經濟部 107 年度
《資策會創新前瞻技術研究計畫》
合作研究計畫

區塊鏈應用資安攻防研究

建議書徵求文件

財團法人資訊工業策進會

中華民國 107 年 03 月 05 日

107年度合作研究計畫建議書徵求文件

一、 簡介

在分散式分類帳中，參與者使用同一個資料庫與平台，可以使支付過程更為便捷與透明。分散式分類帳預期將對有價物品的交易與追蹤方式帶來顛覆式的變革。因此，科技與金融企業皆投入大量資源，對分散式分類帳應用進行早期研究或實驗性的部署。

區塊鏈為分散式分類帳儲存與驗證資料的骨幹，其性能與可靠性受網路狀態與共識機制等因素影響。在部署分散式分類帳前，如能針對各種使用情境（包括不正常的網路狀態與攻擊）進行模擬並分析其反應，找出可能瓶頸與漏洞，將可大幅降低修復與最佳化的成本。

二、 計畫目標

本計畫目標為發展一區塊鏈模擬平台，讓使用者能在受控制的環境下（包括靜態與動態、正常或不正常的網路組態），系統性地模擬區塊鏈應用在不同使用情境下（如：交易頻率及其在空間與時間的分布），以分析其性能瓶頸與可能的安全漏洞。分析結果將有助於後續的最佳化與漏洞修復。

三、 計畫範圍

預計發展的區塊鏈模擬平台應有下列功能：

1. 可部署使用者指定、建構於IBM Hyperledger Fabric上的區塊鏈應用。
2. 可設定網路組態與網路延遲與頻寬。
3. 根據使用者提供的交易分布（時域與空域），產生交易事件，並進行模擬。
4. 紀錄交易資訊，包括起始及完成時間與相關事件。

本計畫應設計、實作並交付上述區塊鏈模擬平台及相關文件與報告。

四、 預期成果

本計畫預期成果如下：

1. 期中、期末報告各一份。
2. 區塊鏈應用模擬器與相關使用文件。

※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

計畫執行方式如下：

- 每月定期召開研究討論會議。
- 期中進度報告。
- 期末總結報告與雛形系統展示。

六、 計畫期程及預估計畫總經費

計畫執行區間： 107 年 01 月 01 日 至 107 年 12 月 07 日

總經費：800,000元

七、 驗收標準(含教育訓練)

- 2018/09/7 交付期中報告1份，內容應包括：研究動機、架構規劃、使用技術、文獻搜尋。
- 2018/11/30 交付區塊鏈模擬平台。
- 2018/11/30 交付期末報告1份，內容應包括：研究動機、架構規劃、使用技術、實驗設計、實驗結果、結論。

八、 技術能力需求

具備網路模擬、Hyperledger Fabric平台部署及應用撰寫與系統整合等技術專長或研究之學術機構與人員。

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