科技部補助專題研究計畫報告

雲端系統服務層級協議違反之自動賠償機制的研究

報 告 類 別 ： 成果報告
計 畫 類 別 ： 個別型計畫
計 畫 編 號 ： MOST 108-2221-E-003-004-
執 行 期 間 ： 108年08月01日至109年10月31日
執 行 單 位 ： 國立臺灣師範大學資訊工程系（所）

計 畫 主 持 人： 黃冠寰

計畫參與人員： 碩士班研究生-兼任助理：江宏文
碩士班研究生-兼任助理：湯亦祥
碩士班研究生-兼任助理：黃英睿
碩士班研究生-兼任助理：吳東霖
碩士班研究生-兼任助理：李仲嘉
碩士班研究生-兼任助理：陸毅軒
碩士班研究生-兼任助理：王麒翔

報 告 附 件 ： 出席國際學術會議心得報告

本研究具有政策應用參考價值：■否 □是，建議提供機關
（勾選「是」者，請列舉建議可提供施政參考之業務主管機關）
本研究具影響公共利益之重大發現：□否 □是

中 華 民 國 109 年 12 月 10 日

中 文 摘 要 ： 雲端系統已成為資訊系統中發展的主流，也成為人們生活的一部份。目前雲端系統的發展中，建立信任（Trust）及交互不可否定性（Mutual non-repudiation）是最重要的課題之一。很多機構、政府、公司甚或個人，因為對於雲端系統所提供服務的安全性尚有疑慮，因此還不敢使用雲端服務。若我們能成功的於雲端系統發展交互不可否定性及信任，將可進一步推進雲端系統的普遍性。

雲端服務商提供的服務可能無法達成服務層級協議（Service-level agreement；SLA）的約定，目前的賠償機制都是由雲端服務商類似球員兼裁判的方式來判斷及執行，對於雲端的信任是一種傷害。本計畫要研究及實作一個雲端系統之自動賠償模式，針對如果雲端服務商違反SLA時，能以區塊鏈的智能合約讓使用者於合約上申訴並且取得加密貨幣作為賠償。

中 文 關 鍵 詞 ： 雲端系統, 雲端信任, 服務層級協議, 行為違反證明, 區塊鏈,智能合約, 賠償模式

英 文 摘 要 ： In the development of Cloud computing system, establishing trust and mutual non-repudiation becomes one of the most important research topics. Some organizations, governments, companies, and users do not dare to use the services from Cloud system because they concern the security of the Cloud system. If we can successfully establish mutual non-repudiation and trust in the Cloud system, we can increase the popular of the Cloud system.

The services provided by the Cloud system may not be able to satisfy the service-level agreement (SLA). The current existing indemnification mechanism is similar to have the player act as the referee. That is, the service provider determines if itself violates the SLA. In this project, we would like to propose and implement an automatic indemnification model for Cloud system. Whenever the SLA is violated, the client can take objection to the Cloud system by appealing to a smart contract in a public blockchain. In case the objection is successful, some cryptocurrencies will be transferred to the client automatically.

英 文 關 鍵 詞 ： Cloud System, Cloud Trust, Service-level Agreement, Proof-of-violation, Blockchain, Smart Contract, Indemnification Model

科技部補助專題研究計畫成果報告

（□期中進度報告/■期末報告）

雲端系統服務層級協議違反之自動賠償機制的研究

計畫類別：■個別型計畫　□整合型計畫
計畫編號：MOST 108-2221-E-003-004 -
執行期間：108 年 8 月 1 日至 109 年 7 月 31 日

執行機構及系所：國立臺灣師範大學資訊工程系

計畫主持人：黃冠寰
共同主持人：無
計畫參與人員：江宏文、湯亦祥、黃英睿、吳東霖、李仲嘉、陸毅軒、王麒翔

本計畫除繳交成果報告外，另含下列出國報告，共 1 份：
□執行國際合作與移地研究心得報告
■出席國際學術會議心得報告

期末報告處理方式：

1. 公開方式：
   ■非列管計畫亦不具下列情形，立即公開查詢
   □涉及專利或其他智慧財產權，□一年□二年後可公開查詢
2.「本研究」是否已有嚴重損及公共利益之發現：■否 □是
3.「本報告」是否建議提供政府單位施政參考 ■否 □是，____（請列舉提供之單位；本部不經審議，依勾選逕予轉送）

中　華　民　國 109 年 12 月 8 日

前言

雲端系統已成為資訊系統中發展的主流，也成為人們生活的一部份。目前雲端系統的發展中，建立信任（Trust）及交互不可否定性（Mutual non-repudiation）是最重要的課題之一。很多機構、政府、公司甚或個人，因為對於雲端系統所提供服務的安全性尚有疑慮，因此還不敢使用雲端服務。若我們能成功的於雲端系統發展交互不可否定性及信任，將可進一步推進雲端系統的普遍性。

以下由目前最風行的雲端儲存（Cloud storage）服務談起，以期能說明雲端信任的重要性及**稽核**、**行為違反證明**（Proof-of-violation、POV）等相關技術。然後進一步說明，即使我們能有效的達成稽核及行為違反證明，雲端系統還是需要一個能受所有人信任的**自動賠償模式**，然後整個雲端系統的信任體系才可能完整。

雲端儲存系統（Cloud storage）是目前十分受歡迎的服務，目前有名的系統有：Google Drive [1]、Dropbox [2]、SugarSync [3]、SkyDrive [4]、及 Box [5]等。使用雲端儲存系統的企業或個人只需要依實際使用的儲存空間支付費用，並不需要在自己的資料中心或辦公室裡安裝實體的儲存裝置，大大減少 IT 和管理的成本。日常維護工作，如備份、資料複製、或是增加儲存裝置添購等工作，都轉移給代管的服務提供商，讓企業更可以專注在自己的核心業務上。

將重要的檔案或資料儲存於雲端儲存系統，相較於儲存於企業內部儲存系統將面對更多的安全威脅。一般認為雲端儲存系統有可能未經同意而將泄漏資料、修改資料、或是回傳錯誤檔案或資料給使用者。這可能是因為系統有缺陷、系統因故毀壞、管理操作錯誤、或是其他任何來自系統內、外的惡意攻擊。很多使用者包括一般自然人、學校、政府機關、公司等，當所欲儲存的資料較為機密時，則對存放於雲端儲存系統的安全性有疑慮。

使用雲端儲存服務，要解決機密性(Confidentiality)的問題其實並不難，只要上傳的檔案先經過密碼演算法加密，使用者自己保管解密的 Key，就可以解決。這也被稱為 Cryptographic cloud storage [6]。欲解決 Integrity 的問題也不是難事，只要儲存每個檔案的時候，也以某種方法附加上使用者對此檔案的電子簽章即可。但是以上兩個方法並有沒辦法解決雲端儲存系統當資料回損時將檔案系統回復到之前備份的狀態，這被稱為**回捲攻擊**（Roll-back attack）[7,8]。雲端儲存服務提供商大都只宣稱其系統安全度很高，如有內部加密、異地備份等機制。但使用者可以相信雲端儲存系統嗎？沒有一個現存的雲端儲存系統在服務層級協議(Service Level Agreement；SLA)中提供 Security guarantee，他們都只有提供 Availability guarantee（可利用性保證：保證一個月內可取用服務的時間百分比）。如 Amazon 的 S3 [9]及 Microsoft 的 Azure [10]只有提供可利用性保證：如果可利用性低於 99.9%，服務提供者將會退款給使用者。

面對雲端儲存系統的安全威脅，學者歷年來進行很多相關研究。Replication 就是將資料儲存於多個雲端儲存系統[11,12,13,14,15,16]。此方法的成本很高，同時若發現不同儲存系統的資料不一致時，也不見得能知道在哪裡的資料是正確的。Proofs of retrievability 是用 Challenge and reply 的模式，持續性及隨機性的要雲端儲存系統回覆某個檔案和一個亂數值合併的 Hash value，以保證雲端儲存系統並沒有丟失或損毀該檔案[17,18,19,20]。因為是隨機詢問，所以也沒有辦法保下載的檔案一定是正確的。

稽核：

對服務商回傳的檔案或資料進行稽核(Auditing)，就是確認檔案內容及版本的正確性，最直覺的作法是保留所有檔案的 Hash values，每次下載檔案時檢查下載到檔案的 Hash value 和原先保留的值是否相同，就可以確認下載到的檔案是否正確 [21,22,23,24,25,26]。但這些作法有一個問題，就是當雲端儲存服務提供商發生錯誤時，使用者無法有足夠的證據來證明，因此無法建立交互不可否定性。同時若有多個裝置共同存取同一個帳戶的資料，如何同步檔案的 Hash values 是一個很大的問題。

行為違反證明（POV）：

欲建立使用者及雲端儲存系統的交互不可否定性的技術稱為行為違反證明（Proof-of-violation、POV），POV 技術除了基本需要稽核外，於取用服務的時候，經由特定的交握協定同時產生一些密碼學證據。POV 技術的目的在於讓雲端服務的使用者及提供者能於系統運行時產生一些**密碼學證據**，這些證據可以用來證明（Prove）服務的提供者是否有違反 SLA。以雲端儲存系統而言，如果服務提供者將錯誤的檔案版本或不正確的檔案給予使用者、亦或宣稱檔案不存在，就是違反合約。如果被證明發生服務提供者違反合約，則可以根據簽訂的規章退費或賠償。另一方面雲端服務的使用者，也無法誣指服務提供者發生錯誤，因為密碼學證據也可以證明服務提供者的清白（Innocence）。

於雲端儲存系統發展 POV 技術，最早可以溯源到 2011 年 Microsoft 和美國 MIT 大學的 CloudProof [27][1]。 CloudProof 提出用 Chain-hash 的方法來串起使用者存取檔案的證據，以使得對於檔案的操作順序能使用密碼學證據來證明，密碼學證據可以用來稽核雲端儲存系統是否回傳舊版或錯誤的檔案。但是他們的方法有一個重要的缺點，就是如果使用多個裝置來輪流存取同一個使用者帳戶的檔案，這些裝置間要不斷的交換密碼學證據，否則雲端服務提供者可以發動回捲攻擊（Roll back attack），讓自己丟失檔案的錯誤情形不被密碼學證據證明。

本計畫提案人黃博士帶領團隊發展技術，順利克服 CloudProof 無法解決多裝置情境共享同一帳戶的問題，相關研究成果發表於 IEEE TrustCom 2013 會議 [28]，並獲得該會議最佳論文獎(One out of 382 papers)：

A Mutual Nonrepudiation Protocol for Cloud Storage with Interchangeable Accesses of a Single Account from Multiple Devices. **Gwan-Hwan Hwang**, Jenn-Zjone Peng, and Wei-Sian Huang. **The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-2013), Melbourne, Australia, 16-18 July, 2013.** Acceptance rate: 27.7% (106/382) This paper received THE BEST PAPER AWARD of the IEEE TrustCom 2013 (One out of 382 papers).

以上論文中，主要提出了一個 Proof of violation（POV）的技術稱為 C&L scheme。但是此論文所提出的方式只能支援 Epoch-based POV，就是在密碼學證據累積一段時間後，才發動稽核。在大多數的情境中 Epoch-based POV 可能足夠，但是某些特殊的情形下，服務的使用者對

[1] 這是個由 Microsoft 公司主導的研究及計劃。

Epoch-based POV 未必滿足，試想以下的情境：

『某律師事務所負責幫某國際公司和另一個境外公司談判及簽訂重要的合約，合約條文項目多且繁瑣，有權責修改的人員很多。為了能確保儲存合約的安全性，律師事務所將文件存於某知名的雲端儲存系統服務商內，如此就算公司內部的系統完全出問題，也不至於文件會完全損毀。但是沒想到最後兩公司簽約時，由雲端儲存系統取出列印的文件卻是錯誤的版本。因此造成服務的國際公司蒙受巨大的經濟損失，此律師事務所必須要負連帶責任，也幾乎倒閉。雖然他們的雲端儲存系統支援 Epoch-based POV，此律師事務所也只能根據稽核的結果要求服務提供者根據簽訂的規章退費，對公司發生的困境沒有什麼幫忙。』

以上的問題是因為服務提供者發生錯誤時，雲端服務的使用者不能立即知道。如果能讓雲端服務的使用者存取檔案的時候立即能稽核正確性，即所謂 Real-time POV，就能解決問題。 針對如何於 Real-time 達到 Proof of violation 的研究，本計畫提案人黃博士亦有成果，發表於 IEEE CloudCom 2014 [29]如下:

Real-time Proof of Violation for Cloud Storage. **Gwan-Hwan Hwang**, Wei-Sian Huang, and Jenn-Zjone Peng. **Accepted for publication in 2014 6th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2014), December 27-29, 2014, Singapore.** Acceptance rate: 28.2% (85/301)

相對於美國 MIT 所發展的 IRIS 系統 [26]，IRIS 雖然可進行即時稽核，但是無法同時產生密碼學證據。但是此論文[29]提出的方法 Overhead 較大，和一般沒有進行 Real-time POV 的檔案存取相比，需要花費 50 到 100 倍的時間。本計畫提案人黃博士的團隊旋即研發一種以 Full hash binary tree(FBHTree)的方式來進行雲端儲存系統的即時稽核及 POV，此論文發表於 IEEE Cloud 2016 [30]，可以將 Overhead 降到平均約 10%以下。比之前的技術[29]加快了兩個級數（快 100 倍），如下：

Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems. **Gwan-Hwan Hwang** and Hung-Fu Chen. **The 9th IEEE International Conference on Cloud Computing (IEEE Cloud 2016), June 27 - July 2, 2016, San Francisco, USA.** Acceptance rate:15% This paper received the best student paper award runner-up).

本實驗室團隊於前些年度的科技部計畫（『雲端資料庫系統的即時稽核及行為違反驗證』、106-2221-E-003-001、106.8.31~107.7.31[31]），提出以本實驗室團隊發表的於 IEEE Cloud 2016 [30]的技術（此技術解決雲端檔案儲存系統的 POV 問題），來實作雲端資料庫系統的即時稽核及行為違反驗證。就是以 Indexed Merkle tree 來解決此問題（Indexed Merkle tree 在論文[30]中名為 FBHTree）。它與一般的 Merkle tree 不同。基於標籤的索引，除了驗證存在外，還可以額外提供驗證不存在。為了證明。目前以完整實作[32]所提出 B+ tree 和 Binary Merkle tree 的方法，根據初步使用 Indexed Merkle tree 的方法相比，很明顯使用 Indexed Merkle tree 在 Query、Update、Delete 運算都有較佳的效能。同時因為不需建議 B+ tree 所以需求的記憶空間大幅減少。

研究目的

目前 POV 的技術是針對雲端檔案系統或雲端資料庫系統，經由設計的經由特定的交握安全協定，客戶端可以僅僅持有不到 1KB 的密碼學證據（雲端檔案系統或資料庫的資料量可以到一千萬筆），於雲端服務提供者發生送回錯誤版本或錯誤資料時，可以根據密碼學證據來證明雲端服務

提供者的錯誤。

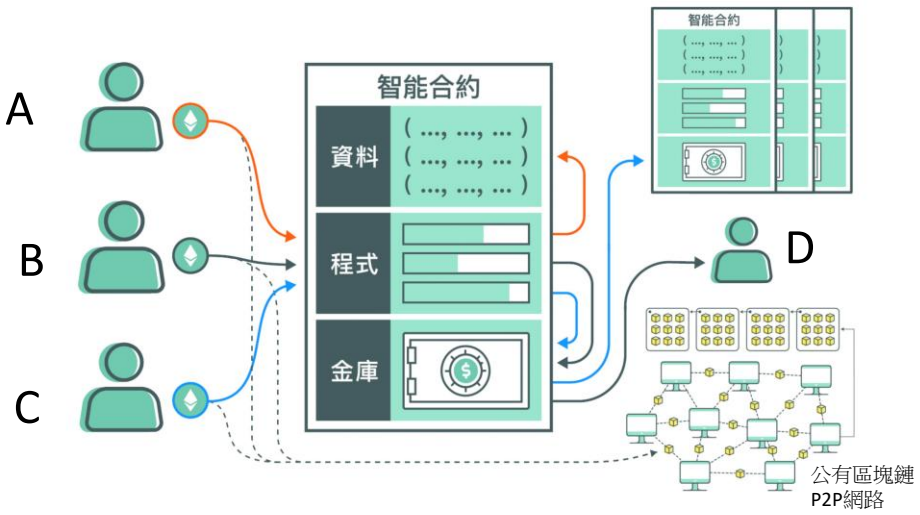
但很明顯有效 POV 的存在還是無法百分百保護客戶的權益，因為雲端服務商通常和客戶端僅靠網路通訊，大多案例都是客戶刷卡付費，連雲端服務商的國籍或是是否於自己國境內有客戶服務單位來處理因為服務不符合 SLA 都不清楚。同時如果客戶提出有效的密碼學證據，雲端服務商以類似球員兼裁判的方式來否定客戶提出的密碼學證據，客戶多半是申訴無門。

由以上論述，我們想研究設計一個自動賠償機制，此機制基於密碼學，不用靠人為操控的可信第三方（Trust Third Party, TTP）來執行賠償的判斷。如此客戶的權益可受到充分的保護。當客戶取得服務時，檢查 POV 協定中由雲端服務商發送的證據，有問題立即和自動賠償機制提出申訴，可以立即得到賠償。

方法

很明顯的，一個雲端系統的自動自動賠償機制必須要有『協定』、『證據』、『判斷機制』的存在。『協定』是客戶端和服務商的溝通機制，通常是一個交握機制。『證據』是根據密碼學產生經由電子簽章認可的訊息，此訊息可以用來驗證服務商是否有違反 SLA。『判斷機制』是一個執行單元，必須能根據『證據』運算，做出正確判斷且於必要時完成賠償機制的運作。

一般進行『判斷機制』多半要使用類似 Trusted Third Party(TTP)的機制，但是在雲端運算的世界，客戶端和服務商常常不隸屬同一個國籍，要建立一個多方都能信任的 TTP 幾乎是不可能的[33]。但是區塊鏈的分散式帳本技術，卻可以解決此問題。比如具有全球共識的公有區塊鏈（如比特幣及以太坊），其礦工數超過一萬，在帳本內的記錄收到超過一萬個以上礦工的複製及監督。要篡改或偽造幾乎是不可能。用來作為雲端系統的自動自動賠償機制的信任基礎是個好主意。



圖一：智能合約運作說明

公有區塊鏈以太坊於 2014 年提出了智能合約的概念及實作，基本上一個智能合約擁有自己的資料、程式（一些函式）、及儲存加密貨幣的能力。需要驅動智能合約函示運作的一個私鑰擁有者，將交易及參數簽章後，交由礦工執行。圖一說明區塊鏈智能合約的運作，私鑰擁有者 A 支付礦工費請礦工執行程式的結果修改了合約內的資料；私鑰擁有者 B 支付礦工費請礦工執行程式的

結果將合約金庫內的加密貨幣轉給了 D；私鑰擁有者 C 支付礦工費請礦工執行程式的結果將合約金庫內的加密貨幣轉給了另一個合約。

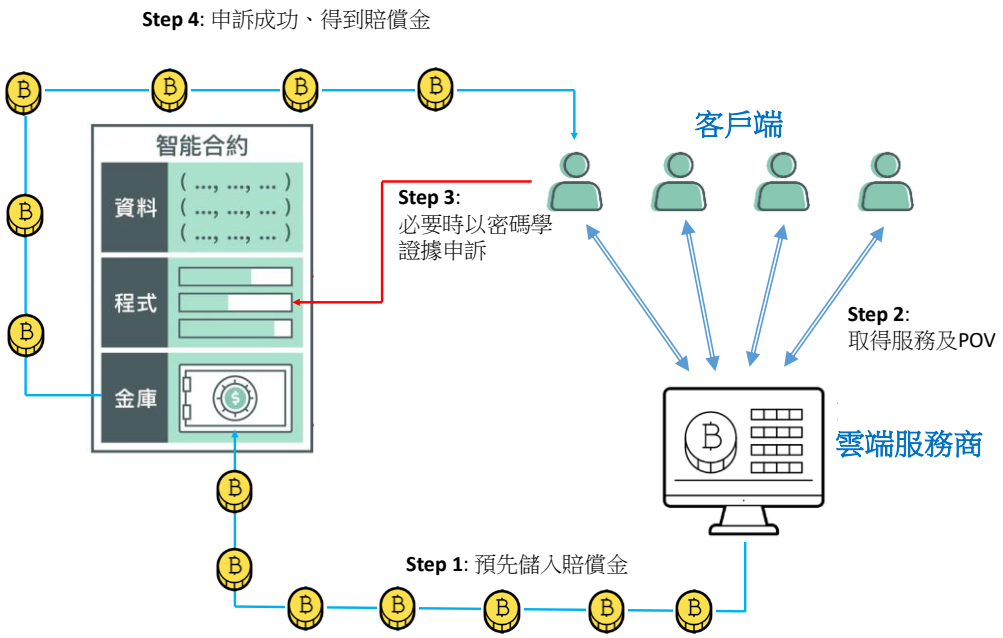
圖二說明了我們要發展及實作的自動賠償機制，首先雲端服務商要公布所採用的 POV 協定，及密碼學證據的格式。同時，將違反 SLA 的申訴程式預先部署在一個智能合約中。接下來：

Step 1: 雲端服務商先將加密貨幣預儲到智能合約的金庫中。所有的客戶都可以查詢此儲金的量，作為服務的保證。

Step 2: 客戶端使用雲端服務商公布的 POV 協定取得雲端服務商的服務，每個 Transaction 結束後都根據得到的密碼學證據驗證服務是否有違反 SLA。

Step 3: 如果發現有違反 SLA 的狀況，則使用 Step 2 得到的證據呼叫智能合約中的申訴函示。

Step 4: 申訴成功，加密貨幣由合約直接即時轉到申訴客戶端的位址。



圖二：自動賠償機制運作說明

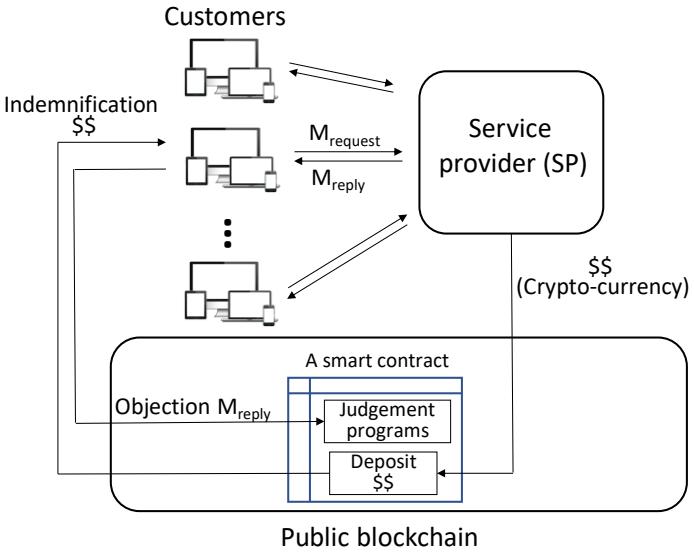
隨著雲端系統提供服務的種類不同，POV 協定及產生密碼學證據的格式及長度當然也不同。目前為止我們可以提供的 POV 技術有雲端檔案系統[30]、雲端資料庫[31]、雲端系統的 Availability[34]、及雲端系統的 Response Time[35]。但是區塊鏈上的智能合約上的抗議上的抗議及申訴函式的撰寫不是沒有限制的，比如以太坊的智能合約有每個函式的執行運算量的限制，目前為大約八百萬個 GAS[36]。所以我們必須實際實驗，瞭解 POV 協定所產生的密碼學證據的大小是否能在申訴函式的運算不超過區塊鏈上的限制。必要時一個申訴函式必須切分成數個子函式來運作，以解決此問題。

結果

實作的自動賠償系統運行在以太坊公有區塊鍊上，首先 SP 佈署智能合約用於判定 SP

是否有違反相關協定，若是違約則將合約中之加密貨幣發送給受影響的客戶作為補償，客戶與 SP 透過一種安全協議進行互動，稱為 request message($M_{request}$)、reply message(M_{reply})，分別由客戶與 SP 簽名後發送。見圖三。

透過 real-time auditing 及 proof of violation (POV)雲端檔案系統解決方案，POV 將產生密碼學證據使得客戶與 SP 釐清違約之責任歸屬，搭配一種 FBHTree 取證架構作為客戶端與 SP 之間的互動協議基礎。



圖三：系統架構

可能的申訴型態計有以下四種，見表一:

表一: 抗議型態及理由

	Objection type	Objection reason
Accept = "YES"	A	SN is wrong.
	B	RH and (Slices, Sets of PB-pairs) does not match.
Accept = "NO"	C	SN and preRH in $M_{request}$ is correct but SP does not accept.
	D	SN and preRH in $M_{request}$ is correct but SP gives an incorrect value of SN or preRH in M_{reply}.

表二列出布署合約需要支付的礦工費用、表三列出要將加密貨幣存入智能合約的費用:

表二: 布署合約需要支付的礦工費用

Gas consumption	Gas Price	ETH	USD
2,307,845	Fastest (20 Gwei)	0.046157	4.61569
	Faster (10 Gwei)	0.023079	2.30785
	Average (4 Gwei)	0.009231	0.92314
	Cheap (3 Gwei)	0.006924	0.69235

表三: 加密貨幣存入智能合約的費用

Gas consumption	Gas Price	ETH	USD
21,491	Fastest (20 Gwei)	0.0004298	0.042
	Faster (10 Gwei)	0.0002149	0.021
	Average (4 Gwei)	0.0000860	0.008
	Cheap (3 Gwei)	0.0000645	0.006

表四、五、六、七分別列出在合約上發起 type-A, B, C, D 的抗議所需的礦工費。

表四: Miner fees required to raise a type-A objection

Height of FBHTree	Ψ[2]	Gas consumption	ETH		USD	
			Gas price (3 Gwei)	Gas price (20 Gwei)	Gas price (3 Gwei)	Gas price (20 Gwei)
14	1	146,639	0.000439917	0.00293278	0.04399	0.29328
	10	168,109	0.000504327	0.00336218	0.05043	0.33622
16	1	156,244	0.000468732	0.00312488	0.04687	0.31249
	10	178,165	0.000534495	0.0035633	0.05345	0.35633
18	1	166,300	0.0004989	0.003326	0.04989	0.33260
	10	187,646	0.000562938	0.00375292	0.05629	0.37529
20	1	175,715	0.000527145	0.0035143	0.05271	0.35143
	10	197,895	0.000593685	0.0039579	0.05937	0.39579
21	1	181,063	0.000543189	0.00362126	0.05432	0.36213
	10	202,796	0.000608388	0.00405592	0.06084	0.40559

表五: Miner fees required to raise a type-B objection

Height of FBHTree	Ψ	Gas consumption	ETH		USD	
			Gas price (3 Gwei)	Gas price (20 Gwei)	Gas price (3 Gwei)	Gas price (20 Gwei)
14	1	458,182	0.001375	0.0091636	4.58182	30.54547
	10	497,272	0.001492	0.0099454	4.97272	33.15147
16	1	483,125	0.001449	0.0096625	4.83125	32.20833
	10	538,658	0.001616	0.0107732	5.38658	35.91053
18	1	524,894	0.001575	0.0104979	5.24894	34.99293
	10	583,355	0.00175	0.0116671	5.83355	38.89033
20	1	569,393	0.001708	0.0113879	5.69393	37.95953
	10	624,815	0.001874	0.0124963	6.24815	41.65433
21	1	590,161	0.00177	0.0118032	5.90161	39.34407

[2] Ψ is the number of PB-pairs in the leaf node.

	10	645,011	0.001935	0.0129002	6.45011	43.00073

表六: Miner fees required to raise a type-C objection

Height of FBHTree	Ψ	Gas consumption	ETH		USD	
			Gas price (3 Gwei)	Gas price (20 Gwei)	Gas price (3 Gwei)	Gas price (20 Gwei)
14	1	220,904	0.000663	0.004418	2.20904	14.72693
	10	246,582	0.00074	0.004932	2.46582	16.43880
16	1	235,595	0.000707	0.004712	2.35595	15.70633
	10	261,341	0.000784	0.005227	2.61341	17.42273
18	1	249,968	0.00075	0.004999	2.49968	16.66453
	10	276,037	0.000828	0.005521	2.76037	18.40247
20	1	265,045	0.000795	0.005301	2.65045	17.66967
	10	290,735	0.000872	0.005815	2.90735	19.38233
21	1	271,949	0.000816	0.005439	2.71949	18.12993
	10	645,011	0.001935	0.0129002	6.45011	43.00073

表七: Miner fees required to raise a type-D objection

Height of FBHTree	Ψ	Gas consumption	ETH		USD	
			Gas price (3 Gwei)	Gas price (20 Gwei)	Gas price (3 Gwei)	Gas price (20 Gwei)
14	1	258,614	0.000776	0.005172	2.58614	17.24093
	10	304,230	0.000913	0.006085	3.04230	20.28200
16	1	277,890	0.000834	0.005558	2.77890	18.52600
	10	323,064	0.000969	0.006461	3.23064	21.53760
18	1	299,603	0.000899	0.005992	2.99603	19.97353
	10	343,566	0.001031	0.006871	3.43566	22.90440
20	1	319,268	0.000958	0.006385	3.19268	21.28453
	10	365,092	0.001095	0.007302	3.65092	24.33947
21	1	329,293	0.000988	0.006586	3.29293	21.95287

結果與討論

本計畫提出一種基於公有於區塊鏈的自動賠償機制。客戶端與服務供應商(SP)透過相關協議交換簽名消息，當客戶端發現 SP 違反基於密碼學證明之服務協議時，他們可以對區塊鏈上的 smart contract 提出申訴。通過區塊鏈合約程序判定申訴成功後，申訴者將獲得加密貨幣作為賠償。

如此一來無需建立需要雇用人員的客服中心處理此類索賠及退款，也不再需要傳統的可信第三方。對於雲端存儲系統，我們提出了以太坊中的賠償制度之協議和實作，並由實驗證明了

所提出之系統的可行性。

下一步我們將進一步整理相關的實驗數據發表論文，並尋求工業界合作的可能。初步論文發表，如下：

- Blockchain-based Automatic Indemnification Mechanism based on Proof of Violation for Cloud Storage Services. Gwan-Hwan Hwang, Pei-Chun Tien, and Yi-Hsiang Tang. **Accepted for publication in The 2nd International Conference on Blockchain Technology (ICBCT 2020)** , Hilo, Hawaii, USA, March 12-14, 2020. (will be published by ACM, Corresponding author: Gwan-Hwan Hwang)

References

1. "Google Drive," https://drive.google.com/start#home.
2. "Dropbox," https://www.dropbox.com/home.
3. "SugarSync," https://www.sugarsync.com/.
4. "Microsoft SkyDrive," http://skydrive.live.com/.
5. "Box," http://www.box.net.
6. Kamara S, Lauter K. Cryptographic cloud storage, Financial Cryptography Workshops, 2010, pp. 136–149.
7. Feng J, Chen Y, Summerville D, Ku WS, Su Z. Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol, IEEE Consumer Communications and Networking Conference (CCNC), 2011.
8. Shraer A, Keidar I, Cachin C, Michalevsky Y, Cidon A, Shaket D. Venus: verification for untrusted cloud storage, ACM CCSW 2010.
9. AMAZON. "Amazon S3 Service Level Agreement,". http://aws.amazon.com/s3-sla/.
10. MICROSOFT CORPORATION. "Windows Azure Pricing and Service Agreement," http://www.microsoft.com/windowsazure/pricing/.
11. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," In USENIX FAST (2003).
12. A. Adya, W. Bolosky, M. Castro, G. Cermak, R. Chaiken, J. Douceur, J. Howell, J. Lorch, M. Theimer, and R. Wattenhofer, "FARSITE: Federated, Available, and Eliable Storage for an Incompletely Trusted Environment," In OSDI, pages 1–14, December 2002.
13. J. Kubiatowicz, D. Bindel, Y. Chen, S. Czerwinski, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao. "Oceanstore: An Architecture for Global-scale Persistent Storage," In ASPLOS, December 2000.
14. G. Ganger, P. Khosla, M. Bakkaloglu, M. Bigrigg, G. Goodson, S. Oguz, V. Pandurangan, C. Soules, J. Strunk, and J. Wylie. Survivable storage systems. In DARPA Information Survivability Conference and Exposition, IEEE, volume 2, pages 184–195, June 2001.
15. P. Druschel and A. Rowstron. Storage management and caching in PAST, a large-scale, persistent peerto-peer storage utility. In SOSP, 2001.
16. J. Strunk, G. Goodson, M. Scheinholtz, C. Soules, and G. Ganger, "Self-securing storage: protecting data in compromised systems," In OSDI, October 2000.
17. Yves Deswarte, Jean-Jacques Quisquater, and Ayda Saïdane, "Remote Integrity Checking," IFIP International Federation for Information Processing Volume 140, 2004, pp 1-11.

18. Ari Juels, Burton S. Kaliski Jr.: Pors: proofs of retrievability for large files. ACM Conference on Computer and Communications Security 2007: 584-597.
19. Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu, “Dynamic Audit Services for Outsourced Storages in Clouds,” IEEE Transactions on Services Computing, , VOL. 6, NO. 2, 2013.
20. Kan Yang and Xiaohua Jia, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing,” IEEE Transactions on Parallel and Distributed Systems, VOL. 24, NO. 9, 2013.
21. Goh E-J, Shacham H, Modadugu N, Boneh D. Sirius: securing remote unstrusted storage, In NDSS (2003).
22. Li J, Krohn M, Mazie`res D, Shasha D, SUNDR: secure untrusted data repository, In OSDI (2004).
23. Cachin C, Shelat A, Shraer A. Efficient fork-linearizable access to untrusted shared memory. In Proc. 26th ACM Symposium on Principles of Distributed Computing (PODC), 2007; 129–138.
24. Majuntke M, Dobre D, Serafini M, Suri N. Abortable fork-linearizable storage. In Abdelzaher TF, Raynal M, Santoro N (eds), Proc. 13th Conference on Principles of Distributed Systems (OPODIS), volume 5923 of Lecture Notes in Computer Science, 2009; 255–269.
25. Cachin C, Geisler M. Integrity protection for revision control. In Abdalla M, Pointcheval D (eds), Proc. Applied Cryptography and Network Security (ACNS), volume 5536 of Lecture Notes in Computer Science, 2009; 382–399.
26. E. Stefanov, M. van Dijk, A. Oprea, and A. Juels, “Iris: A scalable cloud file system with efficient integrity checks,” The 28th Annual Computer Security Applications Conference (ACSAC 2012). ACM, 2012.
27. Raluca Ada Popa, Jacob R. Lorch, David Molnar, Helen J. Wang, and Li Zhuang “Enabling Security in Cloud Storage SLAs with CloudProof,” Proceeding USENIXATC'11 Proceedings of the 2011 USENIX conference on USENIX annual technical conference, Pages 31-31.
28. Gwan-Hwan Hwang, Jenn-Zjone Peng, and Wei-Sian Huang, “A Mutual Nonrepudiation Protocol for Cloud Storage with Interchangeable Accesses of a Single Account from Multiple Devices,” The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-2013), Melbourne, Australia, 16-18 July, 2013.
29. Gwan-Hwan Hwang, Wei-Sian Huang, and Jenn-Zjone Peng, “Real-time Proof of Violation for Cloud Storage,” The 2014 6th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2014), December 27-29, 2014, Singapore.
30. Gwan-Hwan Hwang and Hung-Fu Chen, “Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems,” The 9th IEEE International Conference on Cloud Computing (IEEE Cloud 2016), June 27 - July 2, 2016, San Francisco, USA.
31. 『雲端資料庫系統的即時稽核及行為違反驗證』、106-2221-E-003-001、106.8.31~107.7.31。
32. K. Mouratidis, D. Sacharidis, and H. Pang, “Partially materialized digest scheme: An efficient verification method for outsourced databases,” VLDB J., vol. 18, pp. 363–381, 2009.
33. Thomas Locher, Sebastian Obermeier, Yvonne-Anne Pignolet, "When Can a Distributed Ledger Replace a Trusted Third Party?" IEEE Blockchain 2018.
34. Gwan-Hwan Hwang and Shang-Yu Yeh, “Proof of Violation for Availability in Cloud Computing,” in the 15th IEEE/ACIS International Conference on Computer and Information Science (IEEE/ACIS ICIS 2016), June 26-29, 2016, Okayama, Japan.

35. Proof of Violation for Response Time Auditing in Cloud Systems. Gwan-Hwan Hwang and Yi-Ling Yuan. Journal of Supercomputing (Accepted).
36. http://gavwood.com/Paper.pdf. Accessed 10 Apr 2018.

科技部補助國內專家學者出席國際學術會議報告

2020 年 12 月 31 日

報告人姓名	黃冠寰	服務機構及職稱	國立台灣師範大學 資訊工程學系 教授
會議時間地點	March 12-14, 2020, University of Hawaii-Hilo, Hawaii, USA.		
會議名稱	(中文) 2020 第二屆區塊鏈國際技術研討論會 (英文) 2020 The 2nd International Conference on Blockchain Technology (ICBCT 2020)		
發表論文題目	(中文) 以行為違反驗證為基礎的區塊鏈自動賠償系統 (英文) Blockchain-based Automatic Indemnification Mechanism based on Proof of Violation for Cloud Storage Services		

因為 Covid-19 的原因，選擇不出席會議，於會議中採用 on-line 發表。有上簽文給學校請示不出席會議但是仍然由計畫中的出國經費報支會議註冊費用（author registration）。機票及旅館預定只好作部分退費。

108年度專題研究計畫成果彙整表

計畫主持人：黃冠寰	**計畫編號：**108-2221-E-003-004-
計畫名稱：雲端系統服務層級協議違反之自動賠償機制的研究	

成果項目			量化	單位	質化 （說明：各成果項目請附佐證資料或細項說明，如期刊名稱、年份、卷期、起訖頁數、證號...等）
國內	學術性論文	期刊論文	0	篇	
		研討會論文	0		
		專書	0	本	
		專書論文	0	章	
		技術報告	0	篇	
		其他	0	篇	
國外	學術性論文	期刊論文	0	篇	
		研討會論文	1		Blockchain-based Automatic Indemnification Mechanism based on Proof of Violation for Cloud Storage Services. Gwan-Hwan Hwang, Pei-Chun Tien, and Yi-Hsiang Tang. Accepted for publication in The 2nd International Conference on Blockchain Technology (ICBCT 2020), Hilo, Hawaii, USA, March 12-14, 2020. (will be published by ACM, Corresponding author: Gwan-Hwan Hwang)
		專書	0	本	
		專書論文	0	章	
		技術報告	0	篇	
		其他	0	篇	
參與計畫人力	本國籍	大專生	0	人次	
		碩士生	0		
		博士生	0		
		博士級研究人員	0		
		專任人員	0		
	非本國籍	大專生	0		
		碩士生	0		
		博士生	0		
		博士級研究人員	0		
		專任人員	0		
其他成果 （無法以量化表達之成果如辦理學術活動					

、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。）	