經濟部 111 年度
《區塊鏈創新產業資料管理應用計畫》
合作研究計畫

《結合區塊鏈規格之分散式隱私強化技術架構研發與實作》

建議書徵求文件

財團法人資訊工業策進會

中華民國 111 年 5 月 4 日

111年度合作研究計畫建議書徵求文件

一、 簡介

在各式企業資料運用之情境下，保障資料隱私是非常重要的課題。過往運作於單機之人工智慧與機器學習演算法在訓練時模型時，為了建構精準的模型，需要分析每一筆資料，而這種方式在隱私保護上有所不足；另一方面，如果這些演算法僅分析一部份的資料，則人工智慧與機器學習演算法所建構之模型準確率將十分低落。為了解決上述問題，將從產業資料管理的隱私保護面切入，期能在確保資料隱私的狀態下，提升演算法模組的精準度，但由於目前開源區塊鏈方案越來越多，需要歸納出一個方法及規格需求，發展一個可結合聯盟式學習的區塊鏈規格篩選建議，讓產業資料能夠以更具效率的方式進行管理與避免篡改、造假，以強化產業資料管理的區塊鏈核心技術與效率，提高商業使用區塊鏈服務之意願。

二、 計畫目標

本計畫中，除了持續性探討聯盟式學習（Federated Learning）架構，在確保資料隱私的情況下，大幅提升模型之準確度，並將針對聯邦學習的實務應用系統，不止是客戶端的演算法程式，更包括實務上其他配套或元件的完備程度(例如資料庫、亂數產生器等)，本計畫將歸納、產出一個區塊鏈結合聯盟式學習的架構與建議，提出適合結合聯盟式學習的區塊鏈智能合約實作方法及效能改進方案，以避免產業資料遭篡改做假。

三、 計畫範圍

本計畫將產出

(1) 持續探討聯盟式學習架構，並針對聯盟式學習的實務應用系統，包括實務上其他配套或元件的完備程度，將歸納、產出一個區塊鏈結合聯盟式學習的架構與建議。

(2) 針對結合聯盟式學習的區塊鏈智能合約進行實作驗證，並提出改善方案。

四、 預期成果

本計畫預期將歸納、產出一個區塊鏈結合聯盟式學習的架構與建議，提出適合結合聯盟式學習的區塊鏈智能合約實作方法及效能改進方案，合作研究產出將如下：

(1) 區塊鏈結合聯邦學習的架構設計與平台可行性分析。

(2) 技術驗證與實作分析報告乙份。

(※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後6個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。)

五、 執行方式

邀請大專院校的教師籌組研究團隊，參與區塊鏈技術研究，豐富國內區塊鏈研發能量，藉由參加國內、外知名研討會議展示或發表，增加產學研共同研發的成果技術深度及曝光度。

六、 計畫期程及預估計畫總經費

計畫執行區間： 111 年 6 月 1 日 至 111 年 11 月 30 日

總經費：250,000元

七、 驗收標準

111/11/10前：期末報告、技術實作驗證說明簡報檔

八、 技術能力需求

本計畫執行需具備下列相關技術領域知識：

(1) 熟悉分散式運算技術
(2) 熟悉區塊鏈平台設計與分析方法
(3) 熟悉聯盟式學習
(4) 熟悉密碼學安全協定與應用