經濟部 109 年度
《區塊鏈創新生態體系發展計畫(4/4)》
合作研究計畫

《基於圖論探勘分析技術之惡意行為預警技術》

建議書徵求文件

財團法人資訊工業策進會

中華民國　109 年 03 月 21 日

109年度合作研究計畫建議書徵求文件

一、 簡介

近年來使用區塊鏈技術的蓬勃發展，各種區塊鏈相關的服務已廣泛佈建於人們的生活之中。由於區塊鏈技術與許多生活中的服務息息相關，區塊鏈的安全性是一個非常重要的問題。因此本研究旨在分析現有知名區塊鏈之相關惡意行為，以提供人工智慧與機器學習演算法進行早期預警，期待能帶來相對穩定的區塊鏈環境。

二、 計畫目標

將現有已知區塊鏈惡意或智慧合約之惡意行為擷取並且進行分析再加以歸類後將可疑行為分析判斷是否為需進行預警。分析的內容包含各種行為模式（Behavioral Pattern），如行為之時間、頻率、數量與相關跖蹼等資料。

三、 計畫範圍

本計畫期望借重機器學習與資料探勘技術中「圖論 (graph theory) 與圖探勘 (graph mining)」以有效偵測區塊鏈上之惡意行為並進行分析，預期未來將可成為企業聯盟鏈異常偵測服務，讓基礎運作更穩定。

本計畫包含三個部份：1) 針對近五年區塊鏈惡意行為相關之文獻探討；2) 至少兩種區塊鏈之惡意行為資料擷取、歸納、分析；3) 區塊鏈惡意行為預警系統之開發建議。

四、 **預期成果**(明確說明合作研究成果之產出)

本計畫將以機器學習配合資料探勘技術分析資料中之各種行為模式，找出與預警未來的可疑行為，預期產出為：

(1) 近五年區塊鏈惡意行為資料擷取方式分析成果(併入研究報告中)

(2) 至少兩種惡意行為之模式分析成果(併入研究報告中)

(3) 區塊鏈惡意行為預警系統研究報告一份

※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**(包括計畫時程、計畫分工方式)

(1) 現有知名區塊鏈惡意行為之相關文獻探討。

(2) 擷取區塊鏈之惡意行為之資料，如時間、頻率、數量與相關跖蹼等資料。

(3) 對區塊鏈惡意行為之模式與資料進行分析，並探討何種特徵（feature）可有效區別惡意與非惡意行為，以提供人工智慧與機器學習演算法更有效地建立相關模型。

六、 計畫期程及預估計畫總經費

計畫執行區間：109 年 03 月 01 日 至 109 年 10 月 31 日

總經費：300,000元

七、 **驗收標準**(含教育訓練)

(1) 近五年區塊鏈惡意行為資料擷取方式分析成果(併入研究報告中)

(2) 至少兩種惡意行為之模式分析成果(併入研究報告中)

(3) 區塊鏈惡意行為預警系統研究報告一份

八、 **技術能力需求**(請詳述所需要之技術能力或專長)

(1) 網路爬蟲技術以利區塊鏈惡意行為資料擷取

(2) 資料探勘與分析

(3) 圖論 (graph theory)與圖探勘 (graph mining)

附件1：契約書格式

1-1：計畫書格式

1-2：經費動支報表

1-3：成果報告撰寫須知

1-4：報告格式

1-5：論文格式

1-6：保密聲明書

1-7：委託匯款同意書