WINkLink

——波場TRON的去中心化預言機網絡

2023 年 7 月 1 日（2.0 版）

摘要：智能合約是現代區塊鏈中最重要的組成部分之一。智能合約部署在區塊鏈上，自動觸發，且部署後無法修改，也因此成為了傳統數字契約的最佳解決方案。然而，智能合約無法與其所屬區塊鏈之外的數據進行通信。我們針對這一問題提出了一種解決方案。

該解決方案被稱為「預言機」，將智能合約與區塊鏈以外的世界連接起來。WINkLink 是一個去中心化的預言機網絡。與市面上大多數預言機不同，WINkLink 能提供比傳統預言機更安全的服務。

本文將闡述我們從 FluxAggregator 聚合器升級為鏈下報告（OCR）聚合器的過程，通過 WINkLink 節點將鏈上智能合約與鏈下真實世界數據進行連接。

目錄

引言

智能合約是在去中心化系統上部署和執行的應用程序, 一旦部署至區塊鏈就無法修改。與傳統合約相比, 智能合約更加安全, 因為所有參與方, 包括作者, 在合約中都具有平等的權力。智能合約會在特定要求得到滿足時自動執行, 所有參與方無需信任即可達成一致。

智能合約無法檢索鏈下數據, 例如通過 API 獲取信息, 造成這一局限的是區塊鏈的共識機製。為了解決該問題, 我們設計了去中心化預言機網絡 WINkLink。

WINkLink 是一個去中心化的預言機網絡, 能夠減少對合約各方之間信任的依賴。它能確保智能合約整個執行過程的安全, 該過程也包括從鏈下數據源檢索數據。要連接智能合約和現實世界並最終取代傳統數字契約, 這一前提條件必不可少。

確保輸入/輸出數據準確對於推廣智能合約應用而言至關重要。以下為智能合約對數據的要求示例:

- 債券和利率衍生品等證券智能合約需要訪問 API 以報告市場價格和市場參考數據。
- 保險智能合約需要與投保事件相關的物聯網數據, 如確認倉庫被闖入時磁性庫門是否上鎖, 或驗證公司防火墻的在線狀態。
- 貿易融資智能合約需要貨運的 GPS 數據、供應鏈 ERP 系統數據及運輸貨物相關的海關數據, 此類數據可確保合約義務得到遵守。

付款消息通常需發送至銀行系統等鏈下機構。WINkLink 可通過安全的方式將數據輸出至鏈下系統, 加強與真實世界的聯系, 保障智能合約的防篡改屬性。

WINkLink 系統概覽

WINkLink 致力於打通鏈上與鏈下世界，首發部署於波場網絡，未來計劃支持其他區塊鏈網絡。WINkLink 遵循模塊化的發展路徑，未來可輕松實現各類優化增強措施。

預言機節點

預言機網絡與區塊鏈類似，也由多個節點構成。每個節點均有各自的數據源集，且各節點的數據源集可能存在交集。預言機將從數據源處獲得的數據進行匯總，並將匯總結果發送給請求方。為確保準確性，一次請求可以選擇多個節點。由於可能存在故障節點，因此需要製定相應計劃，減少故障節點可能帶來的影響。

為保障網絡穩健運行，WINkLink 預言機節點遵循拜占庭容錯（BFT）原則，形成點對點（P2P）網絡。在 P2P 網絡中，預言機在網絡上相互交換信息，通過網絡接口（即其加密密鑰材料上的證書）進行識別，從而實現相互鑒權。在 BFT 中，$2f + 1$ 代表容忍 f 個故障/惡意節點或進程所需的最低誠實節點數或進程數。f 代表的是系統在保證其完整性的情況下可以容忍的最大故障數。

由於系統規定了誠實節點的數量必須達到 $2f + 1$，因此可以確保在共識進程中來自誠實節點的投票數將高於故障節點。這一方法能確保在拜占庭故障的情況下網絡也能達成共識，製定可靠決策。

選擇 $2f + 1$ 作為臨界點是至關重要的，因為這是實現拜占庭容錯的最低閾值。這項平衡機製協調了系統韌性與效率，允許網絡中出現一定數量的故障，同時維持共享數據或處理數據的整體可信度與一致性。

設計理念

這一設計服務於多重關鍵目標，包括：

- 確保協議能夠抵禦各類由惡意行為者或軟件漏洞造成的故障。現已落實的安全模式可在不限製故障類型的情況下限製故障預言機的數量。
- 打造簡單且易於實現的設計，能進行快速部署以滿足市場需求。將簡潔作為設計原則以減少系統缺陷，例如使用 Trongrid HTTP 和 gRPC 接口，而非托管全節點，從而簡化鏈上通訊。
- 通過預言機及鏈下計算間幾乎零成本的通訊最大幅度地降低交易費，同時在與特定實體（簡稱為「C」）通訊時考慮波場交易的影響。波場交易手續費本身較低，但設計時仍努力維持較低的整體交易費用，盡管實現這一點需要更多的鏈下計算和網絡資源。

- 盡可能降低延遲，最大程度縮短從啟動簽名協議到交易上鏈之間的時間，這對於向 DeFi 交易平臺提供實時數據非常重要。協議性能主要受限於網絡傳輸延遲，而由於傳輸的數據量較小，因此延遲可忽略不計。這樣做的目的是將報告生成時間控製在幾秒之內，包括將報告傳輸到「C」所需的時間。

開發工作主要分為兩個方面：鏈下報告計算和鏈上報告傳輸。

鏈下計算

鏈下計算可進一步分為管理報告生成的兩個組件，也就是：

1. Pacemaker（步調器）
2. Report Generator（報告生成器）

步調器

C 合約的預言機報告通過 Pacemaker 協議生成，該協議將報告生成過程分為若幹輪次，並為各個輪次指派了對應的領導節點。協議不保證共識，但依賴於 C 合約來解決輪次更替時任何模棱兩可的問題。Pacemaker 協議持續運行並定期啟動新的輪次以及對應的報告生成實例。它通過事件監測進度，當監測到進度不足時，可以中止當前實例。Pacemaker 協議不直接將報告發送給 C，而是將其轉交給傳輸協議。此外，它還響應領導節點事件變更，表明一個輪次結束，並允許開啟下一個輪次，其中可能包含新的實例和領導節點。

報告生成器

報告生成過程分為若幹輪次，每個輪次都有一個唯一標識符及一個領導節點。協議在每個輪次內輪流運行，收集監測數據，根據監測結果報告一個中值，並生成已簽名的預言機報告。滿足特定條件後，該報告就會交由傳輸協議發送給 C。通過從一組超過 $2f$ 的監測結果中選擇中值，該協議能夠保證報告值的合理性，因為拜占庭式預言機無法在誠實預言機提交的監測結果範圍外操縱這一中值。

運行輪次和監測數據收集的頻率由領導節點和一個超時值共同決定。該超時值必須小於進度超時設定且大於一個報告生成協議完整叠代所需的網絡延遲，並預留額外的安全余量。

當收集了足夠數量的監測數據，該報告連同驗證所需的預言機簽名一並通過傳輸協議發送給 C。需要註意的是，領導節點以及預言機僅在數據流值發生顯著變化或距離 C 上次報告已過去特定的時間間隔後才會參與生成報告。這一機製避免了生成不必要的報告。

鏈上傳輸

傳輸

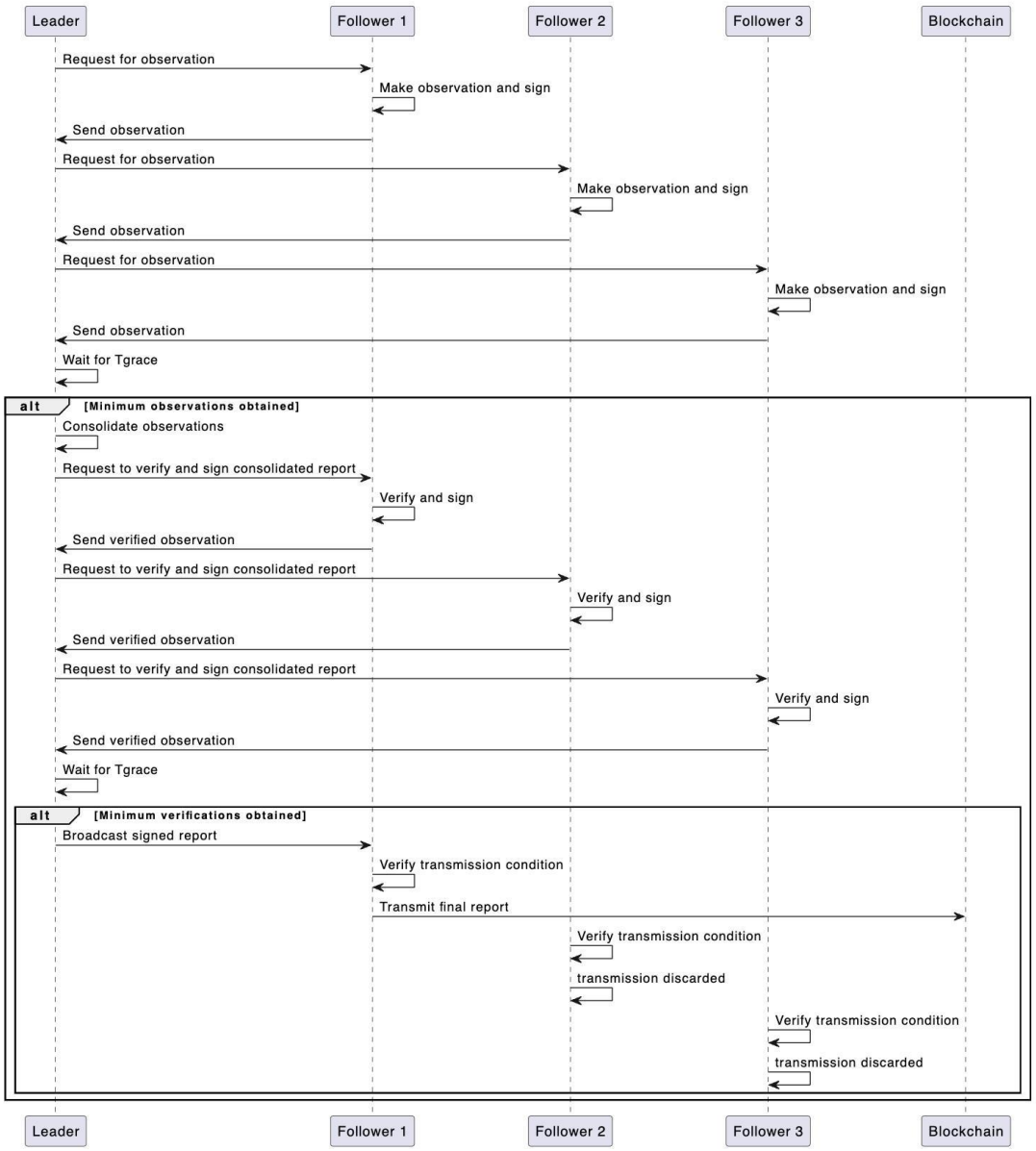
當報告 R生成後，在理想條件下，報告生成算法將同時在所有預言機啟動傳輸協議。

為了最大限度地降低手續費並避免不必要的傳輸，該算法對傳入的報告采用了過濾機製。這種機製在連續多輪生成相似報告時尤為重要。只有初始的報告需要傳輸，而隨後的報告將被忽略。

該算法會保留一份最近收到的報告（稱為 L）。要通過過濾器，報告（標記為 O ）必須滿足兩個條件之一。第一，C 已經收到了時間接近 L 的報告，表明不存在報告積壓；第二，O 的監測值中值與 L 的中值相比出現了明顯的偏差。

一旦滿足過濾條件，預言機網絡中的一個隨機節點將被選中作為發送器向區塊鏈提交報告。這種方法顯著降低了手續費成本，因為即使多個節點均已做出響應，實際也只需要一筆交易。

WINkLink OCR 流程圖



理想的安全預言機

下述實驗提供了一種兼具原則性和啟發性的方式，有助於我們論證預言機的安全性。我們假設存在一個可信任的第三方，能夠始終誠實地執行指令。這個理想狀態下的預言機（下稱「理想預言機」）從可信的數據源獲取數據，並通過以下任務確保其安全性：

- 接收請求：理想預言機收到來自智能合約 USER-SC 的請求 $Req = (Src, \tau, q)$，請求中明確了目標數據來源 Src，一個時間或時間段 τ，以及查詢請求 q。
- 獲取數據：理想預言機在指定的時間 τ 向特定數據源 Src 發送查詢請求。
- 返回數據：在收到答案 a 後，理想預言機將其返回給智能合約。
- 作為數據源和智能合約 USER-SC 之間的橋梁，理想的預言機需要提供及時精準的數據，發揮著極其重要的作用。

很多情況下，請求的數據不適合公開。為了保密，理想的預言機需要始終保證數據請求的安全性。所有請求均加密處理，解密的公鑰由理想的預言機持有。

一臺理想的預言機應該時刻在線，從不停機，也不會拒絕任何請求。

然而，我們必須承認世界上沒有完全值得信任的數據源。漏洞以及詐騙網站等各類因素讓數據無法擺脫被篡改的風險。另外，期許找到一個毫無瑕疵的第三方來運行預言機也是不現實的。

雖然理想中的預言機在現實中並不存在，但我們的目標是讓 WINkLink 在實現上無限接近完美預言機的理念。

數據聚合與安全

為避免出現故障節點, WINkLink 建議以下兩種方式:
分布式數據源與分布式預言機

數據源

我們可以從不同的數據源獲取數據, 以降低數據源異常帶來的影響。數據聚合功能可以將數個結果聚合成單一輸出。數據聚合的方式有很多種, 比如在去除異常數據後算取加權平均數。

考慮到多個數據源的數據可能存在相互重疊, 這會導致聚合的結果不準確。WINkLink 將致力於解決這些問題, 並報告數據來源的獨立性。

數據聚合標準

假設一個預言機網絡擁有七個節點, FluxAggregator 則需要進行 7 次鏈上交易才能完成餵價, 而 OCR 僅需一筆交易即可實現同樣的目標。這意味著 FluxAggregator 餵價需消耗約 350 TRX , 而 OCR 僅需消耗約 110 TRX, 手續費比前者節省了近 65%。如果節點更多, 節省的手續費也會更多, 因為交易次數比為 1:*n*, 其中 *n* 代表節點數量。

合約升級服務

一旦智能合約部署完成, 任何人都無法控製其行為, 因此預言機的安全性尤為重要。一臺提供錯誤數據的預言機會給去中心化交易所造成重大損失。

出於安全考慮, WINkLink 采用合約升級服務。這一服務將由啟動 WINkLink 節點的機構負責管理, 並采用 WINkLink 的去中心化設計理念。

智能合約受到黑客攻擊已經屢見不鮮, 說明其存在重大安全風險。這也正是我們建議使用合約升級服務的原因。

用戶可以根據自身需求決定是否啟用合約升級服務。

當發現漏洞時, 合約升級服務將部署一組新的預言機合約, 用戶可從新舊兩個版本的合約中任意選擇一個使用。為保證去中心化原則, 用戶可使用旗標選擇想要使用的合約集。

WINkLink 是一個去中心化的預言機網絡。是否使用新版本的決定權在用戶手中, 而非合約開發者。服務提供方應可支持各類社區版本的的 WINkLink-SC。

WIN 代幣的使用

WIN 是一種 TRC-20 代幣。WINkLink 節點運營商提供的服務包括獲取來自鏈下數據源的數據、將數據轉化為區塊鏈可讀格式、鏈下計算以及保證節點可靠運行。WINkLink 網絡使用 WIN 代幣向運營商支付服務費用，並將在多個方面賦能該代幣。

路線圖與未來規劃

以下是 WINkLink 預言機未來路線圖中的重點：

1. 增強預言機的安全性和可靠性
2. 提升預言機生態系統中高質量數據源的多樣性
3. 降低 WINkLink 預言機的整合難度，擴大服務範圍

驗證系統

驗證系統應監控預言機的鏈上活動，提供客觀的性能指標，幫助用戶進行選擇。監控主要集中在以下兩方面：

1. 可用性：追蹤預言機故障並及時回應用戶查詢。
2. 準確性：記錄與其他預言機節點的偏差。

WINkLink-SC 能夠監控所有預言機的活動。有關可用性和準確性的數據將在區塊鏈上公開發布。

信用體系

信用體系旨在記錄用戶對預言機服務提供商和節點的評級，主要依據的是驗證系統生成的報告。其他信息也會被納入考量，例如用戶對品牌、運營實體和預言機架構的熟悉程度。

信用體系可以提供從其他智能合約獲取的報告。此外，由於需要分析大量的數據，應考慮在鏈下計算信用指標。

現階段信用體系使用以下指標對預言機運營商進行評級。這些指標既可對特定任務類型進行評估，也可對節點支持的所有任務進行整體評估：

1. 已分配請求總數，表示過去請求的總數，包括已實現和未實現的請求。
2. 已完成請求總數，表示總共有多少請求已被實現。
3. 已接受請求總數，表示已實現請求中最終有多少被用戶接受。
4. 平均響應時間，根據未被接受的已完成請求數計算得出。
5. 已支付罰款金額，表示服務提供商支付的罰金總額。

信用體系將激勵預言機服務提供商維持更高的可用性和性能標準。我們希望這一體系能夠幫助用戶更好地選擇節點與服務。

認證服務

預言機節點容易受到Sybil攻擊的威脅，即攻擊者意圖通過操控多個看似獨立的節點來控製整個預言機池。這些節點在特定時間提供不準確的數據，從而影響高價值合約中的大額交易。

為使成本降至最低，Sybil攻擊者可能會采用一種稱為鏡像的技術，迫使預言機節點從貌似多個實則為單一的來源檢索數據。無論是否選擇傳輸虛假數據，攻擊方都能從中得利。

認證服務會根據預言機部署和行為的各個方面提供背書。它會檢測驗證系統中預言機相關的統計數據，並對鏈上應答進行事後隨機抽查，尤其是針對高價值交易。這些抽取的應答將與從信用良好的數據來源處直接獲取的應答進行比對。

除信用指標和自動化鏈上/鏈下詐騙檢測系統外，認證服務還能識別自動化鏈上系統可能無法發現的Sybil攻擊和其他惡意活動。

結語

本文介紹了去中心化預言機網絡 WINkLink, 包括其鏈上和鏈下的組成部分。本文表明了我們致力於安全和去中心化的決心, 同時指出了 WINkLink 現存的設計缺陷及今後的發展規劃。

去中心化是區塊鏈技術和 WINlkLink 的基本原則。我們將堅定不移地推動去中心化, 努力提升預言機網絡的性能和安全性。

WINkLink是在該領域先驅成就基礎上構建的項目。我們高度重視社區, 將堅持以開源的方式開發 WINkLink。同時也歡迎社區成員們建言獻策, 因為我們堅信共同協作將會推動區塊鏈和智能合約的發展。