

紫諭

SeikaLink

一個針對去區塊鏈提供資訊的諭示機

石蕙瑩、阮悅筑、曹瀚文、許博翔、陳彥凱、劉冠伶、謝秉軒

民國111年6月 (版本 1.0)

一、介紹

預言機，又稱諭示機，是一個提供區塊鏈外部世界資料的協議，在這份白皮書中，我們將會介紹紫諭 (SeikaLink)，是一個旨在提供智能合約加密貨幣選擇權價格，以及其他金融衍伸性商品價格資料的去中心化預言機，同時介紹紫諭的一些保護資料安全性的機制。

我們計畫達成以下目標：

1. 混合式智能合約：藉由結合鏈下數據以及鏈上資源，達成節能以及智能的去中心化服務。
2. 抽離複雜性：開發者在使用函式獲取資訊時，不需要知道是如何達成的。只需專注於數據資訊的應用。
3. 高可信度：透過使用次世代區塊鏈技術保護合約的重要敏感資料
4. 交易公平性：藉由確保交易的順序性使用戶不會受到例如搶先交易或是剝削侵略性挖礦影響。
5. 最小化信任機制：藉由創造一個高度信任合約以管理其他基於合約的系統，讓其他系統對此合約的資料存取權限，以及對合約的影響降至最低。
6. 激勵式安全機制：建立一個經濟模型，使用戶沒有動機行使錯誤的行為。

基於以上的目標，我們將在去中心化金融的大陸上矗立起一個全新領域的王國。並藉由社群的協助，使紫諭成為一個更加新穎的外部世界資料提供者。

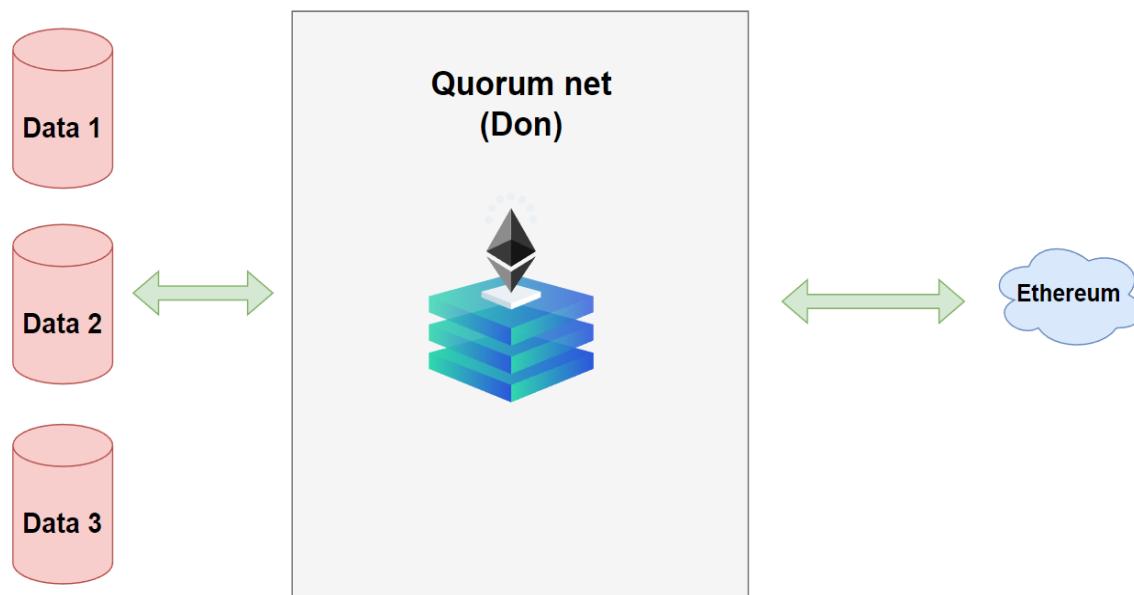
二、目錄

1. 安全性 (後端)
2. 如何有效率的放資料 (合約)
3. 合約介面 (合約)

4. 最小化信任 (後端)
5. 代幣模型 (合約)
6. 總結

三、安全性 (後端)

SeikaLink的分佈式網絡帳本，將利用預言機帶入各大交易所的加密貨幣選擇權，或是金融衍生性商品的價格，並以加權平均計算最適的價格。除此之外，我們使用Quorum net來做去中心化預言機(Decentralize Oracle Network, DON)網路的架設，以解決乙太鏈耗費成本過高以及出塊速度太慢的問題，而具體哪些資料可以被帶入並被認證，我們決定透過陪審團制度做管理以及監督。



(一) 預言機架構模型

A. 發布獨立、獨特、異構的網路節點

在預言機節點部分，我們將每一個節點採專業化設計，且其提供的服務類型方面各自都有所不同，包括：數據饋送、儲備證明、可驗證的隨機性等。此設計可以降低使用者的交易成本、提高服務品質，確保DON的穩定以及安全性。

B. 固定重新分配的機制

各自節點所提供的服務類型將每週隨機替換，以避免同服務類型節點串通攻擊SeikaLink的去中心化預言機網路，以增加網路的安全性。

C. 出塊速度

SeikaLink只有在有交易時進行出塊，再有交易時出塊速度將跟隨Quorum net出塊速度一間隔50ms，以達到環保，節能的目標。

(二) 共識機制—基於Raft

A. Raft共識機制

SeikaLink網絡的共識機制將統一採Raft共識機制，其以相同服務來為節點分組，而每一組節點會出現Follower、Candidate以及Leader三種類型的節點，其工作模式為：

- a. 客戶端的請求發送給Leader，由Leader來調度這些請求的順序，且保證Leader與Followers狀態的一致性。
- b. 將這些請求以及執行順序告知Followers。
- c. Leader和Followers以相同的順序來執行這些請求。

B. 複製狀態機

根據區塊鍊共識算法：

「相同的初始狀態 + 相同的輸入 = 相同的結束狀態」

Leader將已完成之資料狀態儲存，若出現相同情況，將以比照辦理的方法，以增加公平性、效率。

(三) 資料表決方式

A. 其他交易所資料傳入

當其他交易所資料欲傳入SeikaLink去中心化預言機網路時，系統將隨機亂數選出一位鏈上人員，作為將資料上鏈的人員。此時，其他鏈上人員將扮演投票角色，投票後由51%以上人員投票出的結果作為預言機最終的結果，再由上鏈人員進行上鏈的動作。

B. 使用者資料

使用者將隨機亂數來決定一位上鏈人員，而其他鏈上人員可以依據使用者需求，來收集並提供資料給Quorum net，投票後由51%以上人員投票出結果作為預言機的結果，再由上鏈人員進行上鏈。

(四) 陪審團制度

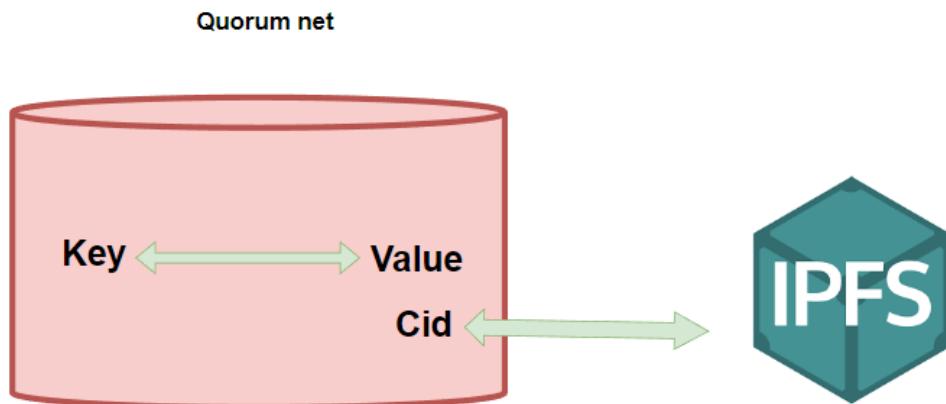
陪審團制度採用 Quorum net 的聯盟鏈特性做人員的管理，只允許本來就在名單上的節點進行貢獻。除此之外，在聯盟鏈上的人員可針對錯誤行為的節點進行投票表決剔除，以確保整體網路的穩定以及安全性。

四、如何有效率的放資料 (合約)

在使用者所請求的資料中，不乏有些是重複的，而怎麼樣儲存那些過去已經獲取的資料，就是一個可以節省資源的目標。基於前面所設立的陪審團制度，我們可以在 Quorum net 上面儲存歷史查詢資料，而在Quorum net儲存資料而不儲存在其他地方有以下幾點好處。

- (1) 比起其他公開鏈, Quorum net 可以降低大量的儲存成本
- (2) Quorum net 使用 零知識證明(Zero Knowledge Proof), 可以將一些使用者查詢的資料做加密，以增加安全性。
- (3) Quorum net 上鏈速度極快，可以支援短時間內大量寫入，降低預言機延遲

我們預計將資料分為兩類型，一種是簡單的一個鑰匙(Key) 對應一個值(Value)的資料，將這類資料儲存在 Quorum net 上的合約可以快速查詢並回覆使用者。而對於一個鑰匙會對應多個資料的狀況下，將多個資料以JSON (JavaScript Object Notation) 的資料方式儲存在星際檔案系統 (InterPlanetary File System, IPFS) 上面，並將該資料的 cid 做該鑰匙對應的值，而上鏈人員只需要將該值對應的JSON資料上鏈給使用者即可完成。



而當資料在第二層報錯[七、代幣模型 (合約)]時，如有需要修正原有的結果，則可直接將投票結果上鏈修改原始結果，由於驗證機制和資料存放是在同一個鏈上，因此可以簡單快速的溝通，同時也增加了修改的安全性。

對於每個結點在上鏈前，為了增加資料的重複利用性，並且減少對於資料來源伺服器的負擔，每個節點在本地端需要架設相應的資料進行資料儲存，在資料進行上鏈後需要保證一定時間的資料緩存，以避免後續需要再度重新驗證時資料遺失，而同時如果鏈上決議新的資料，或是有修改舊有結果時，也必須要同步的維護本地端的資料庫，讓整個鏈上鏈下的數據可以保持一致。

在資料的儲存上，對於複雜的資料採用 IPFS 做紀錄，如果使用公共的 IPFS 伺服器可能會導致攻擊發生，或是資料未被紀錄而被清除掉，為了避免類似問題發生，由每一個節點同時擔任 IPFS 上的結點，除了可以加快上鏈和查詢的資料以外，在安全性和永續性也會比較有保證。

五、合約介面 (合約)

在SeikaLink上的應用程序，是由可執行程序(executables)和適配器(adapters)組成。可執行程序即是智能合約，一個可執行程序伴隨許多的啟動器(initiators)。當某些特定事件發生時，例如在某個時間點當價格超過閾值時，啟動器會呼叫可執行程序中的啟動點。

適配器提供到鏈下資源的接口，並且能夠被可執行程序中的啟動器或核心邏輯呼叫。適配器是在 DON (Decentralized Oracle Network) 上運行的，可執行程序可以透過它發送數據，以及從非 DON 的外部系統接收數據。適配器是雙向的——即它們不只能夠存取，並且能將數據從 DON 推送到 Web 服務器；此外，透過分佈式協議以及加密功能，例如多方安全計算，適配器也參與數據的安全性保障。

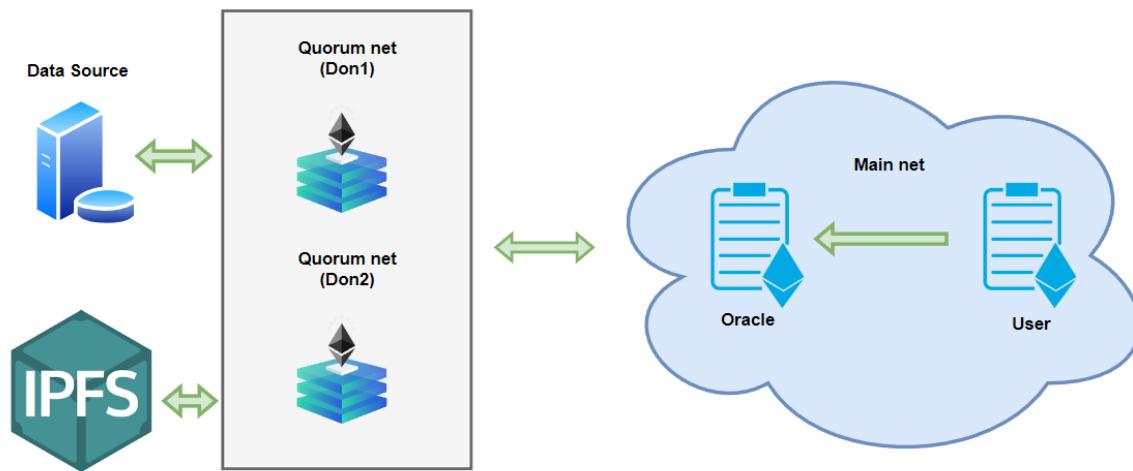


圖 1: 連接 DON1 與一系列不同資源的適配器，包括另一個 DON，記為 DON2，一個區塊鏈(主鏈)、外部存儲、Web 服務器和 User(通過 Web 服務器)。

以上說明了 SeikaLink 透過適配器與外部資源互動的示例。

在圖1中，這些互動包括：

- **區塊鏈**: 適配器可以定義如何將資料發送到其他鏈，和如何從中讀取塊、單個交易或其他狀態。
- **Web 服務器**: 適配器可以定義 API，通過這些 API 可以檢索來自 Web 服務器的數據。DON 連接的 Web 服務器也可用於推送資源，例如發送數據給使用者。
- **外部存儲**: 適配器可以定義讀取和寫入，來自DON 之外的存儲服務，例如去中心化文件系統。
- **其他 DON**: 適配器可以在 DON 之間檢索和傳輸數據。

六、最小化信任 (後端)

作為一個去中心化系統, SeikaLink 網絡在可用性和安全性方面都提供了保護, 防止出現故障。任何去中心化工作的目標都是最小化信任:我們尋求減少 SeikaLink 網絡內系統性損壞或故障的不利影響。在這裡, 我們列出了 SeikaLink 採用的幾種具體機制, 以實現更大的信任最小化。

(一) 數據來源認證

1. 數據簽名

我們在 SeikaLink 中最小化信任的願景的一個重要長期組成部分是通過支持數據簽名的工具和標準來實現更強大的數據源身份驗證。數據源的數位簽名可以幫助加強身份驗證, 也可以幫助實施端到端的完整性保證。

2. 資料保密

用戶可能希望使用預先處理過的數據以幫助確保機密性。我們將從外界獲得的數據經過處理, 將需要保密的數據進行資料保密, 再轉化為不同形式的數據輸出, 例如, 將需要保密的數字資料轉換為{True, False}形式的資料。

3. 合併數據源

為了降低鏈上成本, 合約通常設計為使用來自多個來源的組合數據。

4. 資料來源權重比

我們會依照資料來源的交易所的數據數量佔總體數據數量的比例來決定權重, 將我們從 Binance 等交易所取得的資料計算出每個交易所的權重, 並再由社群在固定時間內表決出該比例權重, 形成資料來源的權重比。

(二) 去中心化預言機網路(DON) 最小化信任

我們設想了兩種減少對 DON 組件的信任的主要方法:故障轉移客戶端和少數報告。

1. 客戶端故障轉移

客戶端故障轉移即是節點可以在面對災難性事件時切換到其他客戶端。

密碼學和分佈式系統文獻中的對抗模型通常考慮能夠破壞節點子集的對手。然而如果所有節點都運行相同的軟件, 則識別出致命漏洞的對手原則上可以同時危害所有節點。這種設置通常被稱為軟件單一文化。軟件多樣性是一個複雜的問題, 例如, 軟件多樣化可能會導致比單一文化更糟糕的安全性, 它增加了系統的攻擊面, 因此它可能的攻擊媒介超過了它提供的安全優勢。

我們認為支持強大的客戶端故障轉移是軟件多樣化的一種特別有吸引力的形式。故障轉移客戶端不會增加潛在攻擊向量的數量, 因為它們不是作為主線軟件部署的。然而作為第二道防線, 它們提供了明顯的好處。我們在 DON 中支持客戶端故障轉移, 作為減少它們對單個客戶端的安全性依賴的關鍵手段。

2. 關鍵報告(Minority Reports)

給定一個足夠大的少數集合，讓此少數集合觀察多數集合是否誠實，並且生成關鍵報告。這是一個並行報告或標誌，由少數集合轉發到鏈上的合約。合約可以根據自己的合約特定政策使用此標誌。

例如對於安全性比活躍性或響應性更重要的合約，關鍵報告可能會導致合約要求另一個 DON 提供補充報告，或觸發斷路器。即使大多數人是誠實的，關鍵報告也可以發揮重要作用，因為任何報告聚合方案，即使它使用功能簽名，也必須以閾值方式運行以確保抵禦預言機或數據故障。

通過增強 DON 協議，使所有節點都知道哪些數據可用以及哪些數據用於構建報告，節點可以檢測並標記統計上顯著的趨勢，以支持一組報告，並生成關鍵報告作為結果。

七、代幣模型(合約)

(一)代幣分配

由35%獎勵，35%公開發售，30%公司發展組成。其中獎勵為提供正確數據者得到報酬，公開發售為在各大交易所上架，供大眾自由買賣，而剩下部分作為公司營運成本。

(二)獎懲制度

提供數據前，每個節點(假設共n個)抵押d數量押金，產生總共 nd 總量 的押金，規定時間到，或是所有節點皆提供數據後，投票出正確值。

(1)正確：獲得獎勵p數量的代幣，並用信譽排名來當作權重分配總代幣。

(2)錯誤：沒收d數量的代幣。

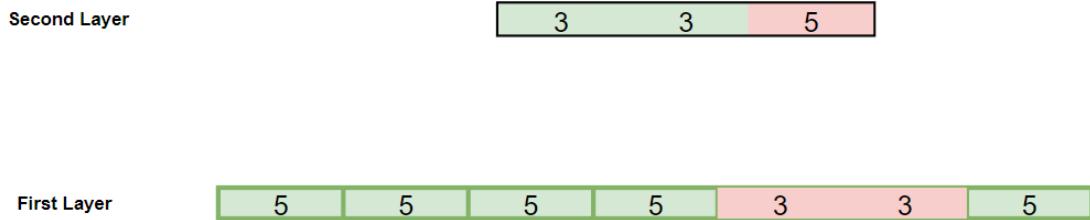
(三)第一層報錯

由上述方法初步決定正確值後，每個節點隨機分配順序，輪到該節點時可以選擇報錯或不報錯，報錯者可以獲得提供錯誤資訊的抵押金。

由於報錯成功代表超過半數的節點提供錯誤資訊，因此報錯者可以獲得的獎會大於所有押金的一半，即獎勵 $>nd/2$ ，如此一來，為了避免任何一節點報錯，惡意攻擊的成本就須高於 $(n)*(nd/2)$ ，遠高於抵押金許多。

(四)第二層

若出現報錯，進入第二層檢驗，由信譽較好的節點重新投票，再次決定正確值。



八、總結

在這份白皮書中，我們介紹了紫諭這個預言機協議的基礎架構，同時為未來的擴展提供基礎。我們根據ChainLink的預言機架構，化繁為簡，為選擇權預言機提供了理論以及實務的基礎，並透過實際建置模型以驗證可行性。在這個版本的預言機主要著重在基礎的構建，多數的項目都屬實驗階段，並沒有詳細的測試以及實際裝入預言機。

未來將以分階段的方法依序實現白皮書中的許多機制，短期內將嘗試建置Quorum net，建立去中心化預言機網路，中期目標以實現代幣模型機制為主。長期目標將著重於擴展資料源，以及提供更加多樣化，即時性的資料。

同樣，我們也希望隨著乙太網的發展，我們可以發展更加新穎，快速與穩定的協議，為去中心化的世界提供發展的基礎。

A、連結

由於技術能力的缺乏，目前後端是透過中心化的機器解決的，而智能合約則已經完成了中心化後端：https://github.com/treeleaves30760/Option_Oracle_Service
 智能合約V1：https://github.com/treeleaves30760/Option_Oracle_Contract