國立政治大學資訊科學系研究所

碩士學位論文

去中心化數位貨幣交易記錄與查詢服務：設計與以太坊實作

A Decentralized Digital Currency Tracing Service: Design and Implementation on Ethereum

指導教授：郭桐惟 教授

研究生：朱奕寧 撰

中 華 民 國 一〇九年 十一月

# 摘 要

在這個數位崛起的時代，區塊鏈是這個時代所造就的新興科技。隨著區塊鏈的發展日漸成熟，該技術也逐漸在金融、物流、穩定幣等各個層面衍生出多樣化的應用與服務。它透過密碼學與分散式系統技術，使區塊鏈中的所有節點彼此交換訊息並共同維護鏈上資料(如交易帳本)。隨著時間的推進，區塊鏈中的資料與交易量不斷成長，因此，如何於龐大的區塊鏈中取得數位貨幣交易紀錄，已成為實務應用上必須面對的問題。為此，本論文設計一去中心化數位貨幣記錄與查詢服務。此服務實作於私有鏈之智能合約中，利用跨鏈技術存取於公有鏈上之交易資料，並於智能合約中使用Binary Search演算法，提升「區塊範圍查詢」、「時間範圍查詢」功能之效率。

關鍵字：區塊鏈、智能合約、跨鏈技術

# ABSTRACT

In this era of digital rise, blockchain is an emerging technology created in this era. As blockchain technology matures, it has gradually derived diversified applications and services at various levels such as finance, logistics, and stable coins. It uses cryptography and decentralized system technology to enable all nodes in the blockchain to exchange messages with each other and jointly maintain chain data (such as transaction ledgers). As time progresses, the data and total amount of transactions in the blockchain for sustained growth. Therefore, how to obtain digital currency transaction history in blockchain has become a problem that must be faced in practical applications. For this reason, this paper designs a decentralized digital currency tracing service. This service is implemented in the private blockchain smart contract, uses cross-chain technology to access transaction data on the public blockchain, and uses the binary search algorithm in the smart contract to improve effectiveness of "block range query" and "time range query".

Keywords: blockchain, smart contract, cross-chain technology

# 目 次

[摘 要 i](#_Toc55907581)

[ABSTRACT ii](#_Toc55907582)

[目 次 iii](#_Toc55907583)

[圖 次 iv](#_Toc55907584)

[第一章 緒論 1](#_Toc55907585)

[第二章 技術背景 3](#_Toc55907586)

[**2.1 區塊鏈** 3](#_Toc55907587)

[**2.2 以太坊區塊鏈** 5](#_Toc55907588)

[**2.3 跨鏈技術** 6](#_Toc55907589)

[**2.4 Oraclize（Provable）服務** 7](#_Toc55907590)

[第三章 相關研究 8](#_Toc55907591)

[**3.1** **BigChainDB** 8](#_Toc55907592)

[**3.2** **BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability** [13] 9](#_Toc55907593)

[**3.3** **Ethereum Query Language** 10](#_Toc55907594)

[**3.4** **Etherscan API** 11](#_Toc55907595)

[第四章 系統設計實作 12](#_Toc55907596)

[**4.1** **實作系統架構** 12](#_Toc55907597)

[**4.2** **Oraclize與Ethereum-Bridge介紹** 13](#_Toc55907598)

[**4.3** **資料處理方式** 15](#_Toc55907599)

[**4.5** **系統介面與操作流程** 17](#_Toc55907600)

[第五章 討論與結論 28](#_Toc55907601)

[**5.1** **討論** 28](#_Toc55907602)

[**5.2** **結論** 29](#_Toc55907603)

[參考文獻 30](#_Toc55907604)

# 圖 次

圖 2. 1：Oraclize(Provable)服務示意圖 7

[圖 3. 1：BigchainDB系統架構圖 9](#_Toc55303340)

[圖 3. 2：BlockIPFS之系統流程圖 10](#_Toc55303341)

[圖 3. 3：EQL語法範例 11](#_Toc55303342)

[圖 4. 1：實作系統架構圖 13](#_Toc55745734)

[圖 4. 2：服務介面之網頁架構圖 17](#_Toc55745735)

[圖 4. 3：數位貨幣交易記錄與查詢服務之首頁畫面 18](#_Toc55745736)

[圖 4. 4：註冊主頁 18](#_Toc55745737)

[圖 4. 5：代幣註冊之畫面 19](#_Toc55745738)

[圖 4. 6：完成註冊服務之畫面 20](#_Toc55745739)

[圖 4. 7：查詢頁面確認註冊完成之畫面 21](#_Toc55745740)

[圖 4. 8：修改代幣資訊之畫面 22](#_Toc55745741)

[圖 4. 9：顯示已同步之所有交易紀錄之畫面 23](#_Toc55745742)

[圖 4. 10：詳細交易內容之畫面 24](#_Toc55745743)

[圖 4. 11：訂定區塊範圍篩選之畫面 24](#_Toc55745744)

[圖 4. 12：區塊範圍篩選結果之畫面 25](#_Toc55745745)

[圖 4. 13：訂定日期範圍篩選之畫面 25](#_Toc55745746)

[圖 4. 14：日期範圍篩選結果之畫面 26](#_Toc55745747)

[圖 4. 15：特定位址篩選之畫面 26](#_Toc55745748)

[圖 4. 16：特定位址篩選結果之畫面 26](#_Toc55745749)

[圖 4. 17：比較Binary Search搜索效能 27](#_Toc55745750)



# 第一章 緒論

隨著網際網路的普及，已有各式各樣的數位化商品與服務陸續出現，隨之改變大眾的生活習慣。然而，因近年來區塊鏈技術日漸成熟，貨幣的數位化才得以被實現。除了數位貨幣之外，也衍生出金融性商品、物流追蹤、產品保固卡等各個層面的應用與服務。重要的是，區塊鏈具備下列三大特性：（一）交易紀錄不得竄改、（二）可追溯性、（三）去中心化，下列分別介紹此三項特性。

（一）交易紀錄不得竄改：採用密碼學原理將交易紀錄儲存於區塊鏈中，並透過時間順序排序，一旦數據寫入至區塊鏈中，任何人都無法輕易擅自更改數據內容。

（二）可追溯性：區塊鏈系統為塊鏈式結構，鏈上數據依時間順序環環相扣，造就了區塊鏈之可追溯性。

（三）去中心化：因這個特性讓區塊鏈被稱之為「分散式帳本」，由系統中所有節點共同維護與更新同一本帳本，且沒有中央伺服器來管理秩序。

區塊鏈便是能同時滿足交易紀錄不得竄改、可追溯性且去中心化的安全系統。隨著區塊鏈技術的演進，現今也發展出了智能合約 [1]，其合約內容與代碼皆由程式所編寫而成，是區塊鏈中一種制定合約時所使用的特殊協議，主要用於提供驗證及執行智能合約內所訂定的條件。目前大多應用於發行數位資產（如ERC-20 Token [2]）、儲存資料或是開發金融類型協議（如DeFi [3]）。智能合約也具有高交易效率，合約的流程幾乎為自動化，使得交易效率提高；也能透過客製化合約，依照用戶的需求進行修改。

因應不同使用者需求及應用場景的不同，區塊鏈主要可分為公有鏈和私有鏈。公有鏈為任何人都能參與的區塊鏈，不需要通過授權，即可自由加入或退出，如比特幣 [4]或以太幣 [5]等；私有鏈則是需要受到授權才能參與的區塊鏈，並非任何人都能加入，像是Facebook Libra [6]、R3 Corda [7]等。因參與私有鏈的節點有權限限制和可控制的區塊鏈系統設置，因此，私有鏈往往可以有較快的交易處理速度、每個區塊可容納更多的交易量且能夠節省需花費的交易手續費。本論文將聚焦於私有鏈上。

隨著時間的演進，區塊鏈中的資料與交易總量不斷成長，因此，如何於龐大的區塊鏈中取得數位資產的交易紀錄，已成為實務應用上必須面對的問題。如今也有少數的現有技術與參考文獻來解決此問題，像是BigchainDB [8]、EQL [9]、Etherscan [10]。然而，BigchainDB主要是針對分散式資料庫與區塊鏈的結合，但無提供智能合約的內部交易資訊的查詢（例如ERC-20 Token代幣之交易數量）；另一方面，EQL提供使用者可透過類似SQL [11]的查詢語言檢索區塊鏈中的數據，但實際上，EQL與BigchainDB皆無法達成這項檢索；雖然Etherscan為現今最為成熟的Ethereum Block Explorer，其檢索區塊鏈中的數據功能齊全，也提供智能合約的內部交易資訊，但沒有提供區塊範圍查詢、時間範圍查詢的功能。本論文欲設計一去中心化數位貨幣交易記錄與查詢服務。更明確地說我們希望在不遺漏任何交易紀錄、無誤的交易內容且交易來源可信任的情況下，設計一查詢數位貨幣之歷史交易服務。重要的是，該服務提供了區塊範圍查詢與時間範圍查詢功能。以下是本篇論文的研究目標：

* 設計一去中心化數位貨幣交易紀錄與查詢服務，並保證不遺漏任何交易紀錄、無誤的交易內容且交易來源可信任
* 將該服務實作於以太坊私有鏈上，並以智能合約開發其服務
* 結合Oraclize（Provable） [12]服務於智能合約中，作為公有鏈與私有鏈間之資料存取之跨鏈技術
* 實作Binary Search於智能合約中，提升使用者查詢速度

# 第二章 技術背景

本研究以探討去中心化數位貨幣交易紀錄與查詢服務為目標，將以太坊區塊鏈作為開發平台，並以智能合約結合Oraclize（Provable）服務實作於區塊鏈跨鏈互操作性應用，將存在於公有鏈上之數位貨幣歷史交易儲存至私有鏈中，使用者可針對儲存於私有鏈中之歷史交易進行查詢。本章共分三小節，首先簡介區塊鏈之相關技術背景，接著針對以太坊區塊鏈平台及其智能合約簡述其相關特性，最後則是介紹Oraclize（Provable）服務是如何可信地與區塊鏈外部溝通。

**2.1 區塊鏈**

「區塊鏈」源自於中本聰（Satoshi Nakamoto）的比特幣，透過複雜的密碼學加密資料，再利用數學分散式演算法，成為「去中心化的系統」，也是作為比特幣的底層技術，或稱為「去中心化的分散式資料庫」。區塊鏈將舊有的資料庫重新改造，把資料分成不同的區塊，每個區塊透過特定的協議鏈結到上一區塊，將區塊互相接連呈現一完整的歷史數據。區塊鏈上的每筆交易，都能由區塊鏈的結構設計達到溯源的功能，並能針對每筆交易進行驗證。在區塊鏈的每一個區塊當中，皆會擁有一時間戳進行紀錄，以表示該區塊是由當時的時間所生成的，造就了不可篡改、不可偽造的系統。區塊鏈中所有參與的節點在沒有中心的情況下，節點們透過去中心化的共識機制、遵循著規則驗證訊息內容，並寫入時間戳後生成區塊，再將其廣播至所有節點。透過分散式的方式達成數據儲存、交易驗證、訊息傳遞即為區塊鏈的核心技術。

自從比特幣的出現後，區塊鏈的技術逐漸受到重視，公開透明、公平競爭。隨後世界便開始探索區塊鏈技術在各行各業中發展的可能性，因此，除了常見的公有鏈以外，隨著應用場景的不同，更衍伸出適合企業、產業界使用的私有鏈與聯盟鏈。依照使用者對區塊鏈的權限程度不同，種類可略劃分為三種類型：

（一）公有鏈：任何人都可以訪問，發送、接收、驗證交易，並參與共識過程的區塊鏈。我們最熟悉的區塊鏈，大多屬於公有鏈，像是比特幣、以太幣等。

（二）私有鏈：區塊鏈的權限被一定程度地進行了限制，須受到授權才能成為節點，並非任何人都能參與。例如摩根大通（JP Morgan）引領的Quorum [13]就是私有鏈的代表之一。

（三）聯盟鏈：聯盟鏈與私有鏈相似，區塊鏈的開放程度與權限也是有所限制的，而授權的節點通常為企業與企業間有合約的關係等。舉例來說，Hyperledger Fabric [14]，以及R3 Corda皆是聯盟鏈的一種。

此外，區塊鏈上的交易是在於打包交易並出塊，通過驗證與確認交易是否有效，使交易順利完成，並讓區塊鏈中的所有節點進行更新、以及擁有相同的帳本內容，這樣打包交易並出塊的機制就是「挖礦」。在以太坊區塊鏈中，Ether（ETH）是其中的燃料，在區塊鏈上進行交易時，必須經由礦工運算打包後上鏈，使用者必須支付礦工該交易的手續費，其交易手續費是以Gas計算，並以Ether支付。於以太坊主網當中，每個區塊都有800M的大小限制（Block Gas Limit），而一般標準交易的Gas Limit約為21,000，一個區塊約可以容納380筆交易。交易的Gas Limit會依據交易的內容而有所不同，每筆交易的發起方都須設置交易的Gas Limit和Gas Price，不同的操作會產生不同的Gas成本，若是交易需花費的Gas Limit太高或是超出區塊鏈所設定的大小限制，則可能發生交易無法打包至區塊中，而滯留在交易池（Transaction Pool）的狀況。

整體而言，區塊鏈的應用技術不斷創新，仍有必要持續探索區塊鏈此一新興科技的潛能，在實務應用上，則必須解決區塊鏈的交易擁塞的情形、須支付的Gas Fee過高，以及區塊的Gas Limit的限制。有鑑於此，為了實現數位貨幣溯源的服務，本研究將實驗環境建立於私有鏈當中，為解決沒有足夠的Ether予以支付交易手續費的狀況、打包交易並出塊的速度、以及自定義足夠大的區塊Gas Limit，且利用智能合約的多元功能，進行數位貨幣溯源的探討與實驗，並針對以太坊區塊鏈的私有鏈平台與Oraclize（Provable）的服務應用結合，儲存以太坊公有鏈上之數位貨幣之相關交易進行溯源，透過跨鏈互操作性的方式傳遞歷史交易，並開發實驗系統進行探討與實作，利於後續搜索區塊鏈之實務應用發展的需求之參考。以下將針對以太坊區塊鏈與Oraclize（Provable）服務分別簡述其相關特性。

**2.2 以太坊區塊鏈**

以太坊區塊鏈在比特幣區塊鏈的基礎上，衍伸了一個具開源性與開發性高的區塊鏈平台，且支援開發多元化區塊鏈分散式應用程式，稱之為智能合約（Smart Contracts），並透過其原生貨幣以太幣（Ether）執行去中心化的運行。以太坊區塊鏈也具有圖靈完備（Turing Complete）的特性，使用者能透過JavaScript和Python等現有語言在以太坊虛擬機（Ethereum Virtual Machine，EVM）上開發分散式應用程式，或稱為Dapps，並共同維護以太坊區塊鏈之完整性。

智能合約是區塊鏈中的一種特殊協議，其合約內容與代碼皆由程式所編寫而成，可用於發行客製化代幣、紀錄資料或是金融交易等功能。智能合約具有高安全性、高交易效率與可客製化等，我們也能透過智能合約儲存資料，且本身也能傳遞資料訊息到外界。智能合約就像是個可以被信任的第三方角色，能在沒有中介的情況下，進行交易。智能合約使得區塊鏈在未來能有更多的可能性。

ERC-20（Ethereum Request for Comment）是一個基於以太坊智能合約的一種Token標準協議（EIP，Ethereum Improvement Proposal），所有的ERC-20代幣都能於以太坊中進行交易、追蹤或是監測等。以太坊中的代幣交易皆須透過發起交易（Transaction）才能完成動作，而這些交易都會被記錄在區塊鏈上，使交易都具有可追溯性。

**2.3 跨鏈技術**

跨鏈技術重要的目標是在於保證資料的正確性。即傳遞一筆來自於區塊鏈A的資料，跨鏈技術校判斷該資料是否來自於區塊鏈A。為了驗證該筆資料，不同的跨鏈技術有不同的驗證方法。依據跨鏈技術對於第三方的依賴程度將該技術概分成兩種：（一）見證人模式（Notary）、（二）中繼模式（Relay），下列分別介紹此兩種跨鏈技術。

（一）見證人模式（Notary）：在見證人模式中，見證人會同時參與多個區塊鏈，且充當區塊鏈間都能共同信任的第三方公證人，作為中介不僅能進行數據收集，還能進行交易確認與資料驗證。在此機制中，它可以通過「單簽名」或「多簽名」的見證人機制來實現。舉例來說，當見證人需要傳遞區塊鏈A的資料至區塊鏈B時，見證人會負責將該資料寫入區塊鏈B中，即區塊鏈B的節點或是智能合約經過查驗得知該資料是由見證人簽章後所存入，便可相信資料確實來自於區塊鏈A。

（二）中繼模式（Relay）：在中繼模式中，中繼者僅提供資料，以及驗證該資料所需的證據。亦即，中繼模式不依賴可信的第三方進行資料驗證，而是在取得發送的資料後自行驗證。例如：若區塊鏈是透過工作量證明（Proof-of-Work）達成共識(如比特幣)，中繼者則需傳遞所有的區塊標頭（Block Header）合該交易的梅克爾證明（Merkle Tree），並由區塊鏈節點或是智能合約進行驗證資料。

本論文主要實作於見證人模式（Notary），並結合Oraclize（Provable）服務於智能合約中，作為公有鏈與私有鏈間之資料存取之跨鏈技術。

**2.4 Oraclize（Provable）服務**

Oraclize（Provable）作為區塊鏈外部世界之資料提供者，能夠在區塊鏈上提供可信任的數據傳送服務，其目的是在區塊鏈建立一條可與外部溝通的橋樑，為了解決智能合約取得數據的限制，在保證可信的情況下，使得智能合約具有取得外部數據的能力。此服務也不僅局限於以太坊，目前也可以使用在其他區塊鏈平台上，例如Bitcoin、EOS、Rootstock、Fabric。

Oraclize（Provable）在以太坊上部署了名為usingOraclize的智能合約，只需要在自己的智能合約當中引用，並依據Web API的使用方法進行調用即可。Oraclize(Provable)主要是透過監聽特定Event來接收合約所發出的Query請求，處理完成後，再由Oraclize（Provable）主動呼叫合約的callback function將資料回傳。此外，Oraclize（Provable）也提供了五種資料來源，使智能合約取得外部資料，包括URL資料來源、WolframAlpha資料來源、IPFS資料來源、Random資料來源、以及Computation資料來源。

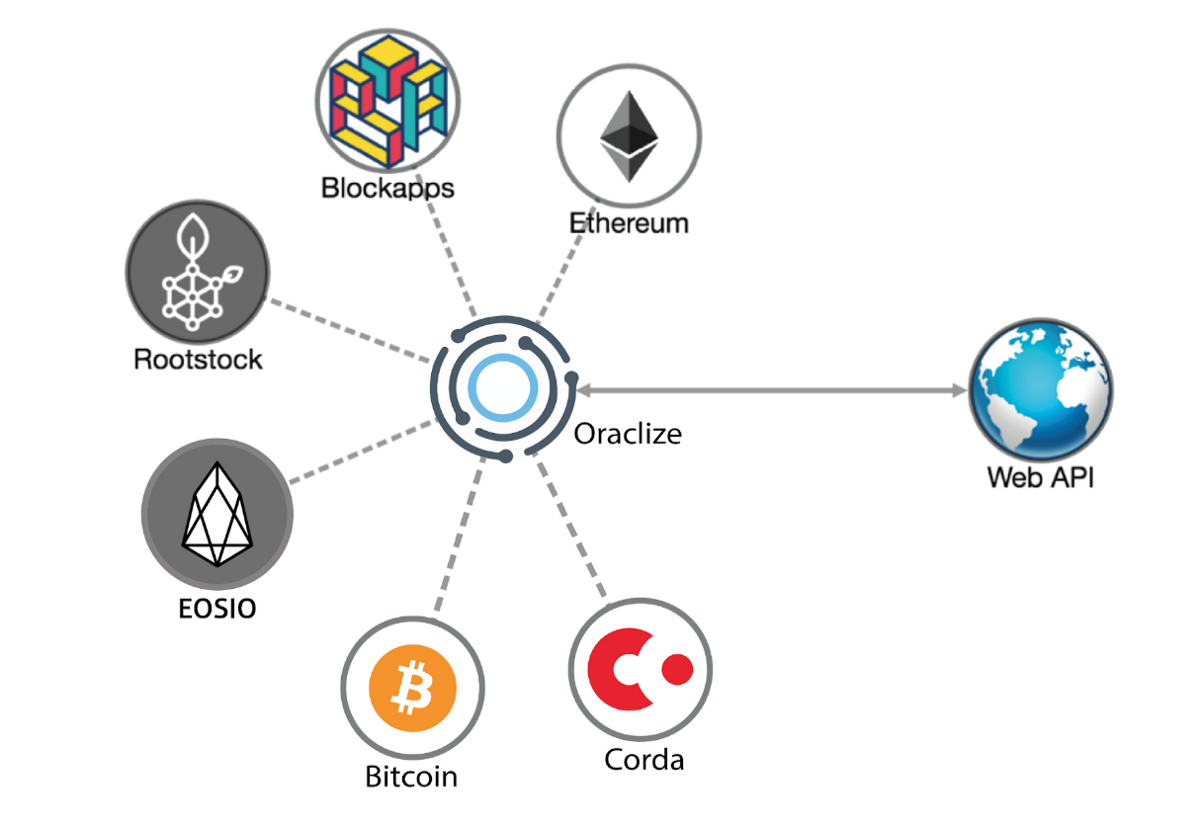


圖 2. 1：Oraclize（Provable）服務示意圖

# 第三章 相關研究

本論文欲設計一建構於區塊鏈智能合約之數位貨幣交易記錄與查詢服務，以參考現有相關技術，並針對該服務之需求進行研究。本論文將以此作為出發點，進行該題目之探討與延伸，並開發該服務系統作為依據。本章共分為四小節，第一小節為BigChainDB，該論文則是針對分散式資料庫與區塊鏈的結合，以達成兩者之特性；第二小節為BlockIPFS，該論文針對分佈式文件系統與區塊鏈整合，並未利用利用區塊鏈作為儲存資料之工具；第三小節為EQL，該論文針對區塊鏈查詢的功能，實作出一查詢語言 EQL(Ethereum Query Language)，此工具可針對區塊(Blocks)與交易(Transactions)進行查詢，但尚未完成智能合約內部數據的查詢；第四小節為Etherscan，是一個Ethereum Block Explorer，可以查看區塊鏈上所有發生的交易及其交易狀態等。

**3.1 BigChainDB**

BigChainDB是一個可用的去中心的資料庫。它的設計起源於分散式資料庫，加入了很多區塊鏈的特性，像是去中心控制、不可改變性、數字資產的建立和移動。BigChainDB繼承了現代分散式資料庫的特性：吞吐量和容量都是與節點數量線性相關、功能齊全的NoSQL查詢語言，以及高效的查詢和許可權管理。因建構在已有的分散式資料庫上，它在程式碼層面也繼承了企業級的健狀性。下圖為BigChainDB之系統架構圖，根據現版本之設計，每個節點都有一 mongoDB資料庫用於儲存鏈上資料之用，以此使用者皆能透過常規之SQL語言進行鏈上資訊（Block、Transaction等）之搜索，即不包含智能合約內部數據查詢。



圖 3. 1：BigchainDB系統架構圖

**3.2 BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability** [15]

在此論文中，探討了將區塊鏈與分佈式文件系統（IPFS，Interplanetary File System）整合，該系統利用區塊鏈（該論文實作於須身份驗證之區塊鏈–Hyperladger Fabric）既有的安全性和可追溯性，其溯源性可用於審核和保護文件的作者身份，並可作為調查的證據和爭議解決。開創一個更安全的文件共享平台，該平台具有清晰的審核記錄，以提高數據的可信度以及作者身份保護，方法提供了一條明確的途徑來追溯與給定文件相關的所有活動（如添加文件、訪問文件等）。下圖為論文中BlockIPFS之架構，用於說明文件上傳之步驟，其文件本身由IPFS加密和管理，而解密文件的密鑰存儲在區塊鏈上的特定通道中。

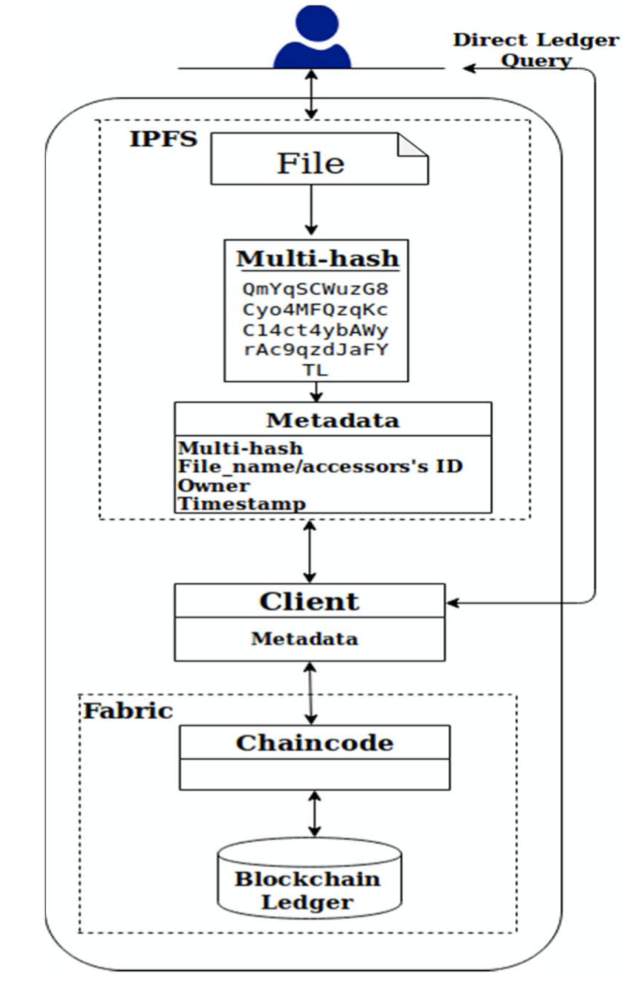


圖 3. 2：BlockIPFS之系統流程圖

**3.3 Ethereum Query Language**

此論文提出了以太坊查詢語言（EQL，Ethereum Query Language），一種允許用戶通過編寫類似SQL的查詢從區塊鏈中檢索信息的查詢語言。查詢提供了豐富的語法，可以指定數據元素來搜索分散在多個記錄中的信息。EQL使從區塊鏈中搜索、獲取、格式化和呈現信息變得更加容易。雖然提供了使用者易於查詢區塊資訊的方法，但還缺乏取得智能合約內部資訊的功能。下圖是EQL對Block查詢的語法範例。



圖 3. 3：EQL語法範例

**3.4 Etherscan API**

Etherscan，是一個Ethereum Block Explorer，可以查看區塊鏈上所有發生的交易、交易狀態或是查詢ETH錢包餘額等功能。其中，Etherscan也能瀏覽相關ERC20、ERC721合約之代幣價格、相關交易以及代幣持有者等。該網站也提供了統計圖表和數據，進而分析供應量的增長、代幣價格的漲幅或是交易頻率等服務。

# 第四章 系統設計實作

本研究依前章所述之相關研究作為延伸，於以太坊區塊鏈平台之智能合約實作數位貨幣溯源與搜索服務，實踐合約導向程式語言Solidity [16]建構資料儲存、資料搜索與資料追溯的機制，使用者能直接對於該智能合約進行搜索。透過智能合約結合跨鏈技術作為提供區塊鏈交易溯源與搜索之功能，利於後續搜索區塊鏈之實務應用發展的需求之參考。

本章共分為五小節，第一小節闡述數位貨幣溯源服務之系統架構；第二小節介紹Oraclize（Provable）服務與Ethereum-Bridge；第三小節說明擷取之交易資料處理方式；第四小節描述Query之功能；第五小節展示系統介面與操作流程。

**4.1 實作系統架構**

本實驗架構主要由以太坊公有鏈（Mainnet）與私有鏈（Private）、多位使用者、一個Time Oracle、以及建立服務於私有鏈之智能合約並結合Oraclize（Provable）服務、以及提供使用者Web UI操作本服務，圖4.1為實作系統架構圖。

為實現數位貨幣溯源之服務於以太坊區塊鏈，使用go-ethereum （geth） [17]工具建立數個節點（enode），其中一個節點架設NodeJS [18]伺服器負責區塊鏈與使用者之溝通。利用以太坊智能合約設計其系統，其智能合約再透過Oraclize（Provable）服務以利用Etherscan提供之API取得相關歷史交易資訊，並將其資訊儲存至合約當中，以利使用者之後續查詢。

Time Oracle為獨立於以太坊區塊鏈外的NodeJS伺服器，每隔一段時間，負責觸發合約中之Oraclize（Provable）服務，以調用API獲取公有鏈（Mainnet）上之交易記錄，以確保數位貨幣追溯交易之功能不會中斷。

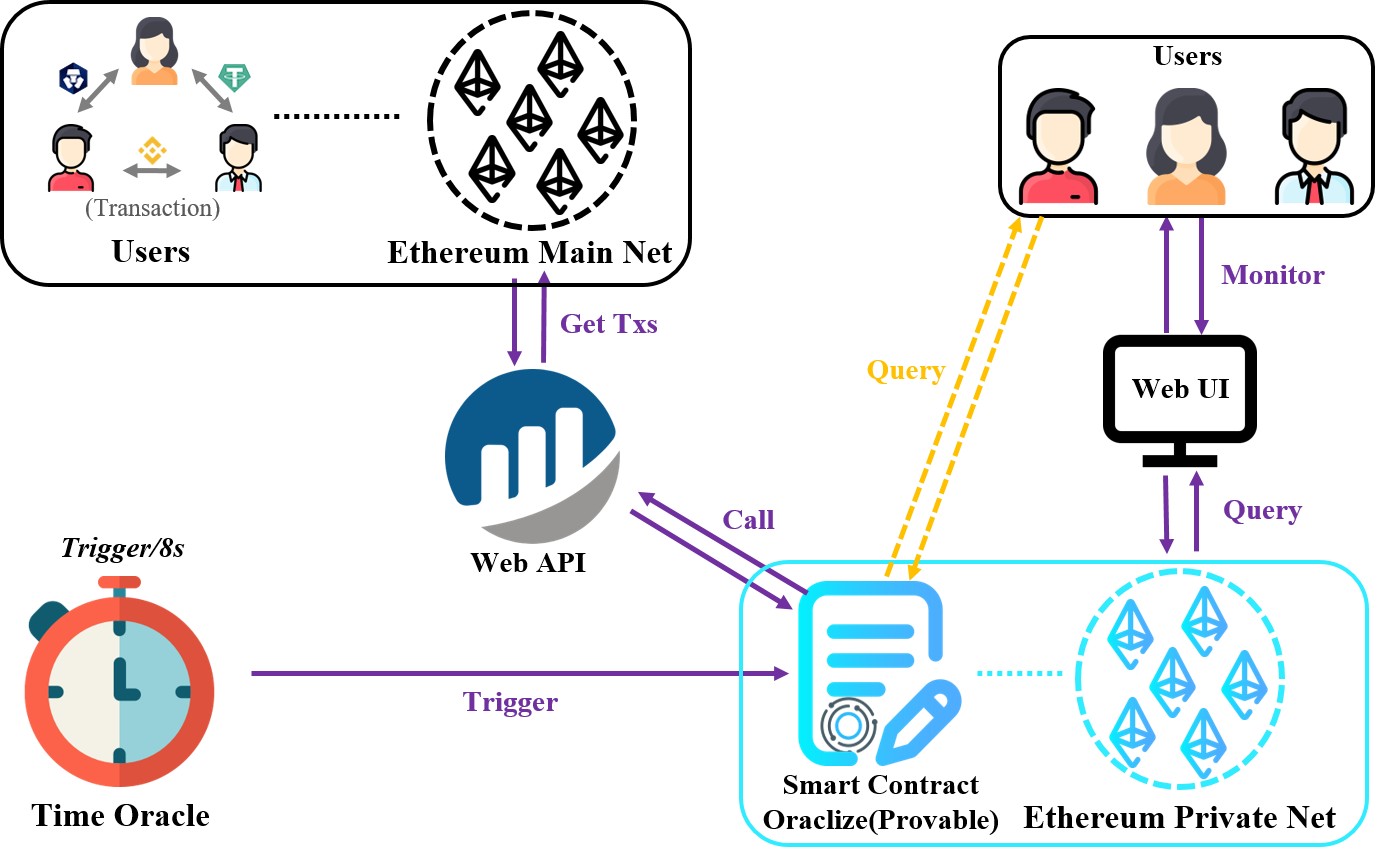


圖 4. 1：實作系統架構圖

**4.2 Oraclize與Ethereum-Bridge介紹**

**4.2.1 Oraclize**

Oraclize（Provable）是一個兼容以太坊智能合約的數據傳送服務，能夠自定義智能合約，在區塊鏈與真實世界之間建立一可信的通道，在保證可信的情況下，使其可透過API取得以太坊外部真實世界的資訊。

1. contract tokenTracer is usingProvable, Parser {
2. // oraclize results
3. **function** \_\_callback(bytes32 myid, string memory \_result) **public** {
4. **if** (msg.sender != provable\_cbAddress()) revert();
5. // 更新合約餘額
6. tracerBalance = address(**this**).balance;
8. oraclizeIsRunning = **false**;
9. // 檢查是否有回傳值
10. **if** (bytes(\_result).length != 0) {
11. savingTx(\_result);
12. }
13. }
15. // call oraclize
16. **function** traceTx() payable **public** {
17. uint gasLimit = 50000000;
18. oraclizeIsRunning = **true**;
20. // 設定為每次Oraclize取得的交易筆數[:Count]
21. string memory apiStr1 = "json(https://api.etherscan.io/api?module=logs&action=getLogs&fromBlock=";
22. string memory apiStr2 = "&toBlock=latest";
23. string memory apiStr3 = "&address=0x";
24. string memory apiStr4 = "&topic0=0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef";
25. string memory apiStr5 = "&apikey=HTI3IX924Z1IBXIIN4992VRAPKHJI149AX).result[";
26. string memory apiStr6 = "][transactionHash, blockNumber, timeStamp, topics, data]";
27. string memory apiUrl = string(abi.encodePacked(apiStr1, uint2str(syncBlockHeight), apiStr2, apiStr3, parseAddrressToString(tokenContract), apiStr4, apiStr5, uint2str(syncIndex), ":", uint2str(syncIndex + 50), apiStr6));
28. provable\_query("URL", apiUrl, gasLimit);
29. }
30. }

如程式碼所示，智能合約調用了provable\_query為oraclize（Provable）提供之方法，並於區塊鏈外調用這個query，得到結果之後，則會調用智能合約中的callback功能將結果作為參數傳入。有了Oraclize（Provable）服務，當以太坊內部需要外部資訊時，只需使用API呼叫，並寫好相對應之callback方法即可。

**4.2.2 Ethereum-Bridge**

本實驗環境為以太坊私有鏈，我們必須使用Ethereum-Bridge [19]作為Oraclize（Provable）對外部世界溝通的橋樑。啟動Ethereum-Bridge後，它則會開始監聽鏈上Oraclize（Provable）發出的Event。作為橋樑的角色，每當它接收到Event時，於區塊鏈外部執行該API請求，並將最終結果傳回該智能合約中。

**4.3 資料處理方式**

透過oraclize（Provable）服務所取得之區塊鏈外部資訊後，我們必須將資料分析後再將其儲存至智能合約中。於我們所開發之智能合約中繼承之「jsmnSol」功能（此工具為GitHub上之開源專案，並以此進行資料處理，且為Solidity語言所開發之JSON parser） [20]，以利處理從區塊鏈外部傳回之資訊內容。

1. contract tokenTracer is usingProvable, Parser {
2. bytes32[] transactionHash;
3. address[] sender;
4. address[] receiver;
5. uint[] value;
6. uint[] blockNumber;
7. uint[] timeStamp;
9. // 取得已儲存之交易筆數
10. uint **public** transactionCount;
12. mapping(bytes32 => bool) **private** isExist;
14. **function** savingTx(string memory json) internal {
15. uint returnValue;
16. JsmnSolLib.Token[] memory tokens;
17. uint actualNum;
19. // (returnValue, tokens, actualNum) = JsmnSolLib.parse(json, 9);
20. (returnValue, tokens, actualNum) = JsmnSolLib.parse(json, 450);
22. // 每次Oraclize取回之交易筆數
23. **for** (uint i = 0; i < 50; i++) {
24. JsmnSolLib.Token memory a = tokens[1 + 8\*i];
25. bytes32 \_transactionHash = parseStringTo32Bytes(JsmnSolLib.getBytes(json, a.start, a.end));
26. // 避免重複紀錄同一筆交易
27. **if** (!isExist[\_transactionHash] && \_transactionHash != "") {
28. isExist[\_transactionHash] = **true**;
29. transactionHash.push(\_transactionHash);
30. JsmnSolLib.Token memory b = tokens[2 + 8\*i];
31. uint \_blockNumber = parseHexToUint256(JsmnSolLib.getBytes(json, b.start, b.end));
32. blockNumber.push(\_blockNumber);
33. JsmnSolLib.Token memory c = tokens[3 + 8\*i];
34. timeStamp.push(parseHexToUint256(JsmnSolLib.getBytes(json, c.start, c.end)));
35. JsmnSolLib.Token memory d = tokens[6 + 8\*i];
36. sender.push(parseAddr(subString(JsmnSolLib.getBytes(json, d.start, d.end), 26, 66)));
37. JsmnSolLib.Token memory e = tokens[7 + 8\*i];
38. receiver.push(parseAddr(subString(JsmnSolLib.getBytes(json, e.start, e.end), 26, 66)));
39. JsmnSolLib.Token memory f = tokens[8 + 8\*i];
40. value.push(parseHexToUint256(JsmnSolLib.getBytes(json, f.start, f.end)));
42. // 更新下回開始搜尋之blockNumber, 需避免同一block有多筆交易
43. syncBlockHeight = \_blockNumber;
44. syncIndex = 0;
45. } **else** **if** (\_transactionHash == "") {
46. syncBlockHeight = realBlockHeight;
47. syncIndex = 0;
48. **break**;
49. }
50. }
51. **if** (transactionCount == transactionHash.length) {
52. syncIndex += 50;
53. }
54. transactionCount = transactionHash.length;
55. }
56. }

**4.4 Query功能介紹**

本實驗為實現數位貨幣溯源之服務，為此我們也提供了Query功能，以利使用者可對儲存於智能合約中之數位貨幣歷史交易進行搜索。於該智能合約中擁有「區塊範圍搜索」與「時間範圍搜索」兩大功能，以及針對交易發送方或接收方進行查找，並於智能合約實作Binary Search演算法提供使用者查詢速度。

**4.5 系統介面與操作流程**

為了讓使用者容易操作其去中心化數位貨幣交易記錄與查詢服務，本研究也為此Dapp設計其介面，提升使用時之便利性。

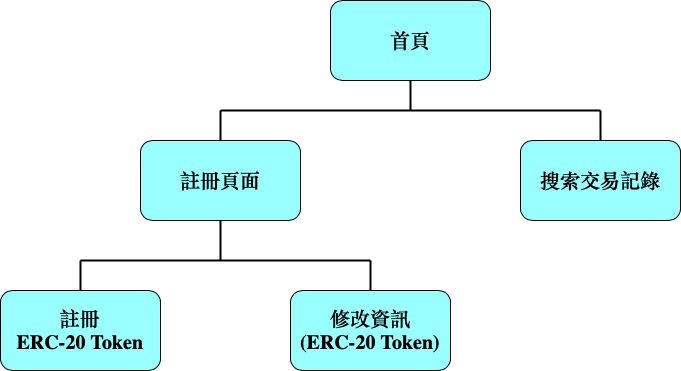


圖 4. 2：服務介面之網頁架構圖

以下將分別介紹「數位貨幣交易記錄與查詢服務」功能，實作示範註冊數位貨幣之合約位址與相關資訊、修改數位貨幣之相關資訊和數位貨幣之交易記錄查找的實作結果做說明：

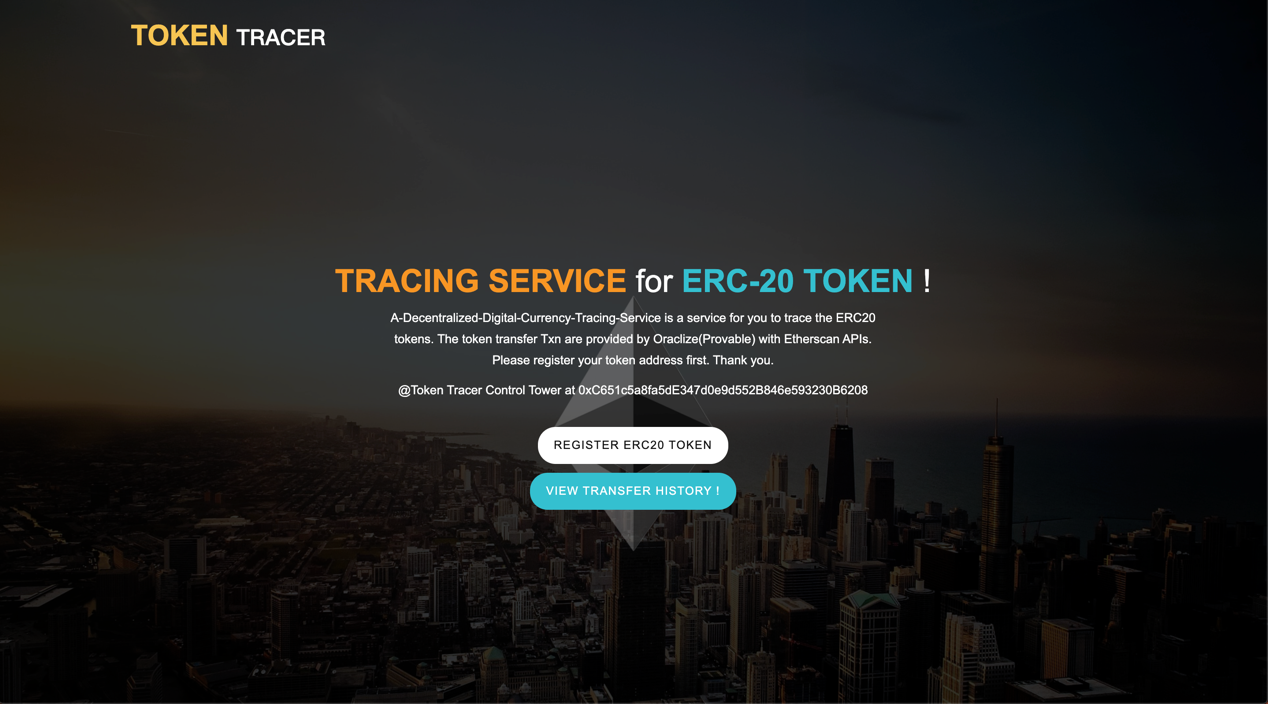


圖 4. 3：數位貨幣交易記錄與查詢服務之首頁畫面

**4.5.1 註冊數位貨幣之合約位址與相關資訊**

本節將說明使用數位貨幣交易記錄與查詢服務之流程，其註冊之操作流程簡述如下：

（一）透過首頁之「REGISTER ERC20 TOKEN」之按鈕，進入註冊服務主頁，如下圖。



圖 4. 4：註冊主頁

（二）按下註冊主頁上之「Register Token」之按鈕，進入代幣註冊頁面，如圖4.5所示。



圖 4. 5：代幣註冊之畫面

（三）填寫欲進行數位貨幣交易記錄與查詢服務之ERC20代幣之合約位址、名稱和單位並送出，其完成註冊服務之畫面如圖4.6所示。



圖 4. 6：完成註冊服務之畫面

（四）註冊完成後，可至交易查找之頁面進行確認，如圖4.7所示。



圖 4. 7：查詢頁面確認註冊完成之畫面

**4.5.2 修改數位貨幣之相關資訊**

使用者完成註冊服務後，仍可針對代幣之名稱與單位進行變更，其操作流程簡述如下：

（一）透過註冊主頁上之「Change Token Info」之按鈕進入後，顯示代幣資訊修改頁面，並將其內容更新後按下送出即可，如圖4.8所示。



圖 4. 8：修改代幣資訊之畫面

**4.5.3 數位貨幣之交易記錄查找**

使用者完成註冊後，服務則開始同步其數位貨幣之交易記錄，使用者即可針對當前所同步之交易進行查找，也可額外對於「區塊範圍」、「日期範圍查」、「發送方位址」和「接收方位址」等功能進行交易篩選，其功能說明如下：

（一）交易查找：顯示目前已同步之所有交易紀錄，如圖4.9所示。使用者也將鼠標移到其中一列表項目中，即可查看其交易之詳細資訊，如圖4.10所示。



圖 4. 9：顯示已同步之所有交易紀錄之畫面



圖 4. 10：詳細交易內容之畫面

（二）區塊範圍篩選：可訂定其區塊範圍篩選交易紀錄，如圖4.11與圖4.12所示。



圖 4. 11：訂定區塊範圍篩選之畫面



圖 4. 12：區塊範圍篩選結果之畫面

（三）日期範圍篩選：可訂定其日期範圍篩選交易紀錄，如圖4.13與圖4.14所示。



圖 4. 13：訂定日期範圍篩選之畫面



圖 4. 14：日期範圍篩選結果之畫面

（四）發送方位址或接收方篩選：可針對其特定發送方或接收方之位址篩選交易紀錄，如圖4.15與圖4.16所示。



圖 4. 15：特定位址篩選之畫面



圖 4. 16：特定位址篩選結果之畫面

**4.5.4 Binary Search效能測試**

本實驗於智能合約實作Binary Search演算法提供使用者查詢速度。此小節我們將探討一般搜索與Binary Search下查詢不同區塊範圍時，觀察資料回傳時間的變化。對於此測試，我們預先儲存100000筆資料於智能合約當中，其儲存資料之區塊高度為1的有10筆資料、高度為2的有10筆資料，以此類推，最高的區塊高度為10000的有10資料。實驗總共進行了七種搜索測試，分別為區塊高度為10、50、100、500、1000、5000、10000。



圖 4. 17：比較Binary Search搜索效能

從圖4.17中可以看到使用一般搜索方式時，其查詢資料之回傳時間，在隨著搜索區塊高度的增加，回傳時間也隨之增加；然而，加入Binary Search搜索方法後，其實驗結果顯示，資料回傳時間不隨著搜索區塊高度的增加而增長。

# 第五章 討論與結論

本章節統整本研究之研究成果，共分為二小節，先是針對本研究提出整體的結論說明，以及本研究的研究貢獻；接著針對本研究之議題提出未來研究方向之建議。

**5.1 討論**

本研究目標在於實作以太坊區塊鏈之數位貨幣溯源服務。透過現有技術方案與相關文獻，根據溯源服務在實務上的可能作法進行研究與探討，再藉由實作與實驗，針對實務應用層面進行探討與評估，甚至找出問題並建議解決方案。

下面我們探討針對區塊鏈數位貨幣之溯源溯源服務，其影響溯源之效率的可能因素，以及實作中遭遇的難題：

* Etherscan API之使用次數限制影響溯源效率：我們能透過Etherscan API取得以太坊公鏈上之數位貨幣歷史交易，但對於一般開發者而言，使用API有對於每個IP位址每秒只能使用五次API的限制。
* Ethereum Bridge處理Oraclize（Provable）服務之Query速度影響溯源效率：由於本實驗將數位貨幣溯源服務建立於私有鏈之上，當使用Oraclize（Provable）服務之Query時，需搭配Ethereum-Bridge工具監聽其智能合約所發出之特定事件（Event），並作為中介者負責傳遞鏈外訊息。Ethereum-Bridge並無多執行緒的多工處理能力，因此當它接收到事件時，只能將其放入佇列中，採先進先出的方式逐一處理。
* Solidity無提供Json資料型態之處理方法：數位貨幣溯源服務乃是利用以太坊區塊鏈智能合約所建立而成，將取得之歷史交易儲存於智能合約當中，以利後續之查找和追溯。不過，於智能合約獲取之歷史交易內容皆為Json格式之資料，而Solidity本身並無提供該資料的處理方式，故透過「jsmnSol」此GitHub上之開源工具，同時也是為Solidity語言所編成之Json Parser進行資料處理。

**5.2 結論**

本研究之「去中心化數位貨幣溯源服務」是一建立於以太坊區塊鏈之私有鏈平台之服務，透過私有鏈上之節點共同維護數位貨幣溯源之交易證明，以保證其公正性和安全性。該服務也利用了Oraclize（Provable）服務作為可信任之交易資料提供者，為了解決智能合約取得外部數據之限制，並結合由Etherscan所提供之API，以確保數據之正確性。在實務應用上，隨著區塊鏈的演進與數位貨幣的發展趨勢，可能須面臨更透明化、更嚴謹之溯源服務，甚至是政府機關之區塊鏈監管機制。因此，未來在區塊鏈數位貨幣之溯源議題時，希望能持續改進，例如：（一）數位貨幣流向追蹤：透過資料分析與追查，評估各個錢包地址是否存有洗錢之動機等。（二）納入監理機制：於每一種數位貨幣之智能合約中加入一監理者角色，並監聽該數位貨幣之所有交易內容；或是所有交易皆需經由監理者認可才能發送，藉此達到監管與治理的效果。

參考文獻

|  |  |
| --- | --- |
| [1] | "Introductiion To Smart Contracts," [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/. |
| [2] | "EIP-20: ERC-20 Token Standard," [Online]. Available: https://eips.ethereum.org/EIPS/eip-20. |
| [3] | "What Is DeFi?," [Online]. Available: https://www.coindesk.com/what-is-defi. |
| [4] | S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. White paper," 31 October 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf. |
| [5] | V. Buterin, "A next-generation smart contract and decentralized application platform. White Paper," 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. |
| [6] | "Facebook Libra," [Online]. Available: https://libra.org/en-US/. |
| [7] | "R3 Corda," [Online]. Available: https://www.corda.net/. |
| [8] | "BigchainDB," [Online]. Available: https://www.bigchaindb.com/. |
| [9] | S. Bragagnolo, H. Rocha, M. Denker and S. Ducasse, "Ethereum Query Language," in *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, Gothenburg, Sweden, 2018. |
| [10] | "Etherscan," [Online]. Available: https://etherscan.io/. |
| [11] | "Introduction to SQL," [Online]. Available: https://www.w3schools.com/sql/sql\_intro.asp. |
| [12] | "Oraclize(Provable)," [Online]. Available: https://provable.xyz/. |
| [13] | "Quorum," [Online]. Available: https://consensys.net/quorum/. |
| [14] | E. Nyaletey, R. M. Parizi, Q. Zhang and K.-K. R. Choo, "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019. |
| [15] | "Solidity," [Online]. Available: https://solidity.readthedocs.io/en/latest/. |
| [16] | "Go Ethereum," [Online]. Available: https://geth.ethereum.org/. |
| [17] | "Node.js," [Online]. Available: https://nodejs.org/en/. |
| [18] | "Ethereum-Bridge," [Online]. Available: https://github.com/provable-things/ethereum-bridge. |
| [19] | "jsmnSol," [Online]. Available: https://github.com/chrisdotn/jsmnSol. |