InfiniteChain無窮鏈
技術白皮書 2018/03/27 Version 3.0

高速頻寬、多量礦工、無窮潛力的區塊鏈可行方案

泰德陽光集團
TIDEiSUN

目 錄

InfiniteChain無窮鏈

技術白皮書 2018/03/27 Version 3.0

InfiniteChain 無窮鏈

打破區塊鏈運算的限制，真正實現去中心化交易的多元化行業應用

自比特幣於 2009 年以去中心化概念建立共識加密貨幣後，人們期待去中心化帶來的社會價值改造，業界也急欲探索如何運用其底層的區塊鏈技術，實現更大商業效益，然而現行的公有鏈存在一些限制，包含速度、交易成本等等的挑戰，使得很多應用皆難以落地發展。

InfiniteChain無窮鏈針對區塊鏈技術發展至今遇到的瓶頸，和區塊鏈在商業應用實作的限制，進而在技術應用上、共識機制上以及經濟模型上都提出了創新的方式來處理這些問題。

- 快速交易：主鏈和側鏈的聯合運作模式，可實現超過一千萬級 TPS（Transaction Per Second, 每秒交易量）
- 公平出塊：利用新的共識協定(輕量級挖礦)，落實真正的去中心化公平
- 鏈上自治：鏈上信用點數的機制促使區塊鏈自治，打造新社會

InfiniteChain無窮鏈打破了交易處理速度和交易數量的限制，以主鏈和多側鏈並行的混合鏈模式，運用新式的分散式稽核技術，建立了一個支援無速度限制、更受信任的去中心化架構。

InfiniteChain無窮鏈解決了傳統區塊鏈面臨的問題：

- 區塊鏈頻寬不足
- 區塊鏈承載空間不足
- 交易成本過高且不即時
- 無法和現有中心化應用融合，行業應用場景受限
- 算力集中，礦池壟斷
- 礦工成本高，門檻高
- 治理受到壟斷
- ICO詐騙頻繁

最後，針對區塊鏈在各行業潛在的應用價值和商業機會，白皮書中列舉了部分領域的應用場景，例如股票股權交易、資產交易、InfiniteChain無窮鏈的混合鏈架構不但實現更快速的交易，對於隱私保障更加優越，真正打造彼此信任的交易生態系。

1. 簡介

本白皮書先介紹當今區塊鏈的問題、瓶頸，再導出InfiniteChain無窮鏈新一代區塊鏈架構的源由、規劃、架構、及生態。InfiniteChain無窮鏈，顧名思義為一支援無速度、無數量限制的去中心化系統架構：以主鏈和側鏈並行的混合鏈模式，運用新式的分散式稽核技術，以解決傳統區塊鏈交易頻寬不足、資料量過大、及隱私不受保護的問題，並輔以輕量挖礦及鏈上信用制度建立一個可以受信任且功能齊全的全新區塊鏈運作架構。

1.1. 背景

比特幣於2009年以去中心化概念建立共識加密貨幣，其底層技術區塊鏈，得到各行各業廣泛地認可和使用的體現。除了成為一個國際認可的貨幣外，目前人們正在期待利用這一共享價值體系，以區塊鏈技術在各行各業開發去中心化電腦程式（Decentralized applications, Dapp ）。

除了加密貨幣交易外，去中心化的訊息對等且資料無法被竄改的優點在不同領域被提出，主要運用型態有：有價資產登錄[1]（Value registry）、價值型聯網[2]（Value web）、價值生態系[3]（Value ecosystem）等。相關運用行業舉例有：物流業、金融系統、醫療記錄、物聯網的資料收集及認證、供應鏈管理、股票或股權交易、社群軟體、電子病歷、小額支付/行動支付系統、資產交易、數位產品代理銷售等。人們期待的是這些系統運作時，區塊鏈能扮演信任機器的角色， 將相關資料詳實記錄下來，解決資訊不對等的問題，以建立可信任的資料訊息。縱看以上提出的運用場景，將有大量資料期待記錄於區塊鏈上。

然而目前區塊鏈技術的發展遇到瓶頸，若無法解決，以上所提的各式運用場景要全盤在區塊鏈上發展是難以實現的。這些問題大致可以分為技術應用、共識機制以及經濟模型上的挑戰，以下一一說明相關的問題。

1.2. 當前問題一：區塊鏈頻寬不足

區塊鏈的去中心化運作模式，仰賴全世界的網民共同維護，再進一步被使用，所以任意使用者都可以藉由區塊中的交易（Transaction）來交換加密貨幣、撰寫智能合約、或是記錄資訊。但是比

---

[1] 將分散式帳本應用在所有權與存在證明（Proof of Existence and Possession，PoEaP）。

[2] 有價資產登錄（Value registry）、智慧型合約（Smart contract）、國內支付（Domestic payment）、國際支付（International payment）、貿易金融（Trade finance）、資本市場（Capital market）。

[3] 應用在非金融服務，將其應用在公開帳本（Public ledger） 提供各種商業應用。

特幣及以太坊每秒鐘可達成的交易數分別不超過7及25個[4]。面對大量交易要放到區塊鏈的需求，若是沒有技術可以解決此問題，希望藉由交易置入區塊鏈來解決訊息不對等的問題，將只是空想。

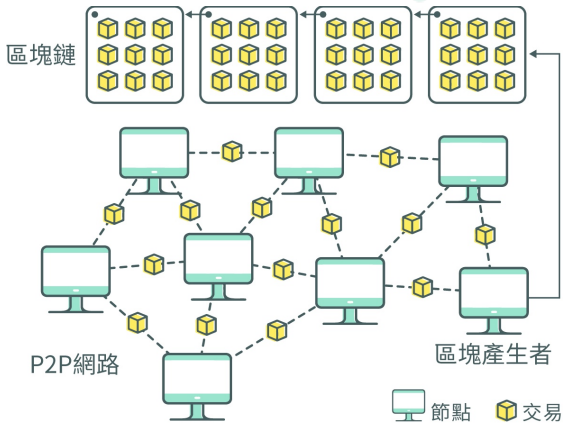


圖1 傳統共識決區塊鏈運作圖

見圖1，區塊鏈的去中心化運作，基本上使用PoW（Proof of Work）或PoS（Proof of Stake）的共識協定（Consensus protocol），由參與節點中，得出或選出一個區塊產生者（Block Producer[5]），然後區塊產生者將經由P2P（Peer-to-Peer[6]）網路運作模式收集到的一些交易，使用電子簽章及雜湊函數[7]將這些交易記錄於區塊鏈某區塊中。公有區塊鏈參與共識協定的節點必須將所有區塊鏈中的資料更動隨時更新並取得一般使用者欲放入區塊鏈中的交易，因此必須經過P2P網路交換[8]大量的資料，其交易頻寬因此無法提升。一般稱公有區塊鏈可以達成全球共識（Global consensus）[9]。詳細論述請參見附錄A。

另外『私有鏈[10]』或『聯盟鏈（Consortium blockchain）』是嘗試解決區塊鏈頻寬不足的方法之一，就是限定可以參加成為區塊鏈節點的數目，因此可以快速的擴散交易及使用特殊的共識法（如各式PoS、BFT、PoA等[11]）以迅速的選出區塊產生者。但是私有鏈的公信度很明顯的和公有鏈有很

---

[4] Yo Banjo, "Ethereum won't scale like you've been told," https://medium.com/@yobanjo/ethereum-wont-scale-like-you-ve-been-told-cae445bef539.

[5] 也稱為「礦工」。

[6] 對等式網路（peer-to-peer， 簡稱P2P），是無中心伺服器、依靠用戶群（peers）交換資訊的網際網路體系，它的作用在於，減低以往網路傳輸中的節點，以降低資料遺失的風險。與有中心伺服器的中央網路系統不同，對等網路的每個用戶端既是一個節點，也有伺服器的功能，任何一個節點無法直接找到其他節點，必須依靠其戶群進行資訊交流。

[7] 對雜湊函式（Hash Function）是一種從任何一種資料中建立小的數字「指紋」的方法。雜湊函式把訊息或資料壓縮成摘要，使得資料量變小，將資料的格式固定下來。該函式將資料打亂混合，重新建立一個叫做雜湊值（Hash values）的指紋。雜湊值也被稱為哈希值。

[8] 「溢散傳遞」（Propagating）。

[9] 比特幣及以太坊的參與節點隨時均有8,000~10,000個，且其中有很多具超高算力的礦池節點。

[10] 如微軟和 Intel 推出的 Coco 架構。

[11] PoS一般需要選出代表來競爭成為區塊產生者；各式BFT因為要進行所有節點間的點對點通訊，節點只能有20~30個；PoA（Proof of Authority）依靠預設好的Authority節點，負責產生區塊。

大差距，因為去中心化系統的核心思想就是讓訪問門檻降低使得能參加的節點沒有限制，以達成無法寡佔的信任機器。私有鏈因為節點數目少，很容易受到51%攻擊[12]，無法達成全球共識。

一些公有鏈的發展欲提升速度也採用節點數目較少的架構，除了上述的51%攻擊外，還可能遭受分散式阻斷服務攻擊（Distributed Denial-of-Service Attack, DDoS），造成全網區塊鏈癱瘓無法運作。

1.3. 當前問題二：區塊鏈承載空間不足

如前一子節所述，各式系統運作為借助公有區塊鏈扮演信任機器的能力，大量的交易紀錄將被推上區塊鏈內，短時間內區塊鏈的資料將迅速增加。根據共識模式，參與區塊鏈的完整節點，必須儲存所有區塊鏈中的區塊及其內的交易。以比特幣而言，其協定運作，限定一年內區塊鏈的容量增長約為70GB[13]，如果不做此限定，區塊的傳播及儲存是一大問題，這也被稱為『區塊鏈膨脹（Blockchain bloat）[14]』。根據VISA在2015年的記錄，全年共產生92,064百萬筆支付交易，折合比特幣交易的資料結構量，需要每秒約2900個交易、47TB的儲存空間。這已超過一般電腦的硬碟空間[15]。

1.4. 當前問題三：交易成本高且不即時

在區塊鏈中，每一筆交易上鏈需讓礦工幫忙打包進新的區塊，所以手續費成本造成許多微支付（像是買飲料或是搭公車等）難以使用，同時也讓支付難以普及；同時，因為礦工打包區塊需要一段時間的確認來避免分叉的可能，這些成本都使得利用加密貨幣支付受到極大的挑戰。

目前許多公司都積極發展加密貨幣的支付系統[16,17,18,19]，以加密貨幣或代幣來進行支付將成為成為重要的加密貨幣金融操作模式。現有的支付系統及交易模式有以下的問題：

---

[12] 51%攻擊（51% attack），就是掌控超過51%的節點就可以修改或控制區塊的產生。

[13] 一天有約30萬個交易，每個交易約占700 Bytes。一年增加的記憶量約為 300,000*365*700 Bytes ≒ 70GB。

[14] 已經有專家警告以太坊將發生此問題（https://read01.com/zh-tw/aKE6A7.html#.WcBzldv3U0o）。

[15] https://www.zhihu.com/question/39067000.

[16] PayPal：目前披露的這系統和方法會向收款人發送包含在虛擬貨幣錢包中的私鑰，錢包裡是事先確定好的需要支付的虛擬貨幣，這樣實際上就消除了收款人等待虛擬貨幣到賬的時間，https://cryptonews.com.hk/2018/03/06/paypal尋求更快的加密貨幣支付技術/。

[17] 日本規模最大的連鎖家電零售商「山田電機」(Yamada Denki) 與加密貨幣交易所 bitFlyer 合作，在東京的兩間店面推出比特幣支付服務。http://blockcast.it/2018/01/30/japanese-electronics-retail-giant-and-koreas-e-commerce-operator-launche-bitcoin-payments/。

[18] Coinbase：http://blockcast.it/2018/02/11/coinbase-launches-paypal-like-plugging/。

[19] Line：https://www.pixpo.net/fiance/0lHONwv7.html。

中央代管支付系統：將加密貨幣或代幣先交由支付系統保管，一段時間結算後由支付系統統一清算將加密貨幣或代幣傳送給受付方的區塊鏈位址，因為中央系統內的金流交易不上區塊鏈記錄，所以速度較快。但是加密貨幣或代幣由支付系統代管，有『安全』及『隱私』的疑慮，顧客也常常詢問此問題。

區塊鏈支付系統：因為加密貨幣或代幣由參與者自管，比較沒有安全上的疑慮。但是所有的交易或支付都要經由區塊鏈記錄，運作『速度』受限於區塊鏈主鏈，同時『交易成本』高。此方法適用於大額少量的支付，如房租、貸款等。對於有微支付需求的場景無法使用。

因此新一代的加密貨幣交易或支付平台一定要解決『安全受質疑』、『交易速度過慢』、『交易成本高』的問題。同時解決方案一定要讓加密貨幣或代幣的交易在具有強勢全球共識的區塊鏈上受監管；在這樣的需求下，有許多的專案試著去解決交易成本的問題，最普遍的做法便是使用交易通道，只送交易簽章給收方，這樣的解決方案在一對一的支付像是分期付款是相當方便的；然而在延伸到支付網路、多方交易錯綜復雜的時候就會產生許多的問題，包含中心化Hub的大筆存款需求、網路充斥著開關通道交易以及用戶得一直在線上待命，這些問題都是通道類型方案需要解決的挑戰。

1.5. 當前問題四：應用場景受限

去中心化的理念雖然受到某些群體的接受，譬如加密貨幣的鑄造及交易，已經完全可以使用去中心化的運作模式實現。但是現今人類生活中的經濟活動，受到法律、生活習慣、舊系統運作、人們相處模式的影響，不可能完全拋棄中心化運作。第1.1節中所提出的運用行業，如：物流業、金融系統、醫療記錄、物聯網的資料收集及認證、供應鏈管理、股票或股權交易、社群軟體、電子病歷、小額支付/行動支付系統、資產交易、數位產品代理銷售等，幾乎每一項的運作都很難拋棄中心化的代理人或中間人。如果公有區塊鏈無法和類似的中心化運用行業相融合，將大大限制區塊鏈信任機器的運用。

以下使用數位產品代理銷售為例來說明。數位產品如電子書、音樂、影片租閱、電子票卷因為網路普及和頻寬變大，使用網路平台來銷售成為目前的趨勢。權利人為了擴大銷售通路，多半會委託代理人於代理人之網路平台上進行銷售。代理人負責向使用者收費，並記錄及統計帳本，於固定週期提供一對帳紀錄給權利人，告知其商品之下載紀錄及對應之權利金等。但是帳本是由代理人所記錄及維護，權利人無從稽核其真實性。舉例而言，代理人可能非因故意但是因為系統瑕疵而導致

記錄上有短缺或其他錯誤或是代理人可能出於故意來刻意偽造或變造紀錄以減少應給付權利人之權利金

也就是說，就算使用區塊鏈，即使代理人將相關帳本放入區塊鏈，權利人亦無從稽核其真實性，當今區塊鏈的信任機器的角色在類似場景無法發揮效用。有一說將相關交易全以加密貨幣來運作，惟此方法受限太大：第一、許多相關消費往往都是小額支付，區塊鏈的交易成本過高也無法負擔大量小額支付的交易頻寬；第二、消費者往往習慣以一般貨幣或信用卡支付；第三、一些和貨幣交易無關的紀錄，則完全沒有使用的空間。若有方法可以突破此限制，也能達成去中心化的目標：『訊息對等』，當可大大增加區塊鏈的用途。

1.6. 當前問題五：算力過於集中、浪費電力

現在的礦池過於集中，全球的算力集中在不超過5個礦池[20]，造成出塊權利的壟斷，也同時讓這些礦池在區塊鏈的影響力過大，康乃爾大學的報告指出：挖礦是非常中心化的，比特幣前四大礦商和以太坊前三大礦商都控制超過50%的算力。這些礦場的門檻非常高，一般用戶難以獲得出塊的權利；同時，這些工作量證明的共識方式需要大量競爭算力，造成了許多資源無謂的浪費，包含電力以及建構礦機的成本。

1.7. 當前問題六：區塊鏈自治難以實現

現當前有許多專案都是由開發團隊制定方向，許多的參數都不見得滿足各個用戶所需；同時在ICO（Initial Coin Offering）募資方面都發生了許多的詐騙事件，很多用戶都難以判別這些dapp或是token是否正常營運以及開發。曾經為區塊鏈行業做出重大貢獻的ICO如今已經被濫用，他最大的問題在於，一旦發起募資方拿到資金後，投資者對於項目擁有者沒有約束力；另一方面，ICO也是監管的灰色地帶，這讓ICO詐騙者有恃無恐。

DAICO由以太坊創始人Vitalik於2018年1月提出[21]，希望可以最大限度的降低ICO風險，他設定了投資人可以藉由投票分期撥款給代幣發起方也可以因為不信任來把剩餘的資金退回，是一個非常好的機制，但依然在最初始的時候對於這些ICO發起沒有限制，任何人都可以隨時隨地發起，也就是說並無一個信用機制來讓大家評估風險。

---

[20] 康乃爾大學研究報告：比特幣和以太坊的去中心化名不副實（https://itw01.com/8MC6EGL.html）。

[21] DAICO: Ethereum's Vitalik Buterin's DAO + ICO Token Model?（https://bitcoinexchangeguide.com/daico/）。

1.8. 問題總結

綜合以上現況，可以歸納出需要解決的問題如下：

技術應用上：

區塊鏈交易速度過慢、隱私難以保護、成本高以及資料太多一般用戶難以成為節點。

共識機制上：

算力過於集中，話語權被壟斷，一般用戶難以參與其中。

經濟模型上：

詐騙頻繁，商業應用也沒有方法評估風險。

這些問題在現在的公有區塊鏈中難以被解決，本白皮書提出的混合鏈架構，將徹底解決此問題，請見第2節。

2. InfiniteChain 無窮鏈技術核心

InfiniteChain無窮鏈的設計是為了徹底解決前一節中所提出目前現存公有區塊鏈的問題。其技術核心如圖2，主要是由『混和鏈架構』、『輕量挖礦協定』、及『主鏈信用制度』所構成。

第一，InfiniteChain無窮鏈利用了主側鏈架構搭配的『混和鏈架構』搭配創新的『分散式稽核』來解決技術問題，主鏈是用做信任機器來維持全球共識，而側鏈則是用做商業邏輯的使用，用戶送出的交易不需每筆都記錄在主鏈上，用戶會送一筆交易給一個代理人並授權讓代理人協助他做紀錄上鏈，代理人會將一段固定時間內的所有授權他的交易產生一個索引莫克樹並將其根雜湊值記錄在主鏈上。同時，為了確保主側鏈資料一致，無窮鏈使用了分散式稽核機制，允許每個用戶在結算帳本時稽核自己的交易，達到資訊對等，防止代理人出錯。詳情請見2.1節。

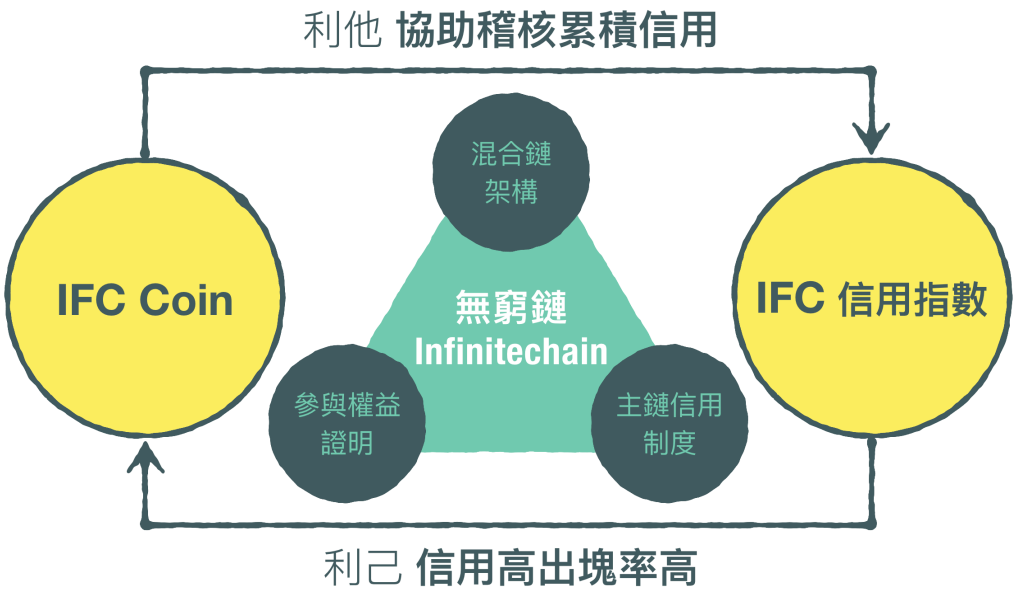


圖2 InfiniteChain無窮鏈系統技術核心

第二，InfiniteChain無窮鏈的目標不只在於效能提升，也是希望可以達到社會公平。在現行的工作量或權益證明中（PoW或各式PoS），出塊權（寫帳權）容易被大型的礦池所壟斷，一般的用戶不容易搶到出塊的權利。輕量級挖礦的機制採用－參與權益證明（Proof of Participation, PoP），每一次的出塊權都是由一個用戶的地址與前一個出塊者的地址所得出的亂數產生；另外，會利用此用戶的信用點數及持有的幣齡做加權計算產生最後的權益，而用戶會委託全節點幫忙出塊，並且共同分享出塊的利潤。在InfiniteChain無窮鏈的出塊協定中，概率函式的設計使得每個人的出塊概率不會相差超過五倍，也不容易讓特定的族群壟斷出塊權。同時因為採用完整節點的偕同制度，使用者可以使用手機來出塊（輕量挖礦協定）。詳情請見2.2節。

最後，InfiniteChain無窮鏈希望建立一個去中心化的信任網路，每個用戶只要良善的送交易，正常的營運側鏈，貢獻每一次的稽核，認真的維護區塊鏈網路的共識，就可以增加自身的信用點數。信用點數不能轉移，隨著時間跟用戶的貢獻持續增加，並且在權益證明上也會參考近期累積的信用點數來做加權，在無窮鏈的生態系中，經濟模型鼓勵用戶參與活動，有錢出錢，有力出力，共同維護鏈上經濟生態。詳情請見2.3節。

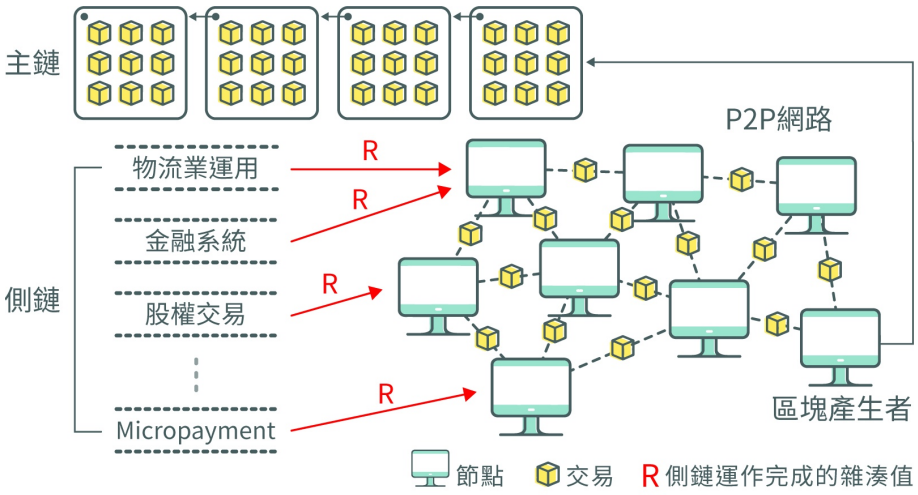


圖3 混合鏈架構運作圖

2.1.混合鏈架構（Hybrid Chain Architecture）

本節中，我們將說明InfiniteChain無窮鏈的混合鏈架構的運作模式，如圖3。所謂混合鏈就是由主鏈及多個側鏈組成的聯合運作模式。一般不需高速運作的交易，如加密貨幣交易或單一合約紀錄，直接送到P2P網路中，最後由成為區塊產生者的節點來固定到主鏈上。但是大量產生或需要中心化撮合的交易則先在側鏈上運作，最後產生交易的雜湊值送給P2P網路中的節點，固定到主鏈。側鏈的運作高速，一段時間後累積大量數目的交易，由負責側鏈運作去中心化運行的稽核節點產生雜湊值及相關識別碼送給節點固定在主鏈。整個InfiniteChain無窮鏈架構有『一般節點』（以下稱為節點）及『稽核節點』來負責主鏈及側鏈的去中心化運作。

將交易先不放上主鏈，在主鏈外運作一陣子然後放上主鏈，有數種技術。以下分別說明，最後我們可以瞭解InfiniteChain無窮鏈的側鏈和其它技術的區別。第一種稱為中繼鏈技術（Relay-Based），在一個主鏈外存在其他區塊鏈[22、23]，主鏈、側鏈間先進行資產轉換後，在側鏈進行交

[22] A SIMPLE EXPLANATION OF BITCOIN “SIDECHAINS” https://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
[23] How Two New Sidechains Proposals Could Change Bitcoin's DNA https://www.coindesk.com/two-new-sidechains-proposals-change-bitcoins-dna/

易，一段時間後再將資產轉換回主鏈，主要的目的是希望達到加密貨幣間（或代幣間）的交換。類似的跨鏈資產轉換系統有BTC-Relay、Rootstock等，其中會遇到的難題便是雙向錨定（2-way peg）的協定，像是比特幣就沒有辦法搭建一個Relayer在本身的區塊鏈之中。

另一種側鏈則是通道類型技術（Channel-Based），一般稱為離鏈（Off-chain），如：Lightning-network， Raiden等，這些皆以鏈下交易來增加TPS，這種方法不需要在側鏈上使用節點固定交易，主要是先在主鏈上建立一個付款通道（Payment channel），然後參與此通道的交易者，在主鏈運作外交換一些有電子簽章的訊息以表示一些交易，最後將交易的總成結果，放回主鏈。然而這樣子的做法需要在通道中預付一筆金額並且需要實時在網路上待命以免收不到別人傳送過來的交易，其實非常難以應用。

InfiniteChain無窮鏈的側鏈採取代理人類型（Proxy-Based），在此類型的情境中，用戶會委託一個平台或是代理人來協助他們將交易上鏈，並將共識系統中的不可篡改性交由最上層主鏈來達成，各自應用的交易有效性則是下層的資料結構來實現，下層的側鏈（可以是任何資料結構所構成）需要時可以隨時產生，數目無限制，非常適合用來解決現實場景與區塊鏈介接的問題，在InfiniteChain無窮鏈所提供的特點中，我們不僅僅是增加頻寬、解決鏈上資料龐大以及隱私保護問題，更解決了現行應用系統與去中心化系統難以融合的情況。InfiniteChain無窮鏈的混合鏈運作中，主鏈的一致性使用公有鏈的全球共識，而側鏈的有效性及如何保持正確及避免代理人（或是稽核節點）的單點失效或惡意攻擊則是利用InfiniteChain無窮鏈所提出的側鏈運作，包含本公司發明專利：『分散式稽核功能[24]』。下表將混合鏈和其它公有鏈及私有鏈做一總比較。

	公有鏈	私有鏈	混合鏈
節點數	沒有限制 (現在約 10K)	受限	沒有限制
共識	全球	本地	全球
51% 攻擊	困難	簡單	困難
每秒交易數量	7-25	1,000-2,000	> 1,000,000 (主鏈＋側鏈)
區塊鏈膨脹	有	無	無
隱私	無	有	有

[24] 發明名稱：分散式稽核系統及方法（Distributed Auditing Method, Device, and System）。此為InfiniteChain無窮鏈C研發團隊擁有的國際專利。

2.1.1 一般型分散式稽核側鏈[25]

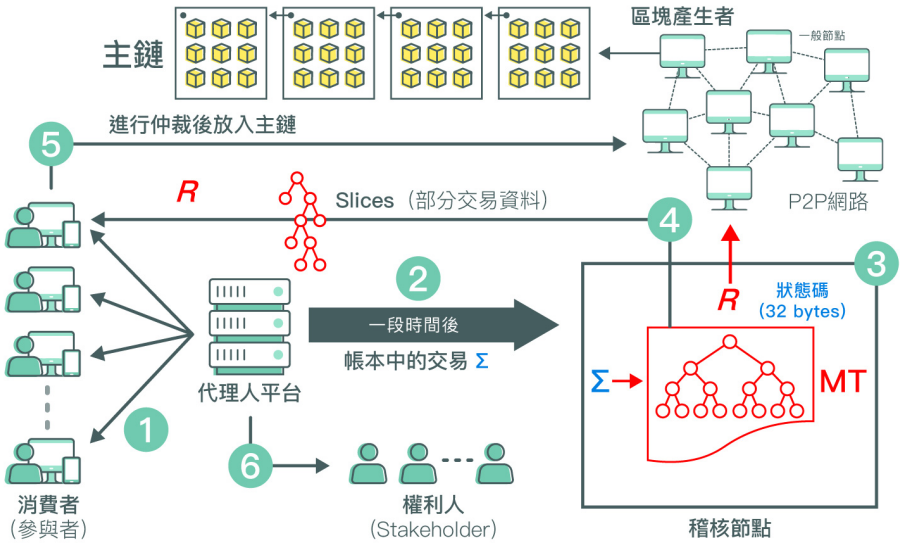


圖4 InfiniteChain無窮鏈一般型分散式稽核側鏈運作圖

InfiniteChain無窮鏈的一般型分散式稽核側鏈的運作請見圖4。依照以下的步驟可以完成某側鏈之一個階段（Stage）的運作：

Step (1)：負責發起側鏈運作的代理人首先和參與者（或消費者）進行一連串的交易活動。

Step (2)：一段時間後（一個階段終結），代理人將Step (1) 中產生的交易∑傳送給稽核節點。

Step (3)：稽核節點將交易∑產生一個索引模克樹（Indexed Merkle Tree），稱為IMT。同時產生IMT的根雜湊值R[26]。將R及相關的識別標籤送到主鏈固定。所有的參與者可以在主鏈中根據識別標籤取得R。

Step (4)：參與者負責稽核自己的交易是否被正確的放在IMT中：

[25] 一般型側鏈已經發布在Github上。 https://github.com/TideiSunTaipei

[26] 索引莫克樹由底層節點資料相接取雜湊函數，一路往根節點取雜湊函數，會在根節點得到一個根雜湊值（Root hash），為32 bytes。加上代理人的電子簽章128 bytes，也只有160 bytes。

- 根據取得的根雜湊值R，請求稽核節點送回自己交易的slices[27]，每個slice對應一筆自己的交易，因為R是被固定在主鏈，slices如果無法稽核出自己該筆交易，就是代理人沒有將自己交易放入IMT的電子證據[28]。

Step (5)：參與者將自己稽核的結果送給P2P網路中的一般節點：

- 稽核通過：參與者傳來簽章過的稽核結果，被區塊產生者打包壓縮放入主鏈，所以只會佔用少許主鏈交易頻寬。
- 稽核不通過：若參與者的稽核結果發現代理人有漏失或放入錯誤的資料，將相關資訊簽章後送給一般節點，最後由區塊產生者執行仲裁。若仲裁結果顯示代理人錯誤，參與者可以取得押金分潤。

Step (6)：代理人支付權利金給權利人。權利人可以使用R及IMT來稽核支付的權利金是否有誤。

每一個階段都會產生一個IMT，代理人負責保管，IMT的根雜湊值必需要放在主鏈上，實作上會在主鏈建立一個合約，將每個階段產生的根雜湊值都儲存於此合約中。同時分散式稽核的費用及押金Token運用此合約來儲存及轉換。

側鏈運作所產生交易的正確性，由全體參與者維護。代理人預先在此側鏈的合約上放入押金，參與者和代理人的交易訊息有雙方的電子簽章達成互不可否認。在Step(4)中，眾多的參與者參與此側鏈交易存在及正確性稽核。若是發現代理人的交易有漏失或錯誤，提交給主鏈的節點仲裁，仲裁為執行合約中的一個函式，仲裁通過則押金自動分給提交仲裁的參與者分潤，否則退回給代理人，以此提高參與者參與稽核的動機。

一般型側鏈的設計適合事務型的記帳，不僅架構簡單實作方便，還可達成不受主鏈頻寬限制的應用，譬如版權登記系統，同時兼顧隱私保護，詳見附錄B。但若是需要使用到高速、低成本微支付的功能，則需要使用到下一節所說明的金流型分散式稽核側鏈，才可滿足此類應用的需求。

2.1.2 金流型分散式稽核側鏈

InfiniteChain無窮鏈的金流分散式側鏈的結構如圖5，由一個發佈在主鏈的合約（以下稱為側鏈合約）來控制及記錄參與者在側鏈的金流交換，一般的金流不須經由主鏈，可以加快金流的速度。一個金流網路由一個召集人擔任代理人發起，一個合約對應一個側鏈。根據需求可以隨時發起一個

---

[27] 切片（Slice）是索引莫克樹的一小部分，儲存500,000筆交易的索引莫克樹帳本，最少需要300MB，若加上一些標籤可能需要數GB的空間儲存。但是一個切片只有整體帳本1/100000的資料量，可用來稽核位於此切片節點中的交易是否存在於此索引莫克樹的帳本中。

[28] 每個交易的稽核可以在1ms內完成。

InfiniteChain無窮鏈的金流側鏈。比如一個網路商城或高速加密貨幣交易所等，參與者可以根據需求參與不同的InfiniteChain無窮鏈金流側鏈。

使用者隨時可以將加密貨幣或代幣存入側鏈合約，也可以提領出來。但是存入側鏈合約的加密貨幣或代幣若流入側鏈中交換，則暫時無法提領出來。必須由在側鏈中提領到側鏈合約，才能轉出到其他主鏈區塊鏈的其他帳戶。

代理人要負責維護消費者在側鏈的交易記錄、Balance tree、及Receipt tree。Balance tree、Receipt tree都是索引模克樹，或可以經由切片支援驗證所儲存記錄的存在或不存在的資料結構。Balance tree記錄每個參與此金流側鏈者的由側鏈合約匯入側鏈加密貨幣或代幣的使用餘額，以側鏈參與者的ID為索引，存到Balance tree中。參與者將側鏈中的加密貨幣或代幣轉給側鏈中其他參與者或是將側鏈中的加密貨幣或代幣轉到合約，都會使餘額減少。Receipt tree存的是交易記錄，和圖4中一般型分散式稽核側鏈的索引模克樹的功能類似。

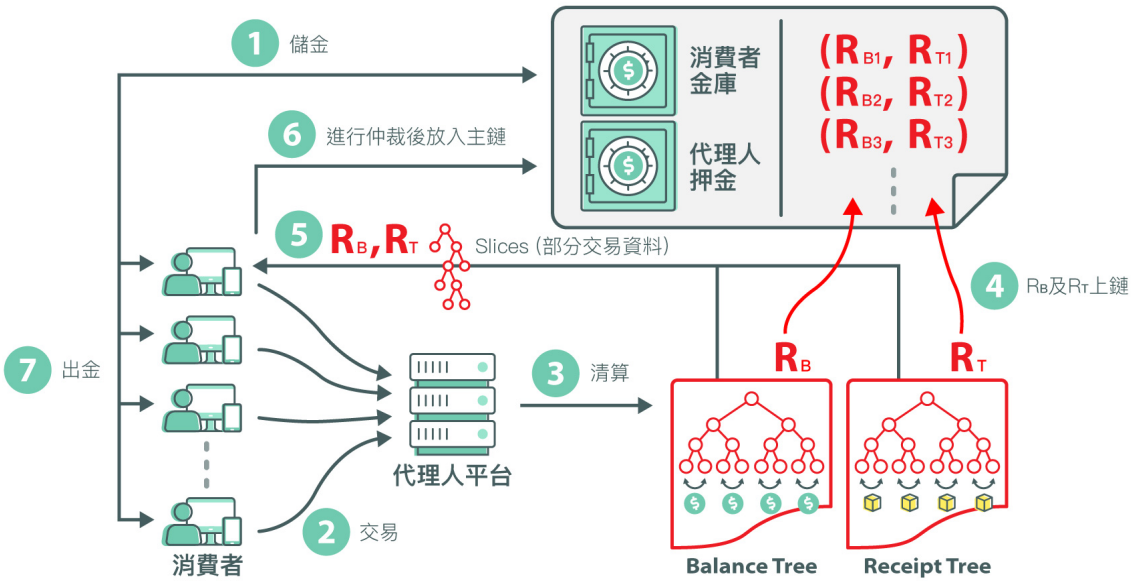


圖5 InfiniteChain無窮鏈之金流分散式稽核側鏈運作圖

InfiniteChain無窮鏈金流側鏈一個階段的運作和一般型側鏈的運作大致類似（見2.1.1節Step(1)-(6)）及圖5，也是由負責發起側鏈運作的代理人首先和參與者（或消費者）進行一連串的交易活動，階段結束後代理人最後將Balance tree及Receipt tree的兩個根雜湊值放到合約中，然後所有參與者負責稽核自己的交易是否被正確的放在Receipt tree中。但是除此之外，最後每個參與者要由自己相關的交易來稽核Balance tree中自己的餘額、合約和側鏈的加密貨幣及代幣的轉換是否正確。最重要的

是在稽核出代理人有發生錯誤時，能產生密碼學證據送回合約進行Fraud proof。詳細的協定十分複雜，為本公司發明專利[29]，請參考附件C。

2.1.3 混合鏈管理

為兼顧公有區塊鏈達成全球共識的可信度，主鏈維護及運作和一般公有區塊鏈的運營和管理相同。側鏈運作由主鏈根據需求發起。側鏈需要定期將信息同步到主鏈，避免側鏈信息造假或者數據被竄改。主鏈和許多側鏈的運作並行，可以實現超過一千萬級TPS。

關於區塊鏈上的權限控管，一般私有鏈或聯盟鏈以限制節點角色或權限來實作，但這違反區塊鏈去中心化的基本概念。InfiniteChain無窮鏈的側鏈控管，為達成全球共識，被設計成可以在公有鏈上運作，不需要中心化的伺服器控管權限。混合鏈的管理架構以區塊鏈上的智能合約來公布其運作協定，參與者在公有鏈取得協定，遵循被公布的協定運作。

運用系統的管理者在主鏈上的發佈一些合約（或稱智能合約）來實行側鏈運作控管。見圖6，管理者，在區塊鏈發佈一個主合約及很多子合約，合約間相連，型成一個網路結構。主合約有一個固定的位址，即為此資產交易系統的進入點。資產交易的成員，如：管理員、不同權限或經營不同側鏈的代理人、參與交易者都由此位址進入系統。此位址為主合約在區塊鏈中的參考點，公告後固定不變，可以增加安全性。

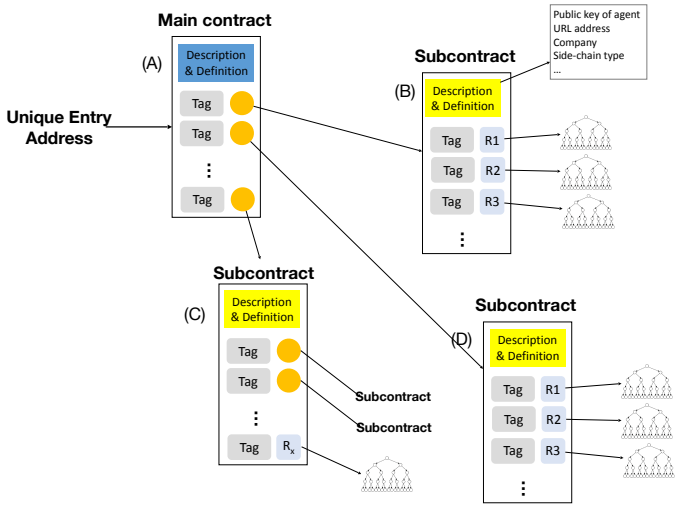


圖6　混合鏈管理合約架構圖

[29] 發明名稱：分散式金流交易稽核協定（Protocol for Distributed Auditing of Payment Flow），此為InfiniteChain無窮鏈研發團隊擁有的國際專利。

主合約(A)公布整個運用系統的運作狀況及協定，一個子合約可能是系統中其他公告事項，或是一個側鏈運作的歷程記錄及現況。所有合約都存放在主鏈中，因為主鏈交易頻寬有限，所以不可能將所有的資產交易結果都存在裡頭。如圖3所示，側鏈運作的雜湊值即存於負責記錄該側鏈的子合約中，實際上表示將很多交易資訊一次放上主鏈。R1、R2、及R3為之前側鏈運作的雜湊值，此側鏈定期將信息同步到主鏈的雜湊值會存於此子合約中。子合約亦可描述資產交易系統的動態資料，如子合約(C)中的R_x為一雜湊值表示有登記的用戶資料。

2.2.Proof of Participation

InfiniteChain無窮鏈的出塊協定為基於權益證明所改良的參與權益證明（Proof of Participation, PoP），首先每個用戶的權益會利用用戶的信用點數（見2.3節）與持有的幣加權後產生；信用點數是不能被轉移的，每個人僅能透過協助稽核以及活躍的參與區塊鏈活動來取得。同時，在計算權益（Stake）時僅會使用近期一段時間的點數來計算，目的是希望用戶可以不斷的參與活動。

$$Stake = \alpha \times Credit_{(recent)} + (1- \alpha) \times Coin$$

為了避免出塊權集中，InfiniteChain無窮鏈想建立一個擬隨機數(pseudo random)的方法，便是利用區塊高度、上個區塊礦工的地址、及現在的礦工候選人地址產生一個雜湊值Rand。Rand再除以$2^{hash\ length}$得到一個介於0及1的數值Weight。

$$Rand = hash(BlockHeight \parallel Address_{(previous\ miner)} \parallel Address_{(candidate\ miner)})$$

$$Weight = Rand \div 2^{hash\ length}$$

最後，再將Weight及Rand兩個變數相乘去檢查是否高於某個閥值，便可以取得出塊權，同時廣播給所有的節點知道。

$$Weight \times Stake > threshold$$

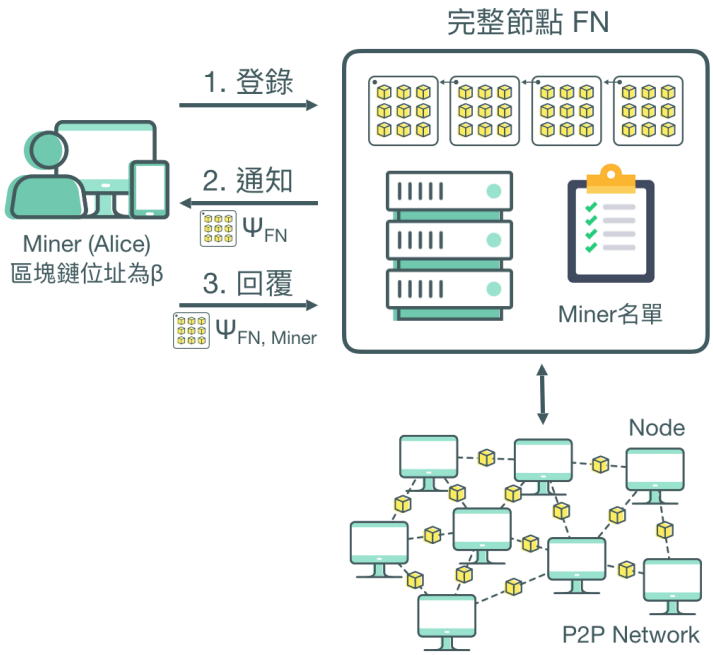


圖7 輕量挖礦協定

見圖7，在這樣的出塊協定中，節點會開放一般用戶註冊他們的地址，而節點會提供打包區塊的服務，當新的區塊被打包完，節點會去找在所有已註冊的地址中，最有可能會超過閥值取得出塊權的地址並且發出通知，而用戶收到通知後會簽名再傳回去節點，而節點即可用此簽名去爭取出塊；當最後如果取得出塊權，則出塊的手續費由節點與用戶共同分潤，這樣的模式即可達成公平出塊的概率分佈。

在圖7中演示了簡單的輕量挖礦流程，首先用戶都需要把自己的地址登錄在完整節點中，讓完整節點會去檢查你的參數，當完整節點檢查加權後的權益是有高於閥值，則完整節點會通知用戶簽名擔任此次的礦工，完整節點會將候選區塊（Block Candidate）簽過名後傳給用戶（ψ_{FN}），而用戶簽完章（$\psi_{FN,\ Miner}$）回傳給完整節點後，這個區塊就有兩個簽名並且去網路上競爭出塊；如果這個區塊成為正式區塊，完整節點跟用戶則可以依照比例分配出塊利潤。

這樣的出塊協定[30]，不僅可以讓一般用戶都有機會取得出塊權，同時也讓移動裝置挖礦可行，也鼓勵完整節點提供良好的服務讓一般用戶登記，當完整節點底下有很多用戶登記時，自己也比較容易獲得出塊分潤。

[30] PoP的出塊協定，也可以設計成不需用戶使用輕量裝置於流程中參與運作。只需有一個主鏈中的合約讓用戶登記委託節點的Address，然後此節點有權力使用此用戶的Weight × Stake來競爭出塊。節點於共識決完成出塊，所獲得的Coin就自動進入此用戶及節點的address中。

2.3.主鏈信用制度（On-chain Credit System）

InfiniteChain無窮鏈希望建立一個區塊鏈信用制度，讓用戶於參與各種區塊鏈活動都可以累積他的信用，利用群眾的利己心理建構一個利他的世界；每個用戶在自己的帳戶中皆有一個信用點數，而其中又可以分為歷史總累積數量以及近期內累積數，只要用戶活躍的參與區塊鏈活動，便可以增加自身的信用點數，以下的勞動皆可以幫助無窮鏈的穩健發展：

- 主鏈的轉帳
- 參與側鏈活動
    - 成為代理人，無異狀的營運側鏈
    - 成為用戶，協助稽核側帳
    - 擔任稽核員，協助檢查索引莫克樹的完整性
- 無異狀的成功出塊
    - 用戶簽名參與出塊
    - 節點協助用戶出塊
- 參與自治投票
- 無異狀的發行ICO

只要上述活動若發生異狀且被稽核員稽核出來，則會大大降低帳戶的信用點數。

信用點數的增加需要花費貨幣，並且在側鏈上運作所獲得的信用是使用時間累積的，難以在短期內快速增加信用點數；另外，信用點數的多寡雖會造成不同帳戶之間的權益高低，但在我們的設計之下，最高與最低的權益概率不應該會超過五倍。

舉ICO為例，用戶可以在合約中看見發起人的地址，並且可以利用此地址去查詢這些發起人的信用點數，在每期撥款以及投票決定是否繼續放款時，如果有順利的通過放款，則發起人的信用點數會增加，表示這些發起人有正常的營運這些應用；若情形剛好相反，投資人想要投票拿回資金，則發起人會被重懲，扣除大量的信用點數，這些相關的記錄也都會在主鏈上永遠留存。這樣子的機制，確保每個人都會謹慎的去處理自己在區塊鏈上的行為。

3. InfiniteChain無窮鏈應用場景

近年區塊鏈發展趨勢扶搖而上，各行各業都在討論區塊鏈潛在的應用價值。在金融領域、交易、支付等不斷發展；在社交領域，人們再探討通過區塊鏈記錄的活動來建立名望的可能性；在醫療領域，人們討論透過區塊鏈存放電子病歷的優勢；在法律領域，區塊鏈在查驗、稽核、支付系統以及智能合約上有廣大的應用前景。

股票、股權交易

在股票交易的情境中，對於買家，購買後需要花費一段時間去追蹤股權的轉換，導致交易的時間過長。對於公司，需要在律師、稽核員、顧問等人員在審查所有投資人的交易過程中投入大量的成本，若使用區塊鏈的信任機制便可以將股票交易時部分的中間人去除，例如稽核員，另外也可以透過將交易固定在區塊鏈上，縮短買家追蹤股權的時間。不過以區塊鏈目前的交易頻寬也不足以面對龐大的股票交易數量。透過InfiniteChain無窮鏈除了提供快速的交易外，更加注重隱私，每個交易者根據自己的權限，只能看到自己的相關記錄，同時擁有快速與隱私的特性。使用InfiniteChain無窮鏈混合鏈架構，可以確實完成可用的系統。

資產交易

所有資產都可以數位化，資產數位化後便可以量化，可流通、買賣、抵押，產生巨大價值，想像未來房子、車子都成為區塊鏈上的資產，透過私鑰決定所有權，所有的不動產，將比現在更容易流通。區塊鏈應用於數位資產，最大的優勢在於，資產一旦發佈到區塊鏈上，流通方式變得更加容易。

InfiniteChain無窮鏈提供多種數位資產轉換的方式，並且提供交易應用，交易的同時，保障相關所有人應有隱私權益，以及交易不可否認性，彼此能夠信任、信賴。

銀行監管 / 法規遵循

銀行可善用公有區塊鏈的信任機器 (Trust machines) 實現企業內控、法規遵循的要求，例如銀行行員何時做何種交易或業務行為，當下就被記錄，有交易序列號和銀行的電子簽章，所以銀行不可否認。所有記錄整合後固定回區塊鏈，無法竄改且資料透明，沒有事後稽核的需要。

相較於目前內控和法規遵循，必須仰賴第三方稽核，並需要事前的內部教育、立法規範，以及事後的稽核確認，運用InfiniteChain無窮鏈和分散式稽核技術，銀行和行員的業務記錄透明，行員可稽核自己的行為記錄是否正確，或對銀行提出某個行為的稽核請求，亦不會有記錄造假的可能。

區塊鏈金融

以VISA為例，全球平均每秒的交易數量約為2000筆（最多每秒有58,000筆），若想將VISA交易系統與區塊鏈的信任機制結合，使用傳統的公有區塊鏈，在短時間內要將VISA龐大的交易量固定在區塊中是非常困難的。若結合InfiniteChain無窮鏈的架構，我們可以在側鏈將每秒產生的數萬筆交易紀錄及完成分散式稽核，解決交易頻寬的問題。InfiniteChain無窮鏈提供快速的交易服務，並透過分散式稽核，維護交易正確性，這將是未來區塊鏈在金融應用的基礎。

社會治理

在傳統領域，身分認證、公證、司法仲裁、投票、借貸系統，都使用中心化服務器來存取數據，存在造假問題。要解決這類問題，使用區塊鏈是很好的方式。區塊鏈具備公開透明，不可造假的特性，且成本低，因此可以預見，未來這類公證應用，都會選用區塊鏈技術來解決造假問題。

InfiniteChain無窮鏈則補足了區塊鏈在隱私上與速度上的不足，可以同時接受大量數據的進行，運用於電子投票中，一方面確認身分，一方面快速投票，保有區塊鏈優點，並補足了區塊鏈的不足

高速加密貨幣支付系統或交易所

現有的加密貨幣支付系統或交易所，都面臨主鏈交易頻寬的問題。隨著加密貨幣的交易熱絡及價值提升，直接在主鏈上執行加密貨幣支付及交易的成本水漲船高，也常常因為執行量太大造成擁塞的現象。使用InfiniteChain無窮鏈金流型分散式側鏈來實作類似系統，將可以實現加密貨幣微支付及高速交易所。

4. InfiniteChain無窮鏈發展現況及合作項目

InfiniteChain無窮鏈團隊目前已提出了數項國際專利，現正在數個國家提案申請中：

(1) 分散式稽核系統及方法（Distributed Auditing Method, Device, and System）。

(2) 一種即時稽核的雲端存取方法（Method for Auditing Cloud Access in Real Time）。

(3) 分散式金流交易稽核協定（Protocol for Distributed Auditing of Payment Flow）。

系統實作部分已完成概念驗證（Proof of concept）的程式設計及運作測試。目前已和數個公司商談合作。

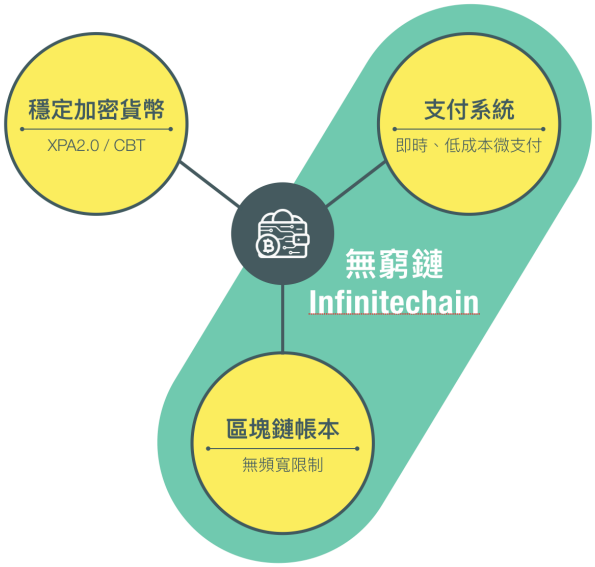
InfiniteChain無窮鏈的大量記帳功能協助日本上市電商打造區塊鏈時間計價模式，以時間計價的娛樂電商在過去因為代理人、用戶以及內容提供商三方資訊不對等難以實現，同時這樣的高頻記帳在公有鏈上的實作成本十分高昂，而InfiniteChain無窮鏈能夠在稽核時間內達成大量、快速地上鏈，讓資訊對等成為可能，目前已經和該公司正式簽約。同時泰德陽光集團也運用InfiniteChain無窮鏈的技術，打造區塊鏈廣告、區塊鏈版權登記等各式運用。相關商業計畫為TideFinTech及TideXMedia。

另一個為國際某知名證券及期貨交易所，其目標是將股權、股票、期貨等各式交易記錄在區塊鏈上，縮短證券商及客戶追蹤的時間，及增加相關查詢的正確及可信度。不過區塊鏈的交易頻寬不足以面對其龐大的交易數量。透過InfiniteChain無窮鏈的混合鏈模式除了提供大量交易記錄的能力外，在隱私上更加注重，每個交易者根據自己的權限，只能看到自己的相關記錄，同時擁有快速與隱私的特性。目前此計畫已幾近完成概念驗證（PoC），即將進入產品實作及發布。

5. 總結

以區塊鏈技術為基礎的去中心化應用系統之發展正開始要進入人類的生活，卻被一些專家點出基本技術遭遇瓶頸，第1.8節提出的技術問題、共識問題以及經濟模式問題上，任何一個問題無法被解決都會使得以區塊鏈成為信任機器的美夢成為枉然，最後區塊鏈只能成為加密貨幣的鑄造及交易平台，或是只能被少數的應用場景使用。

目前泰德陽光集團積極打造TideFinTech，其規劃一個完整的區塊鏈加密貨幣生態系統，關鍵技術包含區塊鏈上的『穩定加密貨幣』、『即時、低成本微支付系統』、『無頻寬限制的帳本系統』、及整合服務的Wallet app，如下圖。InfiniteChain無窮鏈技術實現了『即時、低成本微支付系統』、及『無頻寬限制的帳本系統』的基本技術。



InfiniteChain無窮鏈發展團隊確認去中心化系統打破訊息不對等讓參與安心的參與其中的活動是世界潮流，並以實際的技術提出這些問題的徹底解決方案。相關技術都有雛形實作以評估其效能即可行性。接下來的去中心化應用系統及區塊鏈的發展必定會留下InfiniteChain無窮鏈發展團隊貢獻的身影。

附錄A 公有區塊鏈交易頻寬無法提升的原因

一個區塊鏈的交易速度，一般以平均每秒能被固定於區塊的交易數目TPS（Transactions per second）來表示，亦可稱為交易量頻寬，大約就是平均每秒於區塊鏈產生的區塊數相乘平均每個區塊中所包裹的交易數，如下公式：

每秒交易速度＝（平均每秒產生的區塊數）×（平均每個區塊中的交易數）

比特幣是使用PoW隨機的得出區塊產生者，所以平均每秒於區塊鏈產生的區塊數很少，事實上平均每10分鐘才能產生一個區塊，比特幣區塊鏈的速度限制大約是每秒7個交易。後續發展的區塊鏈為突破此速度限制，大多採用PoS的共識協定來得出區塊產生者，基本上想成為下一個區塊產生者的節點，和其它的競爭者比較彼此的權益（Stake），權益大者根據共識協定成為下一個區塊產生者。因為不需要如PoW使用運算能力來互相競爭，所以速度較快。見圖1，欲擔任下一個區塊產生者（Block producer）的節點，在P2P網路中得到擴散的交易資料，被共識決選出後將區塊產生，再經由P2P網路將區塊擴散給其他節點。

但是PoS的共識運作中，所有的競爭者必須得知其他競爭者的權益，這些競爭者分佈在全世界由網路互相溝通。即使得知有哪些競爭者，往往還需於之前的區塊鏈的區塊中查閱其他競爭者的權益量，所以得出區塊產生者往往需要數秒鐘。也就是說，平均每秒於區塊鏈產生的區塊數一般是小於1。同時平均每個區塊中所包裹的交易數目侷限於節點的網路頻寬及P2P 的資料交換速度。

除此之外，區塊產生者需要驗證[31]所有要被包裹於區塊的交易，這也要花運算時間。一般PoS的共識決定在選出區塊產生者後，會給此區塊產生者一個產生區塊的時間限制，通常是數秒。以太坊目前大約是每秒15個交易量的限制。已經有專家質疑目前於以太坊發展的超過100個以上的Dapps的上線全速運作，認為會讓以太坊區塊鏈無法負擔或崩潰[32]。我們可以得出一個結論，允許所有網民參加的『公有鏈』，因為參加網民必須於P2P交換資訊，因此速度受限的問題無法解決。但是公有鏈的公信度因為參與者眾，且為公開，公信度最高。

[31] 以防止Double spending或非法交易。

[32] Yo Banjo, "How Etheroll and other Dapps will kill Ethereum," https://medium.com/@yobanjo/how-etheroll-and-other-dapps-will-kill-ethereum-e973d8e1c465.

附錄B IFC側鏈隱私權保護技術

數位資產提供人的隱私保護，有兩種方式。第一種是存在索引莫克樹的交易都使用數位資產提供人的公鑰（Public key）加密，消費者在稽核自己某筆交易時，可以先將交易資料使用數位資產提供人的公鑰加密，並比對加密後的資料是否和存在索引莫克樹帳本中的資料相符。數位資產提供人欲進行稽核時，我們可以將整個索引莫克樹帳本交給數位資產提供人，因為此數位資產提供人只能看到及稽核可用自己私鑰可解密的資料，所以隱私權得以保護。雖然此方法的安全機制佳，但是進行一個非對稱解密花費的時間長（大約22 ms），數位資產提供人要對索引莫克樹中的所有的交易都嘗試解密，可以解密出的資料即為自己的相關交易[33]。如果索引莫克樹中的交易數量很大，可能要花費很多時間。比如有100,000筆交易，稽核的時間要超過150秒以上[34]；若是1,000,000筆交易，要花費一小時以上。如果數位資產提供人要使用手機等運算能力較差的裝置來進行稽核，可能較不適合。注意，消費者只稽核與自己相關的少數交易，所以並無此問題。

另一種方式，是為每一個數位資產提供人建立一個索引莫克樹（稱為數位資產提供人交易索引莫克樹、簡稱SubMT），用來存此數位資產提供人的交易，不需加密。同時將所有SubMT的根雜湊值再用來建立一個索引莫克樹（稱為主要索引莫克樹、簡稱MainMT），稽核節點公布MainMT的根雜湊值於區塊鏈。消費者在驗證自己某個交易是否正確或存在時：（1）稽核節點先出示相關數位資產提供人之索引莫克樹SubMT的切片給消費者驗證；（2）消費者再驗證此SubMT的根雜湊值是否存在MainMT中。

數位資產提供人要稽核自己所有相關交易時[35]，稽核節點出示此數位資產提供人的SubMT及MainMT，數位資產提供人確認自己SubMT有出現在MainMT且不重複。然後檢視自己SubMT中所有交易即可。因為SubMT中只有自己的相關交易，所以不會看到其他數位資產提供人的交易資料，可以將隱私保護起來。因為只稽核自己的交易，使用運算能力較差的裝置來進行稽核，如手機，也沒問題。

---

33 解不出的交易為其他數位資產提供人的相關交易。

34 此運算時間還未加上於索引莫克樹上的traversal 花費時間。

35 執行公布的開源程式。

附錄C IFC金流分散式側鏈合約及運作協定

IFC的金流側鏈的結構如圖8，由一個合約來控制及記錄參與者的金流交換，一般的金流不須經由主鏈，可以加快金流的速度。一個金流側鏈由一個召集人擔任代理人發起，對應一個合約及一個側鏈。根據需求可以隨時發起一個IFC的金流側鏈。比如一個網路商城或交易所，參與者可以根據需求參與不同的IFC金流側鏈。

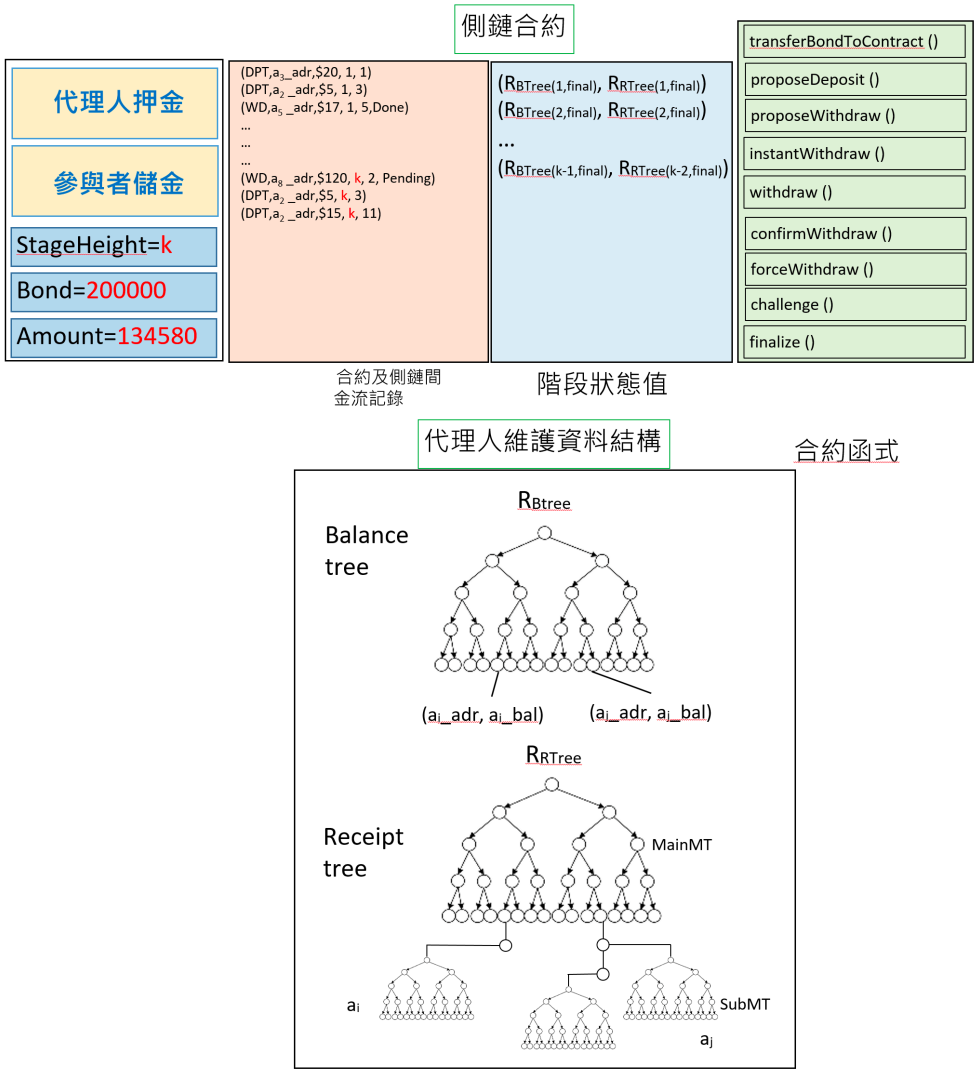


圖8 IFC金流分散式稽核側鏈運作圖

使用者隨時可以將加密貨幣或代幣[36]存入合約（以下簡稱token），也可以提領出來。但是存入側鏈合約的加密貨幣或代幣若流入側鏈中交換，則暫時無法提領出來。使用者必須向合約或代理人提出提幣申請，才能轉出到主鏈的帳戶。

[36] Token表示主鏈中共識決認可的有價加密貨幣。

見圖8，『代理人押金』及『參與者儲金』是表示儲存在合約的tokens。代理人必須先執行transferBondToContact()將足夠的tokens儲存到『代理人押金』，參與者要交換的tokens都先存於『參與者儲金』。『Bond』及『Amount』為兩個變數，分別表示代理人的押金總量及參與者們的儲金總量。側鏈的運作分成很多階段（stages），每次階段結束都會進行金流的清算，以確保代理人的運作正確。合約中的『StageHeight』變數表示目前是第幾個階段。

代理人要負責維護消費者在側鏈的交易記錄、Balance tree、及Receipt tree。其中Balance tree、Receipt tree都是索引模克樹。

- Balance tree存的是一些Key-value pairs。每一個pair為(a_i_adr, a_i_bal)：a_i_adr為側鏈參與者的地址、 a_i_bal為a_i存入側鏈Tokens的使用餘額。以側鏈參與者的a_i_adr為索引，存到Balance tree中。參與者將側鏈中的Tokens轉給側鏈中其他參與者或是將側鏈中的Tokens提出，都會使餘額減少。
- Receipt tree存的是交易記錄，資料結構和附錄B中所述類似，見圖8。MainMT為一索引模克樹，以側鏈參與者的a_i_adr為索引，底下以雜湊值接上一些索引模克樹SubMT，每一個SubMT儲存和某使用者相關的交易，基本上合約上Token移入、移出、和其他參與者匯給此參與者的交易記錄，都存於此SubMT。

參與者可以進行以下四種交易：

- Remittance transaction: 將自己側鏈上的Balance tree上記錄的儲金移到其他使用者在Balance tree上記錄的儲金。
- Deposit transaction: 將自己合約上的儲金移到側鏈的Balance tree。
- Instant withdraw transaction: 將自己側鏈的Balance tree上記錄的儲金小額且快速的移到主鏈地址。
- Withdraw transaction: 將自己側鏈的Balance tree上記錄的儲金移到主鏈地址。

以下分別討論四種交易的運作協定。

Remittance 交易協定（a_i要將在側鏈的Token轉X個單位給a_j）

Step 1: 側鏈參與者a_i將交易需求T_{rmit}=((Remittance, LSN, a_i_adr, a_j_adr, X, SH), $SIG_{PK(a_i)}$)傳給代理人。其中LSN（Local sequence number）為a_i產生的一個不會重複的亂數，a_i_adr為用戶地址，X為交易金額，SH為目前階段高度，$SIG_{PK(a_i)}$為訊息本體的電子簽章由a_i所簽署。

Step 2: 讓Sender_balance = a_i_bal-X、Receiver_balance = a_j_bal+X。代理人將Balance tree中的(a_i_adr, a_i_bal)修改成(a_i_adr, Sender_balance)、(a_j_adr, a_j_bal)修改成(a_j_adr, Receiver_balalance)。

Step 3: 代理人將$T_{receipt}$ = ((T_{rmit}, Sender_balance, Receiver_balance, GSN), $SIG_{PK(Agent)}$)傳給a_i並將其放入Receipt tree。其中GSN（Global sequence number）為代理人產生的一個整數，由0開始，每次處理一個參與者的交易後都會增加1。$SIG_{PK(Agent)}$為訊息本體的電子簽章由交易人所簽署。

Deposit交易協定（側鏈參與者a_i提出存幣申請X個單位的token移到側鏈）

Step 1: 側鏈參與者a_i執行智能合約函示proposeDeposit(DPT, a_i_adr, X, SH, LSN)，此時合約上產生一筆log = [DPT, a_i_adr, X, SH, LSN]，DPT表示為儲金log，a_i_adr為用戶地址，X為存幣金額，SH為目前階段高度，LSN為用戶a_i產生之亂數。

Step 2: 智能合約觸發事件proposeDeposit並將此log傳給代理人。

Step 3: 讓Balance = a_i_bal+X。代理人將Balance tree中的(a_i_adr, a_i_bal)修改成(a_i_adr, Balance)。

Step 4: 代理人產生$T_{receipt}$ = ((DPT, LSN, SH, a_i_adr, Balance, GSN), $SIG_{PK(Agent)}$)，將$T_{receipt}$傳給參與者a_i，並將其放入Receipt tree。

Instant Withdraw 交易協定（側鏈參與人a_i經由代理人將側鏈 X個的tokens立即轉移到主鏈 帳戶address）

Step 1: a_i將交易需求$T_{InstantWithdraw}$=((WD, LSN, a_i_adr, X, SH), $SIG_{PK(a_i)}$)傳給代理人。其中LSN（Local sequence number）為a_i產生的一個不會重複的亂數，a_i_adr為用戶地址，X為交易金額，SH為目前階段高度，$SIG_{PK(a_i)}$為訊息本體的電子簽章由a_i所簽署。

Step 2: 讓Balance = a_i_bal-X。代理人將Balance tree中的(a_i_adr, a_i_bal)修改成(a_i_adr, Balance)。

Step 3: 代理人將$T_{receipt}$ = (($T_{InstantWithdraw}$, Balance, GSN), $SIG_{PK(Agent)}$)回傳給a_i，並將其放入Receipt tree。

Step 4: a_i呼叫智能合約instantWithdraw($T_{receipt}$)，產生一筆log= [WD, a_i_adr, X, SH, LSN]，並立即轉移X個tokens至主鏈a_i_adr。

Withdraw 交易協定（側鏈參與人a_i經由合約將側鏈 X個的tokens立即轉移到主鏈帳戶 address）

Step 1: a_i執行智能合約proposeWithdraw(WD, a_i_adr, X, SH, LSN)，此時智能合約上產生一筆log = [WD, a_i_adr, X, SH, LSN, BKH, pending]，WD表示為提幣log，a_i_adr為用戶地址，X為提幣金額，SH為目前階段高度，LSN為用戶a_i產生之亂數，BKH為主鏈上的目前區塊高度。Pending表示此提幣請求尚未被代理人處理。若代理人於一個設定的時間內沒有處理a_i的請求，a_i可以執行forceWithdraw(log)來強制提幣。

Step 2: 合約觸發事件proposeWithdraw並將log傳給代理人。

Step 3: 讓Balance = a_i_bal-X。代理人將Balance tree中的(a_i_adr, a_i_bal)修改成(a_i_adr, Balance)。

Step 4: 代理人產生$T_{receipt}$ = ((WD, LSN, SH, a_i_adr, Balance, GSN), $SIG_{PK(Agent)}$))，並呼叫confirmWithdraw($T_{receipt}$)，log被改成[WD, a_i_adr, X, SH, LSN, BKH, Granted]，同時觸發合約事件將$T_{receipt}$回傳給側鏈參與人a_i。

Step 5: ai即可執行智能合約withdraw([WD, a_i_adr, X, SH, LSN, BKH])，X個tokens被轉移到主鏈a_i_adr，同時log被改成[WD, a_i_adr, X, SH, LSN, BKH, Done]。

側鏈的運作分成很多階段，假定於階段k開始Balance tree及Receipt tree的Root hash假定分別為$R_{BT(k,init)}$及$R_{RTree(k,init)}$[37]。若一個階段中代理人處理來自不同參與者的N個交易，每次處理都會造成Balance tree及Receipt tree的根雜湊值更改。假定更改的順序如下：

$$R_{BTree(k,init)} \rightarrow R_{BTree(k,1)} \rightarrow R_{BTree(k,2)} \rightarrow R_{BTree(k,3)} \rightarrow \ldots \rightarrow R_{BTree(k,final)}$$

Receipt tree的根雜湊值每次處理完後也會更改，我們假定最後變成$R_{RTree(k,final)}$。階段k結束後，代理人呼叫Finalize()，此函數將$R_{BTree(k,final)}$及$R_{RTree(k,final)}$傳回無窮鏈合約，同時將階段序號Stage值增加1。

代理人運作稽核及密碼學證據

代理人根據協定處理呼叫智能合約及執行Remittance、Deposit、Instant withdraw 、Withdraw等交易協定使整個側鏈不用消耗主鏈的交易頻寬，能處理大量的參與者交互金流交易。但是代理人可能發生錯誤亦或惡意將參與者轉入合約中的Token故意轉給特定人士以圖利。以下說明側鏈的挑戰機制。

為防止代理人作弊圖利，首先代理人必須要將一筆押金（Bond）存入合約，每個參與者都可以實施稽核，稽核發現代理人錯誤，可以根據所持有的密碼學證據呼叫合約的challenge()方法，獲得代理人押金。

如同白皮書圖3的分散式稽核側鏈，每個參與者都可以根據被放到合約中的$R_{RTree(final)}$進行分散式稽核：

[37] 此為一個沒有任何$T_{receipt}$的Receipt tree。

- 若發現自己的交易沒有被放到Receipt tree，根據所持有的密碼學證據呼叫合約的challenge()函式，獲得代理人押金。如此可以防止代理人不將參與者轉帳的錢增加到被轉者在Balance tree的Key-value pair。
- 每個參與者，根據$R_{RTree(k,final)}$取得自己相關的交易，其中Deposit transaction、Withdraw transaction、Instant withdraw、及別人匯入到自己帳戶的Remittance transaction可以在自己的SubMT找到，匯入他人帳戶的Remittance transaction可以在收款者的SubMT找到。因為交易記錄$T_{receipt}$都有GSN，參與者可以將自己的交易根據GSN排序先後，假定一個參與者於Receipt tree中找到n個相關的交易。

  $$T_{receipt(1)} \rightarrow T_{receipt(2)} \rightarrow T_{receipt(3)} \rightarrow T_{receipt(4)} \rightarrow T_{receipt(5)} \rightarrow \ldots \rightarrow T_{receipt(n)}$$

  參與者首先由前一個階段之Balance tree的Root hash，取出自己key-pair的切片得知自己在此Stage開始時於此側鏈的餘額，假設這個Stage中參與者在側鏈裡產生j筆交易，則可以透過這j筆屬於參與者的$T_{receipt}$一一檢視每一個交易執行後的餘額是否正確，其中$T_{receipt(j)}$裡的餘額應該和自己在$R_{BTree(k,final)}$的餘額相同。如果$T_{receipt(j)}$有錯誤則將相鄰的兩交易，$T_{receipt(j-1)}$、$T_{receipt(j)}$，作為密碼學證據呼叫合約的challenge()方法，獲得代理人押金。
- 如果某參與者在執行withdraw()發現無窮鏈合約中的參與者儲金不足時，一定是代理人有和其他參與者勾串或錯誤沒有被稽核出來，withdraw()會由代理人在合約中的押金（Bond）將加密貨幣或代幣轉給參與者指定的帳戶位址。代理人押金必須有足夠的存量，否則無法啟動下一個階段的運作。

本附錄只大略說明IFC分散式金流側鏈，實際詳細協定及各式挑戰、自清的細節，請參考IFC分散式金流側鏈白皮書。