致理科技大學

資訊管理系專題報告

智能合約開發問題與風險專題
Problems and Risks of Smart Contract Development Process

專題生：60810119 陳禹丞
60810126 葉長翰
60810156 吳冠逸
60810175 游承憲
60810187 薛聿惟
60710106 蘇秀汝

指導教授：曲莉莉 老師

中華民國 112 年 5 月

致理科技大學

資訊管理系

畢業專題

智能合約開發問題與風險

一一一學年度

致理科技大學

專題報告審核書

本校 資訊管理 系（所） 陳禹丞(60810119)

葉長翰(60810126)、吳冠逸(60810156)、游承

憲(60810175)、薛聿惟(60810187)、蘇秀汝

(60710106)

等君所提論文 智能合約開發問題與風險

經本委員會審定通過，特此證明。

口試委員會

委員：_____

_____

_____

指導教授：_____

系主任：_____

中華民國 112 年 5 月

致理科技大學

授權書

本授權書所授權之專題報告在致理科技大學

111 學年度第 1 學期所撰寫。

專題名稱：智能合約開發問題與風險

本人具有著作財產權之論文或專題提要，授予致理科技大學，得重製成電子資料檔後收錄於該單位之網路，並與台灣學術網路及科技網路連線，得不限地域時間與次數以光碟或紙本重製發行。

本人具有著作財產權之論文或專題全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限時間與地域，惟每人以一份為限。並可為該圖書館館藏之一。

本論文或專題因涉及專利等智慧財產權之申請，請將本論文或專題全文延至民國 年 月 日後再公開。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。

(上述同意與不同意之欄位若未勾選,本人同意視同授權)

☐同意 ☐不同意

學生簽名：

(親筆正楷簽名)

指導老師姓名：

(親筆正楷簽名)

中華民國 112 年 5 月 日

摘要

專題報告名稱： 智能合約開發問題與風險　　頁數：總頁數 57

校系別：致理科技大學資訊管理系

完成時間：111 學年度第 1 學期

專題生： 陳禹丞、吳冠逸、葉長翰、游承憲、薛聿惟、蘇秀汝

指導教授： 曲莉莉

關鍵詞：智能合約、區塊鏈、電子錢包、資安風險

近年來區塊鏈技術被廣泛運用，相關應用如雨後春筍般相繼而出，其中智能合約是一種特殊協定，在區塊鏈內制定合約時使用，智能合約被放入去中心化的區塊鏈平台，並分佈於各個節點之間，等待執行合約，當中內含了程式碼函式，亦能與其他合約進行互動、做決策、儲存資料及傳送以太幣等功能。這次專題應用 Solidity 開發智能合約，利用 Ganache 電子錢包平台測試程式可行性，讓應用程式開發智能合約使交易變得更透明。

部署在許可私有區塊鏈上的私有智能合約的特點和風險是不同的。私有區塊鏈和智能合約的一個屬性是擁有一個網絡管理員，可以是一個人、一組人或一組規則，這使其成為網絡攻擊的目標。它的另一個重要特徵是代碼的不變性 。因此，它不允許任何部分單獨更改編寫的代碼或術語。它可以防止對代碼的有害網絡攻擊，因為網絡管理員會被警告可能試圖更改代碼的入侵。作為附加屬性，交易是可追溯的並永久記錄在區塊鏈中。 信息安全雜誌> Vol.10 No.1, January 2019。

藉由程式開發過程及文獻探討我們發現區塊鏈常見的風險包括 51%安全性攻擊、私鑰保管、犯罪活動、雙重支付問題、資訊洩漏等問題，另外在交易過程中，如果沒有按照正確的順序執行或礦工惡意修改區塊的時間戳記，都可能影響智能合約的正確性。

智慧型合約允許在沒有第三方的情況下進行可信交易且這些交易可追蹤但不可逆轉，並減少與合約相關的其他交易成本。我們希望最終智能合約可以完成上述內容並解決當前智能合約之不足，完善其機制，改善當前智能合約所遭遇到的問題，並且能將該區塊鏈智能合約應用於商業開發行為中，加速交易速度及安全性。

ABSTRACT

ThesisTitle： Risks of smart contract development process Pages：58

University：Chihlee University of Technology

Graduate School：Departmant of Information Management

Date： November, 2022 Degree：Master

Researcher： Chen,Yu-Cheng、Wu,Guan-Yi、Yeh,Chung-Han 、 Yu,Cheng-Sian、 Syue,Yu-Wei 、Su,Siou-ru

Advisor： Chu,Li-Li

Keywords： Smart contracts, blockchain, e-wallets, Information security risk

In recent years, blockchain technology has been widely used, and related applications have sprung up one after another. Among them, smart contracts are a special agreement that is used when formulating contracts in the blockchain, and smart contracts are put into the decentralized blockchain platform. , and distributed among various nodes, waiting for the execution of the contract, which contains code functions, which can also interact with other contracts, make decisions, store data, and transmit ether. In this special topic, Solidity is used to develop smart contracts, and the Ganache e-wallet platform is used to test the feasibility of the program, allowing applications to develop smart contracts to make transactions more transparent.

The characteristics and risks of private smart contracts deployed on permissioned private blockchains are different. One property of private blockchains and smart contracts is having a network administrator, which can be a person, a group of people, or a set of rules, which makes them a target for cyberattacks. Another important feature of it is the immutability of the code. Therefore, it does not allow any part to change written code or terminology alone. It prevents harmful cyber-attacks on the code, as network administrators are alerted to intrusions that might try to change the code. As an additional property, transactions are traceable and permanently recorded on the blockchain. Journal of Information Security> Vol.10 No.1, January 2019.

Through the program development process and literature discussion, we found that the common risks of blockchain include 51% security attacks, private key custody, criminal activities, double payment problems, information leakage and other issues. Sequential execution or malicious modification of block timestamps by miners can affect the correctness of smart contracts.

Smart contracts allow for trusted transactions that are traceable but irreversible without third parties, and reduce other transaction costs associated with contracts. We hope that the final smart contract can complete the above content and solve the shortcomings of the current smart contract, improve its mechanism, improve the problems encountered by the current smart contract, and apply the blockchain smart contract to business development behaviors to speed up transactions and safety.

誌謝

這次的智能合約開發與風險專題報告，除了感謝全體組員的全力配合，最重要要感謝的是教導我們四年的各科專業老師們的諄諄教誨，大家有緣來自不同領域的名門貴校，今天參與這個專案主題，相信對大家都是一個全新領域。
經過不斷的磨合與相互探討，才有今日專題的完成，有人網頁搜尋可用資料、有人藉由讀書搜尋可用資源加以豐富專題的內容，探討程式的可用性同學更是殫精竭力不能恍惚。當大家在徬徨無助之時專題老師，總是給予適當建議，讓我們能順利的勇往向前邁進一步。

所有組員姓名　謹致
致理科技大學 資訊管理　學士班
中華民國 111 年 12 月

目錄

圖目錄

表目錄

第壹章　緒論

智能合約是什麼?在 1990 年代 Nick Szabo 首次描述了智能合約，那時他將智能合約定義為一種工具，透過協定與使用者介面結合，將電腦正規化並確保其安全性。在加密貨幣的世界裡我們把智能合約定義為一個在區塊鏈上運行的應用程式或程序，通常的情況下它做為一種數位協定工作，由一組特定的規則來強制執行。這些規則由電腦程式碼預先定義，由所有網路節點複製和執行。區塊鏈智能合約允許建立去信任化協定，這表示雙方可以特過區塊鏈做出承諾，而不必去認識或信任對方，他們肯定如果條件不滿足，合約就不會被執行。除此之外智能合約可以消除對中介的需求，大大降底營運的成本。

第 一 節　研究背景

智慧合約於 1994 年由一名身兼電腦科學家及密碼學專家 Nick Szabo 首次提出。智慧型合約是一種特殊協定，在區塊鏈內製定合約時使用，當中內含了程式碼函式，亦能與其他合約進行互動、做決策、儲存資料及傳送以太幣等功能。自從中本聰在 2008 年《比特幣白皮書》中提出「區塊鏈」的概念後，Nick Szabo 的想法才得以被逐步實現。智慧型合約主要提供驗證及執行合約內所訂立的條件。智慧型合約允許在沒有第三方的情況下進行可信交易。這些交易可追蹤且不可逆轉。智慧型合約的目的是提供優於傳統合約方法的安全，並減少與合約相關的其他交易成本。

第 二 節　研究動機

因應疫情，線上辦公模式變為常態，因此我們利用比特幣區塊鏈，訂定了一個以區塊鏈為基礎的程式，為每個交易需求提供安全快速的線上合約平台，以此製作「智能合約」。我們可以把智能合約想像成「自動販賣機」，這樣比較容易理解它的功用及運作方式。自動販賣機能接受並執行外部所給的指令，顧客選定欲購商品並按下選擇鍵，隨後付款即可。首先，我們將資產與擬定的合約條款編碼放入區塊鏈的區塊中，智能合約會在區塊鏈平台中的節點之間多次複製與傳遞資訊。一旦合約中觸發時間被啟動，智能合約就能按照其內容所設定的條款執行，並自動檢查所承諾的條款實施情形如何。以上藉由此開發的歷程，研究並探討智能合約可能遇到的困境與風險。

具體而言本專題研究動機有三：

動機一、國人對區塊鏈之了解程度。

動機二、近年來 NFT 區塊鏈崛起，相關應用開始崛起，智能合約應用也備受關注

動機三、智能合約之風險。2021 年加密貨幣全行業公開報道的安全事故至少有 189 起，至少有 76 億美元的加密資產在這些安全事故中損失。

第 三 節　研究目標

依據維基百科定義智慧型合約內容，本專題希望創造一份智能合約其中包含要素有合約主體（Subject of Contract）、數位簽名、合約條款及去中心化平台

（decentralized platform）。合約主體：智能合約中必須要有合約主體，如此一來才能在智能合約的程式中自動鎖定及解開合約中的相關商品及服務。數位簽名：智能合約需要所有參與者透過他們的私鑰（private key）進行認證之後，才能被啟動。合約條款：此智能合約中的條款所有的操作順序，皆須由所有參與者認同並簽署後才可執行。去中心化平台：讓使用者可以很容易地透過部署一個智能合約，來提供運行於以太坊上的新加密代幣，這份智能合約相容於 ERC20 標準，使用者不需要重新開發從挖礦到交易的整個代幣生態系，使此應用可以更加普及，讓各商業團體，企業都能快速上手省去企業額外成本，而我們希望本智能合約能夠達成的目的有上述的省時省力更希望安全性能優於原始的電子契約，接著解決開發過程中所經歷之問題，提供解決方案並修正後，建立可行之程式。

具體而言本專題研究目的有三：

目標一、本專題將透過問卷發放探討國人對智能合約之了解程度，也順便探討其應用在當前社會之覆蓋程度。

目標二、本專題將探討智能合約的開發過程所遭遇的風險。

目標三、本專題將研究智能合約的問題，修正問題並搭建可行的程式。

第貳章　文獻回顧與探討

本章節主要探討區塊鏈概念及背景知識，區塊鏈發展至今已有深厚技術來支持，其衍伸出許多便捷的應用，以太坊、數位憑證、智能合約等等。其中智能合約即是本文的重點應用，智能合約是以太坊中重要的一環，其運用在商業交易當中使交易流程更加便利安全，她的發展過程及資安風險，是本文章主要研究方向，當中法規及資安風險是我們十分在乎的問題，我們將在以下篇幅進行討論。

第 一 節　區塊鏈與智能合約

2015 年區塊鏈平台－以太坊(Ethereum)提出「新一代智慧合約與分散式應用平台」，使智慧合約成為區塊鏈另一個主要應用場域，被視為「區塊鏈 2.0」的主要技術與應用(林詠章，2019) 。「智慧合約」不見得只限於金融業。如果搭配「智慧財產所有權」(smart property)，也就是契約、權力資格，以及其他所有權的證明，全都轉化成數位形式並由軟體運作執行，這些合約允許自動轉以實體資產如房屋或汽車，或者無形資產如專利權的所有權，同樣的軟體會在合約的責任義務符合條件時開始進行轉移。智能合約研究問題的範圍包含醫療保險、慈善捐款、商業行為、金融科技，智能合約擁有傳統合約的約束性及法律性，並去除傳統合約的缺點，有了完善的機制，讓智能合約的開發路程更加順利。隨後區塊鏈的發展進入到了區塊鏈 3.0 階段。在這一階段，區塊鏈的潛在作用並不僅僅表現在貨幣、經濟和市場上，更延伸到了政治、人道主義、社交和科學領域，區塊鏈技術方面的能力已經可以讓特殊的團體來處理現實中的問題，區塊鏈技術或許將廣泛而深刻的改變人們的生活方式，並重構整個社會，重鑄信用價值，也許將來區塊鏈技術發展到一定程度時，整個社會進入到區塊鏈時代，透過區塊鏈技術來分配社會資源，或許區塊鏈將成為一個促進社會經濟發展的理想框架。蔣亮/李啟雷/梁秀波(2019)，企業級區塊鏈技術開發實戰

區塊鏈技術的崛起引發各個產業莫大的興趣，也進而讓智能合約迅速發展，然而法規想跟上科技的腳步，總是要經歷層層關卡，而新的科技技術也帶來新的法律上的挑戰，有關智能合約的法律議題多樣，其涵蓋面向包括民刑法、智慧財產權法、個資保護到金融監理以及其他產業特別法規 (林玫君，2019)。可見法規的完整性及前段的安全性問題仍然是智能合約的需要跨過的門檻。

近年來許多新起的公有鏈平台也都相容以太坊的智慧合約架構，使用「Solidity」作為智慧合約的主要開發語言。然而智慧合約建置的效能及安全性卻是程式開發者常常忽略的，目前 Solidity 已知的安全性問題有 DOS、阻止時間戳操作或是運用身分驗證進行釣魚攻擊，除了安全性之外的問題，還有區塊鏈交易當中的隱性成本，智能合約會因為程式瑕疵邏輯問題而導致區塊鏈中的礦工費損耗，這些漏洞也會導致資安風險，據統計智慧合約撰寫的效能不良及安全漏洞所造成的損失，已僅次於區塊鏈錢包 (林詠章,林久弘，2018)。資訊安全為智能合約當前所面對之重要風險，若無法有效對應，智能合約將無法進行有效應用，以下將介紹目前已知風險及其可能解。

第 二 節　區塊鏈技術創造期

區塊鏈出現在 1991 年當時 W.Scott Stormetta 和 Stuart Haber 討論了是界公認的”區塊鏈”他們早期包括塑造一個安全的區塊鏈，沒有人可以更改紀錄的時間

戳。1992 年他們更新了技術已鞏固克爾樹，從而提高了熟練度，提供了關於單個區塊的更多報告分類。在 2008 年當中本聰將他對區塊鏈的想法植入於區塊鏈領域時，”區塊鏈”一詞變得重要。區塊鏈在三個用例中表現出色

數據認證和驗證:它側重於加密、不靈活的存儲和數字簽名、創建私鑰和公鑰以及驗證數位簽名。

智能資產管理:重點關注支付、收入、貿易、債券和退休。在加密貨幣中，現實世界的財產以代幣形式表示，例如土地、基礎設施、黃金、白銀等。智能合約著重於交易商和買家之間通過合約進行交易。

一、 選擇區塊鏈平台

在決定使用哪個區塊鏈平台時，作為開發人員，您應該考慮平台的擴展性和吞吐量、信息結構:文檔的質量、結構以及外部教程或指南的可用性，評估社區的力量、所需的開發經驗:新手開發人員開始使用特定的區塊鏈平台有多容易?

漏洞賞金或激勵計畫的可用性、支持開發人員工具的可用性，以增加開發人員的體驗。(米歇爾·穆德斯，2022)

二、 節點設計

區塊鏈系統可以設計私有/公有、無許可以及有許可，甚至混合。在此步驟鑰考慮另一個重要因素是節點在本地運行還是在雲中運行，與硬件配置(處理器、內存和磁盤大小)相關的操作系統和任務的選擇也將在此步驟完成。

三、 設計區塊鏈參數配置

通常區塊鏈平台需要對權限、原子交易、密鑰管理、資產發行、多重簽名、地址格式、握手等元素進行測底配置。

四、 API

大多數平台提供構建的 API，而其他平台則不提供，您需要解決 API 的問題是:用於開發密鑰地址、進行可審計的流程、使用哈希和數字簽名執行數據驗證、用於保存數據及其恢復、管理智能資產:即分配、債券、捐獻、業物等、創建智能合約。

五、 構建管理和用戶介面

這一步您將選擇編程語言，必須選擇外部數據庫和服務器。

六、 添加人工智能

通過添加人工智能(AI)、雲、數據分析、生物識別、機器學習和機器人來提升區塊鏈解決方案的潛力。

第 三 節 智能合約中的安全攻擊、漏洞和安全解決方案

用於智能合約的編程語言可以使用普通軟件編程語言，如:Java、

Javascript、GoLang，這些語言被設計成圖靈完備以實現全部功能。它一樣會面臨人為錯誤，由於智能合約已部署到所有節點，因此它造成的錯誤是指數級的。因為一旦部署了代碼它將分布在整個網路，使得它更難像普通程序一樣修補，因此程序員必須確保合約程序沒有錯誤。程序員能夠使用專用網路來模擬攻擊或正式的滲透測試，以評估智能合約對攻擊的響應。

一、 不同的攻擊和漏洞

智能合約上下文中存在大量攻擊。導致這些攻擊的原因有很多，例如編程錯誤、編程語言的限制和安全漏洞。這些攻擊的結果包括區塊鏈網絡及其準確性的許多複雜性、本地加密貨幣的丟失以及系統可用性的終止。

二、 重新進入漏洞

一般而言，當一個智能合約迭代調用另一個智能合約並且啟動調用的智能合約是惡意的時，利用的重入漏洞。這樣的攻擊在以太坊平台上很常見。一名匿名黑客從 2016 年通過虛擬風險資本籌集的 1.68 億投資中竊取了價值 5000 萬美元的 ETH 稍後平衡而不檢查它是否是遞歸調用。攻擊者遞歸調用拆分函數並在代碼檢查餘額之前檢索他們的資金。

三、 下溢/上溢錯誤

當特定算術運算的結果小於或大於智能合約平台中使用的最小或最大數字數據類型時，就會發生下溢或溢出。以太坊平台正在使用 uint256 。從概念上講，0 的 Ether 餘額可以轉換為 uint256 的最大值，或者最大值的 Ether 餘額可以轉換為 0。但是，程序員在編寫合約時需要考慮這種情況

四、 多數攻擊

大多數攻擊發生在一些惡意用戶或團體接管控制以重寫交易歷史或阻止新交易確認時。當特定區塊鏈聯盟採用多數投票共識時，可能會發生攻擊。根據用戶的要求，有時區塊挖掘和交易驗證會被卸載到聯盟每個成員的一些專門的領先同行。如果大多數領先的同行被惡意用戶劫持，也會發生類似的情況。

五、 可銷毀合約

自毀漏洞通過刪除特定地址的字節碼來刪除智能合約的內容。此外，它將所有合約的資金發送到特定的目標地址，使合約無法運行。

六、 無界計算能力密集型運算

智能合約上的每個操作都需要消耗計算能力。例如，以太坊中計算能力的成本稱為 Gas。用於評估智能合約上特定操作的計算資源消耗的氣體。無界和無限制的計算能力密集型操作會導致各種錯誤並最終影響系統。

第 四 節 智能合約所遭遇的風險

任何一個軟體系統都很難做到十全十美，在實際的使用中會經受各種問題的考驗，區塊鏈應用作為一種特有功能的軟體系統，也有自己特有的問題。我們知道，區塊鏈應用是一個點對點的網路程式，透過一個共識規則來進行資料的一致性同步，這個共識規則也就是一個共識演算法，還有一些其他共識演算法，例如

PoS、DPoS 等。這些演算法各自也有很多變種，無論是哪一類，其目標都是一致，誰來運作這些演算法程式，那就是礦工，也就是運作挖礦程式的節點。

礦工透過完成某些證明演算法，得到區塊資料的打包權可以將已經發起但還沒有打包到主鏈的事物資料打包儲存到新的區塊，並且廣播給其他節點，倘若有人透過某種手段，十之八九的機會都被他占有。我們來設想一下當打包權掌握在自己的手裡，能做些什麼事?

一、 修改自己的交易紀錄

我將自己現有的比特幣儲值到某個交易所(這是為了兌換法幣)，然後我計算出一個區塊鏈，包含了一條訊息，例如發送比特幣到自己的位址中。假設這個自己計算的區塊鏈的長度為 10，此時先不向網路廣播這個新的區塊，而是先到交易所平台將自己現有的比特幣換成現金提取出來，這個提取比特幣的交易事務會記錄在正常的區塊鏈中，假設當提取現金時，正常的區塊鏈主鏈的長度還是 9，而我構造的區塊鏈的長度已經是 10 了，此時向網路廣播出去，網路會確認我的區塊鏈是正確的，並且會記錄到主鏈中去。但此時現金已經被我提出來了，而我廣播出去的 10 號區塊(最新的區塊)中並沒有包含我向交易所儲存的紀錄，等於比特幣還在我的位址中。

二、 阻止其他礦工開採到區塊

當運算力優勢非常明顯時，阻止他人挖礦也就是顯而易見能做的到了，這種情況下還會導致其他礦工失去挖礦積極性，導致最後挖礦運算力更佳集中在少數優勢運算力的礦工手裡。

第 五 節 資產轉移風險

智能合約在區塊鏈平台做程式化的資產移轉，而這些資產都是加密貨幣(數位資產)，會必須承擔交易加密貨幣的風險，像是身分詐欺,釣魚錢包，又或是虛擬貨幣交易發生的損耗。整體來說，過去我們在開發程式所需要注意的資安問題，在區塊鏈的應用上亦然。和傳統資安不同的是，當智能合約在區塊鏈平台是做程式化的資產移轉，而這些資產都是加密貨幣（數位資產）時，會必須承擔交易加密貨幣的風險，而通常會比傳統的資安漏洞所造成的財物損失更多、影響範圍更大。

第參章　研究內容與方法

本專題預定做出一個智能合約的程式架構，再依程式開發過程所遇到的問題製作成問卷，其中該問卷目前暫定 10 題，問卷前段放置智能合約的大致介紹後，再進行問卷填寫，使一些零基礎的填寫者有些許了解在填寫問卷，問卷的難度也由淺入深，透過填寫問卷分析大眾對智能合約的看法及了解的深度有多少，也希望透過該份問卷了解大眾對於智能合約的看法或是疑慮，再以問卷最後蒐集到的結果試著提出解決方案，以利於推廣智能合約之應用。

第 一 節　研究流程

本專題的架構流程如下，第壹章介紹了本研究的背景、動機與目的，透過問卷調查了解大眾對於電子契約、合約問題及法規的了解程度等…，在區塊鏈問題上切入帶出現今相關法規問題及其蘊含資安危機，藉此凸顯本專題電子合約的問題，旨在讓大眾能透過此專題，探討未來相關機構對於智能合約的走向及規範為目的之宗旨。第貳章為文獻相關研究，本專題藉由學術論文及相關資料來設定問卷分析、使用者需求調查，整合定義大眾對於區塊鏈之智能合約應用問題，再以結合文獻閱覽引用法規條文參照加以印證，並將其結果運用於專題並支持本研究基於緒論所闡述之背景、動機與目的，第參參章將以「問卷分析法」進行分析後的結果，並將分析結果作下一階段網站建置內容之基礎，以下為本專題研究流程：

1. 研究背景與動機：了解本專題欲研究的主題內容與相關背景脈絡，提出研究構想，並簡單陳述區塊鏈相關歷史脈絡。
2. 研究目的與問題：確定研究構想後制定欲解決之問題，設定本專題研究之方向及目的，提出解決之道並完成程式。
3. 文獻探討：參考閱覽並引用專家學者過去相關研究期刊論文，釐清研究問題並呼應本專題之內容，做為下一階段程式開發設計內容之基礎。
4. 問卷設計並發放：整理研究問題後，設計網路問卷，將問卷發放於社交平台，再將問卷連結張貼給受訪者協助填答。
5. 研究設計：藉由網路了解程式並查閱其設計過程加以改正，並將結果用於設計最終程式的架構及內容。
6. 資料蒐集與分析：整理回收的問卷資料，並將結果進行分析，以用於專題研究之輔助。
7. 成果報告：專題製作完成並進行報告。專題研究流程如圖 3-1

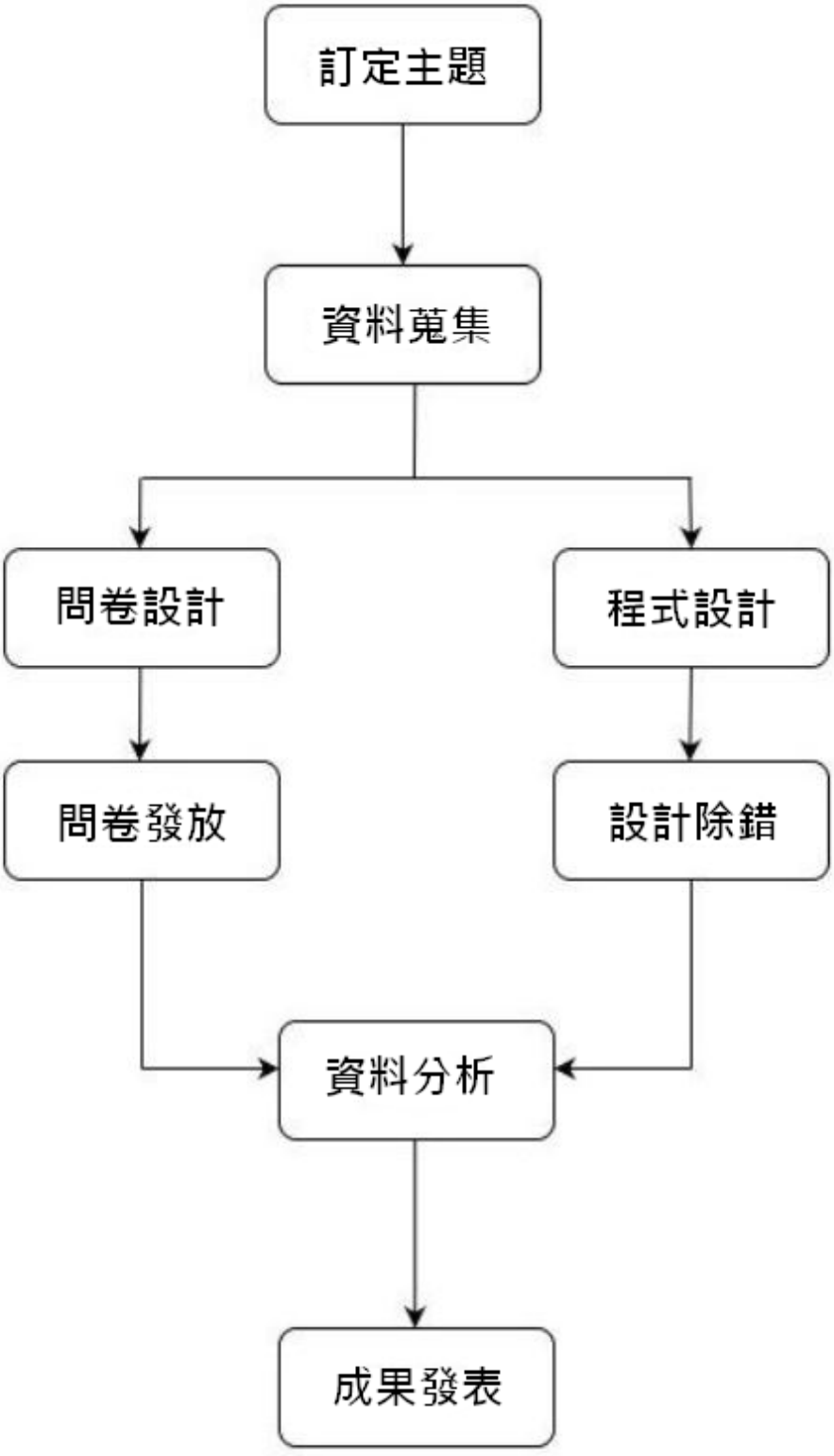


圖 3- 1 專題研究流程

第 二 節　問卷結果分析

本研究以問卷調查法，針對民眾對智能合約之瞭解進行資料搜集，問卷發放期間為 2022/08/20 至 2022/09/18 日止，有效問卷共 253 份，無效問卷為 2 份。主要針對智能合約基本了解及相關風險問題做出討論，以下將以受試者所填答的資料加以整理，並統計出大眾對於智能合約的看法及智能合約的風險，並提出本組的看法和解決方案。如

一、　基本資料

表 3- 1 填答者之基本資料

	女性							女性合計	男性							男性合計	總計
	服務業	金融業	軍公教	資訊業	農牧業	製造業	學生		服務業	金融業	軍公教	資訊業	農牧業	製造業	學生		
大專院校	7	5	3	4	1	2	46	68	1	4	3	7		29	55	99	167
研究所以上	3	4	2			1	5	15	2	1	2	5	1	1	10	22	37
高中職	3	2	1		1	1	4	12	4	3	4		2	1	5	19	31
國中或以下	4	3	1	1		1	1	11		2	2	2	2	1		9	20

總計	17	14	7	5	2	5	56	106	7	10	11	14	5	32	70	149	255

二、 智能合約問卷分析

1. 對智能合約了解程度

由下圖(3-2)所示，大部分填寫該問卷之受訪者，了解及完全了解各佔 41.96%和 24.71%合計近七成，普通也佔近 17%，可見在這網絡發達資訊暢通的時代，民眾對於區塊鏈,電子契約等新知皆有所涉略，也對接下來資料的分析應用有所幫助。

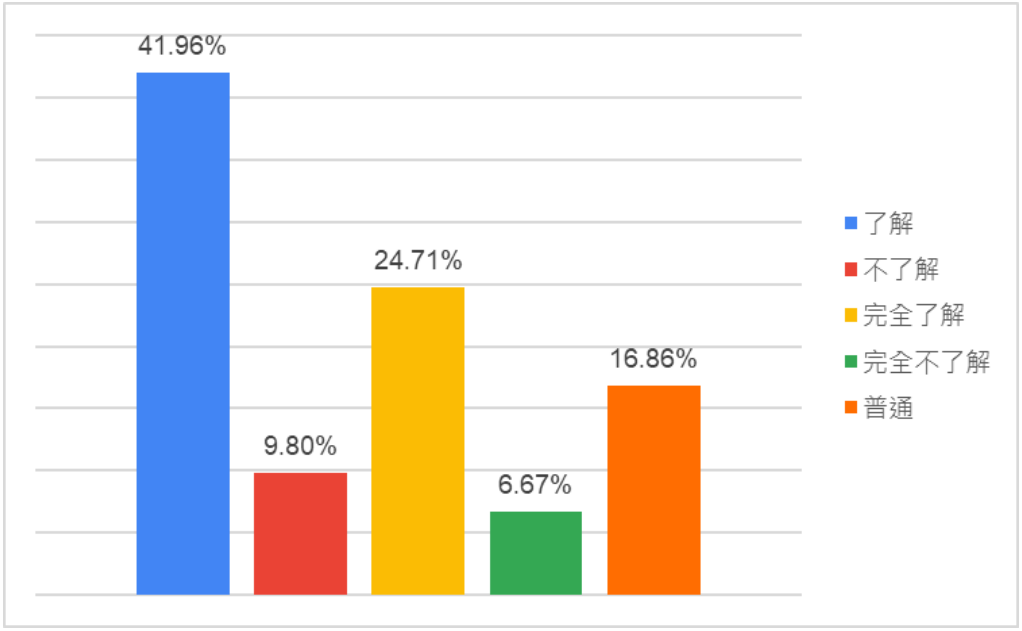


圖 3- 2 民眾對智能合約了解程度

2. 認為現有的電子契約法規已完善?

由下圖(3-3)所示，可知民眾對於電子契約法規，不完善和非常不完善合計達53.75%，有半數民眾認為以現有法規不足以應付現今的科技應用，畢竟在這科技資訊快速膨脹的時代，法規若是無法制衡甚至超車現有之應用，就容易成為有心人士鑽漏洞的地方，我們認為相關機構應該研究未來應用之走向，並預先規範制度或制定合適的法條，在不影響正常使用該應用之情況下，防範於未然，這和我們的看法也十分相近。

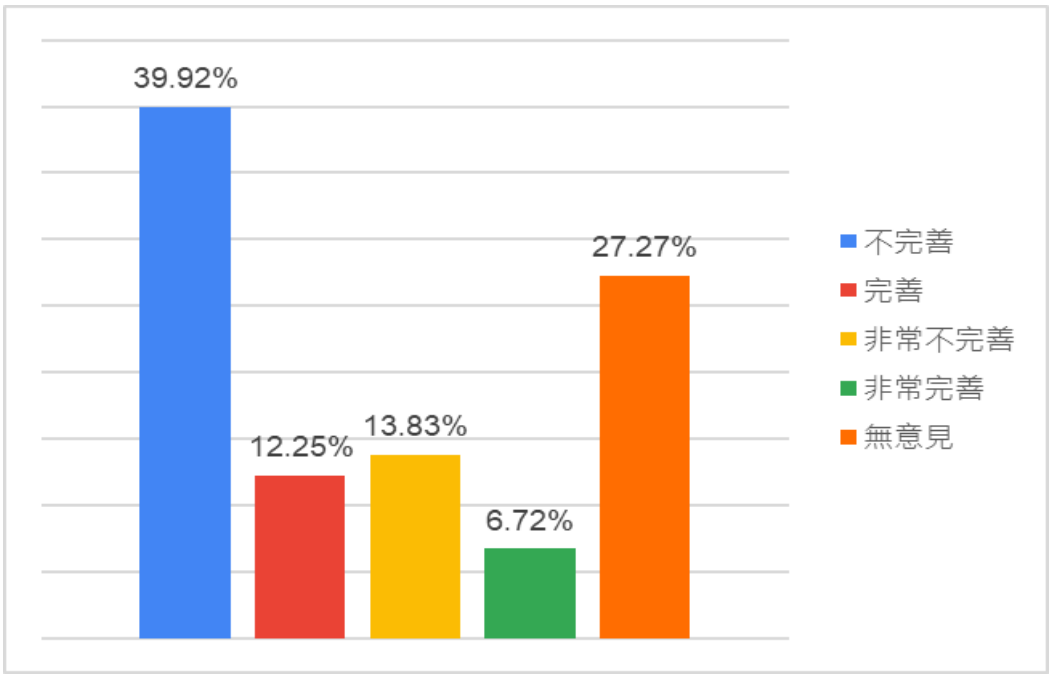


圖 3- 3 民眾對現有電子契約法規之完善程度看法

3. 對使用智能合約的風險存在擔憂?

下圖(3-4)所示，顯示超過七成的民眾對智能合約這項應用抱持保留的態度，也許是擔心法規不夠完善，抑或是害怕該應用資訊內容不夠透明，又或是不信任新技術的安全規則，這些我們會再第八題到第十題進行更深度的分析。

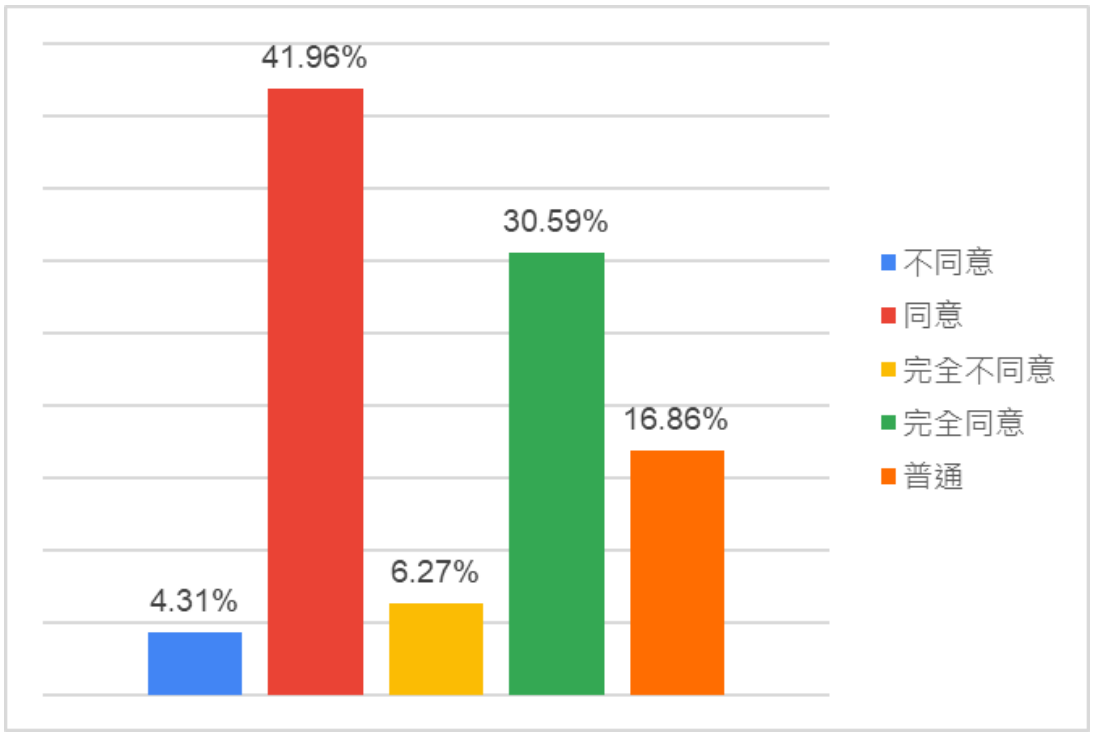


圖 3- 4 民眾對使用智能合約的風險擔憂程度

4. 認為智能合約已然成為未來趨勢?

由下圖(3-5)所示，可知民眾對於智能合約有所期待，同意及完全同意合計達七成以上，也有近兩成的民眾持觀望的態度，並沒有完全否定智能合約這項應用，可見民眾對於新興科技的期望還是非常高，若是能順利解決民眾對該應用的擔憂，智能合約又或是電子支付就能在台灣順利推廣。

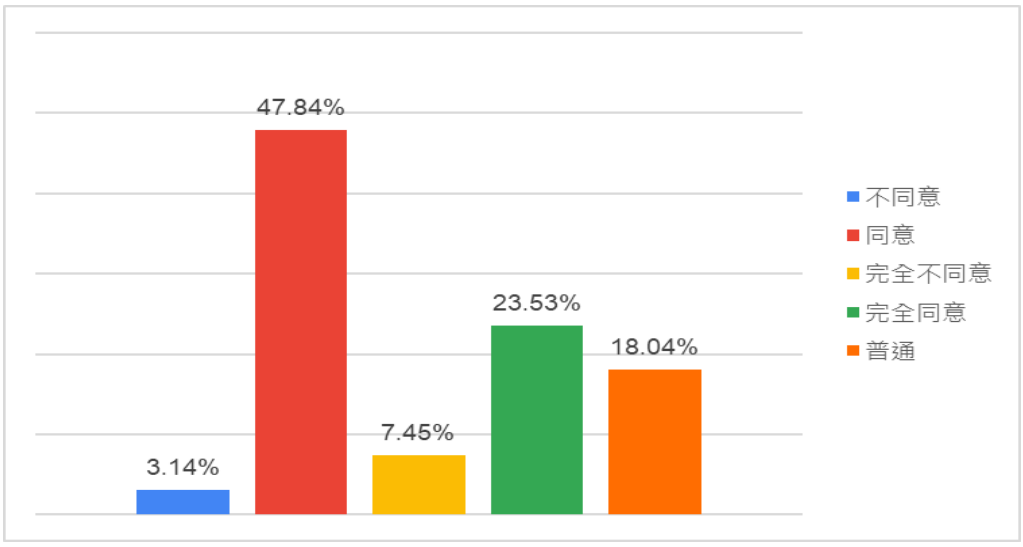


圖 3- 5 民眾對於智能合約有所期待，同意及完全同意合計達七成以上

5. 認為使用智能合約的企業在商業活動上具有優勢？

由下圖(3-6)所示可以看出大部分民眾都認為，智能合約在商業上確實能帶來幫助，或是快速交易之便利性，抑或是藉由區塊鏈技術進行合約的可靠性，還是看好新技術所延伸的未來性，這些都是智能合約之優勢，也是支持該應用能繼續走下去的動力。

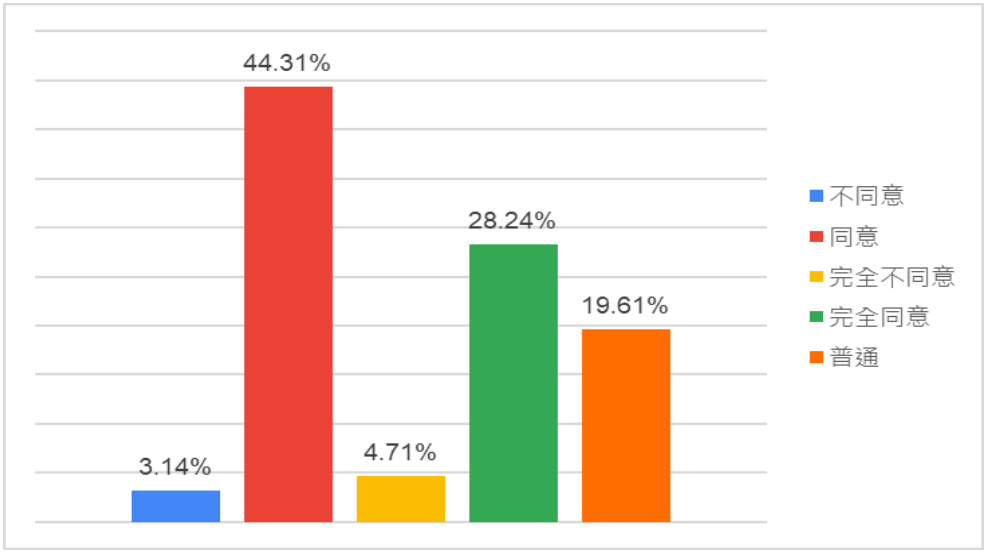


圖 3- 6 大部分民眾都認為，智能合約在商業上確實能帶來幫助

6. 認為公營事業應帶頭使用智能合約？

由下圖(3-7) 所示，可知近八成民眾對於公部門使用智能合約持正向的看法，或許有了政府做為領頭羊，優先使用並假已推廣的重要性，政府部門的各項決策都對民眾有著深遠的影響，若是政府能加以應用，這對推廣智能合約又或是電子支付，都能起到推進的作用。

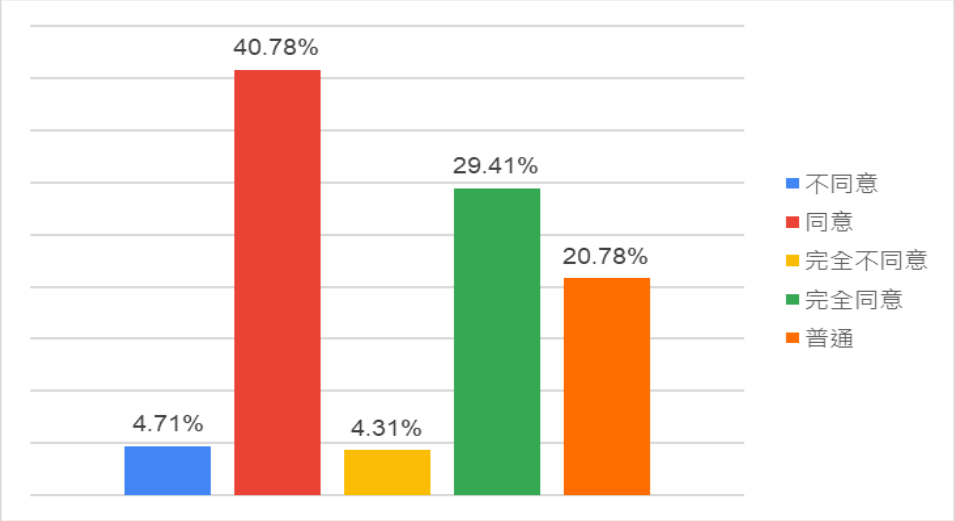


圖 3- 7 政府部門的各項決策都對民眾有著深遠的影響

7. 如果智能合約普及化，會用智能合約進行交易?

由下圖(3-8) 所示，可知超過六成民眾願意嘗試智能合約，雖然並不多，但仍超過半數，也有超過兩成的民眾在觀望，或許是認為沒必要使用，又或是覺得現今普及率不高、流通性不夠廣，如何提升普及率加速該應用推廣，是政府該認真考慮的項目，如果能經由第六題觀點出發，或許民眾對智能合約的接受度能更高。

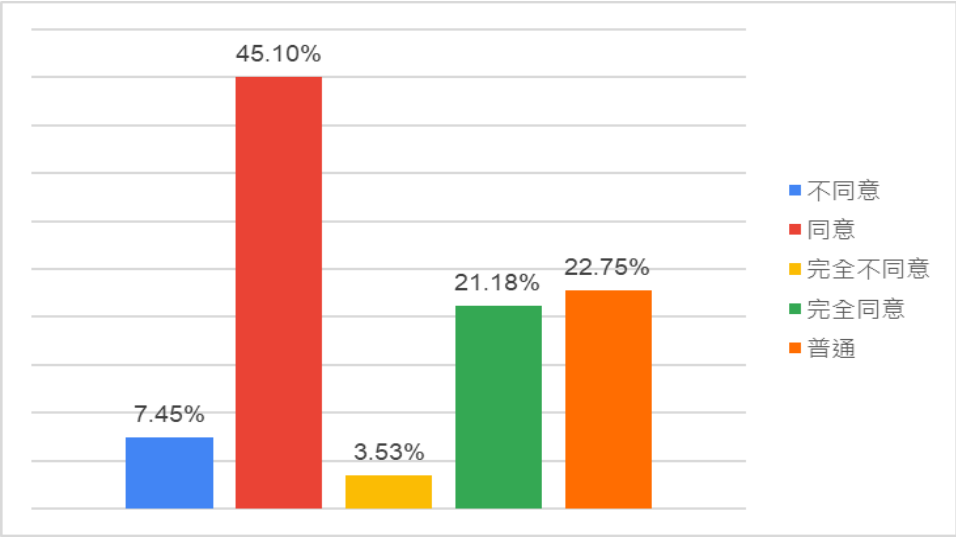


圖 3- 8 六成民眾願意嘗試智能合約

8. 當智能合約的需求規格不夠嚴謹時，會造成開發人員誤解需求，而導致程式的執行結果與用戶的預期不符。(程式開發風險)

由下圖(3-9)所示，可知認為嚴重甚至非常嚴重者占六成，無意見卻也占了兩成五，我們認為或許程式設計或使用者介面，在民眾的認知裡對於智能合約這項應用並非首要風險項目，但某些程式就是因為出現漏洞，進而導致一些不可收拾的後果，或許是因為相關報導相比後兩題來說較少，讓民眾有該項目不夠嚴重之錯覺，或許相關部門應加強宣導，強化民眾的認知。

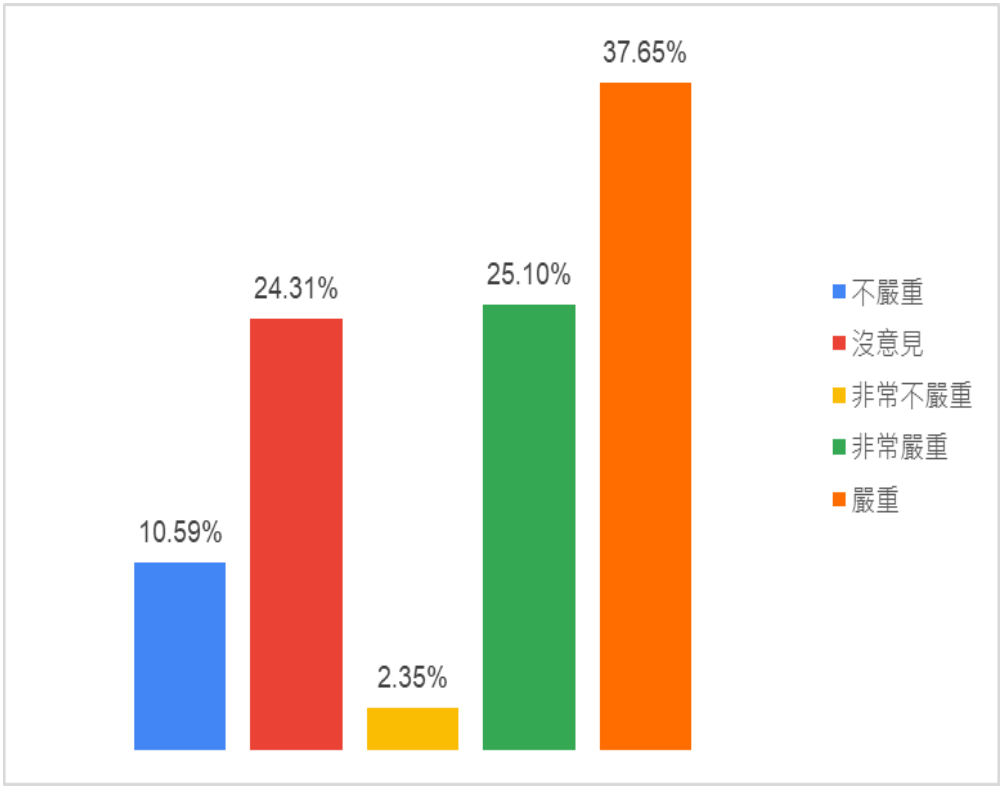


圖 3- 9 民眾的認知裡對於智能合約這項應用並非首要風險項目

9. 智能合約在法律方面有許多的議題與挑戰要考慮，例如當駭客發現程式漏洞拿取了大筆資產、造成他人損失，這樣是否有法律可約束。(資安法規風險)

由下圖(3-10)所示，可知超過八成五的民眾皆認為資安及法規風險，是智能合約最主要之風險來源，當中有 56.08%的受訪者認為其問題十分嚴重，但這就只是與我們第八題當中所說的風險進一步惡化、所導致的結果，若是減少程式漏洞就不會衍生出這種風險問題，我想這與現今相關報章雜誌或政令宣導，所影響的結果，我想現今大眾更在乎事件當中最聳動，各媒體便投其所好，卻沒有深度探討該問題最根本之原因。

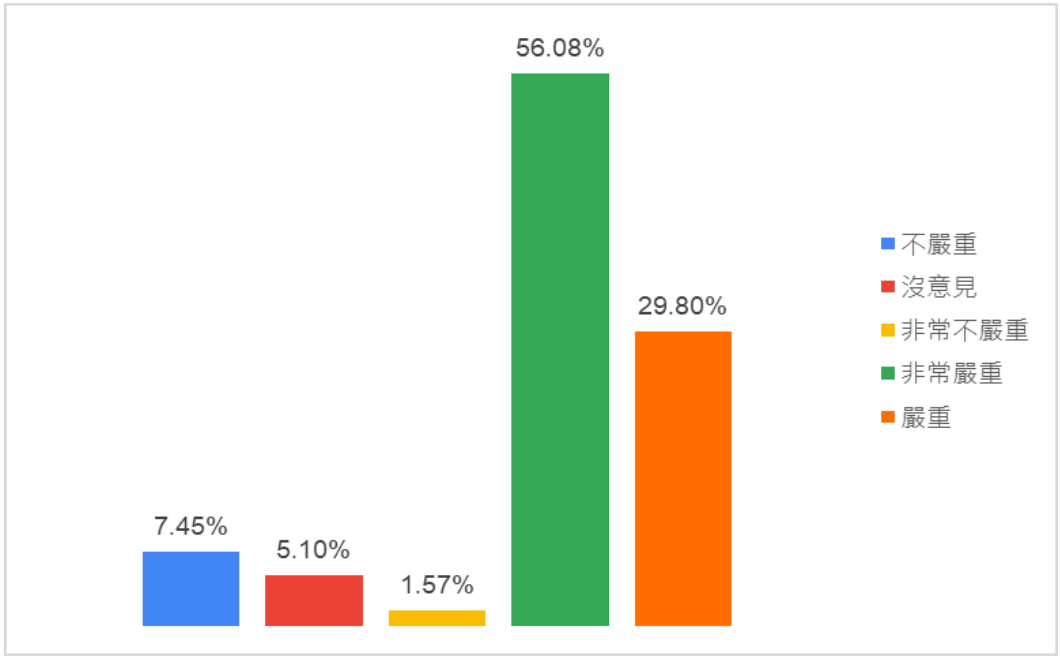


圖 3- 10 八成五的民眾皆認為資安及法規風險，是智能合約最主要之風險來源

10. 智能合約在區塊鏈平台做程式化的資產移轉，而這些資產都是加密貨幣（數位資產），會必須承擔交易加密貨幣的風險。（資產轉移風險）

由下圖(3-11)可知該風險依然有超過八成的民眾認定其嚴重性，當中非常嚴重占 31.37%，相較於第八題 25.10%與第九題的 56.08%來說，算是中間項，我們認為其風險，更需要眾部門的合作，當中涵蓋法規、金融、資安要能使該風險解決，相比上述兩項風險，需要耗費更多心力及資源。對於該問題之風險嚴重性這點，我們的看法與受訪者就很相近，皆認為其中的嚴重及其迫切解決之道。

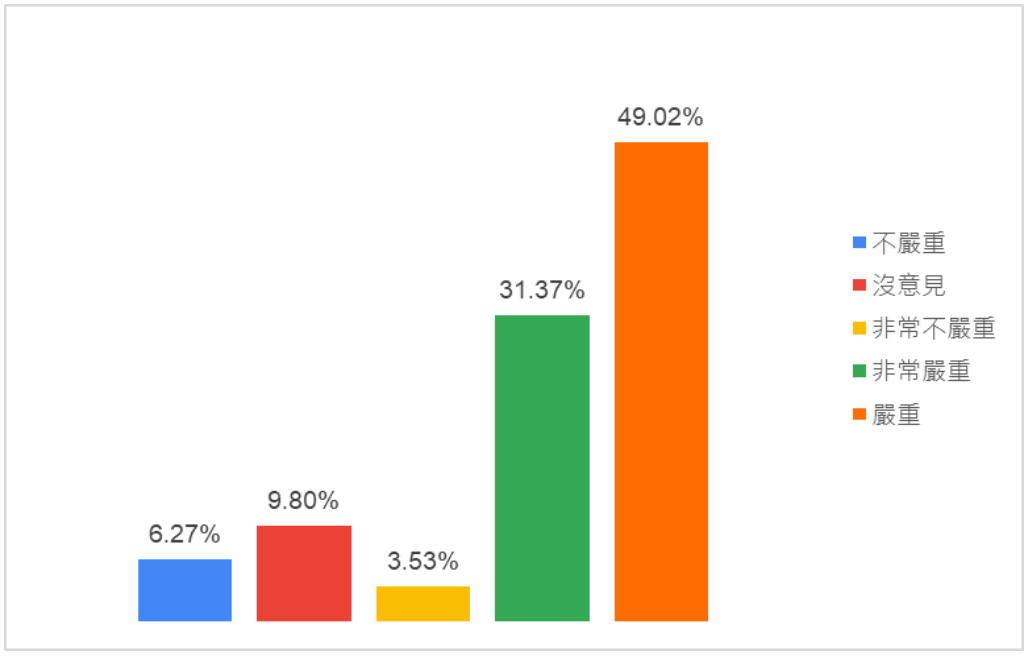


圖 3- 11 依然有超過八成的民眾認定其嚴重性

(一)、 解決方案及看法

經由問卷調查結果之統整與分析，可發現受試者僅六成對智能合約有所了解，再者我們觀察到第八題、第九題、第十題的各情況分布比例，大眾對於法律是否保障人民及其安全性是相對重視的，若想推廣智能合約就需要相關部門齊心協力，加強國民對於新技術的深度了解，及廣泛應用，不管是金融界、立法院、資策會等等甚至是各級行政機關，台灣的電子支付之所以不普及，除了是相較其他國家來說開發的較晚，也有大部分的因素是政府前期不夠積極推廣，導致民眾的信心薄弱，當其他國家已經在推行無紙化甚至電子支付之相關應用的時候，台灣卻還在原地踏步。科技及技術的領先並不是一天兩天就能達成的，不求與時俱進，至少不要落於人後。若是連區塊鏈或智能合約都沒有立即性的作為，我想我們只會越來越跟不上中國、韓國的進程。

(二)、 可行之解決方案

(1.) 強化國民認知

將科技新知納入一般國中小教育體制中，藉由學生來影響到家中的長輩，將新知普及化，根據美國交易所巨頭 Coinbase 8 月 28 號發布了一篇與 Qriously 合作的報告，全球排名前 50 名的大學中有 56% 開設了至少一門關於區塊鏈或加密貨幣領域的課程，超越去年的 42%；另外來自各領域的學生都展現對加密貨幣與區塊鏈的高度興趣，而學校也在各領域科系增加相關課程，由此可見各國對區塊鏈的重視。(Candy Her，2019)

(2.) 試辦區域範圍實驗

將一部分地區圈起試辦並優先推動新科技技術，將試辦過程作為範本，以此為範例來決定要改善或加強擴大範圍。

例如利用台灣的"金融監理沙盒"，監理沙盒可提供業者於一定期間內，免取得相關證照且排除部分法規限制，對創新商品或服務於金融市場運作之可行性進行實驗，以減低新創業者為金融創新之顧慮及成本。因此，新興之金融商品或服務於發行前，進入「監理沙盒」進行實驗，對於業者具有避免刑事責任、維持商品之獨特性、增加廣告效益、創造使用者黏著、政府或主管機關積極協助訂定修正法規等之優勢。簡單來說就是讓新創業者進入官方監理的風險可控環境當中，盡可能測試金融創新業務及產品。

(3.) 宣傳智能合約

透過網絡宣傳智能合約優、缺點，讓更多的人知道它的未來可用性，讓人們因為了解而去信任它。我國現對智能合約未有相關規範，因此態度偏向保守，但如果需要推廣智能合約，政府的支持是最有力的推廣方式，其實，一如許多先進國家已感受到區塊鏈技術的重大影響，澳洲政府更在花費了近一年的研究後，由澳洲聯邦科學與工業研究所（CSIRO）宣布，將與 IBM 和 Herbert Smith Freehills 律師事務所 合作，成立數位聯盟，旨在為澳洲企業建立一個大型的開創性跨業智能合約平台，並在內部開展業務，這種思考國家如何掌握區塊鏈科技之效用，來促升國家整體產業利益。(范建得&劉境棠，2018)

(三)、 我們的看法

我們認為要能成功的推廣智能合約，除了上述三項外還有，還有許多方法能推廣，最簡單直白的即是補助、亦或是簡化其相關流程，不論是申辦或是應用，有個便利且穩定的系統，是順利推廣該應用的關鍵。

第肆章　實驗設計與結果

Solidity 是靜態型別，這表示型別檢查會在編譯時期進行，而非如動態型別語言一般在執行階段進行。 使用靜態型別語言時，您必須指定每個變數的型別。例如，Python 及 JavaScript 是動態型別語言，而 C++ 則是靜態型別。

Solidity 是一種合約導向式語言，被應用於各種不同的區塊鏈平台，其主要開發者為加文·伍德（英語：Gavin Wood），Christian Reitwiessner，Alex Beregszaszi，Liana Husikyan，Yoichi Hirai 和其他幾位早期以太坊核心貢獻者。Solidity 可使程式開發人員能在區塊鏈上（例如以太坊）編寫智慧型合約。本組目前是使用 Visual Studio Code 搭配 Solidity 插件來進行開發。

第一節　Visual Studio Code

Visual Studio Code 是一款由微軟開發且跨平台的免費原始碼編輯器。 該軟體支援語法突顯、程式碼自動補全（又稱 IntelliSense）、程式碼重構功能，並且內建了命令列工具和 Git 版本控制系統。

一、 Solidity 語言

Solidity 是一種靜態型別的程式語言，用於開發在 EVM 上執行的智能合約。Solidity 被編譯為可在 EVM 上執行的位元組碼。

藉由 Solidity，開發人員能夠編寫出可自我執行其欲實現之商業邏輯的應用程式，該語言可被視為一份具權威性且永不可悔改的交易合約。

Ethereum 上的智能合約需要使用 Solidity1 語言來撰寫。雖然還有其他能用來撰寫智能合約的語言如 Serpent(類 Python)、lll(類 Fortran)，但目前看到所有公開的智能合約都是使用 solidity 撰寫。

二、 Ganache cli 模擬器

Ganache 的原理就是幫你用好 Geth 的環境，也就是當你開啟 Ganache，它會在你的電腦上開啟一個節點，並且在這個節點初始化多個帳號，因此當測試的時候就可以直接拿這節點的帳號進行測試，尤其對於智能合約的操作是最方便的。它可以幫我們快速建置 Ethereum 區塊鏈客戶端的環境，可以用於本地部署、開發、測試應用程式、測試程式碼。

三、 程式功能介紹

智慧契約是能夠自動執行合約條款的電腦程序，是將契約條款的文字轉成像程式編碼的形式，進入區塊鏈之後，如果契約的條件成就了，此時因為條款已經轉換成為程式編碼的形式，所以程式預設的條件如果成就，契約會自動執行，並且在區塊鏈上做財產價值的交換與轉移，例如雙方都有比特幣帳戶，就會以比特幣帳戶去支付。Written by 投稿作者• 2018-05-21-區塊鏈讓契約變得更聰明

圖 4- 1 電子契約

要和智能合約互動，除了需要有合約地址外，還需要知道合約所提供的操作介面(Application Binary Interface，ABI)，即知道如何呼叫程式提供的功能，和如何解釋程式回傳的資料。 ABI（JSON 格式）檔案在從原始碼編譯成 ByteCode 時會一併產生。(Application Binary Interface，ABI)，即知道如何呼叫程式提供的功能。

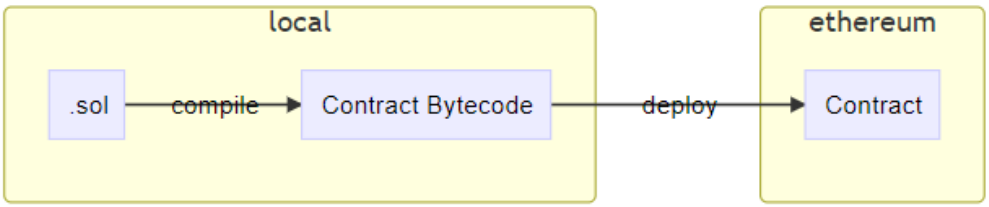


圖 4- 2 操作介面

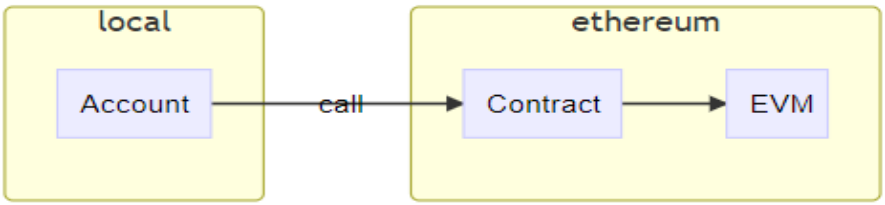


圖 4- 3ABI（JSON 格式）檔案在從原始碼編譯成 ByteCode 時會一併產生。

如圖 4-2 文字寫好 solidity 程式碼後，需要先將程式碼編譯成 EVM(Ethereum Virtual Machine)能讀懂的二進位 Contract ByteCode，才能部署到 Ethereum 的區塊鏈上執行。部署到區塊鏈上的合約會有一個和錢包地址一樣格式的合約地址。

部署後智能合約可自動執行。後續呼叫智能合約的時候，使用者可以使用部署合約的錢包地址(Owner Account)，或依據撰寫的智能合約條件，讓其他錢包地址也能呼叫這個智能合約。 所謂的"呼叫智能合約"，其實就是向這個合約地址發起交易，只是交易的不只是代幣，而可以是智能合約提供的呼叫方法。

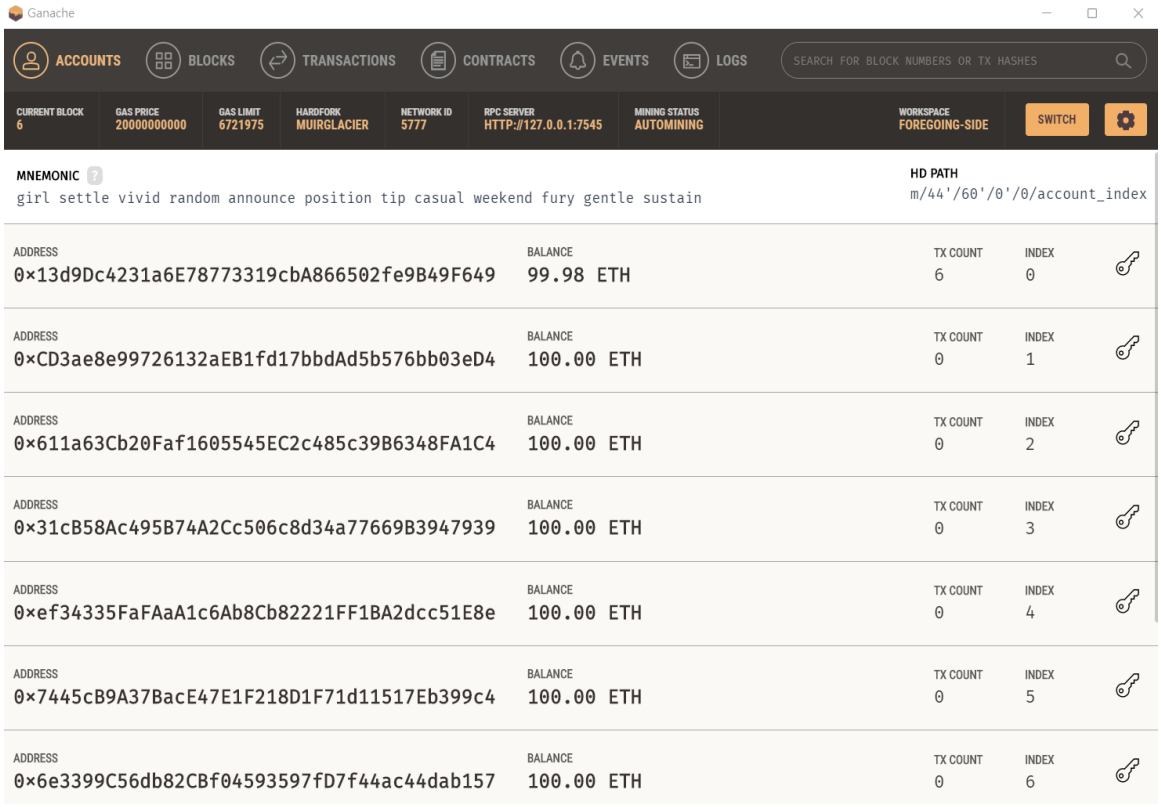


圖 4- 4 電子錢包

Ganache 的原理就是幫你用好 Geth 的環境，也就是當你開啟 Ganache，它會在你的電腦上開啟一個節點，並且在這個節點初始化多個帳號，因此當測試的時候就可以直接拿這節點的帳號進行測試。

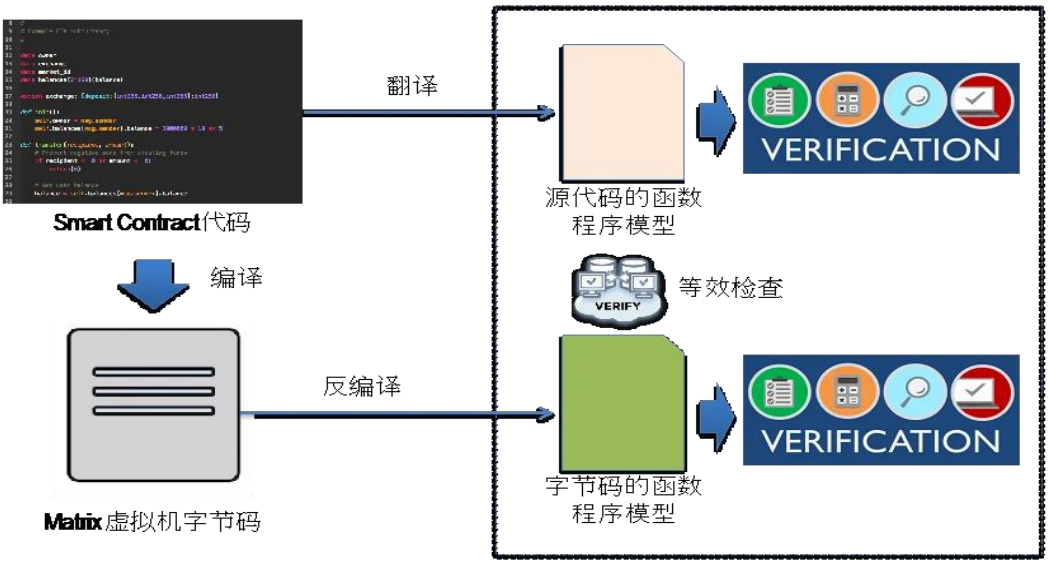


圖 4- 5 安全問題

MATRIX 的一個關鍵特色是使用人工智能方法自動識別程序語義並發現其中的典型模式，從而根據模式自行產生為了滿足安全要求而需要的屬性。當用戶提供智能合約代碼或編譯後的執行代碼後，MATRIX 的 AI 引擎將自動完成代碼的局部相似性匹配和全局相似性匹配，從而推測代碼的行為模型。根據 AI 獲得行為模型，生成對應的形式驗證約束，從而進行深層次的行為驗證，實現代碼安全性。

第伍章　結論與未來展望

第 一 節　　結論

智能合約於 1990 年首次被提出後發展至今仍是在萌芽的階段，一個不夠成熟的技術在現實中還有許多的課題需要解決，我們在專題中主要提及的法律問題只是所有問題中的冰山一角，或許智能合約還有很長的路要走，不過隨著時間的推移，問題會慢慢地被解決。

「信任」是所有貨幣系統的核心，通貨要能有效使用，必須仰賴使用者族群對該貨幣保持適當的尊重。每個人都同意一種貨幣是金錢時，你就可以說他是金錢。要達到這種地步相當困難，雖然企業的採用是觸發改變最有利的催化劑，但人們會觀察其他大眾是如何看待比特幣和其他加密電子貨幣，羊群效應固然是推動加密貨幣的利器，但也有可能成為投機客的工具，一波棄售後可能會干擾到當前的市場，造成市場恐慌，當前加密貨幣的波動過大，或許還不是成為當前交易貨幣的最優選，虛擬貨幣想取代掉實體貨幣仍需要一段的時間，十幾年前，電子商務剛開始盛行，當時的人們也推測電子商務將會完全取代掉實體店面，到了現在，實體店面或多或少有影響，但它們依然大量存在於現代社會中，電子商務和實體店面找到了屬於它們的平衡點，這或許能提供給智能合約作借鏡，我們認為最重要的不是要取代舊有的東西，而是如何在舊有的基礎上找出適合智能合約與傳統合約的平衡點。科技會為人帶來便利，卻也會對我們生活造成的衝擊、以及對隱私的侵犯，但也因為有了這些衝擊才證明了人類正不斷的在進步。

第 二 節　　未來展望

區塊鏈為時下熱門科技，討論度自然很高，尤其近幾年"區塊鏈"、"智能合約"、"NFT"等這些專有名詞更頻繁地出現在各種報章雜誌中，因此這次專題選擇這個題目來討論，期望經過這次專題讓我們更了解未來的產業趨勢，將此次的專題報告做為我們的養分，和智能合約一同成長，如有機會也能在未來進入這項產業盡一份力。

在這個世界裡，幾乎任何東西都有個錢幣，而我們知道的通貨就變得沒那麼重要了。許多形式的貨品和服務都能交易，不需要交易工具，如美元或比特幣。到後來對需求變少，而且肯定不需要集中管理的，因為所有的東西會隨著對應的其他東西而浮動，如果這樣的市場得以運作，就亦為所有東西都能找到某種平衡。

參考文獻

中文部分

1.維基百科 Wiki，智慧型合約，擷取自

https://zh.wikipedia.org/wiki/智能合約

2.加沛(2018)，不可不知 何謂「智能合約」，擷取自
https://blockcast.it/2018/03/11/what-is-a-smart-contract/

3.Luke Handt (2022)，ERC20 Token Standard ，擷取自
https://www.indexuniverse.eu/erc20-token-standard/

4.林詠章 (2020)，智慧合約效能及安全漏洞檢測系統之研發，擷取自
https://www.grb.gov.tw/search/planDetail?id=13530769

5. 林玫君 (2019)，區塊鏈智能合約的契約法問題 ，擷取自

https://www.airitilibrary.com/Publication/alDetailedMesh?docid=17287618-201904-201910220008-201910220008-127-183

6.林詠章； 林久弘 (2018) ，以太坊智能合約安全之研究，擷取自
https://www.airitilibrary.com/Publication/alDetailedMesh?DocID=a0000270-201807-201807250013-201807250013-16-33&PublishTypeID=P001

7. 漏洞蟲用以參考程式漏洞，擷取自 https://paper.seebug.org/632/# 2seebug

8.智能合約的發展與應用-陳　恭 / 政治大學資訊科學系教授
https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9005.pdf

9.區塊鏈智能合約也是契約　程式設計攸關法律效力-擷取自；
https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/38B66871BFC2498CA831556FE9EC023F

10.區塊鏈教育受重視：世界排名前 50 大學，超過一半都已經開設相關課程

https://www.blocktempo.com/coinbase-2019-report-50top-universities-crypto/

11.維基百科:金融監理沙盒-擷取自:https://zh.m.wikipedia.org/zh-tw/%E9%87%91%E8%9E%8D%E7%9B%A3%E7%90%86%E6%B2%99%E7%9B%92

12.讓區塊鏈技術引領我國開創出具國際競爭力的新創產業： 自澳洲與 IBM 合作開發的全國區塊鏈平台談起

https://blpc.site.nthu.edu.tw/p/406-1390-152228,r7141.php?Lang=zh-tw

Written by 投稿作者• 2018-05-21-區塊鏈讓契約變得更聰明擷取自:

https://plainlaw.me/2018/05/21/blockchain07/#:~:text=%E3%80%8C%E6%99

%BA%E6%85%A7%E5%A5%91%E7%B4%84%E3%80%8D%E5%B0%B1%E6%98%AF,%EF%BC%8C%E8%A7%B8%E7%99%BC%E8%B3%87%E7%94%A2%E4%BA%A4%E6%8F%9B%E3%80%82

英文部分

1.Dr Adrian Manning (2018) ， Solidity Security: Comprehensive list of known attack vectors and common anti-patterns ，擷取自 https://blog.sigmaprime.io/solidity-security.html

2.布萊恩·拉弗杜爾(2021)，社區銀行的智能合約，擷取自:

www.icba.org/newsroom/blogs/main-street-matters/2021/11/04/trust-in-code-smart-contracts-defi-and-use-cases-for-community-banking

3.安西卡·巴拉(2021)，了解區塊鏈區塊鏈的詳細歷史：從建立到廣泛採用，擷取自:https://www.blockchain-council.org/

4.T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare and M. Ylianttila(2021)， "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research," in IEEE Access, vol. 9, pp. 87643-87662, 2021, doi: 10.1109/ACCESS.2021.3068178.， 擷取自 http://jultika.oulu.fi/files/nbnfi-fe2021101250680.pdf

【專題執行計畫表】

<table>
<tr><td>組名</td><td colspan="4">智能合約開發問題與風險</td></tr>
<tr><td rowspan="9">組員</td><td>班　級</td><td>學　號</td><td colspan="2">姓　名</td></tr>
<tr><td>夜資四A</td><td>60810119</td><td colspan="2">葉長翰</td></tr>
<tr><td>夜資四A</td><td>60810126</td><td colspan="2">陳禹丞</td></tr>
<tr><td>夜資四A</td><td>60810111</td><td colspan="2">吳冠逸</td></tr>
<tr><td>夜資四A</td><td>60810175</td><td colspan="2">游承憲</td></tr>
<tr><td>夜資四A</td><td>60810111</td><td colspan="2">薛聿惟</td></tr>
<tr><td>夜資四A</td><td>60810111</td><td colspan="2">林宏澤</td></tr>
<tr><td>夜資四A</td><td>60710106</td><td colspan="2">蘇秀汝</td></tr>
<tr><td rowspan="5">選定合作單位</td><td>名稱</td><td colspan="3">無</td></tr>
<tr><td>負責人</td><td>無</td><td>聯絡人</td><td>無</td></tr>
<tr><td>電話</td><td>無</td><td>電話</td><td>無</td></tr>
<tr><td>地址</td><td colspan="3">無</td></tr>
<tr><td colspan="4">業務描述
本次專題無合作單位。</td></tr>
<tr><td>專題名稱</td><td colspan="4">智能合約開發問題與風險</td></tr>
<tr><td colspan="5">專題資訊系統功能描述</td></tr>
<tr><td>指導老師簽名</td><td colspan="2"></td><td>日期</td><td>年 月 日</td></tr>
<tr><td>備註</td><td colspan="4"></td></tr>
</table>

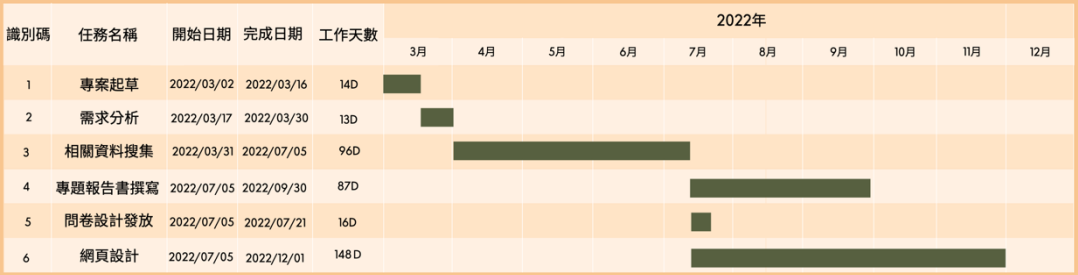
【專題工作分配表】

組名	智能合約開發問題與風險	填寫人	葉長翰
專題名稱	智能合約開發問題與風險	填寫日期	111 年 8 月 29 日

姓名：	工作分配:
葉長翰	資料搜集 資料分析 資料整合 圖表製作 PPT 製作
陳禹丞	資料搜集 資料分析 資料整合 圖表製作 PPT 製作
吳冠逸	程式撰寫 網站設計 網站架設
游承憲	資料搜集
薛聿惟	資料搜集
林宏澤	資料搜集
蘇秀汝	資料搜集

【甘特圖】

組名	智能合約開發問題與風險	填寫人	葉長翰
專題名稱	智能合約開發問題與風險	填寫日期	111 年 8 月 29 日



識別碼	任務名稱	開始日期	完成日期	工作天數
1	專案起草	2022/03/02	2022/03/16	14D
2	需求分析	2022/03/17	2022/03/30	13D
3	相關資料搜集	2022/03/31	2022/07/05	96D
4	專題報告書撰寫	2022/07/05	2022/09/30	87D
5	問卷設計發放	2022/07/05	2022/07/21	16D
6	網頁設計	2022/07/05	2022/12/01	148D

【開發工具清單】

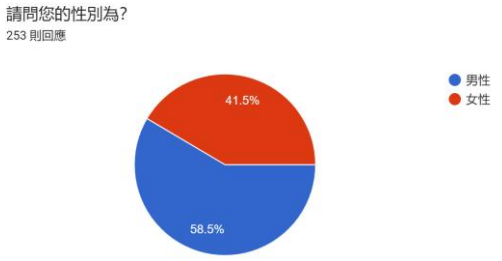
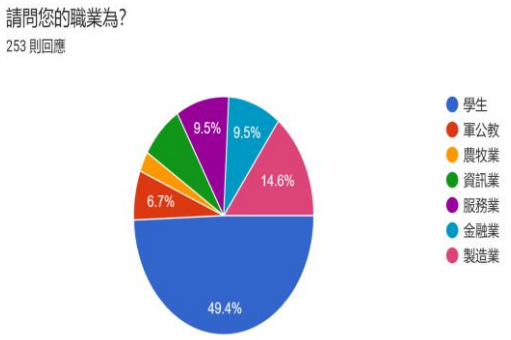
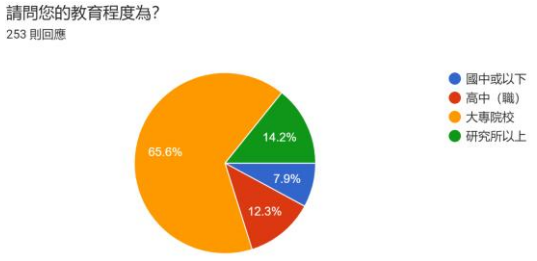
組名	智能合約開發問題與風險	填寫人	葉長翰
專題名稱	智能合約開發問題與風險	填寫日期	111 年 8 月 29 日

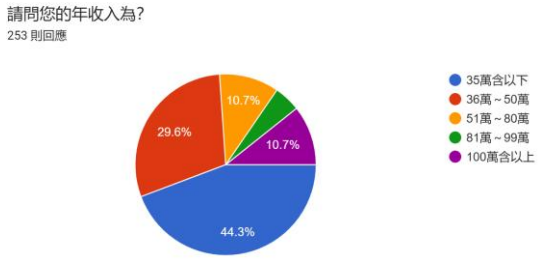
類別	名稱	用途
程式開發軟體	Solidity 、 Ganache	用於撰寫程式內容及電子錢包
美工軟體	FireAlpaca64、Photoshop	用於編輯並修改圖片
文書處理軟體	Microsoft Excel	用於製作資料表格
	Microsoft Word	用於編輯及填寫專題報告

【需求訪談紀錄表】

組名	智能合約開發問題與風險	填寫人	葉長翰
專題名稱	智能合約開發問題與風險	填寫日期	111 年 8 月 29 日

第一部分 基本資料

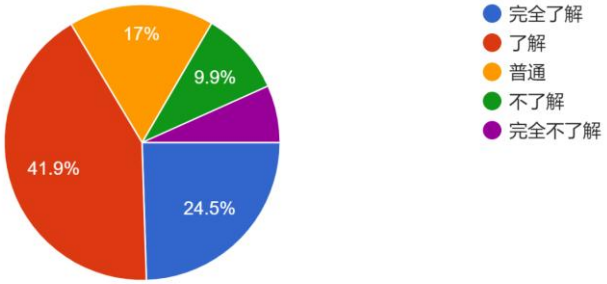
性別比例： 女性占 67.5% 男性占 32.5%	
職業比例： 學生 軍公教 農牧業 資訊業 服務業 金融業 製造業 其他	
教育程度比例： 國中或以下 2.0% 高中職 10.6% 大專院校 74.8 研究所(含以上) 12.6%	

年收入比例： 35 萬(含)以下 42.6% 36 萬-50 萬 20.4% 51 萬-80 萬 9.6% 81 萬-99 萬 6.3% 100 萬(含)以上 13.1%	

第二部分 智能合約調查

1、對智能合約了解程度

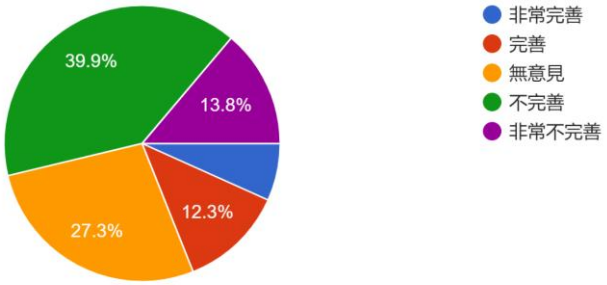
253 則回應



問卷調查中

2、認為現有的電子契約法規已完善?

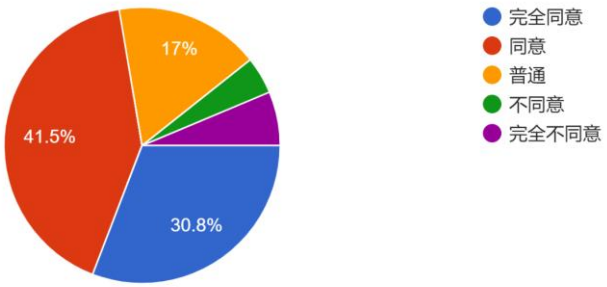
253 則回應



問卷調查中

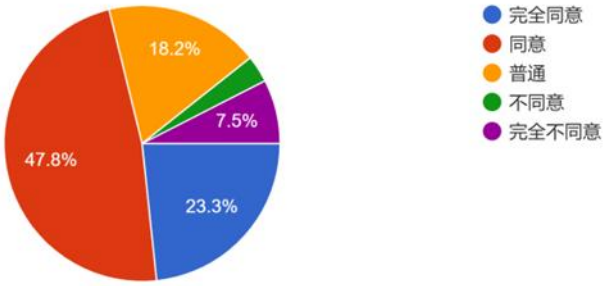
3、對使用智能合約的風險存在擔憂?

253 則回應



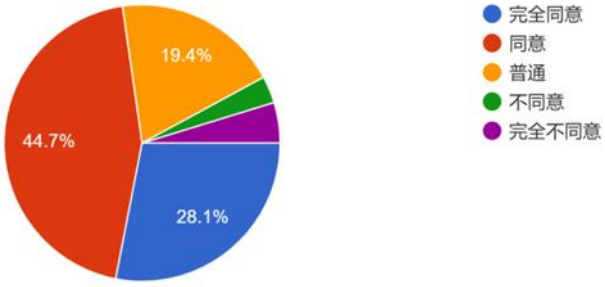
4、認為智能合約已然成為未來趨勢?

253 則回應



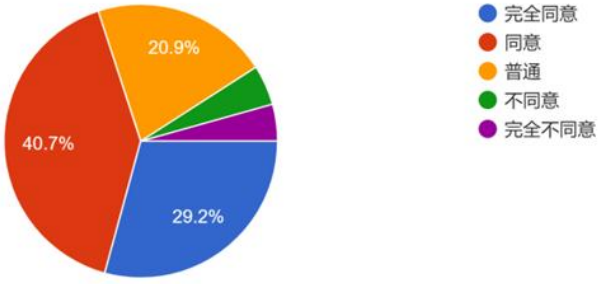
5、認為使用智能合約的企業在商業活動上具有優勢?

253 則回應



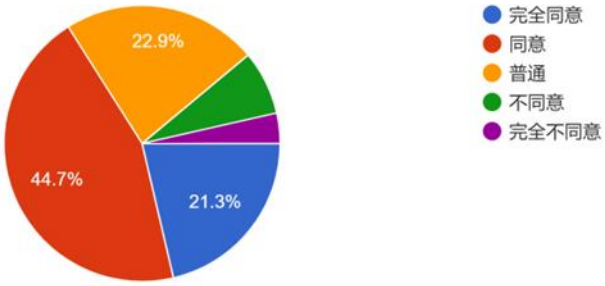
6、認為公營事業應帶頭使用智能合約?

253 則回應



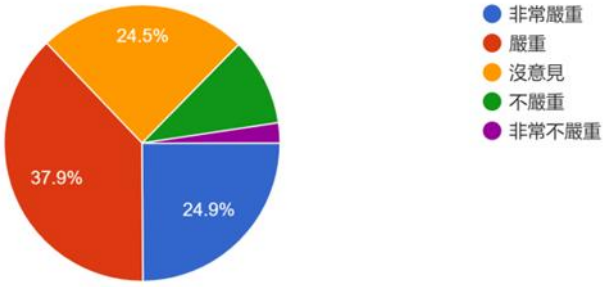
7、如果智能合約普及化，會用智能合約進行交易?

253 則回應



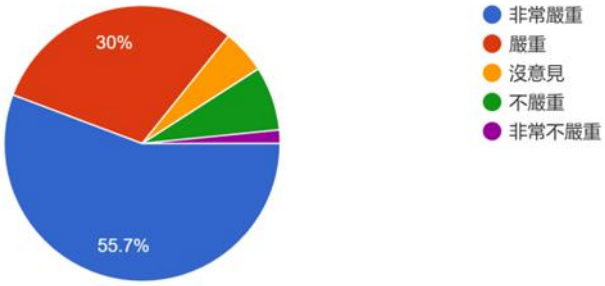
8、當智能合約的需求規格不夠嚴謹時，會造成開發人...項程式開發風險對智能合約的影響程度有多少?)

253 則回應



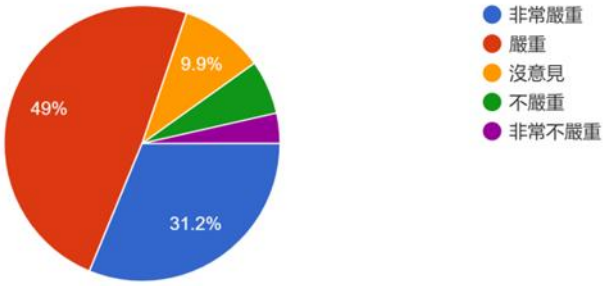
9、智能合約在法律方面有許多的議題與挑戰要考慮，...項相關法規風險對智能合約的影響程度有多少?)

253 則回應



10、智能合約在區塊鏈平台做程式化的資產移轉，而...項資產轉移風險對智能合約的影響程度有多少?)

253 則回應



<table>
<tr><td colspan="8">【會議紀錄】</td></tr>
<tr><td>組名</td><td colspan="2">智能合約</td><td rowspan="2">專案名稱</td><td colspan="4" rowspan="2">智能合約</td></tr>
<tr><td>組別</td><td colspan="2">第四組</td></tr>
<tr><td>會議編號</td><td colspan="2">M1</td><td>召集人兼主席</td><td>曲莉莉老師</td><td>紀錄者</td><td colspan="2">陳禹丞</td></tr>
<tr><td rowspan="2">討論主題</td><td colspan="4" rowspan="2">專題工作分配、文書規則排列</td><td>會議時間</td><td>2022/07/10</td><td>21:00~22:00</td></tr>
<tr><td>會議地點</td><td colspan="2">Google Meet</td></tr>
<tr><td rowspan="2">上次會議</td><td colspan="3">決議事項</td><td colspan="4">執行狀況</td></tr>
<tr><td colspan="3">無</td><td colspan="4">無</td></tr>
<tr><td rowspan="2">本次會議</td><td colspan="2">本週工作進度</td><td colspan="3">本週工作內容</td><td>負責人員</td></tr>
<tr><td colspan="2">1. 程式組:程式完成的部分
2. 文書組:文書第一章</td><td colspan="3">1. 程式組:智能合約的主體部分
2. 文書組:摘要、目錄、緒論</td><td>1.程式組:吳冠逸、陳禹丞
2.文書組:葉長翰等其餘3人</td></tr>
<tr><td>本次會議內容</td><td colspan="7">1. 老師介紹文書範本、專題大綱以及教導同學如何撰寫文書
2. 做好初步的組員分工</td></tr>
<tr><td colspan="8">決議事項 (或 主席裁示)</td></tr>
<tr><td colspan="8">下周日晚上9點準時開會，各組組員做好分配的工作，在下次開會時報告</td></tr>
<tr><td colspan="2">請簽名</td><td colspan="3">請簽名</td><td colspan="3">請簽名</td></tr>
<tr><td rowspan="2">下次會議</td><td rowspan="2">召集人</td><td rowspan="2">陳禹丞</td><td rowspan="2">紀錄者</td><td rowspan="2">葉長翰</td><td>時間</td><td colspan="2">2022/07/17 21:00</td></tr>
<tr><td>地點</td><td colspan="2">Google Meet</td></tr>
<tr><td>預定討論主題</td><td colspan="7">各組報告自己的進度</td></tr>
</table>

<table>
<tr><td colspan="8">【會議紀錄】</td></tr>
<tr><td>組名</td><td colspan="2"></td><td rowspan="2">專案名稱</td><td colspan="4" rowspan="2">智能合約開發問題與風險</td></tr>
<tr><td>組別</td><td colspan="2">第 4 組</td></tr>
<tr><td>會議編號</td><td colspan="2">M3</td><td>召集人兼主席</td><td>曲莉莉老師</td><td>紀錄者</td><td colspan="2">陳禹丞</td></tr>
<tr><td rowspan="2">討論主題</td><td colspan="4" rowspan="2">文書組、程式組進度報告</td><td>會議時間</td><td>2022/07/24</td><td>21:00~22:00</td></tr>
<tr><td>會議地點</td><td colspan="2">Google Meet</td></tr>
<tr><td rowspan="2">上次會議</td><td colspan="3">決議事項</td><td colspan="4">執行狀況</td></tr>
<tr><td colspan="3">1.程式組:程式完成的部分
2.文書組:文書前三章</td><td colspan="4">1.程式組完成其餘錢包測試
2.文書組其中 2 人工作換成蒐集及閱讀資料</td></tr>
<tr><td rowspan="2">本次會議</td><td>本週工作進度</td><td colspan="3">本週工作內容</td><td colspan="3">負責人員</td></tr>
<tr><td>1.程式組:預計優化畫面或是程式碼部分
2.文書組:問卷題目發想
3.閱讀組:閱讀老師提供的檔案，下周做分享</td><td colspan="3">1.程式組:接著完成智能合約的程式主體或美化畫面(待討論)
2.文書組:問卷題目
3.閱讀組:同文書組</td><td colspan="3">1.程式組:吳冠逸、陳禹丞
2.文書組:葉長翰、林宏澤
3.閱讀組:游承憲、薛聿惟</td></tr>
<tr><td>本次會議內容</td><td colspan="7">1.程式組介紹:十個錢包都可順利運作，不需透過虛擬機也可正常運行
2.文書組:文獻二、三章(老師協助修改)
3.另外文書組抽出兩人主要負責文獻蒐集</td></tr>
<tr><td colspan="8">決議事項 (或 主席裁示)</td></tr>
<tr><td colspan="8">下周日晚上 9 點準時開會，各組組員做好分配的工作，在下次開會時報告</td></tr>
<tr><td colspan="3">請簽名</td><td colspan="2">請簽名</td><td colspan="3">請簽名</td></tr>
<tr><td>下次會</td><td>召集</td><td>曲莉莉老師</td><td>紀錄</td><td>陳禹丞</td><td>時間</td><td colspan="2">2022/07/31 (21:00)</td></tr>
</table>

議	人		者		地點	Google Meet
預定討論主題	討論問卷題目					

【會議紀錄】						
組名	智能合約	專案名稱	智能合約開發問題與風險			
組別	第四組					
會議編號	M4	召集人兼主席	曲莉莉老師	紀錄者	陳禹丞	
討論主題	程式組進度報告 問卷討論			會議時間	2022/07/31	21:00~22:00
				會議地點	Google Meet	

上次會議	決議事項	執行狀況
	1.程式組:預計優化畫面或是程式碼部分 2.文書組:問卷題目發想 3.閱讀組:閱讀老師提供的檔案，下周做分享	1. 程式組遇到問題正在解決 2. 題目討論中 3. 閱讀組缺席

本次會議	本週工作進度	本週工作內容	負責人員
	1.程式組:修補程式問題 2.文書組:問卷題目討論 3.閱讀組:下禮拜補報告	1. 冠逸修程式，禹丞協助 2. 長翰、禹丞做問卷 3. 其餘 3 人補報告	1.程式:吳冠逸、陳禹丞 2.問卷:葉長翰、陳禹丞 3.報告:游承憲、薛聿惟、林宏澤

本次會議內容	1. 程式組介紹:講解程式問題所在 2. 葉長翰報告:注意報告格式、講解參考文獻
決議事項 (或 主席裁示)	

下周日晚上 9 點準時開會，各組組員做好分配的工作，在下次開會時報告						
請簽名		請簽名		請簽名		
下次會議	召集人	曲莉莉老師	紀錄者	陳禹丞	時間	2022/08/07 (21:00)
					地點	Google Meet
預定討論主題	確認問卷					

【會議紀錄】						
組名		專案名稱	智能合約開發問題與風險			
組別	第 4 組					
會議編號	M5	召集人兼主席	陳禹丞	紀錄者	葉長翰	
討論主題	問卷討論			會議時間	2022/08/07	21:00~22:00
				會議地點	LINE 群組	
上次會議	決議事項		執行狀況			
	程式組:修補程式問題 文書組:問卷題目討論 閱讀組:下禮拜補報告		程式組:修改完成，但有新問題 文書組:題目如期完工 閱讀組:閱讀完畢			
本次會議	本週工作進度		本週工作內容		負責人員	
	1.程式組:修補程式問題 2.文書組:完成問卷並發放 3.閱讀組:下禮拜補報告		1.冠逸修程式，禹丞協助 2.長翰、禹丞做問卷 3.全組各自挑一篇文獻報告		1.程式吳冠逸、陳禹丞 2.問卷:葉長翰、陳禹丞	

本次會議內容	程式組介紹:講解程式問題所在 問卷探討
決議事項 (或 主席裁示)	
下周日晚上 9 點準時開會，各組組員做好分配的工作，在下次開會時報告	
請簽名	請簽名 請簽名

下次會議	召集人	曲莉莉老師	紀錄者	陳禹丞	時間	8/14 21:00
					地點	Google meet
預定討論主題	文獻					

【會議紀錄】

組名		專案名稱	智能合約開發問題與風險		
組別	第 4 組				
會議編號	M6	召集人兼主席	陳禹丞	紀錄者	葉長翰
討論主題	系統分析暨專題文件分工			會議時間	2022/03/30 22:00~22:25
				會議地點	圖書館 501 教室

上次會議	決議事項	執行狀況
	1. 使用者需求描述修正。 2. 使用者需求描述－情境分割彙整。	如會議討論事項修正完畢。

本	本週工作進度	本週工作內容	負責人員

次會議	1. 系統分析作業 2. 4/11 專題簡報	1. 系統分析表 1P8 ~1P8_1 須完成 2. 系統分析表 2P1~3 須完成 3. 系統分析表 2P4 須完成 4. 4/11 專題簡報分工	全體組員，依會議決議執行
本次會議內容	1. 系統分析作業分工 2. 4/11 專題簡報分工 3. 臨時動議： (1) 專題老師建議系統相關參考文獻、需求問卷需著手蒐集資料。		
決議事項 (或 主席裁示)			
1. 請各組員依照上週藍圖分工項目，依序完成表 1P_8、表 2P_1~3；例如原負責身體總熱量需求計算，則依此功能完成上述表格。 2. 上述事項須於 4/2 下午 15:00 前完成並上傳群組。 3. 請各組員閱覽其他成員作業，了解全系統架構，「暫定」4/4 晚間進行線上會議討論。 4. 4/11 專題簡報分類：需求描述、系統功能、系統流程，由聿惟進行報告、組長進行簡報製作、其餘組員依上述分類進行資料彙整。 5. 依專題指導老師建議，請組長將學校專題所需文件之公告連結張貼於群組記事本，以利各組員閱覽。			
請簽名	請簽名	請簽名	

下次會議	召集人	陳禹丞	紀錄者	葉長翰	時間	2022/04/04
					地點	LINE 群組
預定討論主題	系統分析表 2P4 繪製討論					

【會議紀錄】						
組名		專案名稱	智能合約開發問題與風險			
組別	第 4 組					
會議編號	M7	召集人兼主席	陳禹丞	紀錄者	葉長翰	
討論主題	系統分析暨專題文件分工－文獻探討			會議時間	2022/05/14	21:00~22:40

		會議地點	Line 群組

上次會議	決議事項	執行狀況
	1. 表 1P_8、表 2P_1~3。 2. 表 2P4。 3. 4/11 專題簡報。	如會議討論事項已完成。

本次會議	本週工作進度	本週工作內容	負責人員
	1. 文獻資料探討 2. 程式架構探討 3. 程式資源蒐集	1. 文獻探討蒐集與彙整。 2. 網站架設需求與排程分析。 3. 網頁設計網路資源蒐集。	陳禹丞

本次會議內容	1. 文獻資料探討：除組長、冠逸外，其餘組員各自蒐集文獻資料與彙整，並於 5/21 提交組長審查。 2. 程式架構探討：組長針對網站架設需求排程進行分析，同步各組員以利專案進度追蹤。 3. 程式資源蒐集(ASP.NET、BOOTSTRAP、SQL server)：其他組員進行資源蒐集與整理，完成後與各組員進行探討。

決議事項 (或 主席裁示)
1. 同會議內容。

請簽名	請簽名	請簽名

下次會議	召集人	曲莉莉 專題老師	紀錄者	陳禹丞	時間	TBD

預定討論主題	TBD

【會議紀錄】				
組名		智能合約開發問題與風險		
組別	第 4 組			
會議編號	M8	曲莉莉 專題老師	紀錄者	陳禹丞

討論主題	專題內容分工與討論		會議時間	2022/7/05	09:00~10:05
			會議地點	Google Meet	

上次會議	決議事項	執行狀況
	1. 系統分析作業 2. 4/11 專題簡報	

本次會議	本週工作進度	本週工作內容	負責人員
	1. 網站內容 2. 工作分工	1. 文獻資料與主題相關的尋找 2. 美工製作 3. 網站架構 4. Google 表單製作	全體組員

本次會議內容
1. 文獻資料與主題相關的尋找 2. 美工製作 3. 網站架構 4. Google 表單製作

決議事項 (或 主席裁示)
下次開會時要報告這週做了哪些東西

請簽名	請簽名	請簽名
陳禹丞	陳禹丞	陳禹丞

下次會議	召集人	曲莉莉 專題老師	紀錄者	陳禹丞	時間	
					地點	Google meet
預定討論主題						

【會議紀錄】

組名		專案	智能合約開發問題與風險

<table>
<tr><td>組別</td><td>第 4 組</td><td>名稱</td><td colspan="4"></td></tr>
<tr><td>會議編號</td><td>M9</td><td>召集人兼主席</td><td>曲莉莉 專題老師</td><td>紀錄者</td><td colspan="2"></td></tr>
<tr><td rowspan="2">討論主題</td><td colspan="3" rowspan="2">(例會)每周進度檢討</td><td>會議時間</td><td>2022/7/13</td><td>21:00~22:00</td></tr>
<tr><td>會議地點</td><td colspan="2">Google Meet</td></tr>
<tr><td rowspan="2">上次會議</td><td colspan="2">決議事項</td><td colspan="4">執行狀況</td></tr>
<tr><td colspan="2">1. 文獻資料與主題相關的尋找。
2. 美工製作。
3. 網站架構。
4. Google 表單製作。</td><td colspan="4">1. 由文書組 禹丞組長、宏澤、長翰執行，並於本次會議報告。
2. 由美編組 聿惟、承憲設計，並上傳至 LINE 群組。
3. 由編碼組 冠逸、禹丞執行，並於本次會議報告與展示。
4. 問卷 Google 表單由 禹丞組長執行，並於本周會議進行確認後開放填寫。</td></tr>
<tr><td rowspan="2">本次會議</td><td>本週工作進度</td><td colspan="3">本週工作內容</td><td colspan="2">負責人員</td></tr>
<tr><td>1. 問卷內容檢討與 google 表單調整確認
2. 文書組、美編組、編碼組進行每週進度說明與展示。</td><td colspan="3">1. 問卷已開放填寫，請各組員進行宣導，並於下周會議進行成效檢討。
2. 各組線上會議展示成果，並遵從專題老師建議事項修正。</td><td colspan="2">全體組員</td></tr>
<tr><td>本次會議內容</td><td colspan="6">1. 問卷開放期限與樣本數討論。
2. 專題 logo 討論。
3. 專題所需文件 review 與檢討。
4. 編碼組網站排版展示。</td></tr>
<tr><td colspan="7">決議事項 (或 主席裁示)</td></tr>
<tr><td colspan="7">1. 問卷開放期限為 07/13~07/21，預期問卷回收數量 200 份。</td></tr>
<tr><td colspan="2">請簽名</td><td colspan="2">請簽名</td><td colspan="3">請簽名</td></tr>
<tr><td>下次會議</td><td>召集人</td><td>曲莉莉 專題老師</td><td>紀錄者</td><td>陳禹丞</td><td>時間</td><td>依 line 群組通知</td></tr>
<tr><td colspan="5"></td><td>地點</td><td>Google Meet</td></tr>
</table>

預定討論主題	(例會)每周進度檢討

【會議紀錄】

組名		專案名稱	智能合約開發問題與風險		
組別	第 4 組				
會議編號	M10	召集人兼主席	曲莉莉 專題老師	紀錄者	陳禹丞
討論主題	(例會)每周進度檢討			會議時間	2022/7/20 21:00~22:30
				會議地點	Google Meet

上次會議	決議事項	執行狀況
	1. 問卷內容檢討與 google 表單調整確認。 2. 問卷開放期限為 07/13~07/21，預期問卷回收數量 500 份。 3. 文書組、美編組、編碼組進行每週進度說明與展示。	1. 問卷已開放填寫，請各組員加強宣導。 2. 各組線上會議展示成果，並遵從專題老師建議事項修正。

本次會議	本週工作進度	本週工作內容	負責人員
	1. 問卷進度檢討。 2. 各組本週進度展示與說明。	1. 問卷回收狀況階段性檢討。 2. 各組本週工作內容如附件一說明。	全體組員

本次會議內容
1. 本組問卷自 8/20 開放填寫至 9/18 23:59 為止，已回收 212 份問卷，距離目標尚餘 20~30 份，距 9/18 截止日尚有一天，請各組員加強宣導。 2. 專題 logo 已於 Line 群組開放票選至明日 12:30 為止，每人可選 3 幅圖檔，依得票最高者為本組專題 logo。 3. 請美編組配合編碼組進行功能區標題 icon 設計、網頁背景圖片製作，並將去背圖檔上傳至雲端資料夾以利使用。先以「料理食譜」、「健康餐盒據點」兩功能區進行設計；網頁背景圖檔以淺色系為主。 4. 編碼組於會後將網站網址上傳 Line 群組展示，請老師與各員依使用者角度給予建議。 5. 老師建議可於「致理科技大學圖書館／技術典藏／博碩士論文系統」查詢與專題題目相關文獻進行參考。
決議事項 (或 主席裁示)

1. 請韻砡協助文書組進行文獻資料蒐集。 2. 請各組員於下周會議日期中午前提報本週工作事項與障礙點，以利會議時討論。						
請簽名		請簽名陳禹丞		請簽名		
下次會議	召集人	曲莉莉 專題老師	紀錄者	陳禹丞	時間	依 line 群組通知
					地點	Google Meet
預定討論主題	(例會)每周進度檢討					

【會議紀錄】						
組名		專案名稱	智能合約開發問題與風險			
組別	第 4 組					
會議編號	M11	召集人兼主席	曲莉莉 專題老師	紀錄者	陳禹丞	
討論主題	(例會)每周進度檢討			會議時間	2022/7/28	21:00~22:00
				會議地點	Google Meet	
上次會議	決議事項		執行狀況			
	1. 問卷請各組員加強宣導。 2. 專題 logo 票選。 3. 請美編組配合編碼組進行功能區標題 icon 設計、網頁背景圖片製作。 4. 網頁頁面呈現。 5. 文書組可多至致理圖書館蒐集資料。		1. 問卷已於 9/18 截止，共計 255 份，有效問卷 253 份。 2. 專題 logo 已票選完成。 3. 美編組已將設計圖檔上傳群組雲端空間。 4. 頁面展示功能依專題老師建議，其中兩分頁採用開啟新分頁方式呈現。 5. 文書組依專題老師建議各自蒐集資料。			
本	本週工作進度		本週工作內容		負責人員	

次會議	1. 各組本週進度展示與說明。 2. 文件組資料檢討。 3. 問卷分析 review。 4. 文件第三章節部分請文件組至圖書館機構典藏搜尋歷屆專題報告文件進行參考。	1. 各組本週工作內容如附件一說明。	全體組員
本次會議內容	1. 專題網頁背景圖片與 logo 決議完成；分頁背景色系請編碼組與美編組會後擇期討論。 2. 請文件組同學每周進度於開會前一日提供，已便老師批閱。 3. 網頁用 icon 數量暫時充足，請美編組同學協助編碼組進行網站資料內容建置，如健康餐盒據點、料理食譜內容，詳細資訊請美編組與編碼組於會後擇期討論，並於下周會議時展示。 4. 本組問卷已回收完畢共計 397 份，有效問卷 397 份；請文件組同學進行問卷分析與文件第三章節撰寫。 5. 美編組同學後續須負責簡報製作，需從中了解文件內容，以利後續簡報內容製作。		
決議事項 (或 主席裁示)			
1. 如本次會議內容所述。			
請簽名	請簽名	請簽名	

下次會議	召集人	曲莉莉 專題老師	紀錄者	陳禹丞	時間	依 line 群組通知
					地點	Google Meet
預定討論主題	(例會)每周進度檢討					