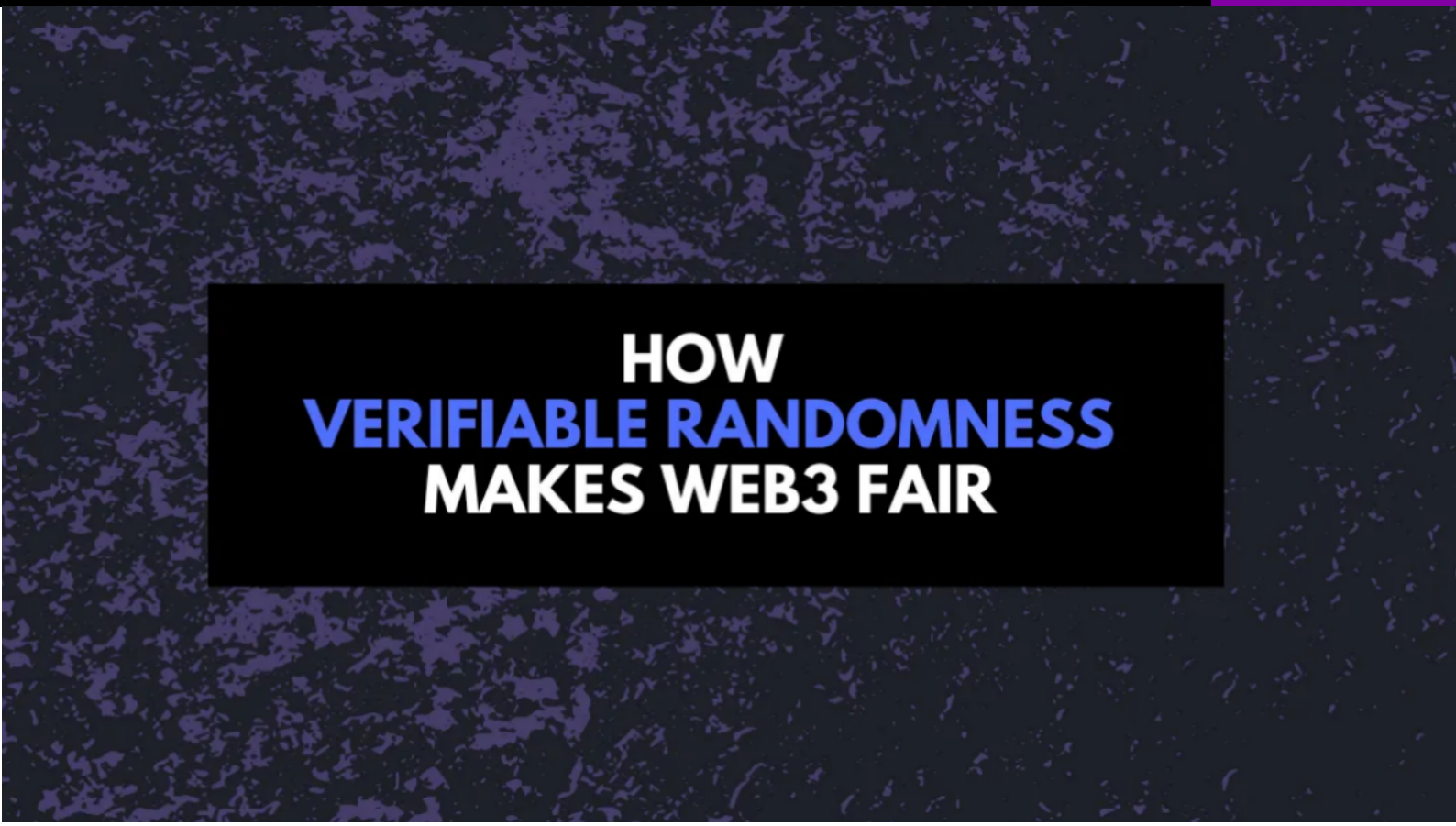


可驗證隨機性如何確保 Web3 公平

從古代的抽籤到現代社會，人類對隨機性的需求始終存在。儘管早期的方法在當時已能滿足基本需要，但由於缺乏公平性和防操縱性的保障，往往在關鍵場景下引發爭議與不信任。

隨機數產生的演進

隨著技術的發展，隨機數產生經歷了從機械方式到數位化的演變。計算機隨機數的出現極大地提升了速度與規模，但仍面臨中心化、可預測性以及潛在操縱等問題。許多生成方法依賴中心化系統，如專有演算法或實體隨機裝置，這些方案普遍缺乏透明度，並容易受到攻擊。

Web3 的出現為實現去中心化隨機性提供了新的可能性。然而，即便是基於鏈上區塊哈希的方案，仍然存在著被礦工操縱的風險。這推動了開發者將目光投向更全面、透明且可驗證的隨機數產生機制，以突破既有的限制。

中心化

中心化的隨機數產生系統將控制權集中在單一實體手中，極易受到偏見、腐敗或操縱的影響。以彩券為例，由中心機構統一管理，參與者缺乏獨立驗證抽獎公平性的手段，因此往往面臨信任缺失的問題。

缺乏可驗證性

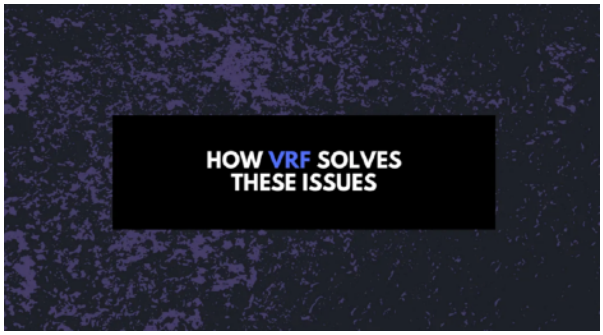
傳統系統通常缺乏讓參與者獨立驗證隨機過程公平性的機制。這種透明度的不足迫使用戶依賴人為信任，而在遊戲、DeFi 等高風險應用場景中，這種脆弱的信任往往難以維繫。

可預測性

許多傳統方法並不能產生真正不可預測的隨機結果。若係統存在可預測性，則惡意行為者便可能透過模式識別、逆向推理或操縱輸入來加以利用，從而破壞例如彩票等場景的公平性。

操縱

鏈上依賴區塊哈希的隨機方法同樣有風險。礦工可以透過選擇性地打包或捨棄交易來影響區塊結果，從而操縱最終隨機數生成過程，這將直接破壞去中心化體系下的信任基礎。

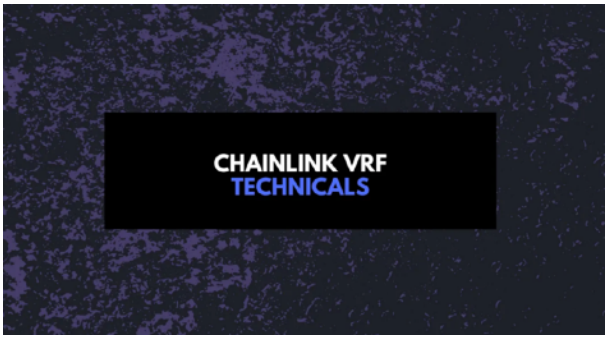


隨機性是 Web3 的核心要素，為去中心化應用注入公平性、透明與信任。它確保依賴隨機性的流程能夠公正運行，不受外部幹擾。

什麼是 Chainlink VRF?

Chainlink VRF 是面向 Web3 的原生解決方案，用於產生安全、透明且防操縱的隨機數。它將區塊鏈中的不可預測資料與加密技術結合，產生隨機數及其加密證明，並在鏈上完成驗證。在此過程中，無需依賴任何第三方信任，即可確保結果真正公平與透明。

透過由獨立預言機組成的去中心化網路產生隨機數，Chainlink VRF 消除了單點控制與操縱的風險。每個隨機結果都會附帶鏈上可驗證的加密證明，從而保證其在對抗性環境下依舊具備防篡改、不可預測與可追溯的特性。



請求隨機數

當智能合約需要隨機數時，會向 Chainlink VRF 發出請求。此請求包含種子等必要參數，以及使用者指定的、可輔助隨機數產生過程的額外資料。在計算過程中，這些輸入會與其他不可預測因子結合，從而產生針對該請求的客製化輸出。

產生隨機數

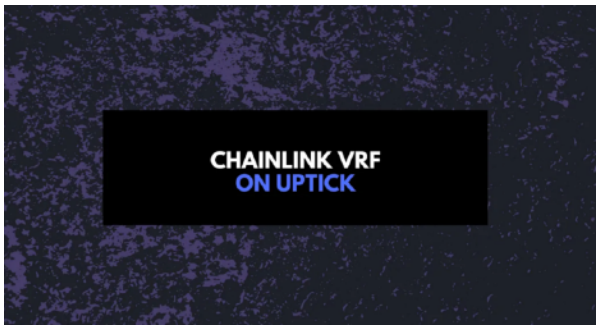
Chainlink VRF 預言機在接收到請求後，會將提供的種子與不可預測的資料（如僅在請求發生後才能獲得的區塊雜湊值）結合。隨後，它利用預先提交的私鑰產生隨機數及對應的加密證明。此證明不僅能驗證隨機數的防篡改性，還與輸入直接關聯，從而確保結果的透明與可靠。

鏈上驗證

隨機數生成後，Chainlink VRF 預言機會將其與加密證明一併傳遞給請求的智能合約。智能合約會在鏈上驗證證明的有效性，以確認隨機數的真實性。若證明通過驗證，隨機數即被採納並應用於合約邏輯，使應用能夠在鏈上實現可證明公平和防篡改的特性。

防篡改

加密證明從根本上保證了隨機數不會受到預言機或任何外部方的操控。整個流程中的每一步都保持透明並可在鏈上驗證，從而使用戶和開發者對 Web3 應用中使用的隨機數的公平性與安全性更具信心。



Uptick 生態系統已整合此功能，以支援具有可靠隨機性的去中心化操作。借助 Chainlink VRF，Uptick 提供可驗證的結果，從而在參與者和開發者之間建立真正的信任。

Chainlink VRF 使用請求時未知的區塊資料和預言機節點預先提交的私鑰來產生隨機數和加密證明。 Uptick 的智慧合約只有在驗證了加密證明後才會驗證並接受隨機數，從而確保 VRF 流程具有防篡改功能。

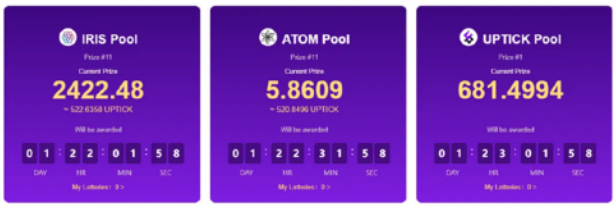
這種方法使用戶能夠在鏈上獨立驗證 Uptick Web3 生態系統中的應用程式是否以可證明的公平性運行，不受預言機、外部實體或 Uptick 團隊的操縱。

Uptick 幸運抽獎

從 Chainlink VRF 的早期採用開始，Uptick 就已經採用遊戲化方式來提升整個生態系統的使用者參與度。可驗證隨機性實現了公平透明的機制，包括隨機獎勵和限時抽獎，從而增強了用戶信任度並推動了平台活躍度。

Uptick 抽獎為 Uptick 市場引入了類似彩票的功能，利用 Chainlink 的可驗證隨機函數 (VRF) 提供防篡改且可證明公平的結果。這讓參與者對整個流程的公平性充滿信心，進一步增強了市場的可信度。

工作原理



每週，用戶透過購買符合資格的NFT參與抽獎，這些NFT可作為獎金池的入場券。抽獎直接在市場平台上進行，獎金由平台收入分成。隨著活躍度的提升，獎金池規模不斷擴大，獎勵金額也逐漸增加。

結果

每次抽獎結束時，系統都會自動隨機選出獲獎者，並將獎品直接發送到他們的錢包。 Uptick 幸運抽獎展示了可驗證隨機性在建立信任和推動參與方面的變革潛力，為整個生態系統的更廣泛應用鋪平了道路。

此功能顯著提升了平台活躍度，並凸顯了可驗證隨機性在實現公平、信任驅動的互動方面的潛力。流程的透明度鼓勵了更廣泛的參與，並增強了平台的可信度。

然而，去中心化隨機性的應用範圍遠遠超出了市場平台的抽獎，本次抽獎只是一個測試案例。這項技術開啟了一系列依賴這種等級隨機性的創新應用浪潮。結合Uptick的模組化基礎架構，它將成為建立真正去中心化的Web3生態系統的關鍵組成部分。

未來發展潛力

VRF 市場展現了其潛力，其應用領域可拓展至：

RWA 獎金池

代幣化的現實世界資產，例如部分房產份額或高價值收藏品，可以組成獎金池。 VRF 可以隨機選擇參與者，授予 VIP 特權、部分所有權或專屬福利，前提是參與者完成質押或資產購買等任務。

社會

非營利組織可以使用 VRF 公平分配捐款或援助物資，確保資源分配公平公正。這種方法可以提高透明度，擴大受助範圍，並增強人們對慈善事業的信任。

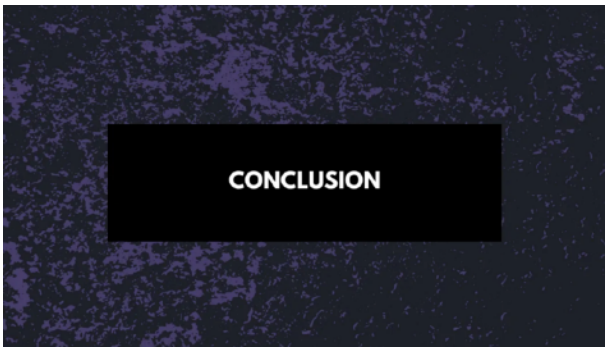
代幣化收藏品

將虛擬交易卡或遊戲內資產整合到去中心化應用程式中，將釋放更多可能性。借助 VRF，平台可以隨機向符合資格標準的參與者分發稀有或專屬物品，這些資格標準包括完成生態系統挑戰、持有特定代幣或參與活動。

教育補助金和獎學金

機構或去中心化平台可以利用可驗證的隨機性公平地分配補助金、獎學金或其他資源，並根據預先定義的資格標準為每位參與者提供平等的機會。

以上每個用例都展示了 VRF 如何為各種 Web3 活動帶來公平性、不可預測性和透明度，並將其應用範圍擴展到市場之外。



Chainlink VRF 為 Web3 世界提供了一個可驗證的公平且防篡改的隨機數模型，這對於重視完整性和透明度的應用至關重要。 VRF 將鏈上區塊資料與鏈下預言機計算相結合，產生隨機數字並進行加密證明，從而保護結果免受操縱，包括預言機運營商或開發者的操縱。

在 Uptick 生態系統中，Chainlink VRF 支援公正的流程，並保護隨機數免受外部影響。其透明、可驗證的方法增強了使用者信任，並提供了真實、無操縱的結果。隨著 Uptick 擴展其 Web3 生態系統，可驗證隨機數仍將至關重要，它將提升使用者體驗，並為其以業務為中心的應用程式帶來新的機會。

hello@uptickproject.com

@Uptickproject

@Uptickproject

Uptick Network

Uptick Network