Regular Paper

Communications of the CCISA
Vol. 27 No. 2 May 2021

以區塊鏈技術建立具有履約保證機制的遞延性商品 (服務) 平台：以補教業為例

壽大衛[1*]、吳善婷[2]
[12]臺北市立大學 資訊科學系
[1]shou@utaipei.edu.tw、[2]shan.wst@gmail.com

摘要

遞延性商品 (服務) 由消費者先預付費用才獲得服務。為避免業者惡性倒閉，行政院明訂所有販售遞延性商品 (服務) 的業者於合約中須聲明履約保證機制；該類業者申請銀行刷卡提供消費者分期服務也須在銀行質押。這將導致業者須提撥兩筆資金才能合法開業及提供刷卡服務。本研究應用區塊鏈技術，在業者不須質押的前提下，建立具有履約保證機制的遞延性商品 (服務) 交易平台。

該解決方案於銀行建構聯盟區塊鏈，將消費者支付的費用透過電子錢包支付並託管在銀行，於業者提供服務後由銀行按交易約定分段撥款給業者；如業者未依約對消費者履行服務，銀行可終止撥款並將剩餘費用返還給消費者。本研究套用補教業場景，建構模型以從技術上展示該平台的運作模式，打造更具安全性、公信力及合法的交易平台。

關鍵詞：區塊鏈、遞延性商品、履約保證、補教業、補習班

Regular Paper

Communications of the CCISA
Vol. 27 No. 2 May 2021

Using Blockchain Technology to Establish a Deferred Commodity (Service) Platform with a Performance Guarantee Mechanism: Take the Supplementary Education Industry as an Example

Da-Wei Shou[1*], Shan-Ting Wu[2]
[12]University of Taipei Department of Computer Science
[1]shou@utaipei.edu.tw, [2]shan.wst@gmail.com

Abstract

Deferred commodity (services) are prepaid by consumers before they get the service. In order to avoid business bankruptcy, the Executive Yuan stipulates that all businesses selling deferred commodity (services) must declare a performance guarantee mechanism in their contracts; such businesses must also pledge in the bank when they apply for bank card swiping to provide consumer installment services. In this way, businesses got to pledge two funds to legally start business and provide credit card services. We uses blockchain technology to establish a deferred commodity (service) trading platform with a performance guarantee mechanism under the premise that the industry does not need to pledge.

The solution builds an federated blockchain in the banks, and pays the fees paid by consumers through e-wallets and escrows them in the bank. After the industry provides services, the bank allocates funds to the industry in stages according to the transaction agreement. If the industry fails to perform services to consumers in accordance with the contract, the bank may terminate the allocation and return the remaining fees to the consumers. This study applies the scene of the supplementary education industry, constructs a model to technically demonstrate the operation mode of the platform, and creates a more secure and credible trading platform.

Keywords: Blockchain, Deferred Commodities, Performance Guarantee, Supplementary Education Industry, Cram School

壹、前言

遞延性商品 (服務) 又稱預付型商品，由消費者先付費才獲得商品或服務。遞延性商品 (服務) 存在的型態與業種繁多，舉凡禮券、儲值金、健身房、美容院、補習班等，因擴及的產業多元，業者惡性倒閉[1]的情況層出不窮。因此，販售遞延性商品 (服務) 的業者，行政院訂定定型化契約規範業者須質押一定比例的收入作為履約保證，確保惡性倒閉時，消費者得以向第三方尋求返還未履行服務的費用。再者，遞延性商品 (服務) 業者在向銀行申請刷卡服務時，銀行要求業者質押若干月的預估刷卡金，目的是要避免業者無力償還或倒閉後，銀行預先替消費者支付的費用有償還保證。綜觀以上所述，遞延性商品 (服務) 業者光是質押金就高達將近 45%[2] 的收入，在達到合規的目的下，同時必須犧牲可動用資金的額度。

補習班銷售的課程屬於遞延性商品 (服務) 的一種，同樣面臨上述的質押問題；而在消費者端，對家長而言教育是不能等待的，不論家庭收入高低，家長都願意花費來培養孩子，也因此對於較弱勢的家庭，爭取不到銀行信用卡做學費的分期服務，可能轉為尋求融資貸款，反而導致窮者更窮的局面。履約保證、業者分期服務、消費者分期還款這三項都圍繞著「信用證明」的問題──事先拿出一筆資金扣押，確保背書機構有能力善後、檢具財產及收入明細證明有還款能力。

區塊鏈技術的優點在於：(1)去中心化；(2)分散式帳本實現不可竄改性；(3)不需要受信的第三方來完成交易；(4)更安全；(5)匿名性。這將是應用區塊鏈取代履約保證的中心化第三方機構的基石。本研究擬建構銀行聯盟區塊鏈，每個參與的銀行都是一個超級節點，任一銀行的每筆交易都將分散儲存於每個銀行資料庫。消費者與業者在聯盟鏈的其中一間銀行擁有銀行帳戶，並透過網路銀行申請電子錢包，送出的交易授權扣款要求經確認後，從消費者端將扣下的款項儲存於銀行，於約定撥款日按金額匯入至業者的電子錢包。經過確認的交易，即被上鏈，任何人都無法竄改交易，會依當初設定的時間、金額及對象付款。

貳、文獻探討

2.1 補教市場與產品型態

調查不同月收入的家庭願意支付補習花費程度發現[20]，每月總收入不到 2 萬元的家庭平均一個月願意支付在補習的花費為 2962.22 元，月收入在 20 萬以上的家庭平均

[1] 惡性倒閉係指公司行號在無預警、未經正當停業程序下結束營運，且倒閉後未妥善處理員工薪資、廠商貨款或消費者權益等事宜而人去樓空的情況。

[2] 以補教業為例，履約保證需信託 30% 的學收收入；銀行刷卡服務質押金以「月收入」計算：補習費大部分一次繳一學期費用，每個月學費約為學收 15% 。合計總信託費用約 45% 收入。

一個月的補習花費為 3083.80 元，兩者月收入相差 10 倍，但每月補習花費只相差 122 元，表示不論家庭收入高低，補習花費是家庭必要及不可替代的支出。

依據天下雜誌於 2016 年調查統計國小、國中生的補習人數占比顯示[15]：國小約有 67.8% 的學生有補習經驗；國中則約有 56.9% 的學生有補習。文理補習班截至 2020 年 10 月份的設立總數為 11,387 家，相較 10 年前的 2010 年總數 10,839 家相比，新增了 5.1% (短期補習班資訊管理系統，2020) ，在少子化的衝擊下不減反增。遠見雜誌[16]更揭露資策會曾在 2013 年估計臺灣補教產業年產值約 1,500 億元臺幣。不斷成長的內需市場及龐大的產值即是本研究認為有價值可以區塊鏈技術重塑其交易模型的因素之一。

補習班課程屬於遞延性商品 (服務) [17]，又稱「預付型商品」。遞延性商品 (服務) 契約具有「預付」、「不定期」及 「繼續性」三種性質。繼續性又分定期和不定期繼續性契約，且因契約當事人任一方「是否已將對價預付給他方」分為「一般型繼續性供給契約」與「預付型繼續性供給契約」[19]，本研究之補習班課程即屬「預付型繼續性供給契約」之性質。

短期補習班定型化契約由行政院擬定並公布範本供補習班使用。按其第十條第 (五) 項[14]規定補習班方須提供履約保證機制，並詳列履約保證內容於合約中供消費者查照。履約保證可為以下方式擇一：

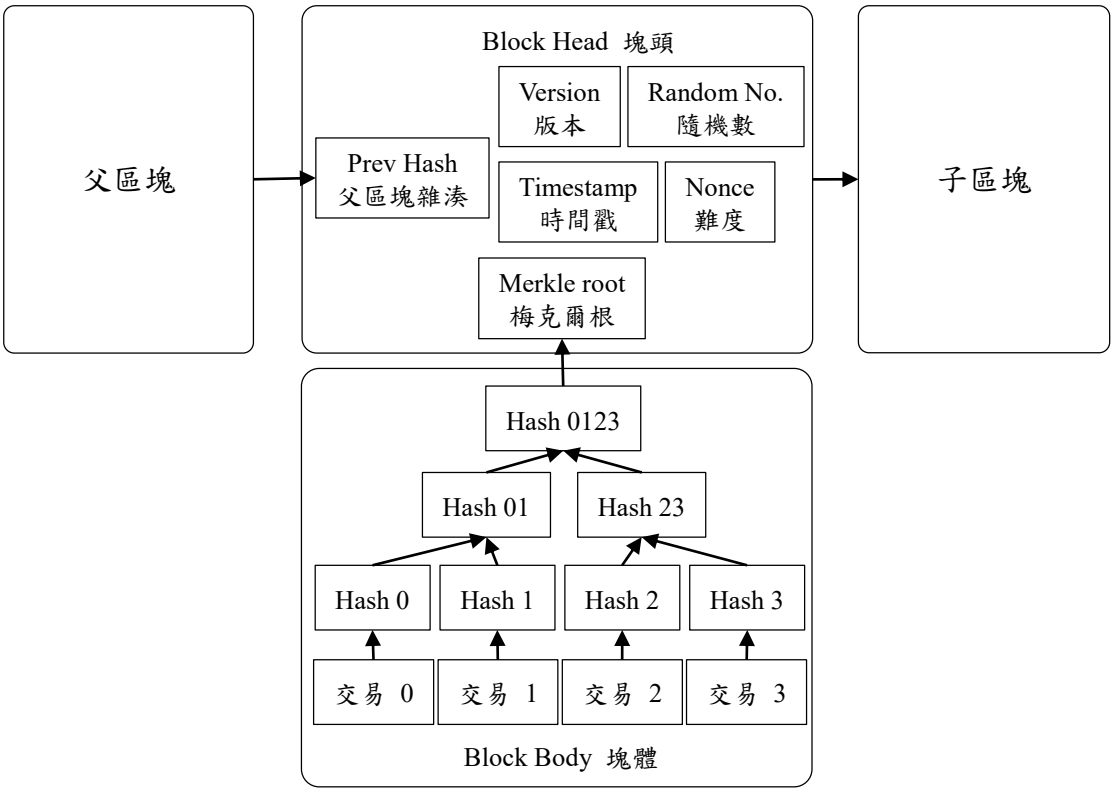
1. 就收取費用總金額 30% 額度提供履約保證，交付金融機構或信託業者開立信託專戶管理。
2. 加入補習服務聯合連帶保證協定。
3. 投保高於新臺幣二百萬元之履約保證保險，作為辦理補習服務之履約保障。

補習班要合法合規營業，必須凍結每期 30% 學費在金融或信託機構，或按月支付協會會費及基金[13]，或支付保險費來作履約保證。

2.2 區塊鏈技術

區塊鏈技術的誕生始於對貨幣及財產登記去中心化的需求上[10]。中本聰[8]通過發表科學文章提出了區塊鏈技術，使用去中心化的點對點 (Peer-to-Peer，P2P) 區塊鏈網路作為雙花問題的解決方案，也就是網路生成交易時間順序的計算證明。中本聰將此想法轉化為比特幣 (Bitcoin, BTC) 的虛擬貨幣，無需受信任的第三方即可用於點對點交易。

區塊鏈的區塊結構如圖一，為每個區塊有塊頭 (Block Header) 和塊體 (Block Body) 兩部分，並包含鏈狀結構、Hash、Merkle 和時間戳 (Timestamp) 等要素[12]。其技術組件則包括交易、區塊、共識、應用程式和智能合約，可視為一區塊鏈生態系統[2]。



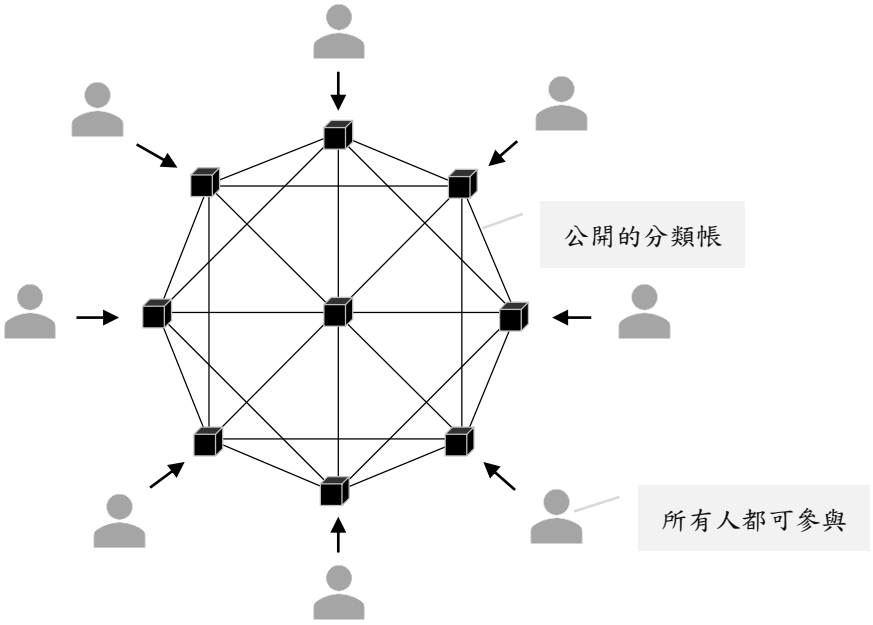
圖一：區塊鏈結構

1. 由單一或組織擁有足夠強大到掌握超過 50% 節點數的礦池算力，進而導致網路中斷並能故意排除或篡改交易順序，也就是俗稱的 51% 攻擊，在截至 2021 年 1 月，比特幣的全球活躍節點數達 11,627 個[1]的前提下，攻擊成功機率幾乎是 0。由此更證明了區塊鏈的安全性是無庸置疑的。
2. 加密：區塊鏈的加密機制，在虛擬貨幣交易中反映了很大一部分的應用。比特幣區塊鏈採用公開金鑰加密演算法 (Public Key Cryptography) 中的橢圓曲線數位簽章演算法 (Elliptic Curve Digital Signature Algorithm，簡稱：ECDSA) [4]。比特幣區塊鏈中的節點使用者，會同時擁有「公鑰、私鑰」這兩把金鑰，以及比特幣位址 (Address) ，公鑰是公開可被區塊鏈網路中的其他人知道的，而私鑰則須自行保管，用來接收及發送貨幣、進行電子簽章，而位址則是用來當作存取比特幣的地址，不過每個位址只能使用一次。在 ECDSA 演算法中，由私鑰推算出公鑰很容易，但要從公鑰回推私鑰卻很困難。公鑰、私鑰的加密機制所衍生的特性，例如電子錢包、資產管理、驗證等，不僅實現了個人資產完全自主管理，也取代了人與人之間的信任問題，大幅提升安全性與交易效率。

區塊鏈主要公有鏈、私有鏈兩種類型。後因不同的應用場景，取公有鏈及私有鏈的優點結合後又衍生出了聯盟鏈及混合鏈的類型[3]。

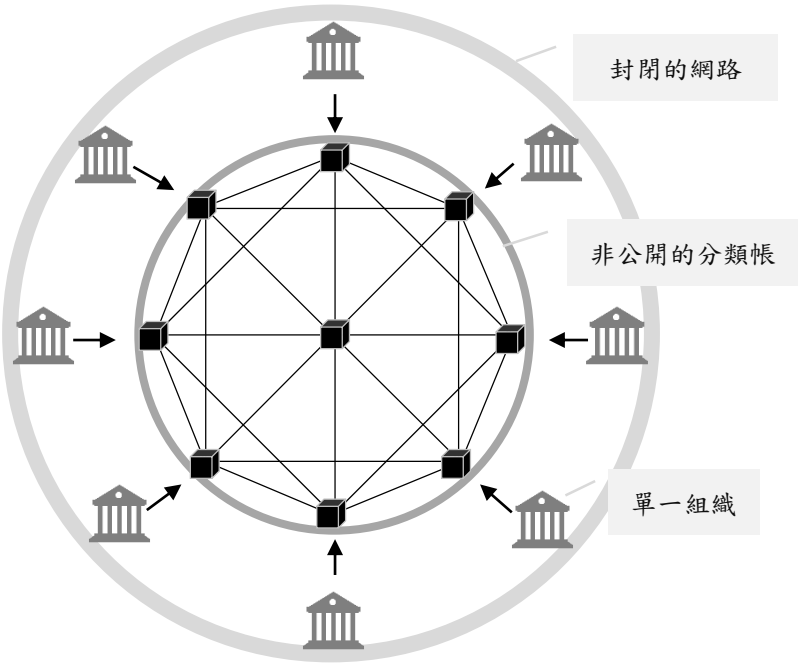
1. 公有鏈 (Public Chain)：公有鏈又稱公鏈。是一種無需被許可就可參與的分散式

分類帳技術，任何人都可以加入並進行交易，如圖二。每個對等方都有一個分類帳的副本，只要有網路連接，任何人都可以訪問公鏈。最早問世的公鏈之一是比特幣公鏈。它使連接到網路的任何人都可以以分散式進行交易，並通過工作量證明 (Proof of Work, PoW) 或權益證明 (Proof of Stake，PoS) 等共識方法來完成交易的驗證[5]。公鏈的優點是訪問門檻低、資料公開透明且無法篡改、匿名性、每個人都感到有動力去改善公共網路、不需要中介機構、安全、由於數據可被驗證，交易透明化；缺點則是交易速度慢。



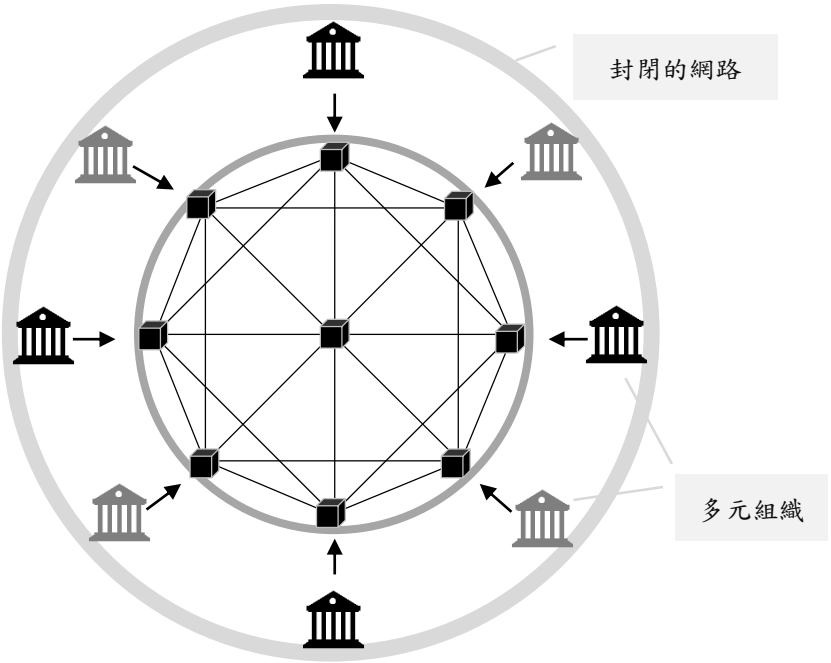
圖二：公有鏈節點與參與者關係

2. 私有鏈 (Private Chain)：私有鏈為在受限的封閉網路環境中工作的區塊鏈。它是一條非公開的鏈，需要「授權」才能加入節點。它也是受實體控制的許可區塊鏈，讀取許可權則視需求有選擇性地對外開放。私有鏈適用於私有公司、組織、特定機構的內部資料管理、審計等金融場景的應用中以便有效地使用區塊鏈，並且僅允許選定的參與者訪問區塊鏈網路，如圖三。私有鏈交易速度快，因為與公鏈相比，參與者較少，相對地花費更少的時間達成共識，從而加快了交易速度。私有鏈也比公鏈更具可擴展性，因為在私有鏈中只有少數幾個節點有權驗證交易，關鍵是決策是集中化的。然而，私有鏈並沒有真正去中心化，因此很難獲得信任，也由於只有少數幾個節點，因此安全性有限[7]。



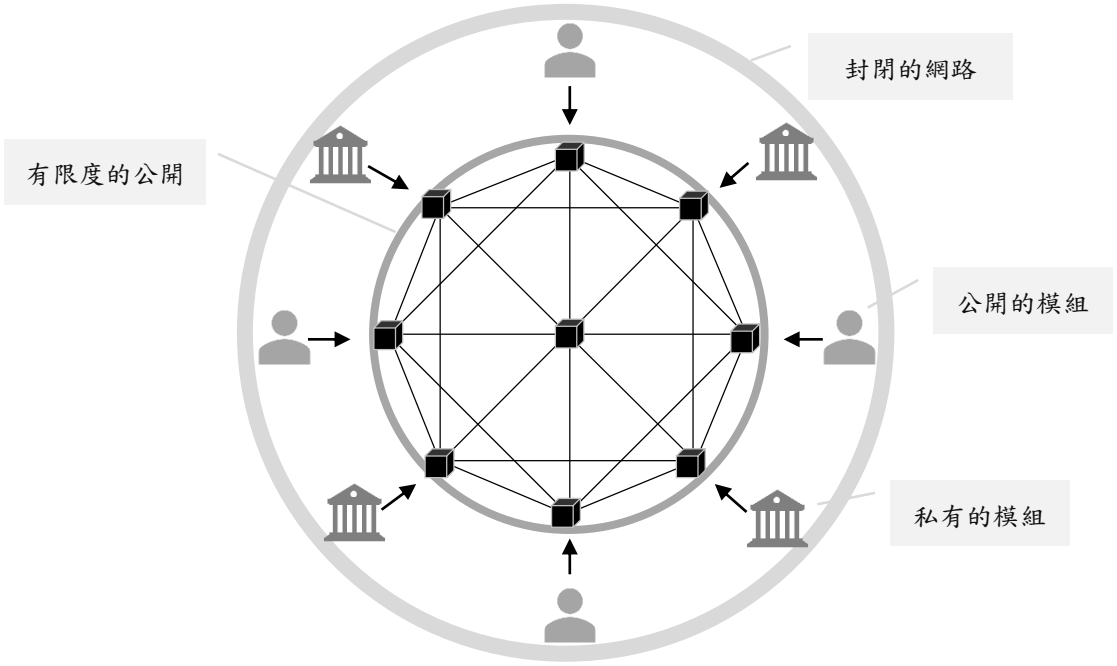
圖三：私有鏈節點與參與

3. 聯盟鏈 (Federated Chain)：聯盟鏈是一種為解決公共需求和私有鏈功能結合的組織需求創新方法。由多個機構共同參與管理，每個組織或機構管理一個至多個節點，其資料只允許聯盟內的機構進行讀寫和發送，如圖四。聯盟鏈中的共識程序由預設節點控制。儘管它不對大眾開放，但它仍然具有去中心化的性質，因為一個財團的區塊鏈是由多個組織管理的，因此沒有權力集中的力量。換句話說，聯盟鏈提供了私有鏈的所有功能，包括透明性、隱私性和效率，而沒有一方具有整合能力[6]。



圖四：聯盟鏈關係圖

4. 混合鏈(Hybrid Chain)：圖五混合鏈為公鏈和私有鏈的組合。它在封閉的生態系統中工作而無需公開所有內容，並且可以根據需要更改規則。它可以在仍與公共網路連接的同時保持隱私性。與公共網路相比，它具有良好的可伸縮性。但混合鏈不完全透明，並且較沒有動機吸引各方參與網路並為網路做出貢獻[11]。



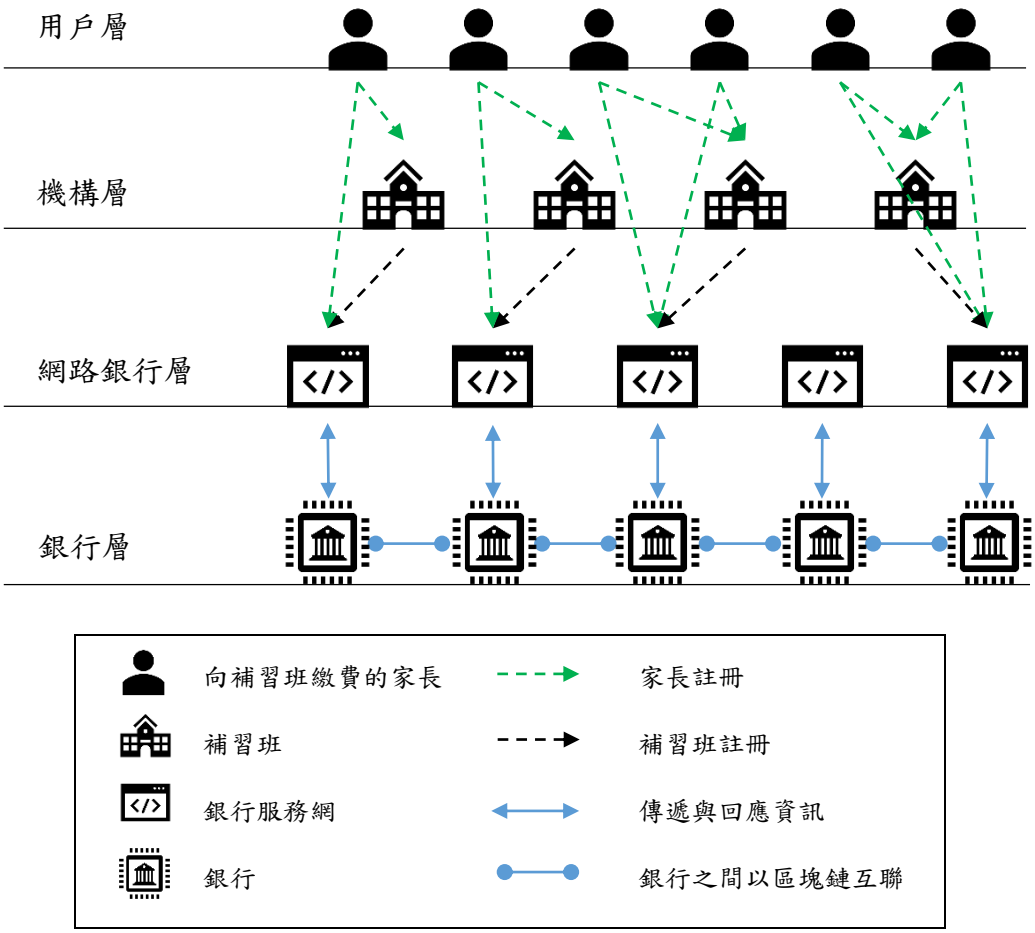
圖五：混合鏈關係

參、設計

消費者向補習班購買遞延性商品 (服務) 時建立合約，在消費者以電子錢包支付費用後由銀行代管費用，按合約中的服務期程透過區塊鏈技術與平台機制分階段撥付費用給補習班，並且在補習班未按合約提供服務時，將未實現服務的餘額撥還給消費者。本章介紹平台系統架構設計及工作流程：

3.1 系統架構

本研究以區塊鏈技術實現替代補教業履約保證機制的系統架構，建構一個以銀行聯盟區塊鏈為基礎的多層次結構，如圖六所示。銀行本身在此架構下作為託管補習費用的主體，參與的銀行是聯盟區塊鏈中的超級節點，以維護交易數據的安全性。



圖六：系統架構圖

系統分為四層，分別是向補習班繳費的家長──用戶層、機構層──此指補習班、網路銀行層與銀行層。各層的功能及描述如下：

1. 用戶層：家長以真實身分註冊電子錢包，用於與補習班進行繳付學費的交易。交易由銀行層生成交易數據並分散式儲存在銀行層的每個節點，以確保數據的完整性及交易不可竄改性。
2. 機構層：機構此指補習班。與用戶一樣需要註冊電子錢包，作為銀行撥款接收的地址。補習班的電子錢包在本研究架構下，主要作為接收家長暫存在銀行的學費在課程結束後撥款的地址。
3. 網路銀行層：每個銀行有自有的網路銀行，家長及補習班申請電子錢包前，需先在指定的銀行網頁上進行開戶或以既有帳戶與電子錢包關聯。如此可便利於在銀行帳戶與電子錢包的資產進行轉移、所有轉移的過程及每筆交易的紀錄都被參與的所有銀行儲存。該層同時串接教育部短期補習班管理系統，於補習班註冊時及銀行撥款前檢核補習班立案狀況，如立案狀態為「已立案」則可進行註冊及接收款項，如為「撤銷」則不可註冊電子錢包也不可接收款項。一旦偵測為立案撤銷，銀行可直接將剩餘的學費費用返還至家長的電子錢包。

4. 銀行層：本研究取代履約保證機制的作法為從家長的電子錢包中扣款的費用暫存於銀行，並於補習班完成授課後，分次撥款至補習班的電子錢包。因交易在區塊鏈上進行，一旦被交易雙方確認的交易即不可逆也不會被竄改，因此不論是家長或補習班，可以安心地讓費用代管在銀行，即便是銀行本身也無法動用已上鏈的代管款項。

3.2 流程設計

本節整理並說明在接下來的小節，描述系統設計的流程中使用到的代號，如表一所示。

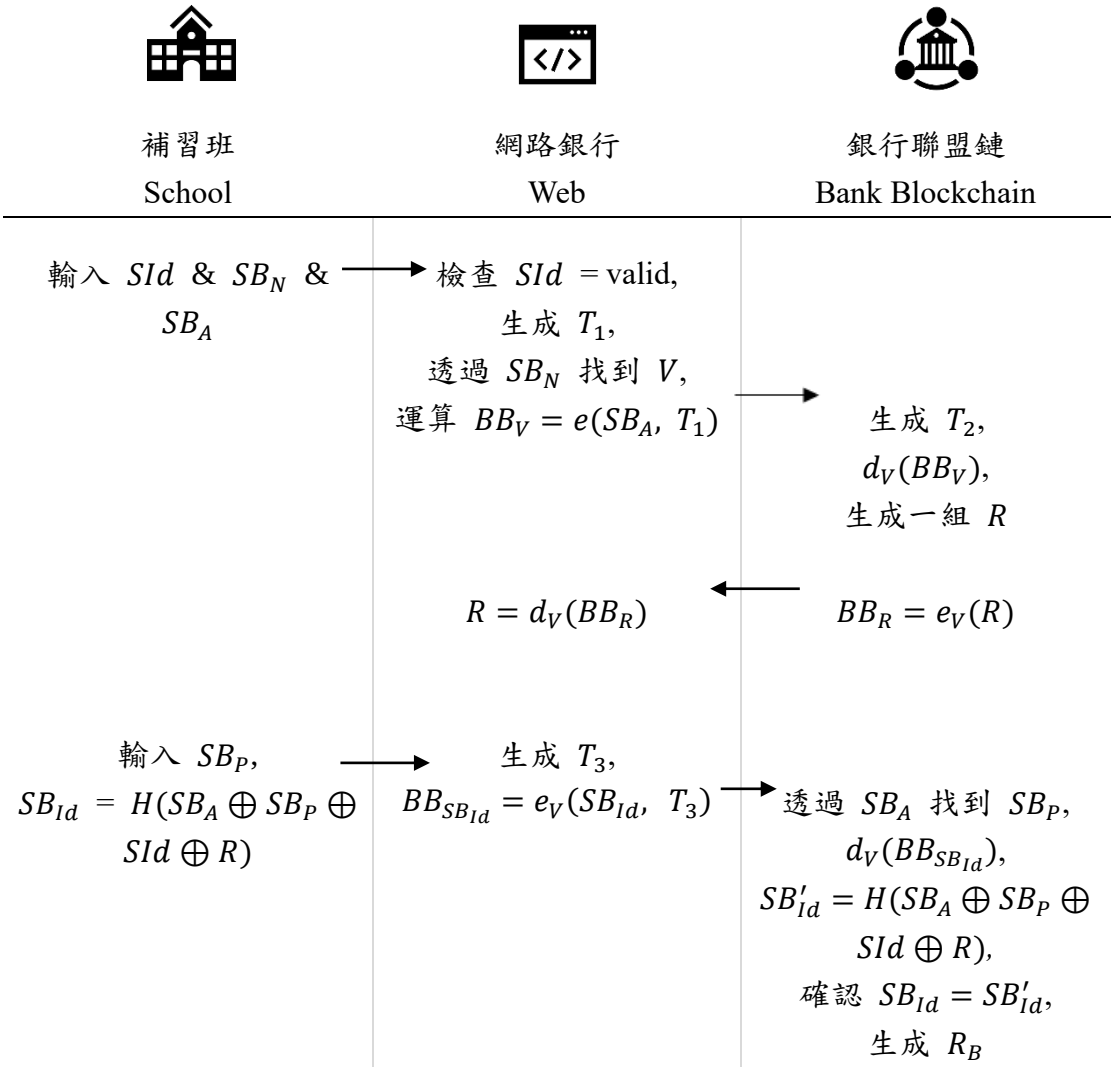
表一：代號與說明

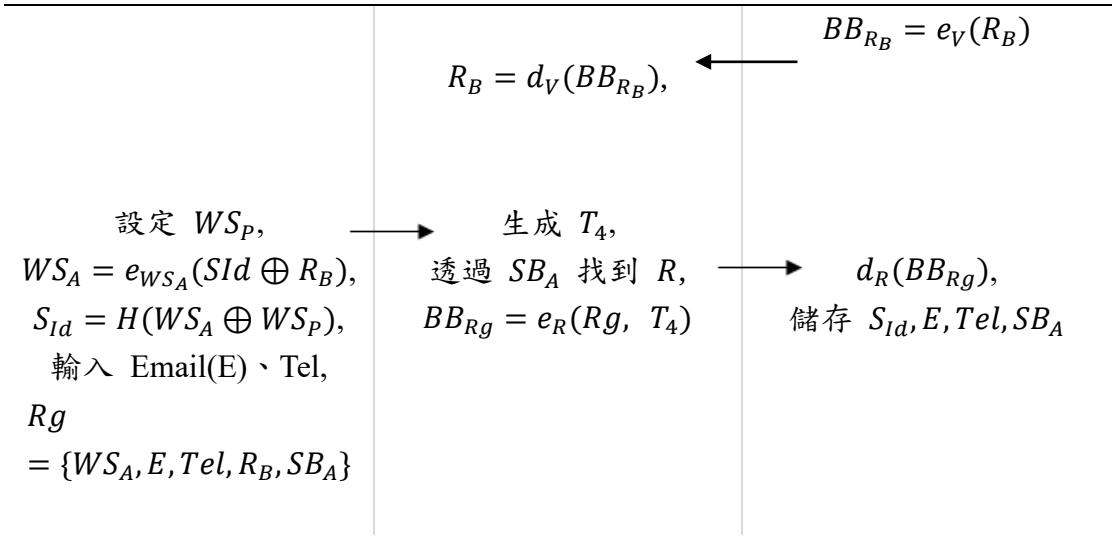
代號	說明
S	School, 此指補習班
U	User, 此指向補習班付費的家長
SId	School Identification, 補習班立案案號
SB_N	School Bank Account Name, 補習班銀行戶名
SB_A	School Bank Account, 補習班銀行帳戶
$T_1, T_2, T_3, T_4,$	Timestamp, 時間戳記
V	Value, 服務網層與銀行區塊鏈間傳遞的值
$e()$	Encryption function, 加密函數
$d()$	Decryption function, 解密函數
R	Random Number, 由銀行區塊鏈生成的隨機碼
SB_P	School Bank Password, 補習班銀行帳戶密碼
$H()$	Hash function, 單向雜湊加密函數
R_B	Bank Random Number, 由銀行於註冊成功時生成的註冊碼
WS_P	School E-Wallet Password, 補習班的電子錢包密碼
WS_A	School E-Wallet Account, 補習班的電子錢包帳號
UB_N	User Bank Account Name, 家長銀行戶名
UB_A	User Bank Account, 家長銀行帳戶
UId	User Identification, 家長身份證字號
UB_P	User Bank Password, 家長銀行帳戶密碼
WU_P	User E-Wallet Password, 家長電子錢包密碼
WU_A	User E-Wallet Account, 家長的電子錢包帳號
Tr_P	Transaction Price, 交易金額
Tr_t	Transaction Time, 款項撥付日

TrM	Transaction Message, 包含交易雙方、金額及付款時間的交易資訊
Tr_U	交易的對象 - 家長
Tr_S	交易的對象 – 補習班
k	User / School 和銀行之間溝通的密鑰
$pool$	交易池
BB	Bank Blockchain, 銀行聯盟鏈
gk	節點間共享的 group key

3.3 補習班註冊錢包流程

補習班需要在銀行開戶，並註冊電子錢包，用以接收銀行撥付學費的目的地。家長繳費後代管在銀行的學費，銀行於補習班完成授課後分段撥付款項至補習班電子錢包的入帳地址，流程如圖七所示。





圖七：補習班註冊錢包流程圖

步驟一、補習班輸入立案證號 SId、銀行戶名 SB_N、銀行帳號 SB_A 並提交。

步驟二、網路銀行透過與補習班管理系統 Api 對接以即時確認 SId 為立案狀態，則可繼續進行註冊流程。

步驟三、網路銀行生成時間戳記 T_1、透過 SB_N 找到網銀與銀行層共享的專屬該補習班帳戶的 secret value V，運算並加密 $e(SB_A, T_1)$ 為 BB_V 後傳送到銀行層。

步驟四、接收到由網銀傳送的要求後，銀行層生成時間戳記 T_2 ，將 BB_V 解密後，產生隨機碼 R，運算並加密 $e_V(R)$ 為 BB_R 後傳送到網銀。

步驟五、補習班接著輸入銀行密碼 SB_P，運算 $H(SB_A \oplus SB_P \oplus SId \oplus R)$ 為 SB_{Id} 傳送。

步驟六、網銀生成時間戳記 T_3，運算並加密 $e_V(SB_{Id},\ T_3)$ 為 $BB_{SB_{Id}}$ 傳送到銀行。

步驟七、在接收到資料後，銀行透過帳號 SB_A 找到密碼 SB_P 並確認時間戳記有效後解碼 $BB_{SB_{Id}}$，接著運算 $H(SB_A \oplus SB_P \oplus SId \oplus R)$ 為 SB'_{Id}，並確認 $SB_{Id} = SB'_{Id}$。

步驟八、驗證正確後生成 R_B，運算並加密 $e_V(R_B)$ 為 BB_{R_B} 傳送到網銀解碼後，透過網銀傳送給補習班註冊成功通知。

步驟九、補習班設定電子錢包的密碼 WS_P，運算並加密 $e_{WS_A}(SId \oplus R_B)$ 為 WS_A；接著運算電子錢包帳戶及密碼 $H(WS_A \oplus WS_P)$ 為 S_{Id}。

步驟十、補習班繼續輸入電子信箱 E 和電話 Tel，將包含 WS_A、E、Tel、R_B、SB_A 的 Rg 傳送到網銀。

步驟十一、網銀生成時間戳記 T_4，透過銀行帳號 SB_A 找到對應隨機碼 R，運算並加密 $e_R(Rg,\ T_4)$ 為 BB_{Rg} 傳送到銀行。

步驟十二、銀行解碼 BB_{Rg} 後儲存 S_{Id}、E、Tel、SB_A。

3.4 家長註冊補習班流程

以文理補習班為例，十二年國教期間的學生皆未成年，因此課程合約簽訂及付款皆應為法定監護人，本研究統稱為家長。在學生選定欲報名的課程時，補習班會向學生及家長留下資料，並進行課程簽約及約定付款。流程如下：

步驟一、選擇欲報名的課程，並談妥課程費用。

步驟二、補習班參照行政院之〈短期補習班短期課程服務契約書〉內容，登錄報名的課程名稱、課程期間、費用等資訊，交由家長簽名完成合約簽署。

步驟三、補習班將學生與家長資訊關聯，該學生的課程費用都將向關聯的家長收取。補習班請家長準備好指定銀行帳戶，並於網銀申請電子錢包。

步驟四、家長於補習班要求的期限內完成電子錢包註冊後，往後該學生報名的課程費用，都將由補習班傳送包含家長姓名(銀行帳戶名稱與姓名同)、家長身份證字號與課程完成日及費用至銀行要求授權扣款。

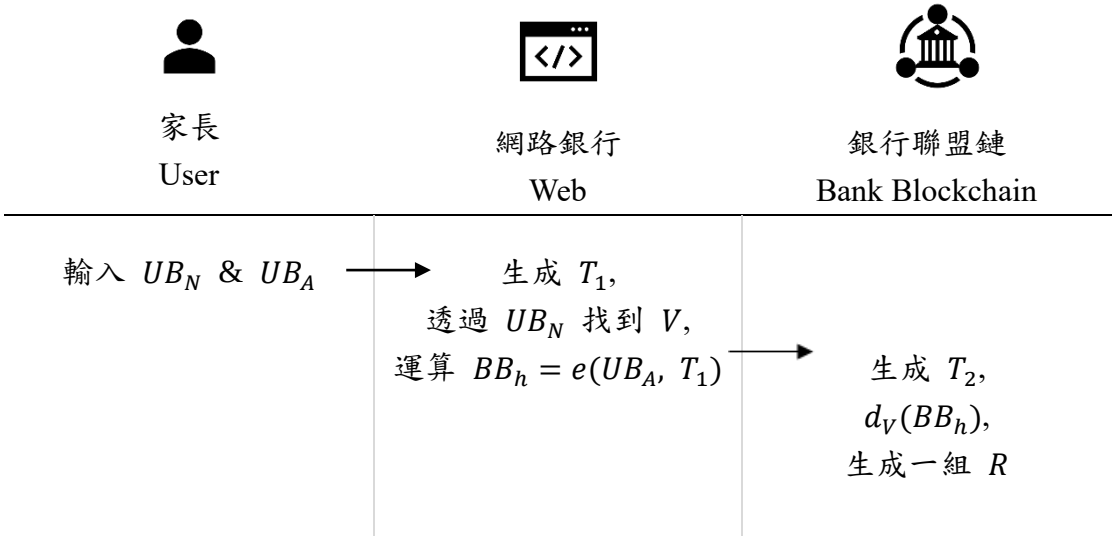
步驟五、銀行通過家長的姓名及身分證字號可找到家長註冊的帳戶，並通知扣款要求，在合約兩造雙方皆同意交易內容後，系統即將該筆交易上鏈，家長的帳戶同時被扣款暫存至銀行。

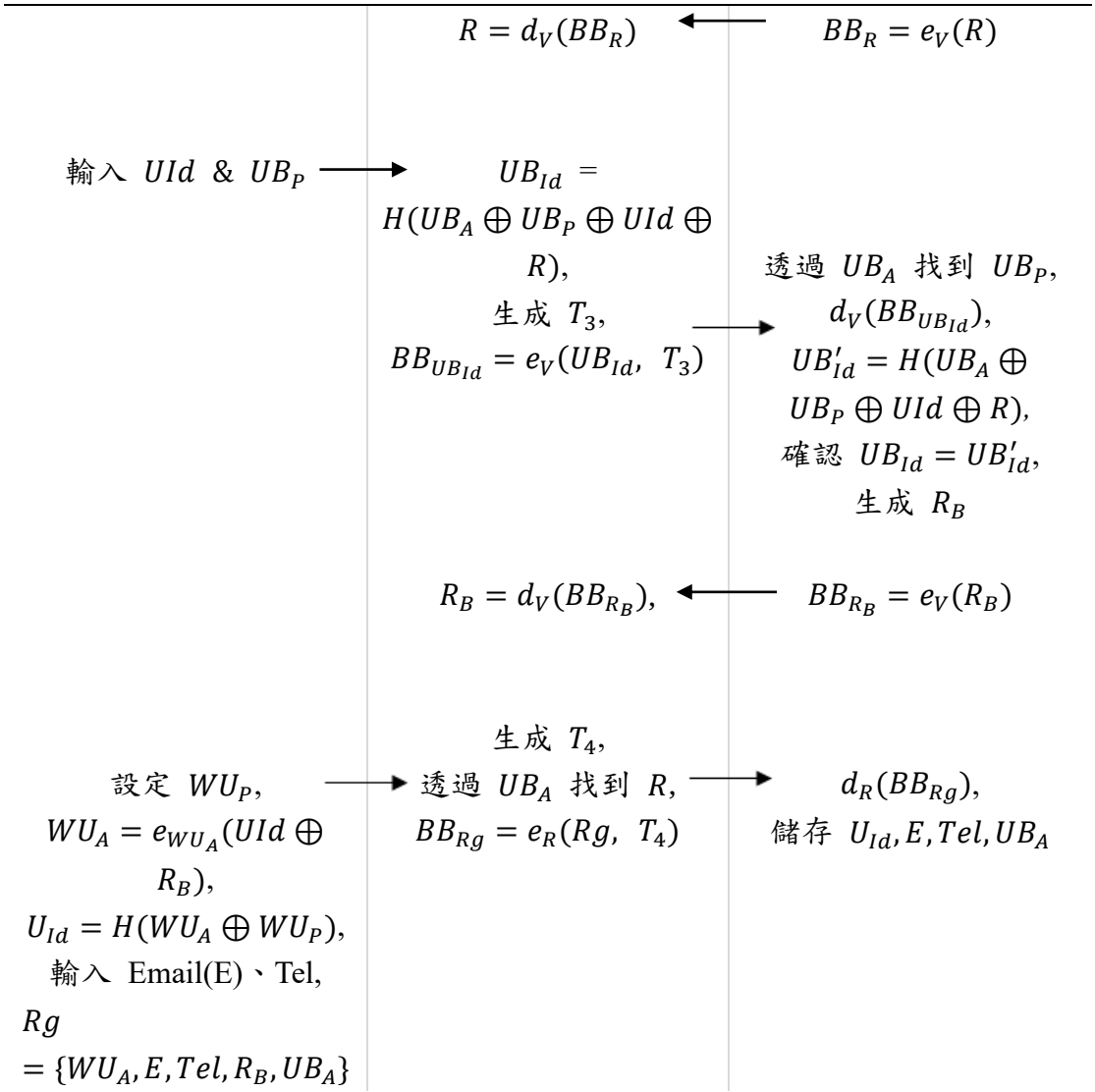
步驟六、待課程陸續完成時，於約定的時間將款項撥付至補習班的電子錢包。

每次到了課程完成日，也就是約定付款日時，系統皆會檢核一次補習班的立案案號是否為有效，有效則進行款項撥付。當系統偵測立案案號為無效，表示補習班停業或倒閉，則已暫存在銀行的學費，將排程返還至家長電子錢包中。

3.5 家長註冊錢包流程

家長與補習班完成課程合約簽訂後，透過補習班告知至指定銀行申請電子錢包，註冊流程如圖八所示。





圖八：家長註冊錢包流程圖

步驟一、家長輸入身份證字號 UId、銀行戶名 UB_N、銀行帳號 UB_A 並提交。

步驟二、網路銀行生成時間戳記 T_1、透過 UB_N 找到網銀與銀行層共享的專屬家長的 secret value V，運算並加密 $e(UB_A, T_1)$ 為 BB_V 後傳送到銀行層。

步驟三、接收到由網銀傳送的要求後，銀行層生成時間戳記 T_2 ，將 BB_V 解密後，產生隨機碼 R，運算並加密 $e_V(R)$ 為 BB_R 後傳送到網銀。

步驟四、家長接著輸入銀行密碼 UB_P，運算 $H(UB_A \oplus UB_P \oplus UId \oplus R)$ 為 UB_{Id} 傳送。

步驟五、網銀生成時間戳記 T_3，運算並加密 $e_V(UB_{Id}, T_3)$ 為 $BB_{UB_{Id}}$ 傳送到銀行。

步驟六、在接收到資料後，銀行透過帳號 UB_A 找到密碼 UB_P 並確認時間戳記有效後解碼 $BB_{UB_{Id}}$，接著運算 $H(UB_A \oplus UB_P \oplus UId \oplus R)$ 為 UB'_{Id}，並確認 $UB_{Id} = UB'_{Id}$。

步驟七、驗證正確後生成 R_B，運算並加密 $e_V(R_B)$ 為 BB_{R_B} 傳送到網銀解碼後，透過網銀傳送給家長註冊成功通知。

步驟八、補習班設定電子錢包的密碼 WU_P，運算並加密 $e_{WU_A}(UId \oplus R_B)$ 為 WU_A；接著運算電子錢包帳戶及密碼 $H(WU_A \oplus WU_P)$ 為 U_{Id}。

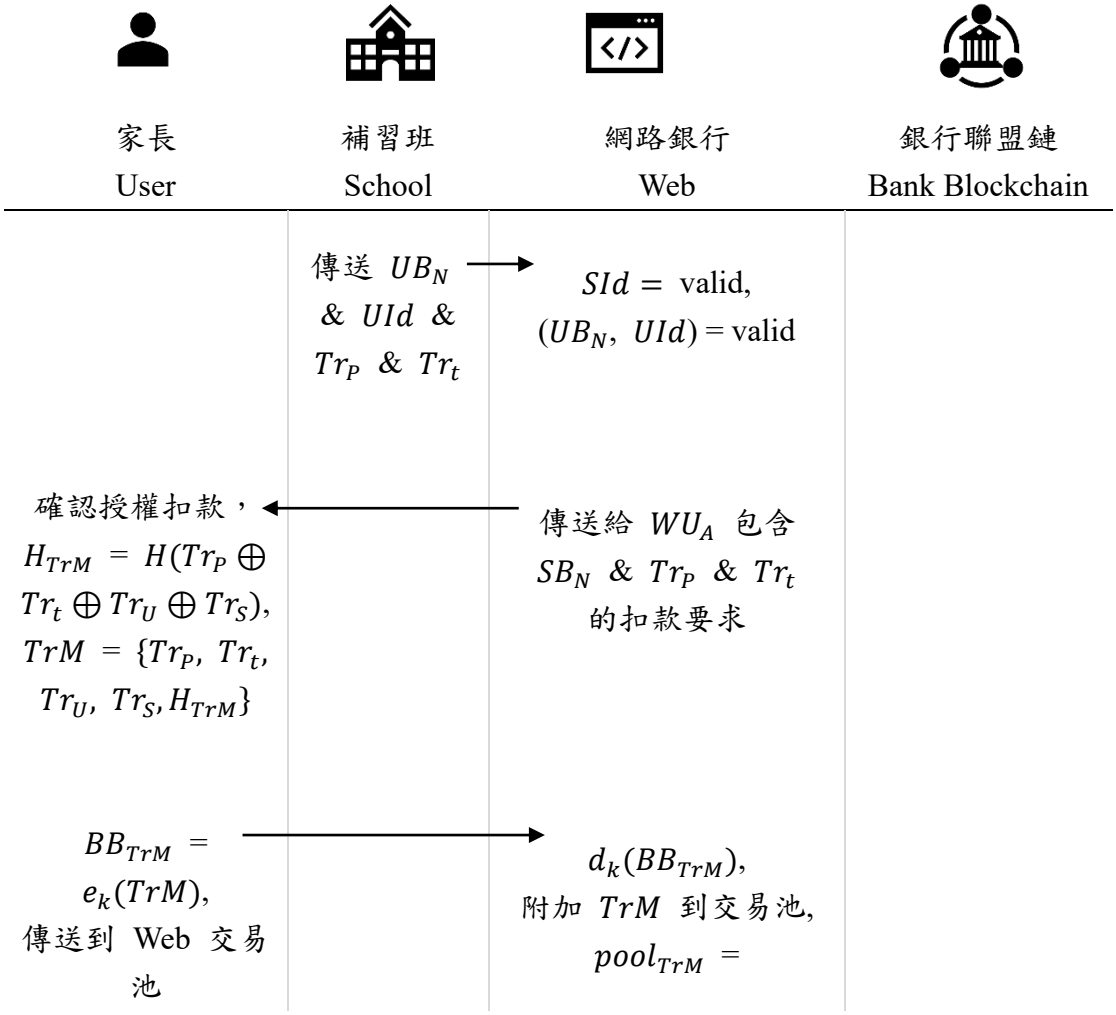
步驟九、家長繼續輸入電子信箱 E 和電話 Tel，將包含 WU_A、E、Tel、R_B、UB_A 的 Rg 傳送到網銀。

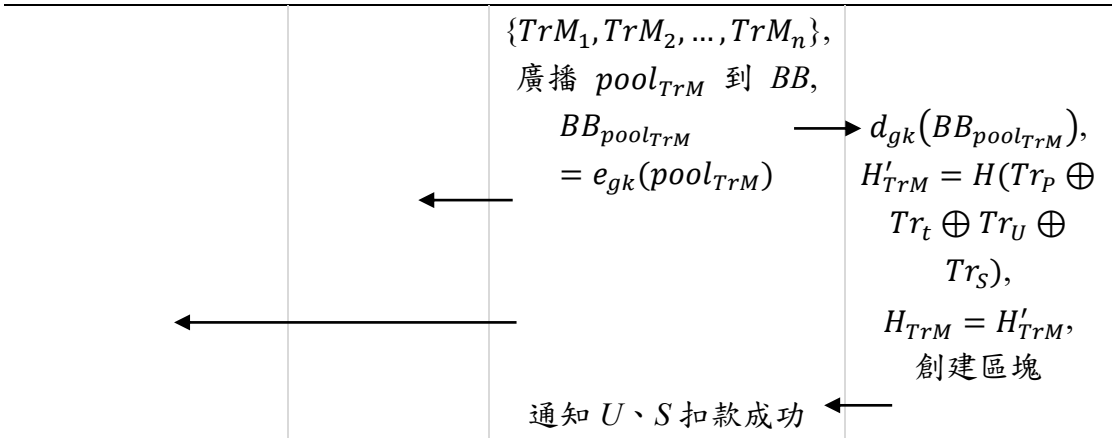
步驟十、網銀生成時間戳記 T_4，透過銀行帳號 UB_A 找到對應隨機碼 R，運算並加密 $e_R(Rg,\ T_4)$ 為 BB_{Rg} 傳送到銀行。

步驟十一、銀行解碼 BB_{Rg} 後儲存 U_{Id}、E、Tel、UB_A。

3.6 扣款流程

補習班作為銀行認證的合作方，可以平台串接方式或定期向銀行發送扣款申請，補習班欲扣款對象(在此指家長)在扣款期效內於銀行開戶並註冊電子錢包後，銀行得以在驗證補習班傳送的扣款需求時，對應到家長的帳戶，即可傳送扣款要求給家長，並在向家長取得授扣同意後，該筆交易即傳送至區塊鏈上鏈，並會按照補習班傳送的課程完成日及金額來發動款項撥付的動作，如圖九。





圖九：扣款流程圖

步驟一、補習班向網銀傳送待授權扣款需求，傳送的項目包含家長的銀行戶名 UB_N、身份證字號 UId、課程完成日期 Tr_t、課程收費 Tr_P。

步驟二、網銀在接收到補習班扣款需求時，會先驗證補習班的立案證號 SId 是否為有效，如為無效，表示停業或倒閉，則不發動授權、扣款和撥款。

步驟三、網銀在家長也完成電子錢包註冊後，透過補習班發送的 UB_N 及 UId 找到對應家長的帳戶，並傳送授權扣款的內容，包括要求授扣的補習班名稱 SB_N、課程完成日期 Tr_t 與課程費用 Tr_P，家長核對內容與補習班簽約的合約內容正確後發送確認授扣。

步驟四、確認授扣時，系統運算 $H(Tr_P \oplus Tr_t \oplus Tr_U \oplus Tr_S)$ 為 H_{TrM} 來產生雜湊函數，再運算及加密 $e_k(TrM)$ 為 BB_{TrM}，傳送到交易池。

步驟五、網銀運算並加密 $e_{gk}(pool_{TrM})$ 為 $BB_{pool_{TrM}}$ 並廣播到區塊鏈層的所有銀行。

步驟六、銀行接到交易數據後，運算 $H(Tr_P \oplus Tr_t \oplus Tr_U \oplus Tr_S)$ 為 H'_{TrM} 並與 H_{TrM} 比較確認有效後合成交易並建立交易 merkle tree。

肆、分析

本研究以補習班販售遞延性商品 (服務) 為研究案例，以區塊鏈技術優化現行履約保證機制，透過建構銀行聯盟區塊鏈，每個銀行都是超級節點，補習班的學費經由家長及補習班皆註冊該區塊鏈的電子錢包，並先將家長支付的學費扣款後暫存於銀行，補習班依完成授課比例來按比例撥款回補習班的電子錢包中。本研究的付款機制相較現今的履約保證機制之可行性與優缺點於本章進行分析比較。

4.1 目前補習班的履約保證機制

1. 透過銀行或信託中心：如圖十將每季或每學期收取學費中的 30% 提撥至金融機構或信託中心，於完成授課時按比例申請提款。補習班總是會有 30% 的收入被凍結，服務完成後又須提交申請才能提款，過程耗費人力及時間。如遇補習班惡性倒閉，因補習班為完成服務後才提領該比例學費，因此消費者可以轉而向金融機構或信託中心要求未授課費用的賠償。

圖十：透過銀行或信託中心履約保證流程

2. 加入補教業品保協會：如圖十一支付入會費及年費成為補教協會會員，並依補習班場域每平方公尺為單位計價永久基金及聯合基金繳交給補教業品保協會，以獲得履約保證書。如遇補習班惡性倒閉，補教協會將協助安置學生至鄰近補習班上課。

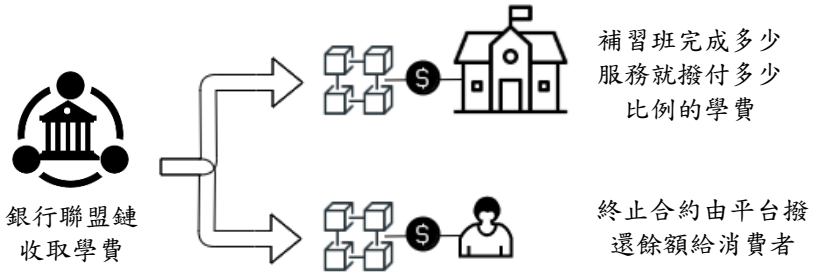
圖十一：品保協會履約保證流程

3. 保險公司投保：於保險公司投保不得低於二百萬的保險。如遇補習班惡性倒閉，則由保險公司拿出投保額度賠償消費者，如圖十二。

圖十二：保險公司履約保證流程

4.2 本研究的區塊鏈履約保證機制

補習班在本研究平台上創建課程產品，消費者購買課程並將費用透過電子錢包支付至銀行託管，補習班完成特定比例服務及撥款該比例額度學費給補習班。遇補習班惡性倒閉，平台將學費餘額歸還消費者，如圖十三。



圖十三：本研究履約保證機制流程圖

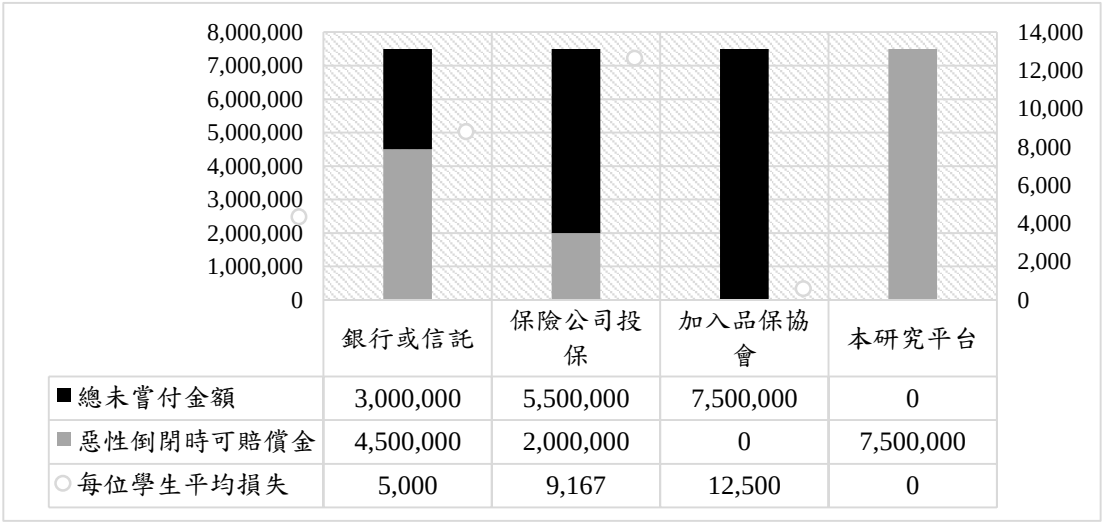
4.3 以中型補習班為案例探討風險評估

以高中中型文理補習班為例，該規模的補習班高一、高二、高三學生數以 600 人計，每位學生約補習 2.5 科次，高中補習一科學費約新臺幣 8,000～12,000 元，以新臺幣 10,000 元計，該補習班一學期的學費收入為新臺幣 15,000,000 元。

1. 消費者端：假設該補習班於學期中間，也就是在履行了 50% 的課程服務後倒閉不再提供服務，總須退還給該 600 位學生學費為新臺幣 7,500,000 元；以目前現行的履約保證機制及本研究機制下，消費者承擔的風險評估如下表二：

表二：各履約保證機制風險評估

單位：新臺幣元



	銀行或信託	保險公司投保	加入品保協會	本研究平台
■總未嘗付金額	3,000,000	5,500,000	7,500,000	0
■惡性倒閉時可賠償金	4,500,000	2,000,000	0	7,500,000
○每位學生平均損失	5,000	9,167	12,500	0

由上表可知現行履約保證機制並無法在補習班惡性倒閉時 100% 返還消費者已繳清的費用。品保協會的履約保證機制是協助轉介學生至鄰近的補習班上課，學生如因師資或環境等因素不接受轉介至新補習班，就得全數認賠。而本研究的費用託管機制，將可全數返還補習班未實現的服務比例費用。

2. 業者端：現行的履約保證機制能夠降低消費者風險的程度從上述已顯見其不足。而在業者端，由下表三呈現業者支出現行履約保證的成本跟惡性倒閉後持有的不當利益金額呈現懸殊的比例：

表三：現行履約保證機制的業者不當獲利金額

履約方案	銀行或信託	保險公司投保	加入品保協會
履約保證成本	新臺幣 45,000 元	新臺幣 4,000 元	新臺幣 32,000 元
惡性倒閉捲款金額	新臺幣 5,250,000 元	新臺幣 7,500,000 元	新臺幣 7,500,000 元

現行履約保證機制能做到的是降低消費者少部分的風險，對於遏阻業者惡性倒閉則無效果。本研究平台的履約保證機制，在成本方面，每筆交易以賣方手續費為交易金額 0.1% 計算，總花費為新臺幣 15,000 元，與現行機制支出成本相比有競爭優勢，這將有助於未來補習班更有意願參與本研究平台的履約保證機制。再者，透過本平台履約保證機制，業者惡性倒閉將無利可圖，可完全遏止該等事件發生，因此這應是政府、業者、消費者三方共好的解決方案。

伍、結論

本研究展示了對補教產業破壞性的區塊鏈技術應用。補習班被要求的「合規、合法、合稅」在本平台獲得了一站式的解決方案：

1. **合規：**取代現行須質押、或繳保費、或繳會費的履約保證機制。本平台應用區塊鏈技術特性取代受信的第三方來代管學費，業者完成服務後才提領費用，可分段提領。這將能在業者惡性倒閉時，未提供服務的費用，本平台可以退還給消費者。
2. **合法：**參與本平台的補習班，需先申請成為合法立案補習班，因此報名未合法立案補習班課程的家長，將面臨業者倒閉無處求償的風險，當此遞延性商品 (服務) 交易方式被廣泛使用，將造成無法提供此等交易方式的補習班受到排擠而難以經營。另外，因本研究的交易模式需要確認課程交易的金額及付款細節，

因此能夠間接呼籲補習班同時落實與家長簽訂課程契約手續。

3. **合稅：**當政府及補教協會認可本研究平台的交易機制，規範補習班必須在本平台做售課，將可達到學費收入完整記錄於本平台，後續更可以做為補習班報稅依據。

對於消費者而言，本平台能夠依照買賣雙方約定的付款期程來制定交易，因此得以提供無後顧之憂、無負擔的消費體驗：

1. **無後顧之憂：**利用本平台交易遞延性商品 (服務) ，最擔心的是消費者害怕業者無預警停業，即使訴訟可能可以爭取到退款，但過程需耗費心力時間。本平台的學費代管機制，保護了業者尚未履行服務的費用，"惡性"倒閉將不復存在，一旦無預警停業，平台會在確認後清算餘款給消費者。
2. **無負擔：**運用平台機制的開發彈性優勢，需要分期繳費的消費者，平台將學費拆分為若干期數，課程堂數比照比例拆分，消費者只要在一期課程開始上課前繳交該期學費即可。這將取代業者與消費者必須依賴銀行的信用審核來爭取刷卡服務，緩解業者須質押的壓力以及維護弱勢家庭的受教機會。

本研究擘劃了補教產業的新經濟藍圖，對於各產業遞延性商品 (服務) 交易也具有催化作用。企盼透過區塊鏈技術的應用，為我們身處的沃土發展智慧城市盡一份心力。

參考文獻

[1] A. Raza, “Bitcoin Sees New All-Time High In Node Numbers,” https://insidebitcoins.com/news/bitcoin-sees-new-all-time-high-in-node-numbers(2021/1/20).

[2] I. Karamitsos, M. Papadaki and N. A. Barghuthi, “Design of the Blockchain smart contract: A use case for real estate,” *Journal of Information Security*, vol. 9, no. 3, pp. 177-190, 2018.

[3] I. Gwyneth, “What Are The Different Types of Blockchain Technology?,” https://101blockchains.com/types-of-blockchain(2021/1/6).

[4] J. Don, M. Alfred and V. Scott, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” *International Journal of Information Security*, vol. 1, pp. 36-63, 2001.

[5] K. Kristián, K. Tomáš, G. Martin, V. Igor, R. Michal and K. Ivan, “On Transition between PoW and PoS,” *International Symposium ELMAR*, 2018/11/15.

[6] K. N. Ambili, M. Sindhu and M. Sethumadhavan, “On Federated and Proof Of Validation Based,” *IOP Conf. Series: Materials Science and Engineering*, 2021/10/14.

[7] L. Roy, L. David and C. Kuo, “Blockchain – From Public to Private,” *Handbook of Blockchain, Digital Finance, and Inclusion*, pp. 145-177, 2018.

[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/en/bitcoin-paper(2008).

[9] T. Philip, G. B. Richard and Y. Danny, "Blockchain Technology in Finance," *IEEE*, vol. 50, pp. 14-17, 2017/9/22.

[10] V. Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum white paper*, 2021/2/9.

[11] W. Lijun, M. Kun, X. Shuo, L. Shuqin, D. Meng and S. Yanfeng, "Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet," *2017 IEEE International Conference on Energy Internet (ICEI)*, 2017/5/15.

[12] Z. Jingyu, Z. Siqi, W. Tian, C. Han-Chieh and W. Jin, "Blockchain-based Systems and Applications: A Survey," *Journal of Internet Technology*, vol. 21, no. 1, Jan. 2020.

[13] 中華民國補教業品保協會, https://www.eqaa.org.tw, 2020.

[14] 行政院, "短期補習班補習服務契約書範本," *臺教社(一)字第1090044569A號函公告修正*, 2010/4/1.

[15] 吳崢詒, "教育愈改愈大洞 補習班 20 年成長 8.8 倍," *天下雜誌*, 第五九九期, pp. 22-23, 2016.

[16] 陳信佑, "教改推動 20 年，補習班反而增加三倍？," *遠見雜誌*, 2017/1/16.

[17] 最高法院, "台上字第 1619 號民事判決," *司法院公報*, 第五十四卷, 第六期, pp. 178-180.

[18] 辜騰玉, "區塊鏈運作原理大剖析：5 大關鍵技術," *iThome*, 2016/4/23.

[19] 楊凱婷, "論遞延性商品 (服務) 契約之相關法律問題," 新北市: 國立政治大學法律學系, 2017.

[20] 劉正, "補習班在臺灣的變遷、效能與階層化," *教育研究集刊*, 第五十二卷, 第四期, pp. 1-33, 2006.