經濟部 110 年度
區塊鏈創新產業資料管理應用計畫
合作研究計畫

《基於區塊鏈技術之分散式隱私強化ＡＩ分析平台技術研發》

建議書徵求文件

財團法人資訊工業策進會

中華民國　110 年 3 月 16 日

110 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，並整合區塊鏈智慧合約技術應用，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，我們探討新的聯盟式學習（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；另一方面，過往之聯盟式學習在資料傳輸過程中，雖有對資料加密，但由於必須依賴集中式的 server 進行匯整，如此一來又再變回集中式學習，但如何可選出些集中式 server 及為何它是可信的，都可能是新的議題。因此，我們提出透過區塊鏈的智慧合約來取代集中式 server 的部分功能，並且協助各資料擁有者進行「梯度」上鏈的效果，避免被集中式 server 篡改做假。

三、 計畫範圍

本計畫將產出

(1) 本計畫探討聯盟式學習架構，使其能在金融與電子商務這類需要高隱私性的環境下，可提升模型之準確度。

(2) 本計畫之聯盟式學習架構結合區塊鏈達成高度去中心化。

(3) 本計畫協助聯盟式學習確保各資料擁有者上傳資訊的正確性。

四、 預期成果

本計畫預期開發分散式隱私強化ＡＩ分析平台，合作研究產出將如下：

(1) 分散式隱私強化ＡＩ分析平台設計方法。

(2) 研究報告乙份。

※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，增加產學研共同研發的成果技術深度及曝光度。

(1) 參舉國內、外知名會議發表

(2) 參訪相關區塊鏈新創公司，鼓勵採用此類技術合作

六、 計畫期程及預估計畫總經費

計畫執行區間： 110 年4月 01 日 至 110 年 11 月 30 日

總經費：200,000 元

七、 驗收標準

110/10/31 前：期末報告、技術驗證說明簡報檔

八、 技術能力需求

(1) 分散式運算技術
(2) 聯盟式學習
(3) 區塊鏈平台
(4) 密碼學安全協定