可验证随机性如何确保 Web3 公平

从古代的抽签到现代社会，人类对随机性的需求始终存在。尽管早期的方法在当时已能满足基本需要，但由于缺乏公平性和防操纵性的保障，往往在关键场景下引发争议与不信任。

随机数生成的演进

随着技术的发展，随机数生成经历了从机械方式到数字化的演变。计算机随机数的出现极大提升了速度与规模，但仍面临中心化、可预测性以及潜在操纵等问题。许多生成方法依赖中心化系统，如专有算法或物理随机装置，这些方案普遍缺乏透明度，并容易受到攻击。

Web3 的出现为实现去中心化随机性提供了新的可能性。然而，即便是基于链上区块哈希的方案，也依然存在被矿工操纵的风险。这推动了开发者们将目光投向更加全面、透明且可验证的随机数生成机制，以突破既有的局限。

中心化

中心化的随机数生成系统将控制权集中在单一实体手中，极易受到偏见、腐败或操纵的影响。以彩票为例，由中心机构统一管理，参与者缺乏独立验证抽奖公平性的手段，因此往往面临信任缺失的问题。

缺乏可验证性

传统系统通常缺少让参与者独立验证随机过程公平性的机制。这种透明度的不足迫使用户依赖人为信任，而在游戏、DeFi 等高风险应用场景中，这种脆弱的信任往往难以维系。

可预测性

许多传统方法并不能产生真正不可预测的随机结果。若系统存在可预测性，恶意行为者便可能通过模式识别、逆向推理或操纵输入来加以利用，从而破坏例如彩票等场景的公平性。

操纵

链上依赖区块哈希的随机方法同样存在风险。矿工可以通过选择性地打包或舍弃交易来影响区块结果，从而操纵最终随机数生成过程，这将直接破坏去中心化体系下的信任基础。

随机性是 Web3 的核心要素，为去中心化应用注入公平性、透明性与信任。它确保依赖随机性的流程能够公正运行，不受外部干扰。

什么是 Chainlink VRF?

Chainlink VRF 是面向 Web3 的原生解决方案，用于生成安全、透明且防操纵的随机数。它将区块链中的不可预测数据与加密技术相结合，生成随机数及其加密证明，并在链上完成验证。在此过程中，无需依赖任何第三方信任，即可确保结果真正公平与透明。

通过由独立预言机组成的去中心化网络生成随机数，Chainlink VRF 消除了单点控制与操纵的风险。每个随机结果都会附带链上可验证的加密证明，从而保证其在对抗性环境下依旧具备防篡改、不可预测与可追溯的特性。

请求随机数

当智能合约需要随机数时，会向 Chainlink VRF 发出请求。该请求包含种子等必要参数，以及用户指定的、可辅助随机数生成过程的额外数据。在计算过程中，这些输入会与其他不可预测因素相结合，从而生成针对该请求的定制化输出。

生成随机数

Chainlink VRF 预言机在接收到请求后，会将提供的种子与不可预测的数据（如仅在请求发生后才能获得的区块哈希值）结合。随后，它利用预先提交的私钥生成随机数及对应的加密证明。该证明不仅能验证随机数的防篡改性，

还与输入直接关联，从而确保结果的透明与可靠。

链上验证

随机数生成后，Chainlink VRF 预言机会将其与加密证明一并传递给请求的智能合约。智能合约会在链上验证证明的有效性，以确认随机数的真实性。若证明通过验证，随机数即被采纳并应用于合约逻辑，使应用能够在链上实现可证明公平和防篡改的特性。

防篡改

加密证明从根本上保证了随机数不会受到预言机或任何外部方的操控。整个流程中的每一步都保持透明并可在链上验证，从而使用户和开发者对 Web3 应用中使用的随机数的公平性与安全性更具信心

Uptick 生态系统已集成此功能，以支持具有可靠随机性的去中心化操作。借助 Chainlink VRF，Uptick 提供可验证的结果，从而在参与者和开发者之间建立真正的信任。

Chainlink VRF 使用请求时未知的区块数据和预言机节点预先提交的私钥来生成随机数和加密证明。Uptick 的智能合约只有在验证了加密证明后才会验证并接受随机数，从而确保 VRF 流程具有防篡改功能。

这种方法使用户能够在链上独立验证 Uptick Web3 生态系统中的应用程序是否以可证明的公平性运行，不受预言机、外部实体或 Uptick 团队的操纵。

Uptick 幸运抽奖

从 Chainlink VRF 的早期采用开始，Uptick 就已采用游戏化方式来提升整个生态系统的用户参与度。可验证随机性实现了公平透明的机制，包括随机奖励和限时抽奖，从而增强了用户信任度并推动了平台活跃度。

Uptick 幸运抽奖为 Uptick 市场引入了类似彩票的功能，利用 Chainlink 的可验证随机函数 (VRF) 提供防篡改且可证明公平的结果。这让参与者对整个流程的公平性充满信心，进一步增强了市场的可信度。

工作原理

每周，用户通过购买符合条件的NFT参与抽奖，这些NFT可作为奖池的入场券。抽奖直接在市场平台上进行，奖金由平台收入分成。随着活跃度的提升，奖池规模不断扩大，奖励金额也逐渐增加。

结果

每次抽奖结束时，系统都会自动随机选出获奖者，并将奖品直接发送到他们的钱包。Uptick

幸运抽奖展示了可验证随机性在建立信任和推动参与方面的变革潜力，为整个生态系统的更广泛应用铺平了道路。

此功能显著提升了平台活跃度，并凸显了可验证随机性在实现公平、信任驱动的互动方面的潜力。流程的透明度鼓励了更广泛的参与，并增强了平台的可信度。

然而，去中心化随机性的应用范围远远超出了市场平台的抽奖，本次抽奖只是一个测试案例。这项技术开启了一系列依赖于这种级别随机性的创新应用浪潮。结合Uptick的模块化基础架构，它将成为构建真正去中心化的Web3生态系统的关键组成部分。

未来发展潜力

VRF 市场展现了其潜力，其应用领域可拓展至：

RWA 奖池

代币化的现实世界资产，例如部分房产份额或高价值收藏品，可以组成奖池。VRF 可以随机选择参与者，授予 VIP 特权、部分所有权或专属福利，前提是参与者完成质押或资产购买等任务。

社会

非营利组织可以使用 VRF 公平分配捐款或援助物资，确保资源分配公平公正。这种方法可以提高透明度，扩大受助范围，增强人们对慈善事业的信任。

代币化收藏品

将虚拟交易卡或游戏内资产集成到去中心化应用中，将释放更多可能性。借助 VRF，平台可以随机向符合资格标准的参与者分发稀有或专属物品，这些资格标准包括完成生态系统挑战、持有特定代币或参与活动。

教育补助金和奖学金

机构或去中心化平台可以利用可验证的随机性公平地分配补助金、奖学金或其他资源，并根据预先定义的资格标准为每位参与者提供平等的机会。

以上每个用例都展示了 VRF 如何为各种 Web3 活动带来公平性、不可预测性和透明度，并将其应用范围扩展到市场之外。

Chainlink VRF 为 Web3 世界提供了一个可验证的公平且防篡改的随机数模型，这对于重视完整性和透明度的应用至关重要。VRF 将链上区块数据与链下预言机计算相结合，生成随机数并进行加密证明，从而保护结果免受操纵，包括预言机运营商或开发者的操纵。

在 Uptick 生态系统中，Chainlink VRF 支持公正的流程，并保护随机数免受外部影响。其透明、可验证的方法增强了用户信任，并提供了

真实、无操纵的结果。随着 Uptick 扩展其 Web3 生态系统，可验证随机数仍将至关重要，它将提升用户体验，并为其以业务为中心的应用带来新的机遇。

hello@uptickproject.com

@Uptickproject

@Uptickproject

Uptick Network

Uptick Network