國立臺東大學理工學院
2019學生學習成果競賽
基於分散式帳本技術打造網域名稱系統

動機 :

目前的網域名稱系統正面臨重大的危機， 如 DNS 挾持, DNS快取污染，以及著名 DDoS 攻擊等的各式攻擊型態，更有些國家利用上述的攻擊方式，限制人民的網路自由，如：中國防火長城。在網域世界中，我們更不能忽略 ICANN 長期以來的壟斷，依規定，若申請新的頂級網域，費用需數十萬美金，如：臺北市政府為了購買 .taipei 頂級網域，每年需編列上千萬預算。通過分析目前提出解決 DNS 問題的相關文獻後，發現大多數的解決方案只是繼續增加安全性，而從未實現對 DNS 的去中心化。因此我們將利用分散式帳本技術打造對 DNS 去中心化的系統，使其從根本具備自主, 開放, 平等, 透明等特徵。

分散式帳本技術 (Distributed Ledger Technology)：

我們使用的 DLT 為 Tangle，此技術相較於傳統區塊鏈，改善了非常多的缺點，以其特性為優勢：

一. 擴展性 (Scalability)：交易量越多，確認速率越快，網路會隨著交易數量越多而越強壯。

二. 去中心化（Decentralisation)：Tangle 中並沒有礦工存在，發起交易者也是驗證者，大家都是都擁有相同的地位。

三. 無交易手續費（No transaction fees)：IOTA 接受 0 元交易，且無需手續費，因此更適合資料儲存應用。

四. 抵抗量子計算（Quantum computing protection)：因採用一次性簽章演算法 (Winternitz OTS)。

研究成果：

我們的 TangleDNS 相較於傳統 DNS，因其分散式帳本特性，不再需要中心化伺服器提供服務，在全球數百萬個節點上，憑著正確的儲存資訊及正確的共識機制，以及無法竄改，得到正確的域名資訊，避免了信任後端伺服器解決請求 (去信任化)。且現在任何人都可以申請頂級域名，省去高額的費用，更能直接註冊二級域名等，並能管理修改刪除。當前的 DNS 每天處理來自全球數十億的訪問請求，若傳統 DNS 遭受攻擊導致竄改或是停擺，網路將會大亂，除了使用上的不便，經濟上的損失更是無法計算，而我們的 TangleDNS 解決了此問題，得利於去中心，整個系統架構僅需裝設客戶端即可使用，全世界都是你的資料庫。

Domain Name 註冊流程圖：