國立高雄科技大學(第一校區)

電子工程系

專題報告書

私有以太坊區塊鏈實作以及其硬體加速方法調查

專題生：

劉益彤 YI-TUNG LIU

指導教授：陳朝烈博士 Dr.Chao-Lieh Chen

中華民國 一一一 年 五 月

摘　　要

本專題主要在私有以太坊區塊鏈(Ethereum)的實作與硬體裝置進行加速運算，以太坊是一個去中心化、開源且支援智慧合約(Smart Contract)的公共區塊鏈平台，

目　　錄

摘要......................................................i

目錄.....................................................ii

圖目錄..................................................iii

第一章 緒論...............................................1

1.1 研究動機與目的....................................2

1.2 專有名詞定義......................................2

第二章 研究架構與方法.....................................3

2.1系統架構........................................4

2.2智慧合約架構..................................5

2.3硬體加速方法調查...........................7

第三章 成果展示............................................9

3.1區塊鏈節點間同步.......................10

3.2 去中心化應用程式..................................11

3.3硬體加速運算之差異..........................12

第四章 未來展望.........................................13

第五章 參考文獻..........................................15

圖目錄

圖一 SOC-7666...................................2

圖二 adventure-ARK-3530.............................................2

圖三 樹梅派..............................................2

圖四 電腦主機...............................................3

圖五IPCam........................................3

圖六 繼電器.............................................3

圖七 階層圖.............................................4

圖八 節點架構圖...........................................4

圖九 專題網路架構...........................................6

圖十 請求與資料傳遞路徑....................................6

圖十一 直播功能運作流程圖.....................................7

圖十二 控制流程............................................................7

圖十三 樣本與辨識模型傳遞路徑........................................8

圖十四 樣本與辨識模型傳遞路徑............................................8

圖十五 監控介面展示......................................10

圖十六 NG回報........................................10

圖十七 及時辨識........................................11

圖十八 ROI框選與樣本產生..........................................11

圖十九 請求樣本..........................................12

圖二十 接收到的樣本 .....................................12

圖二十一 訓練畫面........................................12

圖二十二 科技部110年徵案內容.....................14

第一章　　緒論

1.1研究動機與目的

以太坊目前是規模第二大的公共區塊鏈平台，其功能建立在資料分散於每個人手中，資料難以被竄改，再加上雜湊函式的特性，幾乎無法被逆向推導回來的特性。私有區塊鏈特別適合企業使用，將企業裡的裝置都連接上區塊鏈網路，就能避免有資料被竄改而不自知，又或者是透過智能合約建立自己的虛擬代幣，讓用戶可以透過該代幣購買企業的各種服務。

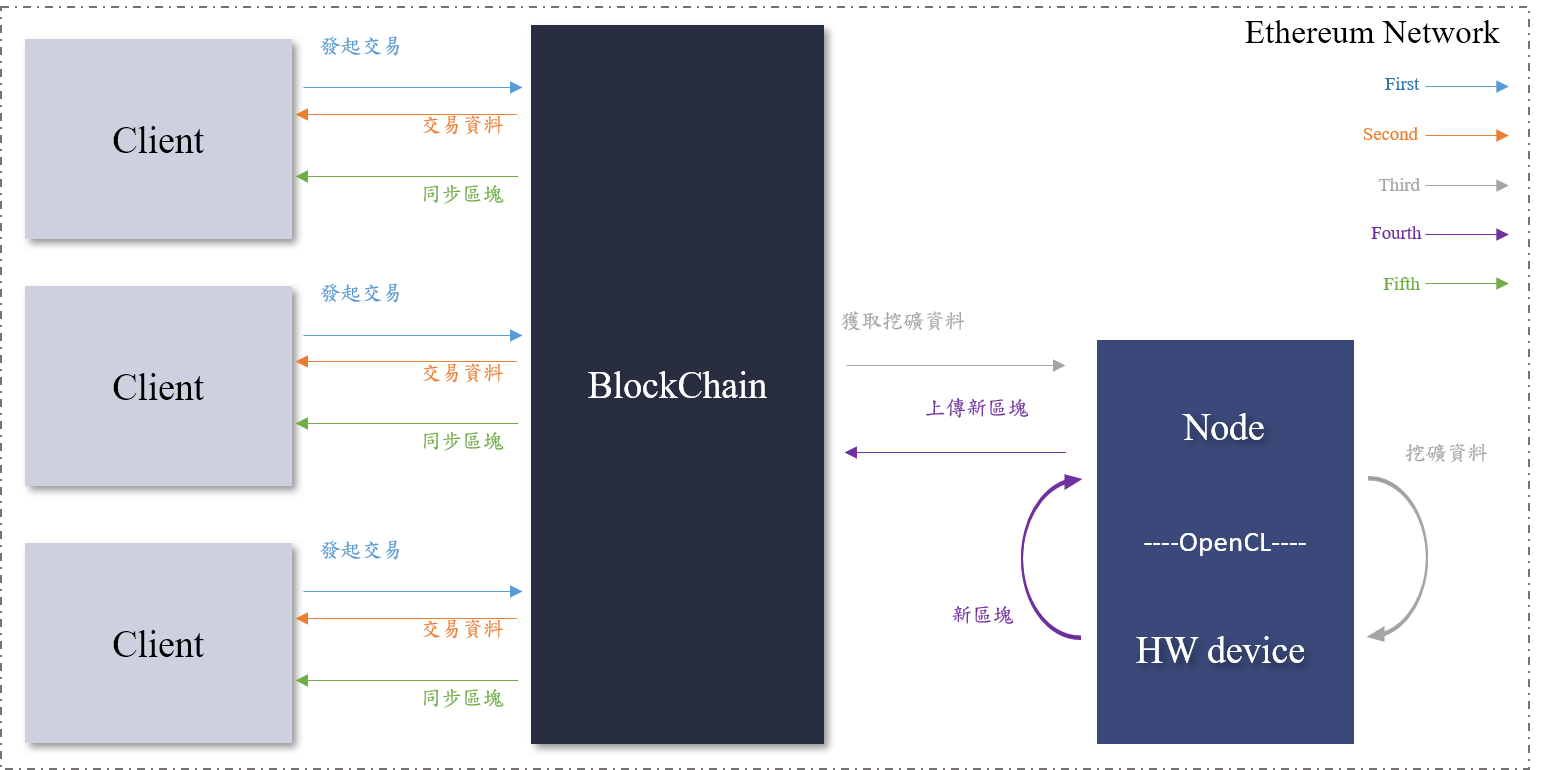
在以太坊上使用各種服務時，給予礦工手續費可以使自己的服務被優先處理，但隨著私有區塊鏈社群的成長，交易量也會越來越大，如果區塊鏈整體算力沒有隨之成長，在用戶們的競爭之下，手續費也會增多，長久以往對於整個社群不是一個好的發展，透過硬體裝置的加速，可以提升礦工的算力，把手續費平衡回來。

1.2 專題相關工具

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

第二章　　研究架構與方法

2.1 系統架構



圖二: 私有以太坊區塊鏈網路架構圖

* First : 用戶端(Client)發起交易。
* Second : 區塊鏈(BlockChain)回傳交易資料，但此時資料正在等待處理 ，查詢該交易資料後會發現，區塊鏈(BlockChain)並不知道該資料該放在哪個區塊(紅框)。



圖二: 處理前的交易資料

* Third : 節點(Node)透過區塊鏈(BlockChain)獲取需要進行處理的資料，再將資料傳送給旗下的硬體加速裝置(HW device)。
* Forth : 運算完成後將結果回傳給節點(Node)，節點(Node)在將結果回傳至區塊鏈(BlockChain)，這個步驟俗稱挖礦、出塊或打包。
* Fifth : 區塊鏈(BlockChain)將新區塊傳送給用戶端(Client)，用戶端(Client)同步新區塊資料，這個時候就能看到該交易資料被放在第1913個區塊裡。



圖三: 處理後的交易資料

2.2 智慧合約架構

第三章　　成果展示

第四章　　未來展望與

第五章　　參考文獻