DeSec：去中心化协议在监控和执法中的潜在应用

原文标题：《DeSec? Where Crypto Meets Security, Surveillance, and Defense》

撰文：Luffistotle，Zee Prime Capital

编译：Tia，Techub News

近来，西方的安全秩序问题开始显现。通常，我们用来衡量秩序是否良好的方法是在白天以及晚上在城市和公园里散步（看是否安全）。但现在这种测量方式变得越来越不可靠。社会秩序是通过三个组成部分来构建和维持的：

法律和社会规范

执法（警察、监视等）

司法（法律的应用）



这三者之间的相互作用是复杂且深度融合的。当大家开始不敢在公园散步，或商店开始转移阵地不在原城市中营业时（通常是一个非常明显的迹象），则表明治理出现了问题。实际上，目前的一些政策确实存在一些问题。其实我们可以试着了解 crypto 改善执法的可能性，这将有助于社会结构的改善。下面我们将对此进行讨论，讨论的重点为 crypto 在监视工具的应用。

遥看历史长河，在对公共机构和协议（法律）信任度下降的时期，通常社会会动用私刑来解决他们的问题。这一权力原本是用来解决社区实际问题的，但最终却走向腐败并演变成敲诈勒索。



也许现在有了更现代的解决方案，比如更便宜的监控技术，通过这些技术，也许可以为执法机构提供「杠杆」，使其能够以规模化的方式解决问题，以确保实现社区的目标和愿望。技术可以让同样数量的人做更多的事情。而去中心化的协议可以帮助确保这种新权力不会用于其他目的。

通过监控来强化执法的想法其实很恐怖的，因为存在滥用权力的威胁。

「绝对的权力导致绝对的腐败。」

加密货币带来了金融自由的可能性——它消除了国家对货币的垄断，并对国家的金融行为进行了制衡。同样，它也可以对新的监控工具进行制衡。通过将无处不在、廉价的机器人、摄像头和传感器与可靠的中立协作网络相结合，可以制衡国家的监控垄断。

在我们称之为 DeSec 的项目类别中，我们通过与优秀人士进行有趣的对话来进行深度探索。安全领域是 crypto 的另一个机会，因为它是客户（政府、社区）愿意以保险方式支付的少数几个领域之一（国防很乐意为冗余支付费用）。冗余费用是 crypto 固有的一个特性。这一特点也是许多加密产品通常无法与其他解决方案竞争的原因，crypto 需要不断为更高级别的安全性/冗余性/验证付费。

话虽如此，冗余并不是一件坏事。它是确定性固定成本和可变未来成本之间的权衡。就比特币而言，它的价值和成功是从为实现无需信任的验证而支付的费用中获得（破坏共识需要支付高昂的费用，因此其安全性极高）。在国防制造业中，对安全的容忍率或故障率也极低，即使需要为此付出高昂代价。

### DePIN 遇见 DeSec：NeighborhoodWatchDAO

DePIN 的大部分价值来自于将资本支出的负担从公司/协议转移到节点运行者身上，以换取一定比例的收入。这为许多类型的网络提供了以其他方式无法实现的扩展的可能性。

利用这些特性，可以向市场推出一些即时应用。举个例子，Dempsey是DePIN 风格的 SoundThinking（以前称为 ShotSpotter）节点网络，它可以向 ShotSpotter 本身销售，也可以拥有自己的协议。对于那些不熟悉的人来说，ShotSpotter 是一个安装在建筑物上的麦克风网络，可以对枪击发生的位置进行三角测量，并向执法机构或急救人员发出警报，以便更快/立即部署资源。



随着节点运行者部署到各自的城市，此类协议可以扩展至全球，其速度比 SoundThinking 等公司的内部再投资周期要快得多。

同样，小型无人机入侵潜在重要空域的风险也越来越大。正如最近兰利空军基地的入侵事件向我们展示的那样。虽然美国军方可能对此类袭击有机密解决方案，但对于其他不太安全的空域，可能需要另一种解决方案。可以通过对相关空域的小型雷达或视觉观察网络进行激励，以帮助执法部门了解发射点的相关情况。

也可以利用类似的模型来观察信号强度。（虽然通常这是由无线提供商提供的，主要用来确保网络质量，但无线提供商也有缺点，其信号通常更短暂。）DePIN 可以为这些网络提供持续的信号质量监控（正如 ROAM 等一些项目已经计划做的那样）。这是一种更简单的执行解决方案。

近年来，小偷手中廉价的手机信号干扰设备数量激增。这些设备非常可怕，因为您可能会发现当有人闯入您的房屋时，您的手机、wifi 或无线电无法联系警察。



罪犯可以将其放在腰带中，然后抢劫您的房屋或偷窃您的汽车。在城市和其他地区进行信号监控其实是可以轻松检测到这类干扰事件的。与 ShotSpotter 类似，也可以向当局发出警报。

我们还可以创建类似的协议，对在问题区域进行监视（Patrol2earn）的小型无人机定期进行激励，或者我们可以利用现有的 DePIN 项目来为监视机构支持。如 Frodobots 或 DIMO 等项目会用相机捕捉关键事件。



### 通信

与监控部分类似，DePIN 网络也可用于增强网络传输（无论是电气网络还是数字网络）的稳健性。好处在于，即使发生灾难，此类网络依旧可以保持稳定。

网状边缘网络可以抵御当今高度中心化的以 CDN 为中心的互联网流量，而去中心化的发电厂可以对小规模的能源生产进行协调，让这些能源设备在主要生产中心成为攻击目标时，能够依旧提供备用电源。

这一逻辑也适用于现代战争。实际上，现代前沿部队更需要去中心化。正如我们在乌克兰看到的那样，FPV 无人机的使用是战争领域的一次重大发展。现在已经实现了小型、低成本（甚至是纸板无人机）和快速精确打击。战场上的任何关键设施（即后勤枢纽、传输/指挥掩体等）都会成为攻击目标。这会导致这些小型设施称为故障点，而应对的最佳方法是使用分布式通信。



### 在这种经济形势下，你还想使用导弹吗？

#### 验证

多方验证可以应用到机器人制造。向制造机器人输入恶意指令可能会对整个制造链造成严重风险。解决这类问题的一种方法可以是，在代码运行时对其进行多方验证。通过对要执行的代码达成共识，来捕获对制造过程的恶意更改。

与验证类似，STAEX 提供了一个公共网络，以促进物联网设备之间无需信任的通信。这为这些设备提供了一种新颖的通信方式，并降低了使用传统渠道进行干扰的风险。鉴于不法行为的风险日益增加，这是一项重要的技术，它可以构建强大的网络，来让这些设备可以传输有价值的数据。

验证的其他用途还包括 Palmer Luckey 上文所述的公民提交证据 (snitch2earn)。在当前法律框架内，隐蔽身份和诱饵车等高度复杂的操作的也许难以执行，但尽管如此，在当今时代，仍有大量记录犯罪行为的方式，可以设置一个简单的场所来部署数据，甚至可以通过加密的方式将位置/时间验证情境化（ZK!!!）。



### DeSci

DeSci 是加密技术与国防/情报行业融合的另一种方式。例如，DeSci DAO 资助了材料科学、生物制造（如 valleyDAO）、低温学（CryoDAO）或长寿（Vita）/人类性能增强（有人想和我一起做肽 DAO 吗？）等原本不受重视的领域的研究。这些 DAO 实际上可以对这些研究领域产生有意义的影响。例如，HairDAO 现在是世界上最大的非脱发研究资助者之一。

我相信，随着越来越多的科学家正在放弃传统研究途径，更多前沿研究的创新将来自这一类 DAO。

#### 协议为何重要

为什么需要协议？上面提出的许多想法显然是在增强国家统治的监视。但是，假设这些监视工具被推向市场并由协议管理。在这种情况下，去中心治理可以检查使用它们的当局是否在正当执法、那些垄断的治理者的价值观是否与他们所治理下的人们相一致？如果不一致，协议可以投票决定不再向执法机构提供增值信息（或许他们会选择支持私人警察部队或私人情报机构）。

#### 怀疑论者的评论



无论谁控制，增加监控能力都可能对社会产生负面影响。不要过度质疑去中心化治理的实际可能性，因为与比特币类似，这种协议必须依赖绝对的无需许可原则，即治理最小化。即最大限度地提高无需信任。

社会在不断发展，实施绝对法治的能力可能会削弱我们的适应能力。不服从是可以促进进步的，尽管这是一种非常特殊的不服从形式（而非街头犯罪）。如何才能消除特定类型的犯罪？如果最大限度地利用监控技术，这可能就会变成一条滑坡。

因此，在实施有助于维持既定秩序的技术时，我们必须小心保护隐私。我们人类必须有能力说出离谱的想法并反抗暴政。如果执法和反抗能力之间的不对称变得太大，我们只是在助长少数派报告式的暴政。

如果我们更深入地研究这种不对称，可以发现，美国的持枪权已经毫无意义了，在建立持枪权时，它的目标是确保潜在反抗的可能性，但一旦我们发明了导弹（更不用说核武器），这种可能性就不复存在了。当然，个人捍卫其财产的权利仍然存在，但其在政府抵抗方面是无效的。

加密技术具有独特的能力，可以将市场带入一个新的境地。未来会是 MerceneryDAO、加密资助的国防技术、社区拥有的无人机，还是自由主义的和平主义？谁也不知道。也许答案存在于更小众的部分，比如去中心化的微型核电站监测器和无人机保护网络，也许答案存在于一些甚至我们没有考虑过的地方。