**計概第12組 小組報告**

**主題:區塊鏈**

**一、問題:探討區塊鏈原理和未來的發展與應用**

**區塊鏈:**區塊鏈（Blockchain）是比特幣的核心技術，區塊鏈是一個去中心化的資料庫，每一段時間就會透過密碼學原理將交易資料編譯、加密，並放置在一個”區塊”裡面，並由一個個區塊按照發生順序(時間)串聯而成”區塊鏈”。區塊鏈是一種分散式帳本。所謂的分散式帳本是將所有加密過的交易紀錄公開的發送到所有區塊鏈網絡的節點(所有下載該區塊鏈應用程式的電腦)儲存。分散式帳本配合密碼學防止交易資料被任意竄改。首先使用分散式帳本﹐帳本儲存於多部電腦的硬碟中，分散式帳本的使用讓交易資料更加的公開透明，同時每台電腦一起被竄改的機會很低，再加上配合密碼學將交易資料加密更能夠降低被破解及竄改的可能性。

以前在交易時需要第三方控管整個交易穩定，並且需要一個能夠大量儲存交易資料的地方，區塊鏈打破了這個運作方式，以去中心化的方式運作，把資料庫分別放在不同的電腦裡保存，並且互相監控數據，資料更動需要經過其餘電腦的共識同意。與以前單一資料庫不同的是區塊鏈裡的電腦會利用分散式運算加快交易、儲存資料速度，而在儲存資料的同時以加密的方式保護資料，在資料交易的過程中，也不需要額外經手第三方驗證。

**名詞解釋**

1. **節點:**區塊鏈系統中的每一台電腦都是一個節點，節點之間可以藉由網路串連，來為區塊鏈提供系統所需要的運算能力，任何一筆交易資料都會傳送到每個節點做公開、透明的儲存。
2. **礦工、挖礦:**電腦的持有者(礦工)提供閒置的電腦給區塊鏈應用程式做資料的運算及儲存，來獲得工資(如:比特幣)的行為成為挖礦
3. **去中心化系統:**區塊鏈系統是一個去中心化的資料庫﹐沒有中心的伺服器管理，每經過一段時間，進行運算的某台電腦會將一段時間內完成的交易加密，然後藉由網路的串聯把資料發送給系統中的每一台電腦。
4. **ICO:**Initial Cryto-Token Offering是透過發行虛擬貨幣來融資的方式，發行貨幣的人透或撰寫計畫(如:我透過虛擬貨幣得到的錢未來要做怎麼樣的使用)，吸引投資者購買虛擬貨幣做投資。當這款虛擬貨幣普遍被大家看好則需求量會上升，導致貨幣價格上漲，投資者賺錢。這是為什麼會有投資者想要投資ICO的原因。

**二、區塊鏈的重要性:**

區塊鏈的出現解決了信任的問題，因為區塊鏈有幾個特點，1.區塊鏈的運作設計是基於程式、數學、密碼學等原理，這意味這系統在設計好開始運作之後就不會因為受到人為因素的介入與影響，而產生不一樣的結果。2.區塊鏈上的所有資訊皆為透明、公開，所有人皆可以查閱，且不易被竄改。這個優點使得區塊鏈系統可以取代原本所需要的第三方(或稱中間人)作為信用背書的角色，讓交易雙方縮短建立信任的時間，完成交易、合作。中間人認證的移除不但可以降低被人為因素介入與影響的可能性，還可以減少交易成本的存在。

經濟學人雜誌將區塊鏈比喻為信任的機器。

**三、目前區塊鏈的應用:**

**虛擬貨幣**

區塊鏈技術出現以前，網路主要是用來傳遞資訊，例如:發送信件、傳送檔案，當時無法將數位化的虛擬貨幣透過網路的方式來傳遞。原因在於交易的時候缺乏某種機制讓交易雙方確認被寄出的錢是否已經從寄出的那一方扣除，或者是寄出的那一方保有一份一樣編號的的虛擬貨幣，產生了重複的虛擬貨幣存在的風險。而這種機制便是第三方認證，也是中間人背書出現的原因。

銀行在我們的日常生活中就扮演了第三方認證的角色，銀行會透過印製鈔票上的編號去確認市場上的每一張貨幣都是獨一無二的，確保市場上沒有存在著印有同樣編號的鈔票。

區塊鏈的出現解決了原本虛擬貨幣無法投過網路方式進行交易的問題，使得虛擬貨幣可以藉由網路做轉移。由於任何一筆交易都會儲存在區塊鏈系統每一個節點的帳簿之中，並且是公開透明的，不會出現有使用者利用同一個虛擬貨幣進行重複交易的行為。

去中心化區塊鏈的發展，人們可以在沒有中央集權機構的信用背書之下，建立起買賣雙方的信用關係。

**四、區塊鏈未來應用的優勢與劣勢:**

區塊鏈日趨成熟 他的應用不再局限於虛擬貨幣。

## 區塊鏈專家Melanie Swan 在 Blockchain:Blueprint for a new economy一書中將區塊鏈的發展分成了三個時期，Blockchain1.0，為數位貨幣應用，Blockchain2.0開始出現如智慧資產、智慧器樂等貨幣以外的應用，將貨幣以外的數位資產做轉移，如；債券、股票、基金等金融衍生產品，Blockchain3.0則是指更複雜的智慧契約，將區塊鏈食用於政府、醫療、科學、文化與藝術等領域。

區塊鏈未來的優勢為去中心化且公開透明的帳本，資料的運算與交易的結果不會因為人為的因素而有變化，並且分散式帳本讓帳本中的資料不易被竄改，保障買賣雙方的權益。

然而公開透明的帳本也是區塊鏈的缺點。公開透明的帳本讓任何想要獲得資訊的需求者都可以看到交易資料，使得買賣雙方的隱私有被侵犯之虞。

另外，區塊鏈技術之所以日漸興盛其中一個原因是區塊鏈系統至今從未被破解過，由於區塊鏈系統目前過於完美無缺，假使某一天被駭客破解，區塊鏈系統的應變能力、如何防禦是值得深思的議題。

未來區塊鏈技術還有可能面對的問題：電子錢包真的需要用到區塊鏈的技術嗎，是不是大材小用了呢？一般民眾會在意去中心化的使用嗎？區塊鏈的普及有沒有可能會造成失業率的上升了？

農產品產銷履歷驗證制度以農產品安全性、可追溯性及農業生產永續性為目標訂定驗證基準，經輔導農產品經營業者據以實施後，經認證符合國際規範之驗證機構評鑑確認其符合性，並給予符合者驗證及使用產銷履歷農產品標章之權限，以營造良好農業生產及農產品消費環境之制度。**從過去政府推動幾個認證措施，成功比率相對不高，讓消費者失去信心和信任而不了了之，其實政府立意良好但是執行上出了問題。舉例而言，若一個有認證的雞肉牧場，賣了200隻的雞給肉販商，因有認證的雞肉可得到消費者較高的信任，也許可以賣得較高的價錢；肉販商心存不良，加進沒有認證的雞肉100隻，也打上了有履歷認證的牧場所生產，那他就可有更多的獲利。但萬一被檢查出這批雞肉是有問題的，那受害者是消費者和有認證的雞肉牧場；請問一下，從此以後，消費者會再信任這個認證嗎？**

在閱讀相關區塊鏈資料後，若畜牧場能登錄其畜養資料至各網路節點資料，讓含消費者在內的查核單位確認雞隻履歷，將可改善農畜產品產銷履歷驗證制度，強化消費市場的商品銷售與保證。根據區塊鏈去中心化、分散式資料及可追溯系統的特性，可以供**牧場中**雞**隻畜養及交易**紀錄的保存，因此農政單位可以查核肉販商的交易紀錄與畜牧場的交易紀錄是否相符合；目前雞隻履歷是掌握在**雞肉牧場**手上的，消費者、農委會或肉販商並不掌握完整的資料，所以沒有辦法獲得雞隻履歷情況。但現在如果可以用區塊鏈技術來進行保存，就有了畜牧場的飼養歷程、雞隻交易數量與雞隻品質的歷史資料，未來檢核雞隻履歷規劃就有完善資料可供使用。但是必須強調，這種應用具有去中心化的特性，更具開放性，消費者、農委會或肉販商也更有自主性。它所實現的是一種新的組織資訊的形態，每個單位都掌握充分的資訊，而不像過去那樣存在資訊不對稱性。

**五、參考書目:**

1. 許孟祥，楊志清，李志賢，吳幸玲，區塊鏈商務應用槪論：實例與分析，新陸書局， 2018。
2. 張渝江，比特幣區塊鏈大未來，臺灣學術電子書暨資料庫聯盟， 2016。
3. [M. Kouhizadeh](https://www.mdpi.com/search?authors=Mahtab%20Kouhizadeh&orcid=), [J.Sarkis](https://www.mdpi.com/search?authors=Joseph%20Sarkis&orcid=), Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains, Sustainability 2018, 10(10), 3652; [https://doi.org/10.3390/su1010365](https://doi.org/10.3390/su10103652).
4. **Melanie Swan，**Blockchain:Blueprint for a new economy，原文出版社Oreilly&Associates Inc