

專題名稱：區塊鏈應用與以太幣的過去現在未來

學生姓名：鄭卉妤、趙珮淳、沈欣穎、王毓綺、陳正昆、陳展翔、鄭勝仁

摘要

隨著時代的演變，越來越多的投資人把資金轉向虛擬貨幣這塊，也會開始去研究以太幣相關的區塊鏈，像以太幣的特性及應用慢慢勝過最廣為流傳的比特幣，這也讓以太幣開始被注意，讓更多的投資人開始注意以太幣之後未來的成長性跟他可以運用的地方，也帶動了一塊新的全新領域，讓未來的投資人不再只有傳統的股票，基金或是外匯商品來做選擇，配合虛擬交易平台有更多的方向可以去參考，藉由此次專題讓投資者了解從零開始的投資者，可以更了解從虛擬貨幣是如何運作的，我們也會介紹裡面的是如何發展到現今被大眾給接受並且活用度越來越高的，如何從一開始不被大眾接受到現今每個網路上都有區塊鏈的身影，以及介紹以太幣過去到未來所展現的成長性。

關鍵字：虛擬貨幣、區塊鏈、以太幣

目錄

摘要.....	0
壹、前言.....	2
一、研究背景與動機.....	2
二、研究目的.....	2
貳、虛擬貨幣與區塊鏈介紹.....	3
一、定義.....	3
(一) 區塊鏈定義.....	3
(二) 虛擬貨幣定義.....	3
二、介紹.....	3
(一) 區塊鏈介紹.....	3
(二) 以太坊介紹.....	7
(三) 以太幣介紹.....	9
三、技術應用.....	12
(一) 區塊鏈應用.....	12
(二) 以太坊應用.....	13
四、虛擬貨幣的比較.....	15
五、以太幣的未來趨勢.....	17
(一)、以太幣 2.0.....	17
(二)、以太坊網路升級.....	17
(三)、以太坊(以太幣)的未來潛力.....	18
參、結論.....	21
肆、參考文獻.....	21

表目錄

表 1:區塊鏈的歷史.....	4
表 2:交易所購買虛擬貨幣比較.....	10
表 3:交易所購買虛擬貨幣優缺點.....	10
表 4:虛擬貨幣比較.....	16

圖目錄

圖 1:區塊鏈運作模式.....	7
圖 2:智能合約的 3 要素.....	8
圖 3:智能合約、傳統合約有什麼不同.....	9
圖 4:台灣虛擬貨幣 ATM 分布.....	11

壹、前言

一、研究背景與動機

近年來虛擬貨幣逐漸盛行，許多交易所紛紛成立，而虛擬貨幣交易過程是公開的不需要透過銀行，只要開戶後就可以提供儲值現金購買虛擬貨幣，主要虛擬貨幣以 USDT(泰達幣)、BTC(比特幣)、ETH(以太幣)三種虛擬貨幣為主流。

可能大家都知道虛擬貨幣但是並沒有深入的去了解以及研究，所以我們使用以太坊(以太幣)為主切入主題做深入的探討及研究。

二、研究目的

科技發展日新月異，貨幣的使用與流通也逐漸從實體走向虛擬化。近年來虛擬貨幣對經濟層面的影響逐漸擴大，然而大眾對於虛擬貨幣的應用原理——區塊鏈技術、虛擬貨幣的交易體系、以及虛擬貨幣普及對未來經社環境可能帶來的改變與其衍生的風險和犯罪議題等可謂是一知半解、似懂非懂的。

希望透過本專題能協助釐清對虛擬貨幣的認知，投資者在面對走向貨幣數位化的時代能更深度掌握加密貨幣的應用範圍與風險性，創造更大的財富。

我們以以太坊(以太幣)為主題進行研究，

主要研究目的為：

1. 了解虛擬貨幣與區塊鏈技術之發展背景及運行系統。
2. 歸納並定義以太坊和以太幣的運作架構、分析以太幣與其他虛擬貨幣的優異比較與應用範圍。
3. 研析以太幣未來發展趨勢和對金融體系可能帶來的變革衝擊與潛在影響。

貳、虛擬貨幣與區塊鏈介紹

一、定義

(一) 區塊鏈定義

區塊鏈是藉由密碼學串接並保護內容的串連文字記錄（又稱區塊）。是不可變的共用分類帳，可在商業網路中促進記錄交易與追蹤資產的程序。幾乎任何有價值的東西都可以透過區塊鏈網路追蹤與交易，分散式帳本能讓兩方有效記錄交易，且可永久查驗，全面降低風險和成本。

(二) 虛擬貨幣定義

在虛擬空間中特定社群內可以購買商品和服務的貨幣，廣泛應用在區塊鏈上與現實做連結，有交易平台和記帳的貨幣功能。例：比特幣（Bitcoin）、以太幣（Ethereum）等，都是沒有實體貨幣。虛擬貨幣沒有地域的區分，只要有網路及電子設備就可以做虛擬交易，不需支付手續費，就能夠讓資產自由轉移的貨幣，買賣透過虛擬貨幣交易所集中市場，減少交易的成本。虛擬貨幣的投機性強，但波動比一般實體貨幣來的劇烈，交易者的心態容易受影響，且不是法定貨幣，不具有法償效力。通常應用在網路遊戲、單向兌換、雙向兌換，單向兌換像是在區塊鏈平台上購買商品或是換取虛擬商品，雙向兌換就是幣與幣之間買賣雙方去達成交易，例：比特幣兌換以太幣、以太幣兌換萊特幣。

二、介紹

(一) 區塊鏈介紹

所謂的區塊鏈其實就是一連串的紀錄，利用密碼學中 hashing 的技巧將之串聯在一起，是用以比喻一套「使用分散式帳本技術的系統」的簡稱，這種系統可以記錄、追蹤任何價值的移轉，不論是金融交易、醫療紀錄、土地所有權甚至是選票。

區塊鏈隨著不同的應用場景，各自的去中心化程度與信任程度皆有所不同，被分為三種主要類型，公有鏈（Public Chain）公平公開，所有人可自由存取、瀏覽，如：以太坊，私有鏈（Private Chain）不具有區塊鏈去中心化的屬性，需授權，僅開放特定使用者或團體使用，如：企業、金融業，以及聯盟鏈（Consortium Blockchain）介於公有鏈與私有鏈之間，結合兩者的主要特色，常見於同類型的企業或有合作關係的不同企業，會依照各自去中心化與信任的程度有所不同。

1. 區塊鏈的歷史：

區塊鏈的歷史大致上可分為三期。

(1.) 醞釀期：2009-2012 年，經濟形態以比特幣及其產業生態為主。

(2.) 萌芽期：時期為 2012-2015 年，區塊鏈隨著比特幣進入公眾視野，以及行動支付和匯款公司的出現，區塊鏈經濟擴散到金融領域。區塊鏈底層技術創新不斷從比特幣系統中剝離出來。

(3.) 發展期：2016 年開始探索行業應用，出現了大量區塊鏈創業公司。

表 1: 區塊鏈的歷史

2008 年—區塊鏈起源的時空背景	在網路上發布了一份名為“比特幣：點對點電子現金系統”的文件。
2009 年—區塊鏈的創世塊誕生	Satoshi 於 2009 年 1 月推出比特幣，作為當前金融體系和權力中心的替代品。
2010 年—區塊鏈加密貨幣交易所成立	比特幣市場(Bitcoin Market)是世界上第一個加密貨幣交易所。
2011 年—區塊鏈搜尋熱度與討論趨勢攀升	Silk Road，又稱絲綢之路的一個線上商城，於 2 月份推出。
2012 年—發展區塊鏈底層技術的應用和其他可能	OpenCoin (現稱為 Ripple) 誕生了。它不是使用像比特幣那樣挖掘來驗證的支付，而是使用網絡成員之間的共識。
2013 年—各地延伸的區塊鏈狂熱與事件	Vitalik Buterin, 一位 19 歲的開發人員，共同創辦了比特幣雜誌，他對新型加密貨幣抱有遠見。一個可以做的不僅僅是付款。他在一份名為“以太坊：下一代智能合約和分散應用平台”的白皮書中提出了這一建議。
2014 年—全球性的區塊鏈討論	Vitalik 和他的團隊帶領一個成功的 ICO (最初的硬幣投放或眾籌活動) 來啟動以太坊。
2015 年—區塊鏈技術的革新	納斯達克(NASDAQ)開始進行區塊鏈試驗，目的為提高速度，效率和降低成本。 以太坊推出自己的區塊鏈。

2016 年－區塊鏈服務的震盪時期	IBM 開始向企業提供 BaaS（區塊鏈服務）。
2017 年－區塊鏈技術進入金融體系的應用	歐洲銀行聯合組建數位貿易鏈，用區塊鏈提供企業貿易融資。比特幣在日本被認定為合法貨幣。
2018 年－區塊鏈社群的全球化發展	加密貨幣 EOS 在有史以來最大的 ICO 中籌集了 40 億美元，許多人相信它有一天會取代以太坊。 Santander 與 Ripple 合作，為客戶提供次日國際轉機服務。這是第一家使用區塊鏈技術的英國銀行。
2019 年－區塊鏈的多元運用與區塊鏈生態系	全球最大的區塊鏈 ETF（指數型證券投資信託基金）在倫敦證交所正式上市交易。

2. 區塊鏈的特性：

- (1.) 去中心化：強調區塊鏈的共享性，讓使用者可以不依靠額外的管理機構和硬體設施，讓它不需要中心機制，因此每一個區塊鏈上的資料都分別儲存在不同的雲端上，核算和儲存都是分散式的，每個節點都需要自我驗證、傳遞和管理，是區塊鏈最核心的本質特色。
- (2.) 不可竄改性：區塊鏈中的每一筆資料一旦寫入就不可以再改動，只要資料被驗證完就永久的寫入該區塊中，透過一對一的函數來確保資料不會輕易被竄改，這種函數很容易被驗證但卻非常難以破解，無法輕易回推出原本的數值，資料就不能被竄改，每個區塊得出的值也會被放進下一個區塊中，讓區塊鏈之間的資料也都被正確的保障。區塊鏈就是比特幣的底層技術，也可以說比特幣帶動了區塊鏈觀念的興起，去中心化的公開性讓所有人都能夠自由購入與售出，交易的匿名性和金流資料的安全性更是比特幣所依靠的基礎。
- (3.) 加密安全：加密技術在區塊鏈裡是最重要的特性之一，每一個數據庫都有屬於自己的金鑰，用戶要讀取數據庫或是寫入資料都需要有正確的加密密鑰，所以駭客要入侵區塊鏈系統並做出任何破壞或竄改幾乎不可能。

(4.)透明的流程：區塊鏈系統是公開透明的，除了私有訊息經過密碼學加密，其他數據皆公開在網路上，任何人都可以通過公開的接口查詢區塊鏈數據記錄或者開發相關應用，這也是區塊鏈系統值得信任的基礎。如此特性也使得區塊鏈技術，能夠減去過去一些需要程序複雜的程序，資料的透明性也就有助於減少大量的人力與紙上作業，甚至發展出所謂的智能合約應用。

3. 區塊鏈優缺點：

(1.)優點：

- a. 無人工參與與中介便能提高資料準確性
- b. 不需第三方驗證就能降低成本
- c. 去中心化使得資料的竄改顯得很困難
- d. 交易安全、私密且效率極高
- e. 資訊透明
- f. 能為政府不穩或低度發展的國家，提供更安全可靠銀行的替代方案與個人資訊保存的方法

(2.)缺點：

- a. 像是比特幣這類採取工作量證明的區塊鏈需要耗費大量的資源（如電力、算力）
- b. 目前交易流動較低
- c. 存在著非法使用的可能
- d. 各國法規的限制與不適用
- e. 當程式碼出問題或是遭遇駭客時個人權益難以被保障

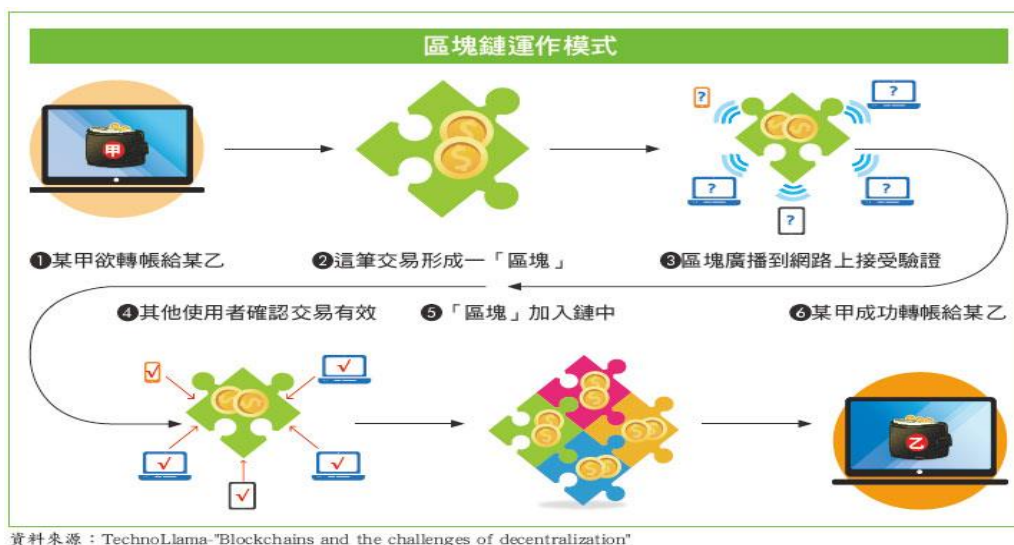


圖 1: 區塊鏈運作模式

(二) 以太坊介紹

以太坊是維塔利克·布特林所提出一個用戶自己創建和運行的系統，他最有特色的地方就是去中心化，她沒有一個集中的發行台，每台計算機都能保留自己的分類帳，爾且由於分布式的特色，以太坊很難受到嚴重的攻擊，並且僅依靠其歷史記錄來確保交易的合法性，來確保每一項交易都有紀錄存在讓越來越多人相信這個系統。

1. 以太坊運作：

數字應用可廣泛應用於任何場景，從租賃到僱傭合同等，但必須使用以太坊貨幣，即以太幣。這些應用不依賴於人工參與，而是由事件觸發，因此不需要人為干預。

2. 以太坊與加密貨幣：

以太幣目前作為市值第二大的貨幣在交易量來說，是讓以太坊區塊鏈讓目前人們使用最多的一種原因，是加密貨幣的一種。一些人將「以太幣」和「以太坊」混為一談，實際上對於大多數人來說平台所使用的加密貨幣比它們的系統更廣為人知。

3. 智能合約：

最早由身兼電腦科學家及密碼學專家的 Nick Szabo 在 1994 年所提出，並將其定義為協議與用戶界面相結合的一種工具，從而對計算機網絡進行規範和安全加固。而後中本聰在 2008 年《比特幣白皮書》中提出「區塊鏈」的概念，Nick Szabo 的想法才得以被逐步實現。比特幣區塊鏈訂定了「區塊鏈合約」的基礎，但

因其基礎於當時無法滿足所有需求下，出現了以太坊區塊鏈，以太坊為每個交易需求，特別打造了「智能合約」。

是區塊鏈中一種制訂合約時使用的特殊協議，主要用於提供驗證及執行智能合約內所訂定的條件。智能合約中內含程式碼函式，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。這些交易具有可追蹤、難以竄改與不可逆轉的特性，使智能合約在沒有第三方的情況下，也能進行安全的交易，且智能合約由創建者定義、區塊鏈網路執行所建構而成，與合約條款相關的所有訊息，全都是按照合約當中所設定的操作自動執行。

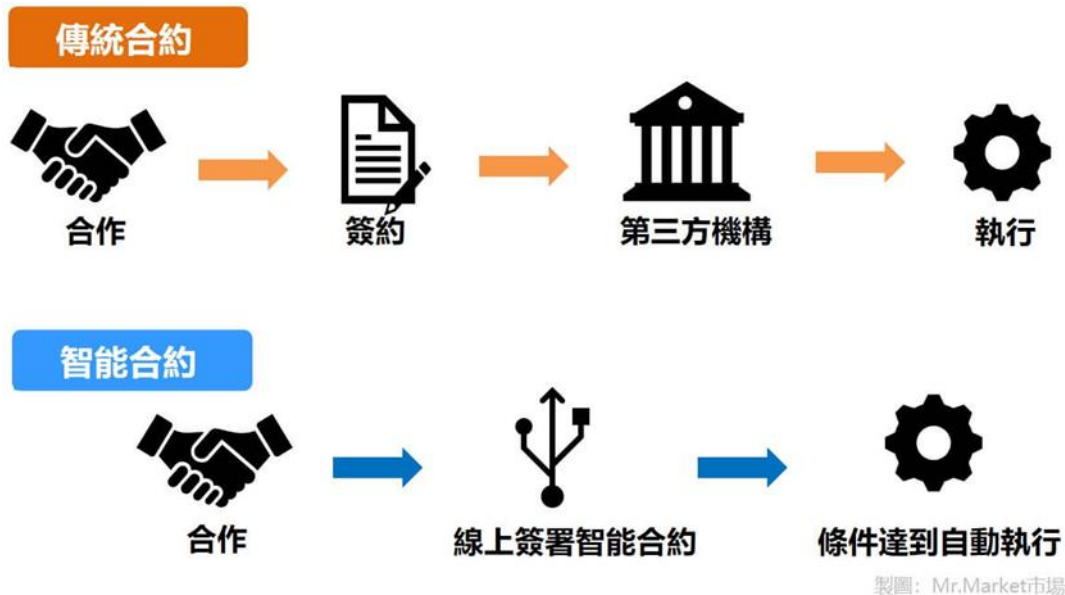


圖片來源: <https://rich01.com/what-is-smart-contract/>

圖 2: 智能合約的 3 要素

- (1.) 自治：合約啟動就會自動執行，將雙方的協議條款寫入代碼中，不需要任何人為的干預。
- (2.) 自足：智能合約可以在資源整合能力上自給自足，比如有權限調配合約雙方的資金和財產。
- (3.) 去中心化：通過分散式的節點來自動運行，而不用透過中心化的單個伺服器。

以太坊把智能合約的應用程式，稱為去中心化應用程式(Decentralized App, Dapp)。智能合約可以用來串聯 Dapp 與區塊鏈，當做它們兩者間的橋樑，Dapp 前端介面加上去中心化的智能合約，因為放在區塊鏈上，所以不需要伺服器。簡單來說，可以把以太坊想像成是作業系統，而 Dapp 是安裝在作業系統的 APP，具備去中心化、數據不可竄改、公開透明的特性，因此比使用中心化的傳統 APP 更安全。



圖片來源：<https://rich01.com/what-is-smart-contract/>

圖 3: 智能合約、傳統合約有什麼不同

傳統合約中的任何一方必須信任彼此並履行義務，同時還必須有第三方的執法機構介入，若是有一方違反條款，就需要這個執法機構進行判決；智能合約雙方或者多方可以通過區塊鏈做出承諾，無需相互了解、信任彼此，因為合約內容如果達到觸發條件，會完全自動強制執行，公開透明且不會被更改。因此使用智能合約可以消除對中介的需求，從而顯著降低運營成本。

(三) 以太幣介紹

以太幣是以太坊下所開發的區塊鏈平台，能正常運作的一種原生加密貨幣，目前是價值第二大的數字貨幣，運用在各式虛擬交易的項目裡，並且目前以太幣也可以作為挖礦的獎勵並計算交易手續費等等的工作，然而以太幣跟比特幣最大的不同是以太幣的數量沒有限制，但他的年增供量目前可能不太夠用，因為供應

量增長存在限制，而且新供應需求得產生讓他不得不找出一個更有效的控管方式來幫助以太幣成長，讓以太幣才能更好的去運用在更多產品上。而且目前的 NFT(數位藝術品)，幾乎都是以以太幣來做為計算的，所以以太幣在 NFT 的應用下運行智能合約，並且在以太坊製作區塊鏈，相信會讓他變得越來越有價值。

目前購買以太幣的方式較為常見的方式是和持有以太幣的人購買。那麼誰持有以太幣呢？台灣現在有許多虛擬貨幣交易所以及受監管的差價合約平台也推出了虛擬貨幣的業務，甚至可以從超商或虛擬貨幣 ATM 處購買。以下將分別介紹：

(1.)交易所購買：

用戶可直接從交易所購買虛擬貨幣。我們舉出台灣用戶較為熟知的四間交易所為例並比較：

表 2:交易所購買虛擬貨幣比較









	交易方式	資金保管 銀行	每日交易量	幣種數量	相關費用（掛單、吃單、入金、出金）
 Bitopro	現貨	無	約台幣 2.6 億	14	最高
 Ace	現貨	凱基銀行	約台幣 1 億	14	最低
 Max	現貨	遠東銀行	約台幣 3.6 億	16	次高
 Bitasset	現貨、合約	無	X	X	次低

表 3:交易所購買虛擬貨幣優缺點

	優點	缺點
 Bitopro	操作介面清晰 提供限價停損	優惠活動較少 手續費用較高
 Ace	手續費較便宜 客戶資金安全性較高	入金速度較慢 認證流程繁瑣
 Max	入金速度較快 提供限價停損	出金手續費較高
 Bitasset	提供任務獎勵 提供止盈止損	教學資源難搜尋 網站系統速度較慢

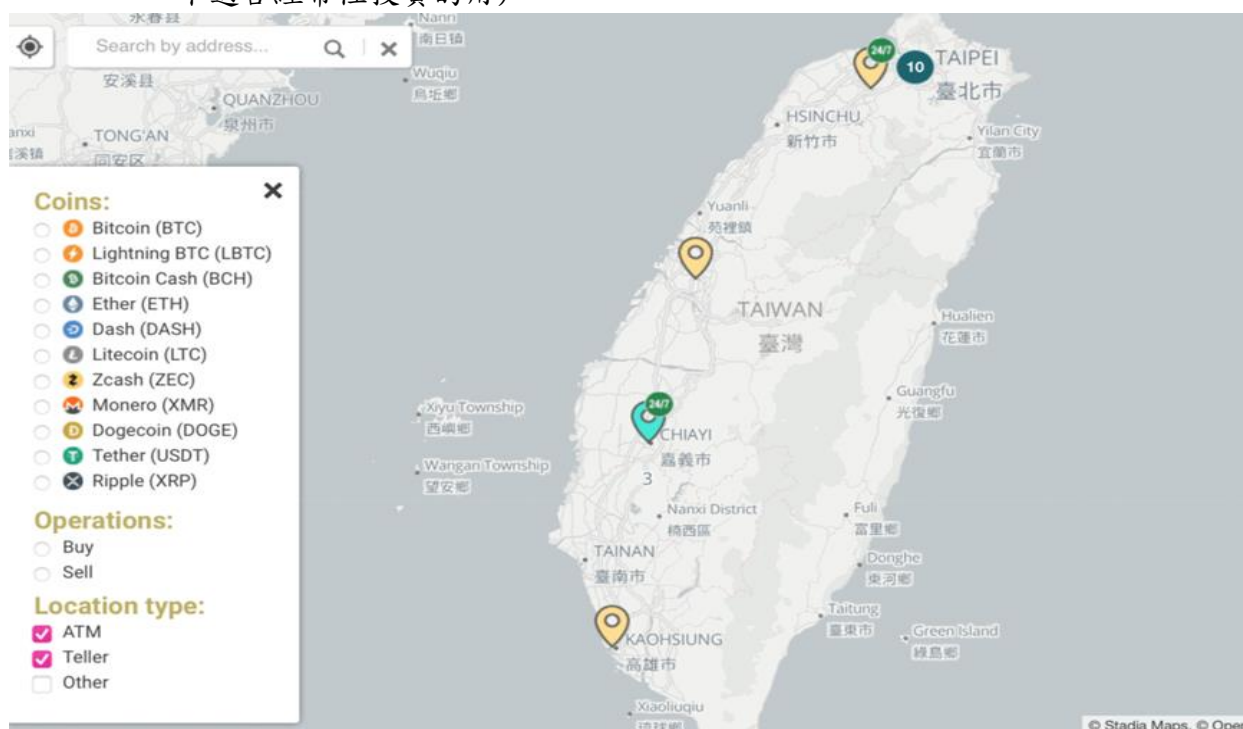
*Bitasset 於 2019 年傳出詐騙事件，於 2021 年 4 月公告維修並暫停服務，至今仍無更新，可能成為跑路平台。

(2.) 差價合約(CFD)平台購買：

差價合約交易平台提供的並非買賣真正的虛擬貨幣，而是差價合約，用戶並不會實際持有虛擬貨幣，且出金時需要先通過場外交易將台幣轉換為虛擬貨幣才能進行交易。差價合約是利用槓桿買賣金融衍生品價差的方式，增加了用戶的投資機會，適合想透過簡單方式買幣賺取價差的用戶。然而槓桿放大盈利的同時也增加了虧損的風險，因此建議新手可選擇配置靈活槓桿的 CFD 平台，如 Mitrade。Mitrade 不但交易成本極低，且受權威金融監管，用戶金資安全較有保障；其配置靈活槓桿能夠滿足不同風險偏好的用戶需求。

(3.) 台灣超商/ATM 購買：

台灣超商遍佈、業務種類繁多，在超商即可購買對於忙碌的現代人來說非常方便。然而超商收取的代收手續費相較於只收取極低交易手續費的 Binance、Mitrade 等而言，成本可說是相當高。也可以透過虛擬貨幣 ATM 購買，不過機台目前並不普及，機台大部分集中在台北，而台中、台南、高雄則各僅設有一部，且手續費與超商一樣比較貴，因此較不適合經常性投資的用戶。



圖片來源：<https://www.investors.tw/buy-bitcoin/>

圖 4: 台灣虛擬貨幣 ATM 分布

(4.) 場外購買：

由於場外交易 (OTC) 並非在常規的交易所，而是在網路、銀行等購買，因此既不會公開買賣雙方交易資訊，且不受交易所開收盤時間限制隨時可進行，對於想進行大手交易的高淨值用戶以及散戶而言，場外交

易是最理想的選擇。比較常見的方法有私下直接交易及透過 OTC 平台購買。私下直接交易即為和持有以太幣的人約定交易，用戶轉帳台幣給對方，而對方將以太幣轉帳給用戶，進而達成交易；而透過 OTC 平台購買則是由買賣其中一方以廣告等方式提供交易資訊，兩方再進行約定交易，模式類似於網購。場外交易雖較不受市場限制且能依雙方需求訂立交易協議，但因其不受監管的性質，交易對象違約風險也相對較高。

三、技術應用

(一) 區塊鏈應用

1. 區塊鏈演化三部曲：

第一個階段是啟發型區塊鏈解決方案，也是當前區塊鏈所處的階段，解決方案主要是利用區塊鏈的分布式、加密、不可篡改等三大技術特點，提供單一流程的效率提升或者現有流程的精簡。

第二階段是完整型區塊鏈解決方案，利用基礎的分布式、加密、不可篡改的技術特點以外，同時利用智能合約、治理去中心化和價值交換的技術特點，創造全新的商業模式，提供端到端的客戶體驗閉環，提升企業總體生產效率。

第三階段是增強型區塊鏈解決方案，意在構建一個分布式可編程的數字經濟，結合萬物互聯和萬物智能的技術演進，在外來數字世界和物理世界越來越融合的數字經濟中，構建一個人、組織、物、數據和價值之間的關係網、區塊鏈除了在金融領域被廣泛運用外，也開始漸漸在法律、零售、醫療等領域，未來更可能在更多領域中作用。區塊鏈的邏輯能夠解決不同組織間的信任問題，去中心化的模式也能夠優化點對點的效率，發展到最後也可能跟本地顛覆現有的資本主義型態，使全球協作模式成為可能。

2. 目前常用的區塊鏈應用：

區塊鏈應用不是只有金融業事情，在現在生活中廣泛應用到區塊鏈無論是轉帳、物聯網、交易、管理、醫療方面，區塊鏈都能改善現在既有的生活品質與商業模式。

(1.)NFT：就應用到了區塊鏈認證服務，讓藝術家或者是想透過這個技術來發表個人作品的人一個舞台，利用數位藝術可以透過區塊鏈線上保護作品，數位資產的智慧財產權。

(2.) 身分驗證:

- a. 數位身分驗證:現在很多網站、軟體使用中心化幫助廠商登入，可以在網路世界自由地做交易與轉帳。
- b. 區塊鏈身分驗證:每個人的資訊都是公開的，人人都可以查閱只要有網路的地方都可以，可以減少需多的不方便。

(3.) 醫療去中心化: 做主要是個人醫療紀錄保存，如果用區塊鏈技術來保存紀錄，病人可以透過這技術來查閱自己的歷史資料，掌握自己的健康。

(4.) 網路安全: 雖然公開個人資訊但應用區塊鏈的技術可以來確保安全，不被駭客入侵。

(二) 以太坊應用

以太坊的功能不只有支付的功能而已，它還可以編寫智慧合約。簡單來說的話就是，讓開發者能在區塊鏈上寫程式，發展多元應用。智能合約最基本的應用，就是做出新的加密代幣！只要製作一份智能合約到以太坊的區塊鏈上，遵循一定的規範來製作的話，就能製造出一個屬於自己的代幣，任何人都可以很容易地創造出自己的加密代幣，擴展到數字應用。

數字應用可廣泛應用於任何場景，從租賃到僱傭合同等，但必須使用以太坊貨幣，即以太幣。這些應用不依賴於人工參與，而是由事件觸發，因此不需要人為干預。例如，一旦成功交付的配送被登記後，將自動從一個以太坊錢包轉賬支付以太幣到另一個錢包。這有助於實現快速付款，避免財務確認接收、等待文書、付款及等待收款等一系列繁瑣的流程。

1. 智能合約運作方式:

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。

智能合約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。智能合約的運作方式也與自動販賣機有點相似——它會自動執行合約上的指令。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。

那麼，創造一份智能合約有哪些構成要素呢？——合約主體 (Subject of Contract)、數位簽名、合約條款及去中心化平台 (decentralized platform) 的應用：

- (1.) 合約主體 (Subject of Contract)：智能合約中必須要有合約主體才能自動鎖定及解開合約中的相關商品或服務。
- (2.) 數位簽名 (Digital Signature)：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。
- (3.) 合約條款 (Contract Terms)：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。
- (4.) 去中心化平台 (Decentralized Platform)：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。

注意：由於區塊鏈特性，智能合約編寫並被放入區塊鏈後，所有合約條款就不能夠再被改變！

2. 智能合約的應用：

根據智能合約的特性，智能合約可被用於現實生活上很多領域，比如：投票選舉、物聯網、流程管理、銀行業務、房地產業務證明、保險業務等等一些需要 "中介" 及缺乏 "互信" 的行業或服務，都可以使用上智能合約去簡化，甚至解決問題。

編譯和部署智能合約：話說在 Ethereum 智能合約可以被大家使用前，必須先被部署到區塊鏈上。從智能合約的原始碼到使用智能合約，大概包含幾個步驟：

- (1.) 撰寫智能合約的原始碼 (一般是用 Solidity 寫)。
- (2.) 編譯智能合約的原始碼成可在 EVM 上執行的 bytecode (binary code)。同時可以透過編譯取得智能合約的 ABI。
- (3.) 部署智能合約，實際上是把 bytecode 儲存在鏈上 (透過一個 transaction)，並取得一個專屬這個合約的地址。
- (4.) 如果要寫個程式呼叫這個智能合約，就要把資料發送到這個合約的地址 (一樣透過一個 transaction)。Ethereum 節點會根據輸入的資料，選擇要執行合約中的哪一個 function 和要輸入的參數。

3. 智能合約優缺點：

(1.)優點:

a. 安全性很高:

隨著區塊鏈的發展越來越穩定，智能合約加密儲存在區塊鏈點上會更加的安全，爾且也不會因為人為疏失而搞丟或隨意的篡改合約內容。

b. 交易效率高:

因為交易方法幾乎為全自動化，所以智能合約對於第三方機構的需求也降低許多，這也會讓交易的時候少一個步驟讓合約執行的速度快上許多。

c. 合約內容不能被篡改:

在智能合約代碼被寫好送進區塊鏈時，裡面的內容就不能有任何的更改，也不會有後續的兩方合約不同的問題。

(2.)缺點:

a. 智能合約可客制化:

智能合約跟傳統的合約一樣可以由自己來決定內容，但是簽訂後合約內容部屬在區塊鏈上所以合約不能篡改。

b. 法律問題:

在這方面的法律規定還沒有傳統的那麼完善，所以主管機構不一定會擔保智能合約這方面，可能目前大多人還會更偏向傳統合約。

c. 成本問題:

因為智能合約要通過編碼過後才能執行，所以這也是一項技術執行，要去尋找這方面的工程師來保障智能合約的執行以及上傳，會比傳統合約多出不少成本。

四、虛擬貨幣的比較

2022 最新虛擬貨幣排名(市值)

第一名：比特幣 (Bitcoin)

第二名：以太幣 (Ethereum)

第三名：瑞波幣 (XRP)

第四名：萊特幣 (Litecoin)

以下為我們對於 2022 年最新虛擬貨幣排名做出的比較。

表 4: 虛擬貨幣比較

	比特幣	以太幣	瑞波幣	萊特幣
代號	BTC	ETH	XRP	Litecoin
貨幣符號				
發行時間	2009 年 1 月	2008 年 1 月	2012 年	2011 年 10 月
創辦人	忠本聰(Satoshi Nakamoto)	維塔利克·布特林	Ripple	李查理(計算機科學家)
發行數量	1700 萬	100, 927, 956	一千億	8400 萬
流通數量	18, 968, 400	119, 727, 946	47, 949, 281, 138	69. 72M
價格	1, 095, 436. 93	77, 915. 40	21. 36	3, 100. 76
市價	8300 億美元	3300 億美元	367. 1 億美元	115. 8 億美元
交易時間	慢(10 分鐘)	快(幾秒)	快(3-5 秒)	中(2. 5 分鐘)
優點	在主流經濟被接受度高、交易途徑多。	活用區塊鏈技術，應用範圍廣、交易時間只需幾秒，比比特幣快上許多。	國際轉帳速度最快，只需幾秒即可完成。	交易時間比比特幣短、手續費也低於比特幣。
缺點	交易速度慢、交易成本高。	挖礦困難度較比特幣高。	瑞波幣公司持有超過總量一半的貨幣，過於集中化。	發展定位相較於其他加密貨幣較不明確，無明確發展優勢。

這四個虛擬貨幣比較，比特幣在比較之間幣擁有其他三個沒有的黃金稀少性，以太幣的比比特幣更好的相容特性，更運用在生活當中，而且以太坊是最受歡迎的平台，在也以太坊關鍵升級，讓相關開發更為環保其他兩個幣就的功能與價值就沒有優

於比特幣與以太幣。

以太幣與其他三個幣比較下來運用上面遠遠超越三個虛擬貨幣，在未來的發展一定能超越比特幣。

五、以太幣的未來趨勢

以太坊(Ethereum) 在加密貨幣市值方面僅次於比特幣，它是一個智能合約區塊鏈協議平台，為用戶提供了一個安全和去中心化的環境來運行不同的區塊鏈應用程式。它一直是 2020 年 DeFi 熱潮、2021 年 NFT 爆炸的核心平台，並將預計於 2022 年出現的元宇宙熱潮中保持這頭龍地位。

(一)、以太幣 2.0

在 NFT 與 DeFi 的推動下，以太幣從一年前的 700 美元，一路飆漲至今超過 4,000 美元，高昂的手續費與漫長的等待驗證時間，催生了一海票替代鏈與幣雞犬升天。

儘管眾多替代貨幣(Altcoin) 都有各自的願景與理想，但在 2021 年他們能夠漲價的主因只有一個，就是以太幣太貴了。0.01 ETH 的手續費，在一年前不過是 7 美元，現在則是瘋狂的 40 美元，促使投資人必須尋找替代管道來交易，可以節省超高昂的手續費。

Ethereum 2.0 升級的目標就是要改變驗證機制，節省驗證時間，並減少手續費飆升問題。如果以太坊真的在 2022 年完成升級，除了目前用顯卡挖以太幣的礦工要煩惱，這些替代幣可能也要煩惱了。

當 ETH 的新驗證機制確定可行之後，投資者將不需要大費周章轉換幣種，而可以直接用以太幣在錢包、交易所、NFT 平台或是其他服務上交易，因此許多分析師認為這將讓以太幣達到空前的歷史新高，保守者估計會超過 8 千美元，激進者則認為將達到 2 萬美元以上。

2021 有各種瘋狂的大事不斷誕生，整體來說是加密貨幣爆發成長的一年，而 2022 年加密貨幣產業整體將會持續成長，但也會有一些泡沫逐漸破滅，就像比特幣誕生至今，永遠都是充滿機會與超高風險。

(二)、以太坊網路升級

去年，我們終於看到了備受期待的以太坊 2.0 的網路升級，即倫敦硬分叉。今年，我們期望看到所謂的合併，與信標鏈(Beacon Chain) 整合，用更環保、更高效、更安

全的權益證明 (PoS) 共識機制來取代目前的工作證明 (PoW) 共識機制。當合併成功時，以太坊目前的 PoW 共識機制將被完全廢除，而以太坊的所有區塊將通過 PoS 產生。

底層升級和新的股權證明共識機制所奠定的基礎將使以太坊實現以下的幾個方向：

1. 更低的耗能，因為 PoS 共識層移無需網路中的礦工，而透過驗證者取代了他們。這使網路在運行時的能耗大大降低，以太坊基金會預測，它的能耗將比目前的網路低 99.95%。
2. 以太坊目前的執行層將被移植到即將到來的股權證明共識層，並由目前負責以太坊 1.0 的客戶端支援。
3. 轉向 PoS 模式也降低了參與驗證者網路的門檻，因為用戶將不再需要昂貴的硬件來創建區塊。網路中更多的節點將增加對中心化的免疫力，為增加去中心化和可擴展性鋪平道路。

交易費用是否會下降仍是未知數。一方面在 PoS 下，網路將有能力實施分片和其他以擴展性為重點的升級，以降低交易成本。另一方面，新的用戶和實體可能會加入以太坊網路，增加目前對區塊空間的需求。大家即管期待以太坊在 2022 年是否能進一步帶動加密貨幣市場。

(三)、以太坊(以太幣)的未來潛力

Michael McGuiness 覺得以太坊將贏得價值儲存之戰，主要有四個原因。

1. 更加稀缺：

以太坊沒有固定供應量，轉向 PoS 將大幅減少 ETH 的發行，同時保持相同的網路安全水平。新的 ETH 發行將由質押了 ETH 的驗證者通過處理交易並就網路狀態達成共識來增發，而不是交給礦工，並且在 ETH 質押總量和質押者的年利率之間會有一個浮動的比例。

隨著以太坊改進提案 EIP-1559 的發布，以太坊已經開始解決關於其貨幣政策的許多擔憂，該提案被稱為「以太坊的稀缺性引擎」或「ETH 的銷毀機制」。除了改善以太坊 gas 費用的用戶體驗，EIP-1559 將銷毀一部分 ETH 交易費用。這將永久性地從流通中移除一部分 ETH 供應，並減少 ETH 的每日淨發行量。

2. 更加安全：

安全性也是至關重要的因素。就像黃金不會腐爛、腐蝕或者經歷其他類型的變質一樣，加密貨幣必須通過適當的激勵設計才能持久，也就是要有礦工和驗證者存在維持整個系統運作。畢竟，一項幾十年後不再存在的資產也不可能成為價值儲存工具。

「覆巢攻擊」，即一個發起 51% 攻擊的礦工聯盟會連續不斷地攻擊，使這條鏈無用。就 PoW 系統而言，沒有辦法破壞（或懲罰）攻擊者的挖礦能力。因為區塊鏈有個致命缺點，雖然他是去中心化的帳本，但只要有超過一半的人(51%以上)帳本數字同時修改，這些帳本就會被更改。

以太坊（PoS）不太容易受到這種攻擊。這是因為以太坊網絡可以「罰沒」（罰款並沒收）或懲罰攻擊者。如果攻擊者做了不好的事情，網絡將通過沒收他們質押的 ETH 來懲罰攻擊者。這也是為何以太坊要朝向 2.0 發展，提升安全性，。

在安全方面，參與以太坊質押不會帶來任何「足跡」，這是一個巨大的優勢：要成為一名以太坊驗證者，所有你需要的只是 ETH、一台樹莓派、一個 SSD 以及網路連接。這與比特幣形成了鮮明的對比，在比特幣挖礦中，成為一名礦工將帶來大量「足跡」：礦工需要消耗巨大的能源和使用巨大的倉庫來存放挖礦設備。這樣的「足跡」使得政府可以相對容易地發現並關閉挖礦活動。

3. 有機需求：

美元最早叫做美金，因為最初是黃金本位，擁有多少黃金，才能印相對價值數量的美元。但尼克森總統，在 1971 年結束了美元對黃金的掛鉤，從此美元轉變成沒有任何支撐的紙幣，這些貨幣本身並沒有什麼價值，它們之所以有價值的，是因為政府宣布它們有價值，並強制將其作為一種交易媒介和記賬單位。

在美國之外，外國企業和政府仍然沒有什麼理由接受（美元）紙幣，因為這些紙幣可以無休止地印刷，而且沒有堅實的支撐。因此美國通過石油美元體系創造了各國對美元的持續國際需求，從而迫使全球採用美元。1974 年，美國和沙烏地阿拉伯達成協議。沙烏地阿拉伯將只以美元出售石油，以換取美國的保護和合作。例如，即使德國想從沙烏地阿拉伯購買石油，他們也只能用美元購買。從那時起，任何想要石油的國家都需要使用美元來支付。導致世界上每個人都接受美國政府發行的廢紙，以換取有形商品和服務。這絕對是美元成為全球儲備資產的根本原因。

而以太坊，就是類似的體系，而且是良性循環。你需要使用 ETH 從而在以太坊網絡上做事情，而且人們正在這個網絡中做很多事情：他們購買域名、交易代幣、借貸、發行債券、使用預測市場、付款、購買保險、藝術品、遊戲、虛擬土地、賽馬等等。所有這些事情都要求使用 ETH 來支付交易費。就連愈來愈火紅的 NFT 也是建構在以太坊上。不知道 NFT 是什麼的可以參考 NFT 到底紅什麼？NFT 懶人包一次告訴你，小蛙自己也是有玩一款區塊鏈遊戲玩遊戲還能賺錢？區塊鏈遊戲 Axie Infinity 做得到！，也是需要以太幣支付手續費。

隨著構建在以太坊之上的應用愈來愈多，對以太坊的需求將會增長。排名前 100 的加密項目中有 94 個是在以太坊上構建的，超過 3000 個 Dapps 和 20 萬種 ERC-20 代幣在以太坊上運行。以太坊上的總交易量每天都達到歷史新高，以太坊上的平均交易價值是比特幣的兩倍多。以太坊本質上是一個去中心化的計算機，計算能力需要花錢。這些費用被稱為「Gas」，與石油非常相似。

4. 實際收益：

通過質押 ETH，你可以額外獲得 6% 以上的無風險質押收益，這將激勵一些投資者將資金從比特幣轉移到以太坊。這就是市場的運作方式，投機性資本自然會流向預期實際收益率最高的資產。

但其實以太坊也是有風險存在，每個加密貨幣的誕生都是為了解決問題，可以解決的問題愈大，他可以產生的價值愈大。當然現在以太幣價高，交易手續費昂貴都是讓人詬病的地方，也有愈來愈多公司跳出來想開發類似的區塊鏈取代以太坊，我相信以太坊的創辦團隊一定知道，才會進行 2.0 改革。至於能不能如預期克服這些問題，因為小蛙也不是區塊鏈高手，但我相信 V 神小小年紀就那麼厲害，一定會找到方法的，這也是為何我很看好以太坊跟以太幣，我看到的是它的價值而不是價錢。

參、結論

以太幣與其他虛擬貨幣的出現讓人們對於金融商品的選擇又更多元化了，有更多的選擇，目前開發的還不夠完善，在各項數據的歷史統計還沒有辦法做大量的回測，但從以太幣現在各項的發展可以發現未來一定能創造更多想像不到的虛擬機會，像現在元宇宙的開端讓 NFT 的話題風靡全球，NFT 就是用到以太幣做為交易媒介使全球交易沒有國界的限制，在未來以太幣能在交易時廣泛利用，徹底消除國與國之間的問題，NFT 用途非常多例如：還能利用 NFT 來創造自己的虛擬世界在虛擬世界裡面打造自己的國度、可以保護數位藝術圖片、發行的 NFT 當身分認證。雖然現在的技術還不夠成熟但已經成為一個未來的趨勢。

以太幣的應用已經超乎我們所預期的範圍，它的出現帶動了全球的金融發展，隨著科技的進步顯的虛擬貨幣越來越有價值，現在的金融業也都開始虛擬化發展可以解決懶人的問題。現在不管是公司還是投資者都注重 ESG，ESG 的投資風氣大增越來越看重綠色經濟，比特幣挖礦視為浪費能源的碳排行為導致全球加密貨幣產業風向已經從比特幣變成以太幣成為了業界的焦點，因為以太幣更符合現在綠色經濟的投資趨勢，以太幣的價值來去中心化的應用當 Defi 的應用越受歡迎，投資者與市場的需求就會越來越大，另外可以利用 POS 抵押以太幣可以獲得額外的出塊獎勵，以太幣不只能廣泛運用還能提供投資者穩定的報酬，以太幣不是價值儲藏的工具，更有創造價值的能力。

建議利用非常盛行的 DeFi，也就是所謂的「去中心化的金融」。一般人的金融活動，不論是資金借貸、匯兌還是買賣股票，都必須透過銀行之類的傳統金融機構。但現在人們只要把智能合約的內容寫好，再把它放上以太坊，就能扮演傳統金融機構的角色，把金融活動搬到區塊鏈上面。不論是想借錢的人和想存錢賺利息的人，或是確保借錢的人依約還本付息，系統都會自動執行智能合約的內容。

肆、參考文獻

黃婷容(2021)。【專題報導】區塊鏈上的金融新趨勢 加密貨幣如何建構虛實新世界。取自：<https://www.ectimes.org.tw/?p=69628>

Chen Kobe(2021)。《關鍵趨勢》拆解加密貨幣 2022 風向，從比特幣到 NFT。取自：<https://finance.technews.tw/2021/12/31/crypto-2022-trend-watch/>

AAX(2022)。2022 年以太坊將有甚麼新動向？取自：<https://www.abmedia.io/20220114-ethereum-prediction-for-2022>

區塊鏈妹(2021)。以太幣「供應短缺」庫存暴跌 27%！分析：後市有望創新高。取自：<https://blockcast.it/2021/01/15/eth-may-soon-hit-a-new-ath-after-reserves-on-centralized-exchanges-fell-by-27/>

吉姆(2020)。未來貨幣之爭！以太坊流通量再遭批，Vitalik：別搞得像宗教信仰。取自：<https://www.abmedia.io/bitcoiners-insist-that-ethereums-total-supply-is-impossible-to-calculate>

KOINBULTENI(2021)。為什麼以太坊沒有最大供給？取自：<https://0xzx.com/zh-tw/2021020708331158640.html>

Jason Liu(2020)。以太坊 2.0「年增發量」是多少？V 神曝：這二年平均 470 萬顆 ETH、其後每年 0-200 萬。取自：<https://www.blocktempo.com/print-2m-eth-average-says-vitalik/>

Jason Liu(2020)。推特混戰 | Kraken 研究員：以太坊「未知的供給量」恐釀隱憂，2.0 上線後風險擴大。取自：<https://www.blocktempo.com/how-exactly-is-the-eth-total-supply/>

Plus500。什麼是以太坊？取自：<https://www.plus500.com/zh/Instruments/ETHUSD/What-is-Ethereum-1>

維基百科。區塊鏈。取自：<https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE>

Lydia、Quen(2020)。「區塊鏈」到底是什麼？專業懶人包在這裡。取自：<https://www.mile.cloud/zh/resources/blog/187>

維基百科。虛擬貨幣。取自：<https://zh.wikipedia.org/wiki/%E8%99%9A%E6%8B%9F%E8%B4%A7%E5%B8%81>

Yahoo 奇摩(新聞)(2021)。「虛擬貨幣」是什麼？虛擬貨幣怎麼買？背後原理是什麼？取自：<https://tw.news.yahoo.com/%E3%80%8C%E8%99%9B%E6%93%AC%E8%B2%A8%E5%B9%A3%E3%>

[80%8D%E6%98%AF%E4%BB%80%E9%BA%BC%EF%BC%9F%E8%99%9B%E6%93%AC%E8%B2%A8%E5%B9%A3%E6%80%8E%E9%BA%BC%E8%B2%B7%EF%BC%9F%E8%83%8C%E5%BE%8C%E5%8E%9F%E7%90%86%E6%98%AF%E4%BB%80%E9%BA%BC%EF%BC%9F-032214185.html](https://www.tpce.org.tw/data/data5/668-1.pdf)

林志坤。虛擬貨幣概述。取自：<https://www.tpce.org.tw/data/data5/668-1.pdf>

高敬原(2017)。虛擬貨幣崛起！比特幣帶頭衝，另外 4 種也不能錯過。取自：<https://www.bnext.com.tw/article/47456/bitcoin-ether-litecoin-ripple-differences-between-cryptocurrencies>

Charlotte(2022)。2022 最新虛擬貨幣排名及虛擬貨幣交易所/平台評測。取自：<https://tw.mitrade.com/crypto/cryptocurrency-rank-list/cryptocurrency-ranking>

Mr. Market 市場先生(2021)。智能合約是什麼意思？有什麼優點與缺點要注意？。取自：<https://rich01.com/what-is-smart-contract/>

Mr. Market 市場先生(2021)。關於區塊鏈，你需要知道些什麼？取自：<https://rich01.com/what-is-blockchain/>

幣安學院(2019)。什麼是智能合約？取自：<https://academy.binance.com/zt/articles/what-are-smart-contracts>

加沛(2018)。不可不知何謂「智能合約」？取自：<https://blockcast.it/2018/03/11/what-is-a-smart-contract/>

徐明星、劉勇、段新星、郭大治(2017)。區塊鏈的 18 種應用：將轉變身分驗證到人工智慧，顛覆人類未來生活。取自：<https://benevo.pixnet.net/blog/post/50051584-%E5%8D%80%E5%A1%8A%E9%8F%88%E7%9A%8418%E7%A8%AE%E9%81%8B%E7%94%A8>

區塊鏈客(2021)。人人都說「區塊鏈是未來」，到底有哪些應用場景？取自：<https://blockcast.it/2021/06/10/top-blockchain-industry-applications/>

林佳賢(2018)。不懂技術沒關係！圖解告訴你區塊鏈可以這樣用。取自：<https://www.cw.com.tw/article/5090842>

Chelsie Yang(2021)。區塊鏈的定義與原理為何？各個產業如何應用區塊鏈？取自：<https://zh.oosga.com/pillars/blockchain/>

區塊鏈先鋒站(2018)。區塊鏈，未來已來！取自：<https://kknews.cc/tech/ry8yayx.html>

區塊吧 BLOCKBAR(2019)。區塊鏈的歷史已走過 10 年，區塊鏈發展的簡史整理。取自：<https://blockbar.io/blockchain/%E5%8D%80%E5%A1%8A%E9%8F%88%E7%9A%84%E6%AD%B7%E5%8F%B2%E8%88%87%E7%99%BC%E5%B1%95-the-timeline-of-blockchain/>

Shirley(2021)。以太幣價值在哪？認識以太坊與智能合約。取自：<https://moneymate.space/%E4%BB%A5%E5%A4%AA%E5%9D%8A/#%E4%BB%80%E9%BA%BC%E6%98%AF%E4%BB%A5%E5%A4%AA%E5%9D%8A%EF%BC%9F>

小君(2021)。在台灣怎麼買比特幣/以太幣？虛擬貨幣投資管道一覽，5 分鐘搞定比特幣/以太幣交易！取自：<https://www.investors.tw/buy-bitcoin/>

Simon(2021)。【台灣加密貨幣交易所分析】台灣 4 大常見加密貨幣交易所怎麼選？詳細分析告訴你！取自：<https://iyaogrowth.com/taiwan-crypto-exchanges/>

IG International Ltd(2003-2021)。OTC 場外交易。取自：<https://www.ig.com/cn/glossary-trading-terms/otc-definition>

【MICA RESEARCH】ESG 投資趨勢已定，以太幣才是區塊鏈的未來？【MICA RESEARCH】ESG 投資趨勢已定，以太幣才是區塊鏈的未來？ - 區塊客 (blockcast.it)