2019 智慧企業資訊應用發展國際研討會 台灣，
2019/06/29(六)

基於狀態的可修改智能合約

劉皪
國立政治大學 資訊管理學系
106356003@nccu.edu.tw

林韋廷
國立政治大學 資訊管理學系
106356001@nccu.edu.tw

郁方
國立政治大學 資訊管理學系
yuf918@gmail.com

蕭舜文
國立政治大學 資訊管理學系
hsiaom@gmail.com

摘要

部署在區塊鏈上的智能合約意味著不可改變；然而在不同的時間點，各方在實作的過程中，實作的方向跟內容可能會有改變。例如，修復安全問題，因此合約需要被調整或修改。我們提出了一種基於狀態的智能合約框架，可以讓合約順利被修改，已部署的智能合約可以部分地更新邏輯，同時保持先前的狀態一致。

具體來說，我們將普通合約劃分為四種不同類型的合約，在框架中合約分別負責不同部分。控制合約使用有限狀態機管理控制邏輯，其中狀態受版本控制保護以區分合約的不同版本；儲存合約會負責儲存不同使用者每一個狀態下的全域變數；主要合約實作應用邏輯的主要部分；更新契約實作以基於狀態的方式設計的程式碼，如此會比較容易更新合約內容。

並且，我們已經實施了概念驗證保險智能合約，如何在此框架下開發、部署、執行和更改可修改的智能合約。

關鍵詞：區塊鏈、智能合約、有限狀態機、Solidity

Abstract

This sample document provides the authors with instructions to prepare camera-ready abstract. The abstract should summarize the contents of the paper within 250 words, written in English, A4 paper, single-spaced, justified, with a font size of 9.5pt Times New Roman. In the first page, the title should be written centered, in 9.5pt, boldface Times New Roman, initial capital letters and the authors' names, affiliations, and e-mail addresses should be written centered, in 9.5pt, Times New Roman. Please do not number the pages for your paper. The file should be in Windows Microsoft Word format.

Keywords: Blockchain, Smart Contract, Finite state machine, Solidity