Regular Paper

Communications of the CCISA
Vol. 29 No. 1 Feb. 2023

以區塊鏈技術為基礎的評價回饋與紅利優惠券協定

林秀蓉[1]、薛夙珍[2*]、曾嘉禾[3]
[1,2,3]朝陽科技大學資訊管理系
s11014618@gm.cyut.edu.tw[1]、schsueh@cyut.edu.tw[2]、flying87945@gmail.com[3]

摘要

在競爭激烈的電子商務環境中，商家為提升消費者購物意願，推出了各式各樣的行銷手段，例如電子優惠券 (E-Coupon)。藉由電子優惠券的發行，不但能推廣產品與擴展銷售市場，也能提高銷售額的成效。為了讓所發行的優惠券能夠誘發潛在網路消費者購買機率，往往運用了折扣、紅利回饋等技巧，讓優惠券發揮更大的行銷效果。本論文希望能發揮口碑效應的成效，根據電子優惠券分享與使用歷程來提供不同程度的紅利回饋設計優惠券協定，藉此提升電子優惠券的行銷效果。

在電子商務中由於交易雙方不一定熟識，因此難以建立信任基礎，需要透過相關資訊如評價系統的參考，幫助消費者從中挑選可靠買賣方。協定中透過區塊鏈技術實現可信任第三方單位，有匿名並確保資料安全的特性。我們的方法透過區塊鏈技術去中心化、分散、不可竄改的三大特性，結合了數位簽章以及雜湊加密應用於評價系統，提出一個具安全隱私保護與差異化紅利回饋機制的評價系統協定。所設計的協定，不但能保障評價資訊的安全性，也能因其所具備的匿名特性達到消費隱私的保護。

關鍵詞：區塊鏈、線上評價、行動優惠券、紅利回饋、電子商務

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 29 No. 1 Feb. 2023

A Block-chain based Coupon Protocol with Online Evaluations and Bonus Rewards

Xiu-Rong Lin[1], Sue-Chen Hsueh [2*], Jia-He Zeng [3]
[1,2,3]Department of Information Management, Chaoyang University of Technology, Taiwan
s11014618@gm.cyut.edu.tw[1], schsueh@cyut.edu.tw[2], flying87945@gmail.com[3]

Abstract

The competitive e-commerce pushes merchants to use various marketing methods such as E-coupons to enhance consumer purchasing. Not only the product sales but also the sales performance are increased by issuing E-Coupons. In order to increase the purchasing possibilities of online consumers, discounts and bonus rewards are often used to maximize marketing effects. This paper aims to leverage the effect of word-of-mouth by providing distinct levels of bonus rewards based on the sharing and usage history of E-Coupons, thus boosting the promotional effects of E-Coupons. Because the transaction parties in e-commerce might be unfamiliar with each other, evaluation systems are needed to help consumers select reliable trading partners without trusts. A coupon protocol applying the blockchain technology, which has the anonymous and secure data characteristics, is designed to achieve trustworthy third parties. We use the decentralization, distribution, and tamper-resistant characteristics of blockchain technology, combine with digital signatures and hash encryption, and present an e-coupon protocol with privacy protection, online evaluations, and differentiated bonus reward mechanisms. The proposed protocol can not only ensure the security of evaluations, but also achieve customer privacy protection due to its anonymous features.

Keywords: Block-chain, Online Evaluations, Mobile Coupon, Bonus Reward, E-Commerce

壹、前言

網路與行動裝置的普及，改變了商業營運型態，交易雙方可以透過網路進行交易活動、交流訊息或完成合約，將交易模式演變為數位化方式，進入電子商務的時代。然而電子商務和傳統商業模式最大的差別就在於消費者無法事先查看商品實體再進行購買，因此消費者和商家間必須有一定的信任基礎。在C2C的交易環境中，買賣雙方的不信任程度較高，因此消費者會自行使用網際網路來搜尋賣場資訊和產品相關資訊。網際網路中資訊的傳遞有多樣化的管道，如：購物網站、社群或討論區等等，消費者透過這些管道來尋找所需資訊。消費者使用產品或服務後，根據自身經驗、心得或相關知識再進行分享[6]。商家可透過網路方式將商品資訊傳遞給消費者，例如：電子優惠券 (E-Coupon)。優惠券是商家常見的促銷方案，從早期紙本優惠券，發展成為數位化電子優惠券，消費者可以透過網路搜尋商家平台領取優惠券再至店家使用[4]。消費者由線上平台領取優惠券後，可提升消費者購買意願，進而提升銷售額，也可藉此作為行銷工具，宣傳產品擴增銷售市場，以提高市場佔有率。優惠券的使用只需將二維條碼或是QR碼給店家進行掃描即可使用，能提升消費者黏著度也可增加品牌忠誠度。

消費者在購物時無法直接面對商家與商品的狀況[2]，使網路購物存在信任問題，因為消費者需承擔潛在風險，如：商品或是服務不如預期、網路詐騙、消費者隱私遭到竊取等安全風險。因此需要可信任的第三方單位輔助交易進行，以維護雙方權益。網路中的消費者，通常在網路購物前會先上網搜尋網路評價[20]，致網路評價資訊成為直接影響消費者購買的因素。目前評價資訊的潛在問題有評價灌水、評價中含有利益操作和評價內容包含個人隱私資訊等等。不實評價讓買賣雙方都受到影響，需要資訊安全控管。

除使用評價機制外，為提升消費者購物欲望也推出了各種行銷手段，如：紅利回饋、滿額贈獎和優惠券等活動。此方式激勵潛在網路消費者購買率，增加商家銷售量[1,14]。優惠券通常具有使用期限，若優惠券存放於某位消費者帳戶中未使用，將導致該優惠券成為無效優惠券。因優惠券的發行量和使用率會影響商品銷售量，為提升優惠券使用率，降低無效優惠券的發生，Kangasharju 和 Heinemann 學者提出了紅利回饋機制的概念[12]，期望透過回饋機制，將不使用之優惠券轉讓至潛在客戶手中。回饋機制則會在優惠券成功使用時觸發，讓原先的持有者獲得回饋，以解決無效優惠券問題。因此本論文的研究主軸之一為透過區塊鏈技術設計優惠券轉讓回饋機制。

評價資訊的不實評價、洗評價等可靠性問題，需要一個良好的環境設計來改善。區塊鏈具有去中間化、分散和不可竄改三大特性[17]，適合用於無信任環境下的電子商務。選擇區塊鏈進行評價應用的原因如下：

1. 去中間化：一般電商平台中大多採集中化的管理模式，需要透過第三方單位輔助交易，因此雙方都需要支付額外手續費給第三方單位。使用區塊鏈技術可以取代第三方單位，交易驗證和交易數據可以由區塊鏈網路中節點完成，而且每個節點都有儲存副本，因此可以使每筆交易公開透明。

2. 分散：雙方透過自身私密金鑰即可管理網路中自身的數據資訊，而其不需要任何管理權限，交易過程中使用數位簽章，可以確保交易雙方無法否認在網路中的所有操作。
3. 防竄改：交易區塊產生中，會使用公開金鑰加密法以及雜湊函數保護區塊鏈中資訊，不容易在短時間內被破解或是逆轉竄改交易內容。在區塊鏈網路中所散布的使用者公開金鑰，無法透過該公開金鑰來獲得相應的私密金鑰。因此，若有心人士要透過破壞網路來竄改獲取資訊需要付一定程度的代價。

由於電子優惠券的分享與使用牽涉紅利回饋等有價資訊，在電子商務環境中屬於重要資料，為避免不當謀利操作必須加以保護。透過區塊鏈技術特性的導入不但能對電子優惠券資訊做好安全保護，也能防止與分享轉傳歷程有關的紅利回饋被不當偽造與竄改，還能提供消費者隱私保護。因此，區塊鏈技術讓紅利回饋機制的運作更順暢且安全。

所設計協定藉由 Peer to Peer (P2P) 的分享精神結合區塊鏈技術特性，透過行動設備的便攜性與人群互動，讓人際交流互動中的信任關係協助優惠券轉移至想要使用的消費者手中。若優惠券是透過親朋好友轉移所得，接收者更能接受並相信該優惠券的價值以及實用性，藉此更能將商家產品推廣出去[19]。當該優惠券被成功使用後，轉讓者將能透過優惠券中的轉讓資訊獲取相對應的紅利回饋。最後，透過公開金鑰密碼系統的方法可以保護資訊的安全性，結合Hash Chain與數位簽章的方式來設計安全機制，降低公開金鑰的計算次數，使優惠券應用更為流暢。

在網路購物的環境中，消費者沒有填寫評價的習慣，因此平台無法蒐集到全面的消費者回饋資訊。在整合式系統的研究中，希望有反饋的機制提高消費者填寫評價意願，因而設計填寫評價獲取專屬優惠券或現金等紅利反饋。紅利反饋為會員專屬，因此須進行會員註冊，才能獲取紅利反饋。除了能夠較完整更貼近消費者感受，回饋的機制也能鞏固商家與消費者之間關係並吸引消費者回流。評價資訊存在可信的問題，如為了增加銷售量或信譽，透過利誘的方式使評論者提供不實評價，進而影響消費者購買決策，甚至會影響未來評價趨勢。因此在研究中將使用憑證 (Token) 與區塊鏈技術來減少上述問題，該架構與電子投票系統相似，消費者必須完成交易後方可取得憑證用於評價。當憑證驗證無誤後，消費者才可進行評價程序，透過一系列機制建立具有可信度的評價系統。透過系統評分資訊，不論是使用者、商家或是虛擬商城中的潛在使用者都能透過該評分資訊，來決定購買決策亦或是新的活動促銷。

本論文以電子商務的優惠券使用與分享情境，加入區塊鏈技術應用，提升電子商務交易安全性與口碑效應。透過區塊鏈的共識決算法限制，達到幾乎無法單方面竄改節點更改整個區塊鏈。

貳、文獻回顧

本小節先對於區塊鏈相關特性進行介紹，接著藉由研讀以往學者的研究以了解如何將區塊鏈技術帶入我們的生活。

2.1. 區塊鏈相關之研究

在「區塊鏈革命」一書中提到[3]，區塊鏈是一種無法篡改的全球資料庫，能夠提供一個數位帳本，來記錄金融交易以及其他有價值的東西，如資產所有權、教育文憑、醫療程序、選票等各種應用[10]。區塊鏈 (Block Chain) 技術是一種不依賴第三方，透過自身的分散式節點在網路中進行數據的儲存、驗證、傳遞與交流的一種方法。藉由密碼學來串連與保護每一筆交易記錄 (又稱為區塊)，每一個區塊都包含了前一個區塊的雜湊值 (Hash Value)、對應的時間戳記 (Timestamp) 以及交易資料[8]。透過這樣的設計，使得區塊中的內容具有了難以竄改的特性。使用區塊鏈所串連的分散式帳本，不論是交易的雙方亦或是潛在的使用者都能夠藉此來查驗鏈結中的交易記錄[3, 10]。

區塊鏈技術起源於比特幣 (Bitcoin)，是一種去中間化的加密貨幣，由中本聰學者於 2008 年提出[15]，比特幣是基於區塊鏈技術創造出的 P2P 電子貨幣系統，三大特性分別是[3]：

1. 交易識別確認：透過公開金鑰的驗證機制，來驗證每筆交易的真實性。使用者透過私鑰產生數位簽章，使交易具有不可否認性。而整體環境是屬於「可驗證且匿名」，因此保有貨幣交易的特性[5]。
2. 資料無法竄改：使用「區塊」與「鏈結」來確保交易中的資料無法竄改。其中「區塊」是使用雜湊函式來保護交易資料，是一種從資料中建立數位指紋 (Digital Fingerprint) 的方法。而「鏈結」是將區塊與區塊之間透過「前區塊雜

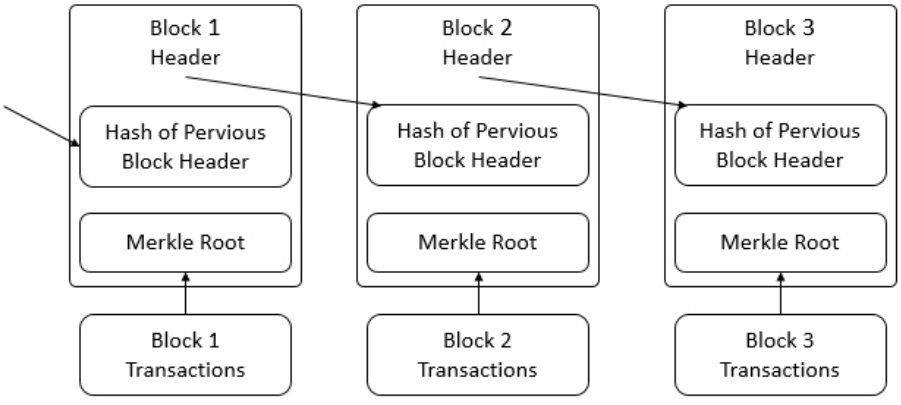

圖1：比特幣區塊鏈

湊」(Previous Block Hash)將彼此連結起來，由於要竄改交易中的資料已經很困難了，加上區塊彼此都透過雜湊值來進行連結，因此要竄改一個區塊必須要將整體鏈結中的所有區塊進行竄改，在短時間內是不可能達成。如圖1所示[3]。

3. 節點資料同步：使用工作量證明 (Proof of Work, POW) 來達到收斂同步，區塊中包含前一個區塊的雜湊值 (Prev Hash)，計算雜湊值所使用的參數 (Nonce)，區塊中的多筆交易 (Tx) [16]。由於比特幣是使用「分散式拓樸」，因此刪除困難指數較低的分支來達成節點資料的同步。

2.2. 優惠券之相關研究

電子優惠券是商家透過網際網路來發行，消費者能藉由商家的官方網站得知優惠券的相關資訊，並且印製自己所需的優惠券至實體商店中使用。電子優惠券具有以下幾點特性[4, 7, 11]：

1. 低傳遞成本：紙製優惠券的發行需仰賴人力來進行發送或郵寄方式送到消費者手中，而電子優惠券則是透過網際網路作為管道，讓消費者能夠自行取得優惠券，透過此方式發送優惠券，減少了許多在宣傳商品時所需的傳遞成本。
2. 高散播速度：由於是透過網際網路方式來進行散播，相較於一般傳統方法為快速。
3. 能針對特定對象來發行：相較紙製優惠券，電子優惠券更能夠鎖定特定目標的客群，如：消費者於網路拍賣網站瀏覽時，商家可以依據消費者偏好來給予相對應優惠券。
4. 消費者可自行索取：消費者能自行從網路下載電子優惠券使用，因此較於傳統被動式的接收優惠券，較能提高優惠券的使用率，並且能依據自己所需領取相對應優惠券。
5. 低發行成本：數位化的資訊有容易複製的特性與消費者可以自行下載優惠券，相較於紙製優惠券印製成本，較能控制發行數量，因此發行電子優惠券所需成本較為低廉。

其中這兩種類型的優惠券，依據發行的對象、目的、內容又有所不同，以下將依據這四類優惠券來進行介紹：

1. 特定對象優惠券

消費者可以透過年齡、學歷、工作或興趣等特性來區分整體的消費者族群，而這類型的優惠券發想的目的是發行商想針對某一個客群進行行銷，使特定的消費者族群在購物時感受到自己是獨一無二。

2. 限量發行優惠券

零售商或商品供應商發行優惠券的目的主要吸引消費者前來商店購物刺激購買慾望，優惠券的使用數量將會影響商家的獲利程度，因此適量的優惠券可以協助商家達到

最大的收益。而兌現使用過多的優惠券將會使商家的利潤降低或是增加額外的行銷成本，因此控制適當的優惠券數量才能有效的達到商家所想達到的目標。

3. 金額數字標示優惠券/百分比折扣標示優惠券

優惠券的折扣表示方式有兩種，一種為直接以數值顯示該次消費可以折抵多少現金，另一種為以百分比的方式來呈現給消費者。如：該次消費滿500元即可獲得100元折扣；單筆消費金額滿1000元即享85%折扣優惠。

4. 面額價格優惠券/最終購買價格優惠券

這兩種類型的優惠券在價格的標示上有所不同。如：以商品價格為500元來舉例，當商家想以300元來販售給消費者時，前者優惠券會標示為購買此商品可以獲得200元的折扣，使消費者可以很明顯的得知該張優惠券顯示的是這次消費所能節省的金額；而後者優惠券則是直接標示為300元，讓消費者可以得知若購買此商品至櫃台結帳時所需支付的金額為300元。

消費者在使用優惠券時會有不同的傾向，一類型的消費者對於優惠券較為在意，覺得優惠券上的折扣將會影響這次消費的感覺，因此習慣在優惠券上看到關於折扣的資訊；另一類型的消費者對於優惠券較為無感，他們只想知道此次消費時最終所支付的金額是多少，而不在乎在這次的消費得到了多少折扣。因此，優惠券上的折扣標示將影響消費者的購物感受。

2.3. 回饋機制相關之研究

1. 具回饋機制的點對點電子優惠券系統

在Shojima等學者的研究中，目的在於使用電子優惠券的過程中記錄每一個人的身分資訊，使其成為電子優惠券的發送紀錄，透過這樣的歷程紀錄就可以輕鬆地計算這些歷程中的每個人可以獲得的紅利回饋，因此發送的歷程是獲得紅利回饋的關鍵資訊，必須被加以保護。

Shojima等學者在此研究中認為在具有紅利回饋機制的電子優惠券系統中[21]，其發送的歷程與優惠券的內容都有可能遭受竄改，惡意的使用者也可能刪除發送歷程中上一個轉發者的資訊，使具有轉讓貢獻的使用者無法得到紅利回饋，或竄改優惠券的內容，使最後使用的優惠券的使用者無法通過零售商的驗證，使其優惠券的發行商的商譽受損。因此，學者採用了非對稱式金鑰密碼系統的加密方式並計算其Hash值後，透過數位浮水印的方式嵌入於圖像之中以確保紅利回饋的關鍵資訊，並以數位簽章的方式確保優惠券

的內容再被使用前的完整性。如圖2所示。

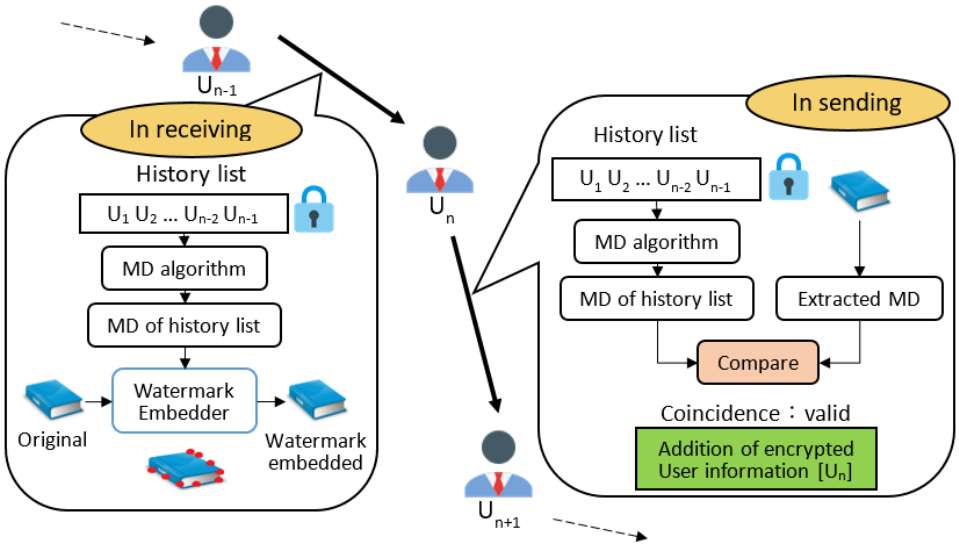

圖2：紅利回饋機制的電子優惠券加密

2. 消費者對於行動優惠券的反映：購買決策與監管契合的作用

在Khajehzadeh等的學者的研究中發現，行動優惠券是各個零售商作為促銷活動的獎勵發給消費者的數位化優惠券，通常都以短訊息服務 (SMS) 的形式來進行發送。消費者可以將這些行動優惠券儲存於他們的行動設備中，並且在購買的過程中使用，進而獲取消費折扣[13]。

促銷優惠通常目的在於吸引消費者的注意，使其遠離原有重點產品的購買目標，引導他們考慮購買最初不打算購買的替代商品。在過往的研究中顯示，行動優惠券的有效性取決於背景或優惠券的特徵。例如：消費者發現行動促銷活動在公眾場所比私人場所更有用，並且更喜歡在非工作與非工作環境下接收到這方面的促銷資訊。

正如同在研究中所論證的結果，消費者的購物動機偏離取決於所提供的產品是否與消費者的購物動機兼容，以及產品是否能與消費者當前或未來的需求一致。具體來說，享樂型購物者對於享受購物的情境與產品的實用性都具有良好的反應，無論優惠是否與他們當前或是未來需求是否一致。反之，在利益主義型購物者認為產品的實質效益與當前相符合的優惠服務能一致更能對於購物有吸引力。

2.4. 評價資訊相關研究

C2C電子交易中，消費者可以透過平台與其他消費者進行交易或交換所需的產品或是服務，同時參與者在某種程度上保有其匿名的特性。然而在買賣雙方往往缺乏可靠交易資訊，加上資訊不對稱容易產生交易糾紛，為減少紛爭，網路平台使用聲譽機制向平

台使用者提供相關參與市場的個人訊息。在這樣的機制中，允許買賣雙方的參與者在交易後進行互相評價，透過系統彙總顯示正向評價與負向評價的總和以得出買賣雙方各自的信任值。

現今大多數的線上購物網站都具有反饋評價機制，以減少線上交易的不確定性與風險。但有些許惡意的商家可能會串謀交易的參與者給予不正確的回饋資訊，進而影響整體線上購物網站潛在使用者的權益。為了減少這樣的行為發生，因此識別惡意的參與者是很重要的。信任對於商業活動中是很重要的事情，買賣雙方應該要能夠互相信任，在彼此互相不熟識的情況下，網路評價資訊便是很好的決策依據。以下說明與評價有關的文獻研究。

1. C2C環境中選擇可信任商家及聲譽評估

在網際網路中C2C的交易模式很受到歡迎，因提供消費者提供了一個私密、便利、高效率的價格談判平台。資訊缺乏或買賣雙方的匿名可能會導致利用此特性獲取不當的利潤或產生惡意的參與者。

在Wu等學者的研究中[22]，學者模擬了一種方法顯示在線上購物平台是否有惡意的參與者並且為此進行標示，同時也提出對於信任評價系統來進行了實證的分析。實證的結果顯示，Wu等學者的方法能比eBay平台更早的識別惡意的網路購物參與者。

2. 採區塊鏈技術提高電子商務評價可信任度

消費者評價在做出購買決策時具有相當關鍵的作用，甚至會影響未來評價整體的趨勢。但是這些線上評價的可信度始終存在問題，商家可能會給予評估者或評論者獎勵，以獲得詐欺或是具有偏見的評論，透過這樣的方式來增加銷售量或是名氣。在Ramachandiran學者的研究報告中[18]，透過區塊鏈技術來消除聲譽經濟中信任問題的方法。區塊鏈技術是一種分散式的電子平台，以不可任意修改的方式來進行維護，透過這樣的方式防止了舊有的陳舊評論來影響商家改進後所生產的產品銷售。

參、具安全及隱私的評價系統

本章節將介紹如何將區塊鏈技術運用於商務平台的評價系統。透過區塊鏈技術的特性結合電子投票系統的概念來實現安全性、可靠性以及匿名性。評價流程於整體交易流程完成後，買方取得商務平台給予的憑證後才能進行評價工作。評價系統分為給予評價資格、評價流程、評價查詢、與評價驗證四個階段。

3.1 商務平台評價系統之交易個體

參與的五個個體包括評價系統公司、商務平台、優惠券管理公司、買方與賣方，如圖3所示。其中，系統評價公司負責提供驗證用的憑證 (Token) 以及評價區塊的驗證節點，商務平台負責提供買賣雙方交易的平台、驗證初始憑證的正確性、彙整評價資訊，優惠券管理公司負責優惠券發行工作等等。

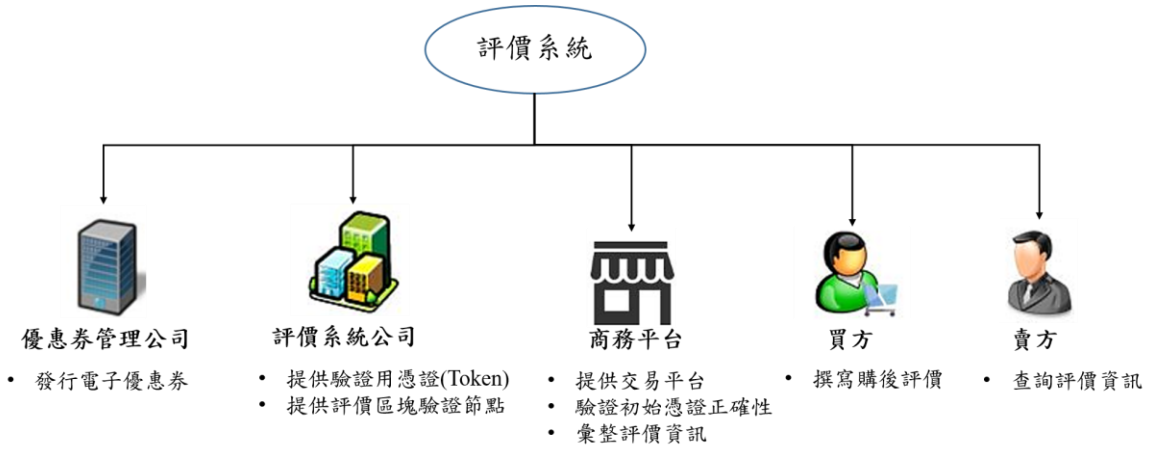

圖3：商務平台評價系統之交易個體

整體的評價系統運行流程如下。在買賣雙方交易後，由商務平台確認完成該交易後發送評價用憑證給予買方。當買方收到憑證後，透過憑證於商務平台撰寫該次交易的評價。這些評價資訊由商務平台所紀錄並且彙總，最後傳送至評價系統公司來進行評價資訊區塊的驗證。驗證評價區塊所需的驗證節點由評價系統公司所提供，在系統的設計概念上將評價系統公司視為可信任的第三方單位，以避免商務平台的權力過大，進而導致惡意的攻擊行為發生。驗證節點完成評價區塊後，將回傳驗證結果給予商務平台，賣家透過評價查詢服務可以得知自己在商務平台的總評價資訊。當評價完成後，將會回饋紅利至買方帳戶中。當達到一定數量後，買方可至優惠券管理公司進行優惠券兌換，如圖

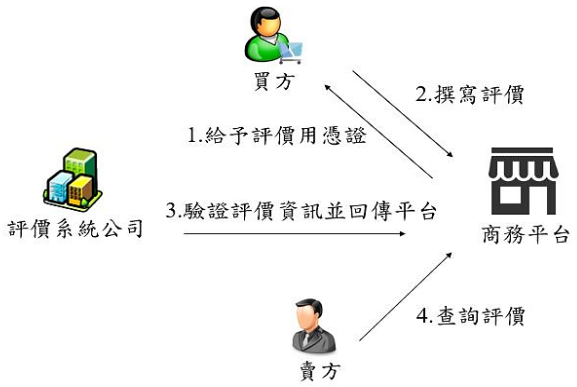

圖4：商務平台評價系統運作流程圖

4所示。表一為本論文所使用的各項符號。

表一：商務平台評價系統之符號表

符號	表示內容
U_{ID}	買方 ID
M_{ID}	賣方 ID
ESC	評價系統公司 (Evaluation System Company)
TN	交易編號 (Transaction Number)
T_i	進行評價用之憑證 Token
Ev_i	評價資訊 i=0, 1, 2, …n
$S_{5\text{-}1\_i}$	評價分數陣列 Score。(5 分到 1 分) i=0, 1, 2, …n
SK	使用私鑰進行數位簽章
Timestamp	時間戳記
$S_{SK\text{-}ESC}$	評價公司用私鑰進行數位簽章
CM_{PK}	優惠券管理公司公開金鑰
C_D	優惠券資訊
C_{ID}	優惠券 ID
C_t	行動優惠券 Coupon (t=0, 1, 2, …n)
R	亂數值
H()	單向 Hash
‖	連結資訊

3.2 評價流程四步驟

所設計的評價程序是建構於交易完成後才能進行的，透過電子投票系統的概念來建立整體的環境。而評價的過程中，買方所取得的評價憑證是由買方、賣方以及交易編號所構成，當確認憑證無誤後才可以進行評價填寫。

3.2.1給予評價資格

買方於商務平台完成交易後請求評價的資格，商務平台確認交易成功後回覆評價系統公司，同時請求評價時使用之憑證。此憑證類似於通行證，買方需要持有該憑證才可以至商務平台進行評價程序。接著評價系統公司確認回覆訊息後，傳送評價用憑證給予商務平台，憑證是透過買方的ID、賣方的ID以及交易時所產生的交易編號所構成。為了避免憑證的資訊被有心人士追蹤，因此透過單向雜湊加密，保護其資訊並傳送給商務平台。商務平台收到憑證後，透過評價系統公司的公鑰進行初始憑證的數位簽章驗證，以

確保初始憑證的正確性，最後透過商務平台發送憑證給欲進行評價的買方。在此架構中假設評價系統公司為可信任的，不會將資訊外流，憑證透過User ID、Merchant ID、

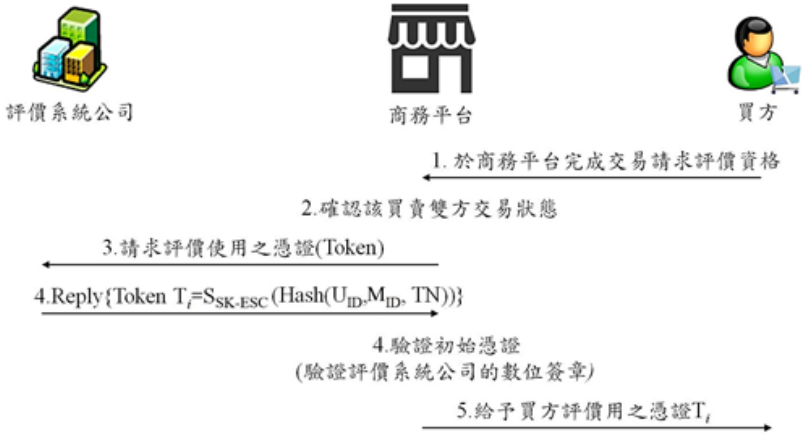

圖5：給予評價資格示意圖

Transaction Number (TN) 所構成，憑證的時效性可以由商家或商務平台與評價系統公司來進行協商，確保評價評分可以在特定的時間內完成填寫，以利後續進行資料的蒐集與市場分析。如圖5所示。

3.2.2評價流程

買方透過商務平台給予之憑證請求驗證及評價機會，當商務平台收到買方請求後開始驗證憑證，由於憑證是使用User ID、Merchant ID、TN透過雜湊和數位簽章加密所產生的，因此商務平台可以透過相同的資訊進行雜湊加密比對。驗證成功時，商務平台將允許該買方進行評價；驗證失敗，商務平台將會告知買方憑證錯誤，並結束評價流程。

當買方進行評價程序時，系統會將評價分數存入相對應的陣列內。以評分1到5分為例，S1到S5對應評價個數。例如：新增一筆新的評價分數為5分，分數陣列的S5中會1。完成評價後，買方會將評價陣列連結並透過雜湊加密，以確保評價資訊不會被竄改，最後加上Has (TN) 作為索引傳送給商務平台。

商務平台收到買方的評價資訊後，先驗證H (TN) 以確保整體評價資訊未遭到竄改，驗證成功後將其評價資訊建立為總評價區塊鏈 Block T。Block T內包含前一個評價資訊 (Ev_{i-1})、當前的評價資訊 (Ev_i)、H (TN) 以及時戳 (timestamp)。最後，買方將透過商務平台回傳的評價資訊以確認是否為自己評價的內容。如圖6與圖7所示。買方請求驗證憑證及評價機會，商務平台驗證買方給予之憑證，並回覆買方驗證訊息 (成功/失敗)，接著買方撰寫評價後，平台驗證買方資訊並建立總評價區塊鏈。最後，顯示評價結果給予買方確認。

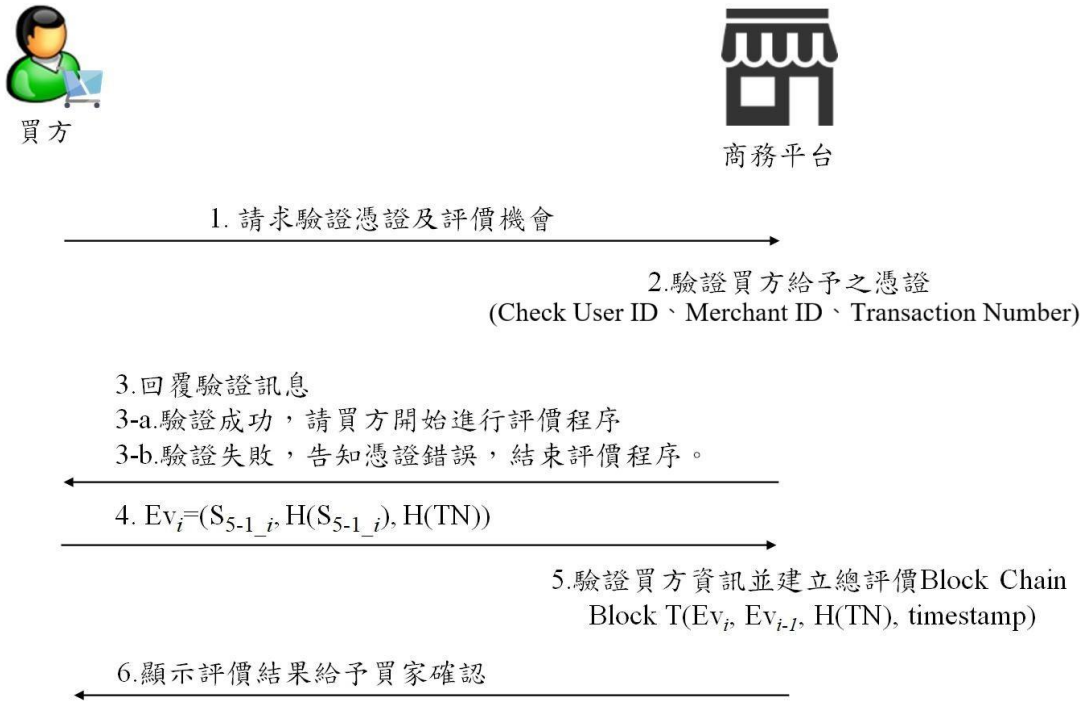

圖6：評給予評價資格示意圖

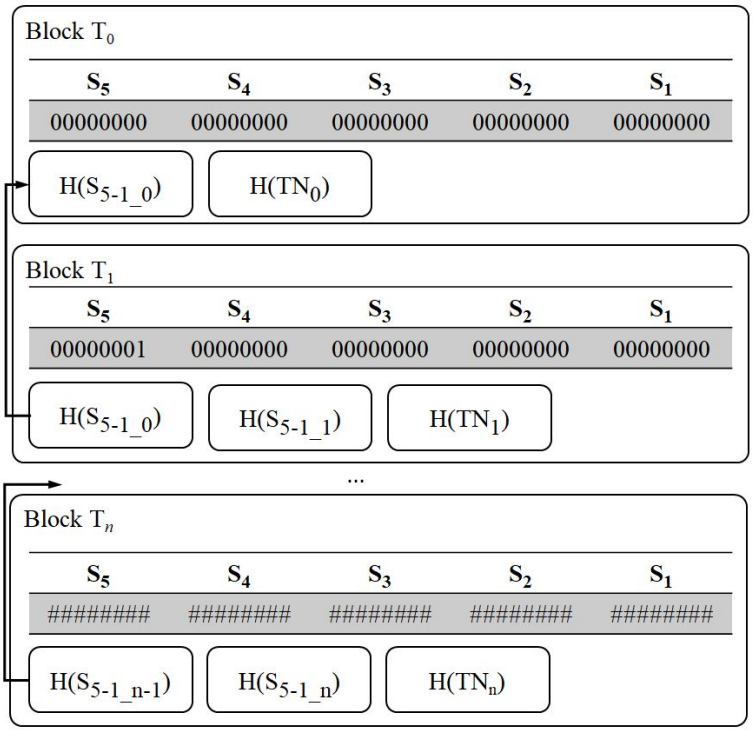

圖 7：評總評價區塊鏈示意圖

3.2.3評價驗證

商務平台建立總評價區塊鏈的過程中，每新增一筆新的評價區塊，就會透過評價系統公司所提供的驗證節點來進行區塊的驗證。而驗證節點所需進行的驗證項目包括了評價區塊Ev_i與前一個評價區塊Ev_{i-1}是否為原始的連結規則、評價區塊Ev_i的評價資訊S5-1_i與H(S5-1_i) 的內容是否相符，以及透過雜湊加密所保護的交易編號TN是否與商務平台給予的交易編號一致。

3.2.4評價查詢

商務平台透過總評價區塊鏈彙總各賣家的評價資訊表。賣方要進行總評價查詢時，透過賣方自己的ID向商務平台請求查詢，商務平台收到請求後，將依據其賣方的ID回覆相對應的評價資訊。如圖8所示，在總評價資訊表中所見的S5~S1分別為該賣家在各個評分項總共拿到了幾筆 (5分到1分)，如圖8所示。

賣方

商務平台

1. 彙整各賣家之總評價資訊

Merchant ID	Ev *i*	Total Ev				
Merchant A	Ev 1	S_5	S_4	S_3	S_2	S_1
		8	5	4	3	0
Merchant B	Ev 2	S_5	S_4	S_3	S_2	S_1
		9	6	7	0	1
…	…	…				

2.請求查詢總評價資訊
Request{Total Ev M_{ID}}

3.回覆各賣家之總評價資訊
Reply{Total Ev M_{ID}}

圖8：評價查詢示意圖

3.3 紅利發放與兌換優惠券

當以上評價流程完成後，商務平台會將紅利點數發送至買方帳戶中，買方可以透過累積紅利點數進行優惠券的兌換，如圖9所示。商務平台會將買方U_{ID}和欲兌換的優

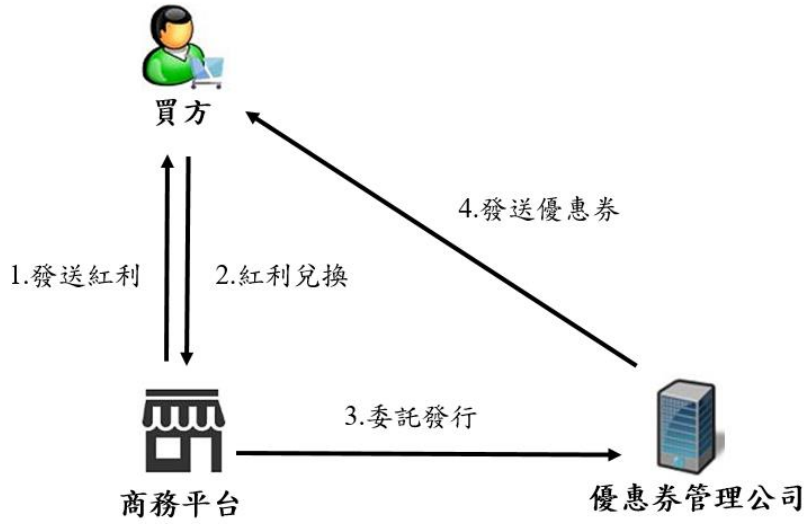

圖 9：評價查詢示意圖

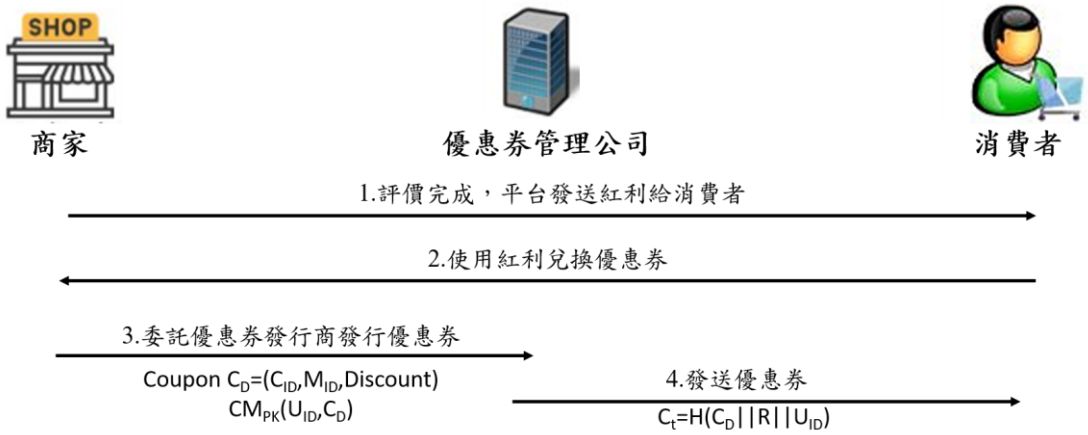

圖 10：使用紅利點數兌換優惠券示意圖

惠券資訊C_D(內包含優惠券ID、店家名稱和折扣內容) 使用優惠券管理公司的公開金鑰(CM_{PK}) 進行加密後進行傳送；優惠券管理公司透過私密金鑰解密後得出U_{ID}和C_D，再加入亂數值 (R) 進行串聯，最後進行雜湊得到行動優惠券 (C_t)，再傳送至買方帳戶中，完成優惠券兌換流程，如圖10所示。

肆、協定分析

此章節將探討本研究中所設計的方法是否解決商務平台購物的隱憂，以及在方法中的安全設計能否保護評價資訊不被竄改與惡意灌水。首先，使用者在商務平台欲購買商

品時，不知該賣家能不能信賴，可以透過評價分數來衡量該賣家的信賴程度，再下單購買。

評價分數的生成是透過完成交易後與商務平台領取憑證才有評價資格，而憑證必須經過商務平台驗證成功才能進行評價程序，因此減少了評價惡意灌水之問題，使其評價分數能讓使用者信賴。賣方可能會透過買帳號的方式來攻擊評價系統產生灌水的相關問題，在這個問題中，產生憑證可以向商務平台系統收費，因此若要獲取大量的憑證來取得評價機會，需要負擔一些額外的費用。

接著，在評價系統的驗證節點設計中，透過私有鏈的概念進行設計，整體的網路由成員機構之間共同維護，驗證共識的過程由預先選好的節點來進行控制。而擔任驗證節點的角色為與評價系統公司合作的每個商務平台。由於這些商務平台彼此是對立的競爭者，因此適合擔任整體優惠券區塊鏈的驗證節點，以減少驗證節點串謀的機會。

評價資訊的建立是否能有重新評論的機制，以下將有兩點情況來進行討論。情況一：透過電子投票系統的概念來進行評價的建立。在這樣的評價環境中，每個評價採取一次交易一個評價，當完成評價之後就無法去更改其評價的內容；情況二：賣方透過售後服務的方式，希望挽回消費者的心，能給予商家正向的評價。因此，若要修改原有的評價資訊，則需重新發放評價用之憑證再重新進行一次評價程序。最後，以下將對於整體評價系統進行安全性分析：

1. 機密性 (Confidentiality)：本研究中，在商務平台的交易過程，僅只有買方、賣方與商務平台知道其交易資訊，潛在的商務平台使用者無法得知其資訊，因此買賣雙方的交易資訊具有機密性。評價資訊的內容於買方完成評價後，商務平台會透過單向雜湊將評價資訊進行加密後彙總至各賣家的總評價區塊鏈中，能得知的僅只有總評價分數；而買方的評價資訊只有買方與商務平台知道，因此評價資訊具有機密性。
2. 完整性 (Integrity)：憑證的建立與評價資訊的傳送，其內容都包含著交易完成所產生的交易編號。透過將交易編號進行雜湊加密，是為了能確保其憑證或評價資訊避免被商務平台或是惡意的攻擊者進行偽造或是竄改。而交易編號具有唯一性，倘若發生偽造之行為，在驗證的過程中將無法通過，因此整體評價系統環境具有完整性。
3. 可驗證性 (Verifiability)：評價資訊是透過評價資訊的明文以及將評價資訊陣列使用雜湊加密產生的密文所生成。其中買方完成評價流程後，透過自己的評價資訊可以去驗證商務平台所建檔的評價是否與自己傳送的評價資訊相同，確保評價資訊沒有受到竄改；而商務平台可以透過Timestamp與交易編號TN去驗證總評價區塊鏈中的資訊，因此評價資訊具有可驗證性。
4. 可靠性 (Reliability)：所有的評價資訊都經過商務平台的H(TN) 驗證，確認其評價資訊的正確性後建立總評價區塊鏈。其中總評價區塊鏈內容包含前一次的評價資訊 (Ev_{i-1})、當前的評價資訊 (Ev_i)、雜湊加密的交易編號H(TN) 以及時

戳 (timestamp)。每個評價資訊區塊都將透過這樣的規則來進行建立。當Ev_{i-1}與Ev_i的數值資訊進行相減後，其位元數差值不是1bit時，將捨棄該區塊，因為該區塊的資訊可能遭到竄改的行為或是生成的過程有發生錯誤，因此不將此區塊加入到整體的總評價區塊鏈節中。

5. 匿名性 (Anonymity)：買家進行評價流程到結束時，其過程僅有商務平台能確認買家身分，並且進行評價資訊的撰寫。而賣方在查詢評價的過程中，無法得知該評價資訊是由哪位買家評分，最後在評價總區塊鏈中，儲存資訊僅包含評價評分、連結規則的相關雜湊資訊以及時戳，並沒有包含使用者個人資訊，因此整體的評價環境中具有匿名性。

伍、結論

網路購物有別於過去實體店面的選購，顧客無法得知其商品有無瑕疵或是滿足自己的需求，因此評價資訊顯得格外重要。然而，電商平台的賣家為了穩固客源，可能將評價進行灌水，讓其評價資訊失去了原有的可靠性。透過本研究所設計的使用區塊鏈技術評價系統架構將能解決現今商務平台所產生的評價問題。區塊鏈技術的特性以及電子投票系統的概念，讓整體架構中具有安全性與匿名性。

所設計的協定，讓顧客於商務平台完成交易程序後，持有平台給予的憑證才能進行評價程序，用以防止未交易的顧客進行評價行為，避免灌水之行為，以確保資訊的可信度。憑證的設計由評價系統公司製作，其中憑證內容透過商務平台交易資訊來建立，使用交易編號作為驗證關鍵資訊。由於交易編號具有唯一性，因此無法任意地進行變更。顧客完成評價後，商務平台將彙總評價資訊並建立總評價區塊鏈，評價資訊區塊的驗證委由評價資訊系統所提供的驗證節點，一方面能減少商務平台的工作，在評價程序中可以各司其職。另一方面則能透過評價系統公司作為可信任的第三方單位，以避免商務平台權力過大，進而引起評價資訊操弄所帶來的風險。在顧客評價的過程中，只有商務平台知道其身分，平台的潛在顧客以及商家無從得知，僅能知道評價資訊的結果，因此符合區塊鏈技術的匿名性。除區塊鏈的安全技術外，亦使用其他的資訊安全機制來預防機密訊息遭受竊取或竄改。結合紅利回饋的機制，可以透過消費進行紅利累積，來兌換優惠券，促進消費者回購的動機，也可作為評價系統的獎勵，鼓勵消費者進行意見回饋。

此外，在協定設計考量若使用行動設備運算量與儲存量不足問題，以數位簽章以及雜湊加密法來減少行動設備負擔，並能防止惡意人士的攻擊。未來將研究如何使買賣雙方進行互相評價，使雙方在網路買賣活動中都能保障自身的權益。

參考文獻

[1] 金之中(2011)，折價券特性對消費者購買意願之影響-以大學生為例，碩士論文，東海大學，台中。

[2] 邱顯貴、楊亨利(2003)，「線上購物網站值得消費者信任的因素之研究」，資訊社會研究，第5期，第139-174頁。

[3] 陳以禮、李芳齡 譯、唐・泰普史考特、亞力士・泰普史考特(2016)，區塊鏈革命：比特幣技術如何影響貨幣、商業和世界運作，天下文化。

[4] 陳俊銘(2008)，行動優惠券之研究，碩士論文，朝陽科技大學資訊管理系，台中。

[5] 黃明祥、林詠章(2014)，資訊與網路安全概論 看見比特幣 第五版，東華書局

[6] 蔡至欣、賴玲玲(2011)，虛擬社群的資訊分享行為，圖書資訊學刊，第9卷，第1期，第161-196頁。

[7] C. Blundo, S. Cimato, and A. D. Bonis (2002), "A Lightweight Protocol for The Generation and Distribution of Secure E-Coupons," *Proceedings of the 11th* international *conference on World Wide Web*, pp. 542-552.

[8] K. Christidis and M. Devetsikiotis (2016), "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, Vol. 4, pp. 2292-2303.

[9] M. Crosby, N., P. Pattanayak, S. Verma, and V. Kalyanaraman (2015), "BlockChain Technology Beyond Bitcoin," S*utardja Center for Entrepreneurship & Technology Technical Report, 2150 Shattuck Ave 11th Floor*, Berkeley, CA 94704.

[10] S. Das, J. Rout and M. Mishra (2022), "Blockchain Technology: Applications and Open Issues," 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT).

[11] J. Han, Y. Son and H. Eom (2022), "A Secure E-Coupon Service Based on Blockchain Systems," *IEEE Access*, Vol. 10, pp. 21836-21846.

[12] J. Kangasharju and A. Heinemann (2006), "Incentives for Electronic Coupon Systems," *Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking*, Los Angeles, California, pp. 60-62.

[13] S. Khajehzadeh, H. Oppewal, and D. Tojib (2014), "Consumer Responses to Mobile Coupons: The Roles of Shopping Motivation and Regulatory Fit," *Journal of Business Research*, Vol. 67, No. 11, pp. 2447-2455.

[14] F. Liuab, S. Liua, and G. Jiang (2022), "Consumers' decision-making process in redeeming and sharing behaviors toward app-based mobile coupons in social commerce," *International Journal of Information Management*, vol. 67, 102550.

[15] S. Nakamoto (2009), "Bitcoin: A Peer-to-Peer Electronic Cash System," retrieved from www.bitcoin.org.

[16] J. Newell, Q. Mamun, S. Rehman and M. Z. Islam (2022), "Proof-of-Enough-Work Consensus Algorithm for Enhanced Transaction Processing in Blockchain," Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1188-1193.

[17] V. Prakash (2018), "4 Ways Blockchains Will Redefine eCommerce," retrieved from https://www.globalsign.com/en/blog/4-ways-blockchain-will-redefine-ecommerce/.

[18] R. Ramachandiran (2018), Using Blockchain Technology To Improve Trust In eCommerce Reviews, University of Maryland, College Park, pp. 1-15.

[19] Y. Ren, P. Fu and W. Yu (2021), "Prediction of Coupon Usage Behavior Based on Customer Segmentation and XGBoost algorithm," Proceedings of the International Conference on Big Data Economy and Information Management (BDEIM).

[20] S. Somal (2018), "How to Improve or Restore Your Online Reputation," retrieved from https://www.socialmediaexaminer.com/improve-restore-online-reputation/.

[21] T. Shojima, Y. Ikkai, and N. Komoda(2004), "An Incentive Attached Peer to Peer Electronic Coupon System," Studies in Informatics and Control, Vol. 13, No. 4, pp. 233-242.

[22] F. Wu, H. H. Li, and Y. H. Kuo (2011), "Reputation Evaluation for Choosing a Trustworthy Counterparty in C2C E-commerce," Electronic Commerce Research and Applications, Vol. 10, No. 4, pp. 428-436.