {
    uint256 upvotes;
    uint256 downvotes;
    uint256 pool_trade_times;
    uint256 pool_state;
}

struct userState {
    uint256 upvotes;
```

```
        uint256 downvotes;
        //uint256 pool_trade_nums;
        uint256 extracted_premium;
        uint256 extracetd_interest;
        bool extracetd_compensate;
    }

    struct factoryState {
        uint256 upvotes;
        uint256 downvotes;
        uint256[] website_list;
    }

    mapping(uint256 => factoryState) public web_factory_state;

    mapping(string => mapping(uint256 => poolState)) public web_pool_state;

    //网址/交割日期/交易次数
    mapping(string => mapping(uint256 => mapping(uint256 => poolTrade)))
        public web_pool_trade;

    mapping(address => mapping(string => mapping(uint256 => userState)))
        public userVotes;

```

```
{
"web_pool_state 网址质押状态": {
  "website_name": {
    "交割日期": {
      "upvotes": 0 //正方质押tvl,
      "downvotes": 0 //反方质押tvl,
      "pool_trade_times": 0, //池子交易次数，以构建循环索引
      "pool_state": 0  //池状态
    }
  }
},

"web_pool_trade": {
  "your_website_name": {
    "0": {
      "0": {
        "trade_address": "0x0",  //地址
        "trade_timestamp": 0,    //交易发生时间
        "amount": 0,             //交易发生数量
```

```
            "trust_score": 0,          //交易发生时记录预言机评分
            "other_score": 0,          //交易发生时记录预言机其余分数
            "isUpvote": false          //质押方向
          }
        }
      }
    },

    "userVotes": {  //用户侧数据，用户为查询
      "0x0": {
        "your_website_name": {
          "0": {
            "upvotes": 0,            //up方质押
            "downvotes": 0,          //down方质押
            "extracted_premium": 0,      //已经提取的保费收入
            "extracetd_interest": 0,     //已经提取的协议质押收入
            "extracetd_compensate": false     //赔付与本金已经取出
          }
        }
      }
    }
}

```

8. 未来规划

通过上述介绍，我们可以发现 Truth Protocol 不仅可以服务于钓鱼网站的标记和共享事业，其对赌式的经济模型设计还将有效运用于金融领域。因此，在早期产品和协议发布的时候，Truth Protocol 将主要通过 Signer 这个危险网站监测插件来进行冷启动和推广。

当协议被大量用户使用和理解之后，我们将会推出更多应用层产品（例如上述的 CDS 保险服务）来迎合更多元的市场需求。并且为了增加协议的可拓展性，我们还将考虑在未来接受其他的代币在 Truth Protocol 当中进行质押，这将极大地提升协议的适用范围，更大地发挥协议的价值。

我们还将在未来把 DAO 仲裁的投票权转移到以太坊，让 SIG 和 ETH 的共同持有者参与 DAO 仲裁，这样 Truth Protocol 协议的安全性和共识性将会趋同于以太坊的安全性。

9. 结论

通过上述介绍，我们可以知道 Truth Protocol 将有效服务于 Signer 危险网站提醒插件，帮助更多的用户把被黑的风险阻断在第一步，以此来避免用户之后可能造成的损失。Truth Protocol 与 Signer 是两个相辅相成的项目，Signer 很好地契合了当下用户对于防危险网站的迫切需求，也将十分有利于 Truth Protocol 协议在最初期的冷启动；Truth Protocol 也为 Signer 提供了一个完美的激励机制，以此来大大降低危险网站库的维护成本，提高网站标记真实性。

从 Truth Protocol 的对赌性质和 6.2 的 CDS 保险案例，我们也可以发现 Truth Protocol 在 DeFi 领域有着巨大的潜力。该协议的抽象形式，其实是一种基于特定风险场景下的“双边点对点保险池”，这类的金融产品包括保险和去中心化预测项目、二元期权等。在 Truth Protocol 中，参保的双方将无需流动性提供者，算法将会公平地计算当下的风险价值和时间价值，这将高效地服务于想要进行风险对冲和风险投资的用户。可以预见的是，随着未来越来越多的基于 Truth Protocol 的 DeFi 创新协议，我们将迎来下一轮 DeFi 的繁荣！

10. 参考阅读

- https://github.com/slowmist/Blockchain-dark-forest-selfguard-handbook/blob/main/README_CN.md
- https://ethereum.org/zh/developers/docs/consensus-mechanisms/pos/