



BOLT: Booster of Ledger Technology

白皮書

2018/05/25 Version 1.1

區塊鏈加速器、擴容加速解決方案
解決公有區塊鏈頻寬不足、私有鏈缺乏全球共識

泰德陽光集團 TIDEiSUN

泰德陽光無窮鏈有限公司：我們致力於全方位區塊鏈技術開發，開發技術涵蓋主鏈、擴容解決方案、側鏈、區塊鏈演算法、人工智能和商業解決方案。

目錄

BOLT: Booster of Ledger Technology

白皮書 2018/05/25 Version 1.1

| | |
|----------------------|----|
| 1. 簡介 | 4 |
| 1.1. 背景 | 4 |
| 1.2. 當前問題一：區塊鏈頻寬不足 | 4 |
| 1.3. 當前問題二：區塊鏈承載空間不足 | 6 |
| 1.4. 當前問題三：隱私權缺乏 | 6 |
| 1.5. 當前問題四：交易成本高且不即時 | 7 |
| 1.6. 當前問題五：應用場景受限 | 8 |
| 1.7. 問題總結 | 8 |
| 2. 技術核心 | 10 |
| 3. 應用場景 | 17 |
| 股票、股權交易 | 17 |
| 資產交易 | 17 |
| 銀行監管 / 法規遵循 | 17 |
| 區塊鏈金融 | 18 |
| 社會治理 | 18 |
| 高速加密貨幣支付系統或交易所 | 18 |
| 4. 發展現況及合作項目 | 19 |
| 5. 總結 | 21 |
| 附錄A 公有區塊鏈交易頻寬無法提升的原因 | 22 |
| 附錄B BOLT加速器隱私權保護技術 | 23 |
| 附錄C BOLT金流加速器合約及運作協定 | 24 |

BOLT

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。

BOLT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，提出全新的分散式稽核、即時高速金流協定，具備以下優勢：

- 無交易速限：鏈下運作的密碼學協定和海量交易打包上鏈技術，可實現超過一千萬級 TPS (每秒交易)
- 確保交易的隱私：在完成交易的過程中，提供消費者和數位資產提供者隱私保護
- 與現有中心化的商業場景融合：結合代理人模式，同時保有去中心化資訊對等的價值

BOLT打破了交易處理速度和交易數量的限制，解決公有區塊鏈頻不足，亦解決私有鏈缺乏全球共識的問題。建立了一個支援無速度限制、更受信任的去中心化架構。可運用在所有具備智能合約功能的公有或私有區塊鏈，解決了現今區塊鏈面臨的問題：

- 區塊鏈頻寬不足
- 區塊鏈承載空間不足
- 交易成本高且不即時
- 隱私權缺乏
- 無法和現有中心化應用融合，行業應用場景受限

最後，針對區塊鏈在各行業潛在的應用價值和商業機會，白皮書中列舉了在金融、法律、醫療、供應鏈、金流支付、交易所等領域的應用場景，BOLT的技術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去中心化交易生態系。

BOLT是橋接中心化服務到區塊鏈的最佳選擇。

1. 簡介

本白皮書先介紹當今區塊鏈的問題、瓶頸，再導出BOLT的源由、規劃、架構、及生態。BOLT為一支援無速度、無數量限制的去中心化系統技術：以鏈下運作的密碼學協定和海量交易打包上鏈技術，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、交易成本高且不即時、及隱私不受保護的問題，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。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。

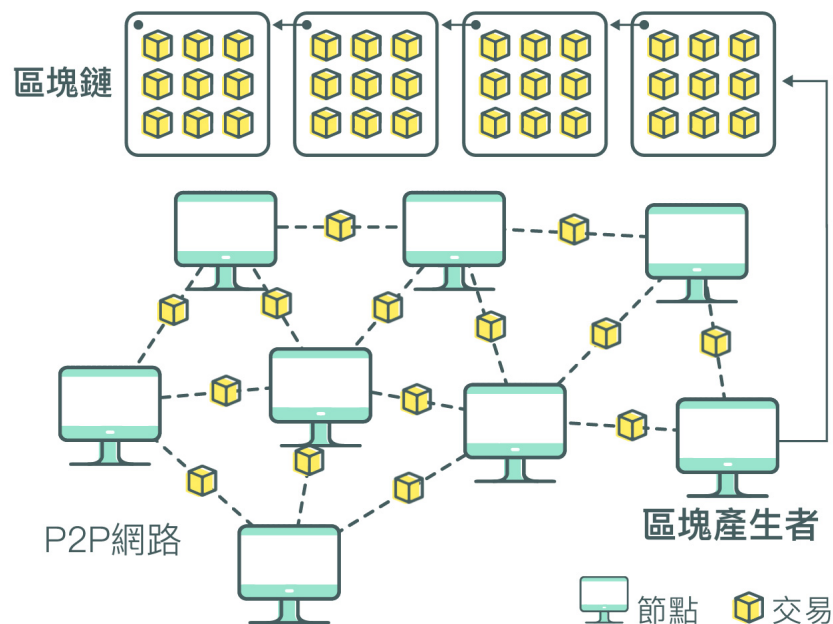


圖1：傳統共識決區塊鏈運作圖

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 Producer⁵)，然後區塊產生者將經由P2P (Peer-to-Peer⁶) 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。

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，必須依靠其用戶群進行資訊交流。

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。

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70GB¹³，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：隱私權缺乏

目前區塊鏈中的隱私保護，主要是使用類似洗錢的機制將加密貨幣交換的資訊隱藏起來。主要有兩種方式：(1)Cryptography accumulator：被Zerocoin使用；(2)CoinJoin：被SharedCoins, Dark Wallet, CoinShuffle, PrivateSend feature of Dash，及 JoinMarket 等使用。檢視由區塊鏈中記錄的交易資料，無法得知接收者的加密貨幣是由那個匯款者來的。

¹⁰ 如微軟和 Intel 推出的 Cocco 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。

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>。

以上兩種方式的使用受限於加密貨幣交換，所以無法應用於除了加密貨幣交換以外的廣泛性交易或合約。當今以太坊的智能合約大受歡迎，就是因為除了加密貨幣交換外還可以處理廣泛性的交易或合約，如各式資產交易、權利授與、及合約、文件、資訊記錄等。非加密貨幣交換的智能合約無法用加密貨幣保護隱私權的技術，這讓系統使用的範圍受限。

1.5. 當前問題四：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問題：

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、多方交易錯綜複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

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-launch-bitcoin-payments/>。

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

¹⁹ Line：<https://www.pixpo.net/fiance/OIHONwv7.html>。

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。

1.6. 當前問題五：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。

1.7. 問題總結

綜合以上現況，可以歸納出需要解決的問題如下：區塊鏈交易速度過慢，面對短時間大量數目交易時，要怎麼處理？大量交易記錄至入區塊鏈，如何解決區塊鏈資料過於巨大的問題呢？交易成本高且不即時該怎麼解決呢？非加密貨幣的交易紀錄寫入區塊鏈的同時，應該如何保障相關人的隱



私呢？在分工的商業現實環境下，中間人（或代理人）難以取代，卻又容易成為數位資產發行商與消費者間的一道牆，如何保有中間人，並提供透明可靠且可稽核的消費記錄？

以上問題彼此之間十分相關，比如若能將區塊鏈的交易頻寬大幅提昇，區塊鏈資料過於巨大的問題似乎勢必發生，因為區塊鏈中大量紀錄交易，會使得內存資料量過大。如果能讓交易相關人的隱私得以保全，相關交易的資訊無法被他人得知，則中間人作假的問題很可能就更嚴重。本白皮書提出的技術架構，將徹底解決此問題，請見第2節。

2. 技術核心

本節中，我們將先說明BOLT的運作模式，然後討論為何第1.7節中所總結的問題可以被解決。

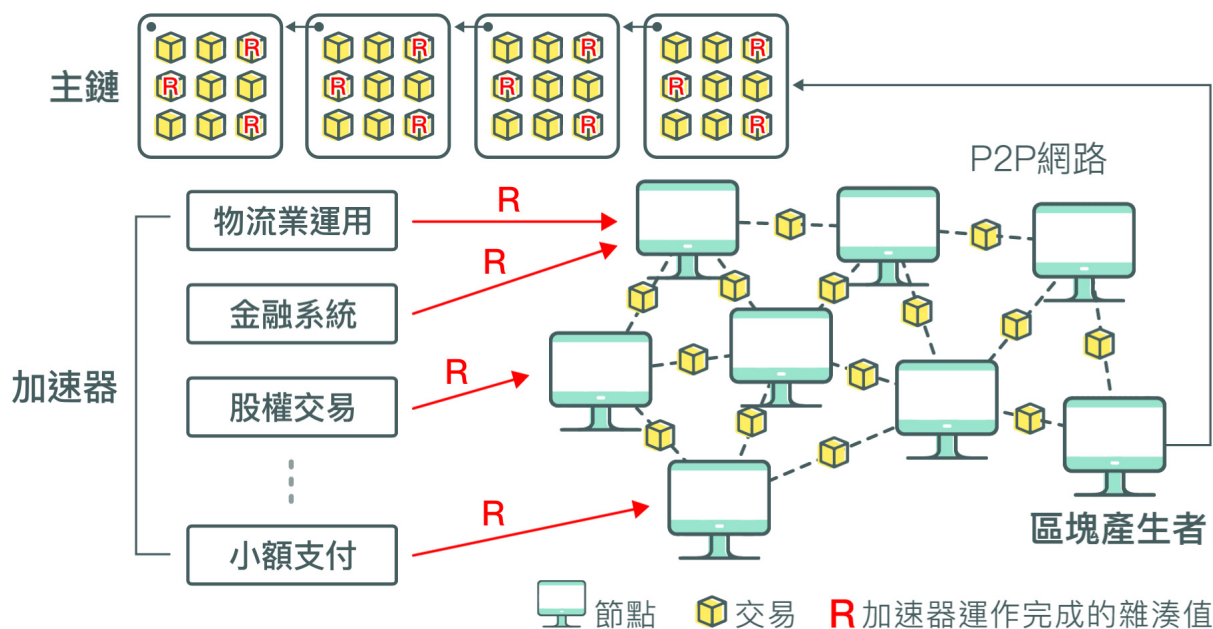


圖2：BOLT運作架構圖

BOLT架構的運作模式如圖2是由主鏈及多個**加速器（Booster）**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加速器運作，最後產生交易的雜湊值送給P2P網路中的節點，固定到主鏈。加速器的運作高速，一段時間後累積大量數目的交易，由負責加速器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BOLT架構有『一般節點』（以下稱為節點）及『稽核節點』來負責主鏈及加速器的去中心化運作。

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BOLT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²⁰、²¹，主鏈、側鏈間先進行資產轉換後，在側鏈進行交易，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-

²⁰ A SIMPLE EXPLANATION OF BITCOIN "SIDECHAINS" <https://gendai.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/>

²¹ How Two New Sidechains Proposals Could Change Bitcoin's DNA <https://www.coindesk.com/two-new-sidechains-proposals-change-bitcoins-dna/>

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。

BOLT採代理人類型（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，下層的加速器需要時可以隨時產生，數目無限制，非常適用來解決現實場景與區塊鏈介接的問題。在BOLT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。BOLT的運作中，主鏈的一致性使用公有鏈的全球共識，而加速器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由加速器的密碼安全協定維護。相關專利詳見第四節。下表將BOLT和公有鏈、私有鏈做一比較：

| | 公有鏈 | 私有鏈 | BOLT |
|--------|-------------------|-------------|---------------------------|
| 節點數 | 沒有限制 (現在約 20K) | 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 + 加速器) |
| 區塊鏈膨脹 | 有 | 無 | 無 |
| 隱私 | 無 | 有 | 有 |

在此版的白皮書中，我們提出三種BOLT加速器，第一種是用在區塊鏈上記錄一般型的資料，第二種是加速區鏈上的金流支付，第三種適用於智能合約運作的加速。以下我們一一說明。

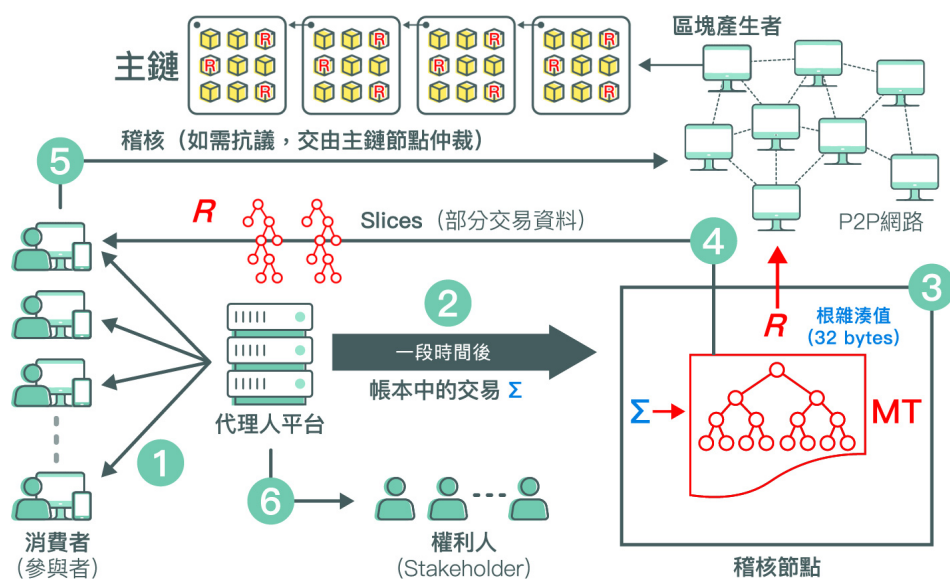


圖3：BOLT帳本加速器運作圖

2.1.1 BOLT帳本加速器²²

BOLT的帳本加速器的運作基於分散式稽核專利²³請見圖3。依照以下的步驟可以完成某加速器之一個階段 (Stage) 的運作：

Step (1)：負責發起加速器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 Σ 傳送給稽核節點。

Step (3)：稽核節點將交易 Σ 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 ²⁴。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：

²² BOLT帳本加速器已經發布在Github上，<https://github.com/BOLT-Protocol>。

²³ 發明名稱：分散式金流交易稽核協定（Protocol for Distributed Auditing of Payment Flow），此為BOLT研發團隊擁有的國際專利。此研究成果發表於ICBC 2018，詳見論文『InfiniteChain: A Multi-chain Architecture with Distributed Auditing of Sidechains for Public Blockchains. Gwan-Hwan Hwang, Po-Han Chen, Chun-Hao Lu, Chun Chiu, Hsuan-Cheng Lin, and An-Jie Jheng. Accepted for publication in 2018 International Conference on Blockchain, June 25 - June 30, 2018, Seattle, USA.』

²⁴ 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。詳見論文『Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems. Gwan-Hwan Hwang and Hung-Fu Chen. Published in the 9th IEEE International Conference on Cloud Computing (IEEE Cloud 2016), June 27 - July 2, 2016, San Francisco, USA.』之Table II。此論文申請專利發明名稱：一種即時稽核的雲端存取方法（Method for Auditing Cloud Access in Real Time），為BOLT研發團隊擁有的國際專利。

- 根據取得的根雜湊值R，請求稽核節點送回自己交易的slices²⁵，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²⁶。

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。

加速器運作所產生交易的正確性，由全體參與者維護。代理人預先在此加速器的合約上放入押金，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加速器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。

帳本加速器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加速器，才可滿足此類應用的需求。

2.1.2 BOLT金流加速器

BOLT的金流加速器（Crypto-payment booster）的結構如圖4，由一個發佈在主鏈的合約（以下稱為加速器合約）來控制及記錄參與者在加速器的金流交換，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，一個合約對應一個加速器。根據需求可

²⁵ 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。

²⁶ 每個交易的稽核可以在1ms內完成。

以隨時發起一個BOLT的金流加速器。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BOLT金流加速器。

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

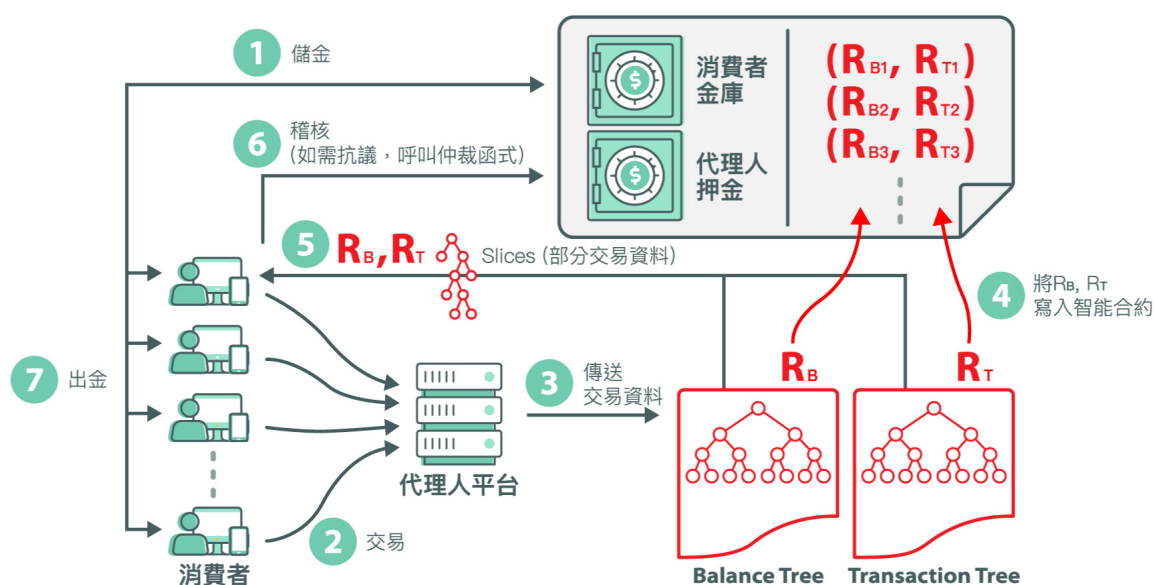


圖4：BOLT之金流加速器運作圖

代理人要負責維護消費者在加速器的交易記錄、Balance tree、及Receipt tree (或稱Transaction 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加速器者的由加速器合約匯入加速器加密貨幣或代幣的使用餘額，以參與者的ID為索引，存到Balance tree中。參與者將加速器中的加密貨幣或代幣轉給其他參與者或是將加速器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3中帳本加速器的索引模克樹的功能類似。

BOLT的金流加速器一個階段的運作和帳本加速器的運作大致類似（見2.1.1節Step(1)-(6)）及圖3，也是由負責發起加速器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、合約和加速器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²⁷，請參考附件C。因為每個交易的回條（ $T_{receipt}$ ）都包含一個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。所以足夠讓稽核出代理人有發生錯誤時，能產生足夠小的密碼學證據送回合約進行Fraud proof。

2.1.3 BOLT智能合約加速器

區塊鏈的應用除了一般的上鏈記錄及加密貨幣交換，智能合約的執行也是重要的需求。一個智能合約主要有兩個重要的部分：（1）儲存的合約變數；（2）定義的合約函式。合約函式的執行可以造成合約變數的狀態改變，基本上由主鏈的礦工執行，一次執行一個合約函式。

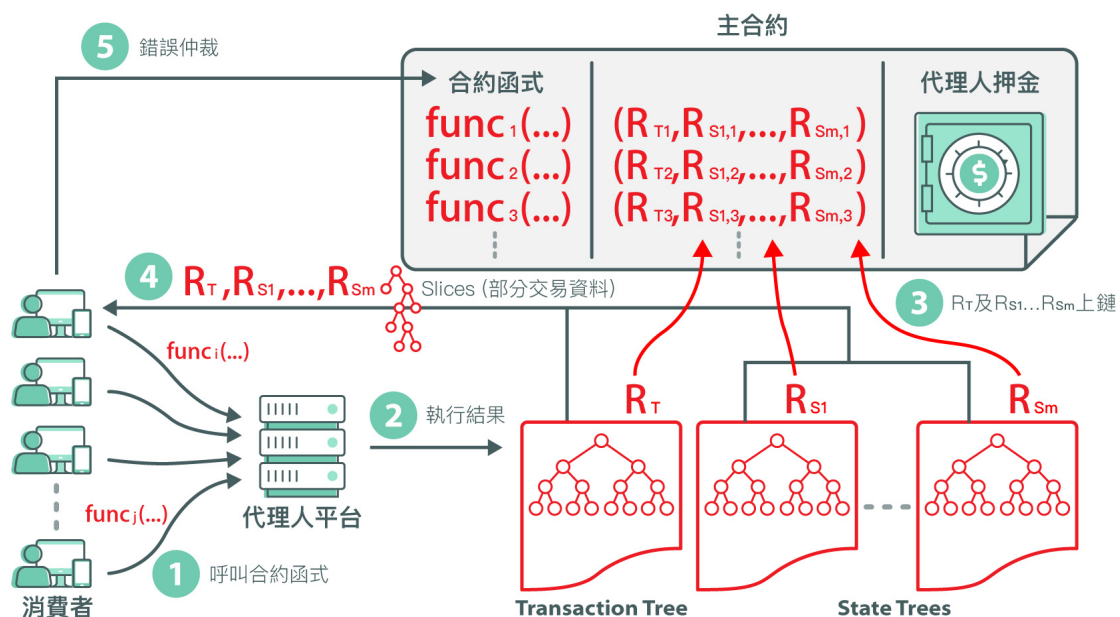



圖5：BOLT之智能合約加速器運作圖

BOLT智能合約加速器（Smart contract booster）基本上是crypto-payment booster的功能擴充，見圖5。可以被執行的合約函式及其相對的驗證函式都預先被定義在主合約中，同時公告發佈。參與者傳送簽章過的訊息，要求代理人執行。代理人於鏈下執行，並將參與者要求執行的合約函式及其

²⁷ 發明名稱：分散式金流交易稽核協定（Protocol for Distributed Auditing of Payment Flow），此為BOLT研發團隊擁有的國際專利。



參數及合約執行造成的狀態改變放入交易的回條並放入Transaction tree中，同時合約變數的狀態在State tree中儲存。Transaction tree及State tree都是索引模克樹。

階段結束後代理人最後將Balance tree及State trees的根雜湊值放到合約中，然後所有參與者負責稽核自己的合約函式執行是否被正確的放在Transaction trees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State tree中的合約函式狀態轉換是否正確。在稽核出代理人有發生錯誤時，產生密碼學證據送回合約進行Fraud proof。

3. 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BOLT加速器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BOLT加速器架構，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。

BOLT加速器可以支援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BOLT的帳本加速器，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BOLT的架構，我們可以在加速器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。BOLT加速器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。

BOLT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BOLT金流加速器來實作類似系統，將可以實現加密貨幣微支付及高速交易所。

4. 發展現況及合作項目

BOLT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) 。

BOLT首先已以太坊主鏈的加速為標的，系統實作部分已完成BOLT SDK程式設計及運作測試。目前已和數個公司商談合作，茲羅列出一些，供讀者參考。

BOLT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BOLT帳本加速器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BOLT加速器技術，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。除了透過BOLT加速器來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。

日本手遊公司Auras計畫建立新產品，是以太坊上的合約遊戲，目前白皮書已經完成，正募資中。惟以太坊主鏈的頻寬不足，所以近期一直拜訪區塊鏈的技術公司，希望能解決此問題。經過瞭解BOLT加速器的技術及功能，決定付費取得BOLT三個加速器的使用授權，已和無窮鏈公司完成簽約。

K公司為一個Mobile APP的設計者，其APP使用者遍佈全球總數有數百萬人，近期已完成A輪融資。目前欲建立一個於以太坊上的版權登記及版權使用的支付系統，目前和BOLT團隊簽約，計畫先使用BOLT帳本加速器於以太坊對其客戶提供數位媒體版權登記系統，目標是使用BOLT金流加速器完成ERC20 token的即時版權使用支付系統。

C公司為一個服務政府教育部的IT公司，有許多教育部軟體專案的合約執行成功，今欲幫該國教育部建立公有鏈（以太坊）上區塊鏈學歷登記系統。即將簽約使用BOLT帳本加速器完成此專案，以啟動踏足區塊鏈相關專案的公司目標。

H公司計畫進軍基金相關的代買代賣及投資者撮合業務，成功通過該國監理沙盒(Regulatory Sandbox)的列管，成為該國金融新創業者。今欲將代買代賣及撮合交易登記於公有區塊鏈，給其投資人查閱，以建立其投資人對其公司資產保管的信任。第一步將簽約使用BOLT帳本加速器實作其公有區塊鏈系統，第二步會以BOLT金流加速器建立以ERC 20代幣為資產交換的撮合交易系統。

G公司一個是商業點數整合方案的先驅者，目前積極想利用以太坊ERC20代幣建立去中心化的商業點數平台，無奈以太坊主鏈的頻寬不足、確認時間不即時。即將簽約使用BOLT金流加速器完成此平台的設計。

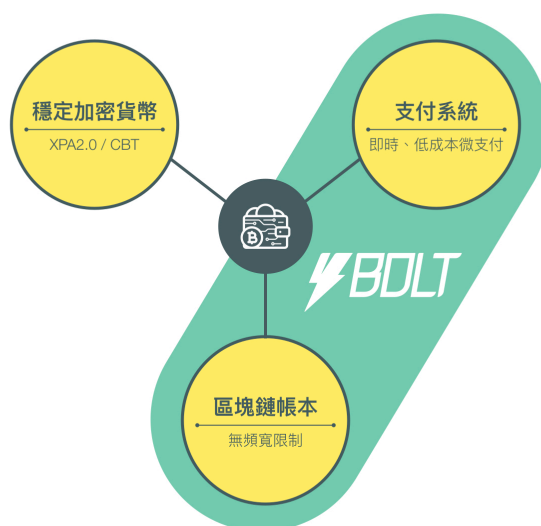
I公司是一個高端加密通訊APP的產品開發商，其APP可以配合藍芽溝通的橢圓曲線硬體卡片來進行電子簽章及加密。目前顧客詢問是否同將其產品整合區塊鏈支付的功能，除了一般區塊鏈錢包的主鏈轉錢功能，該公司期待能於其產品中提供高速、低成本的支付系統，正在商談使用BOLT金流加速器完成此功能的設計。

尚有數個公司洽談中，篇幅有限，不一一揭露。

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，第一節提出的一些現今公有區塊鏈問題，任何一個項目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。BOLT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。



BOLT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BOLT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：

$$\text{每秒交易速度} = (\text{平均每秒產生的區塊數}) \times (\text{平均每個區塊中的交易數})$$

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²⁸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²⁹。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。

²⁸ 以防止Double spending或非法交易。

²⁹ 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 BOLT加速器隱私權保護技術

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³⁰。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³¹；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³²，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。

³⁰ 解不出的交易為其他數位資產提供人的相關交易。

³¹ 此運算時間還未加上於索引莫克樹上的traversal 花費時間。

³² 執行公布的開源程式。

附錄C BOLT金流加速器合約及運作協定

BOLT金流加速器的結構如圖6，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。一個金流加速器由一個召集人擔任代理人發起，對應一個合約及一個加速器。根據需求可以隨時發起一個BOLT金流加速器。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BOLT金流加速器。

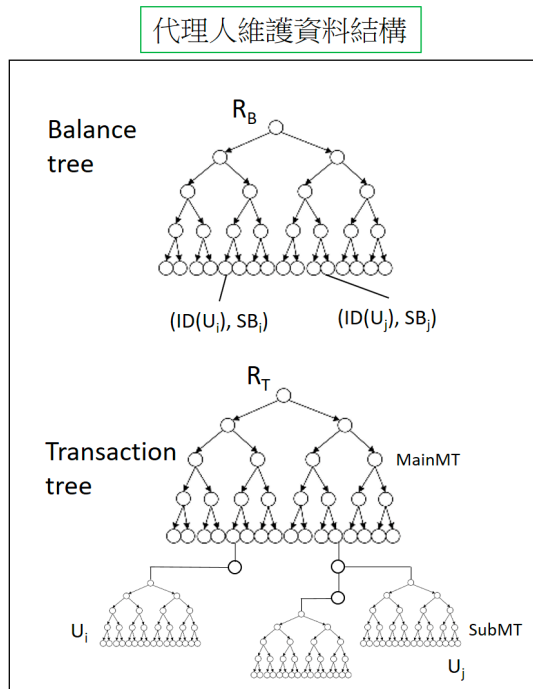
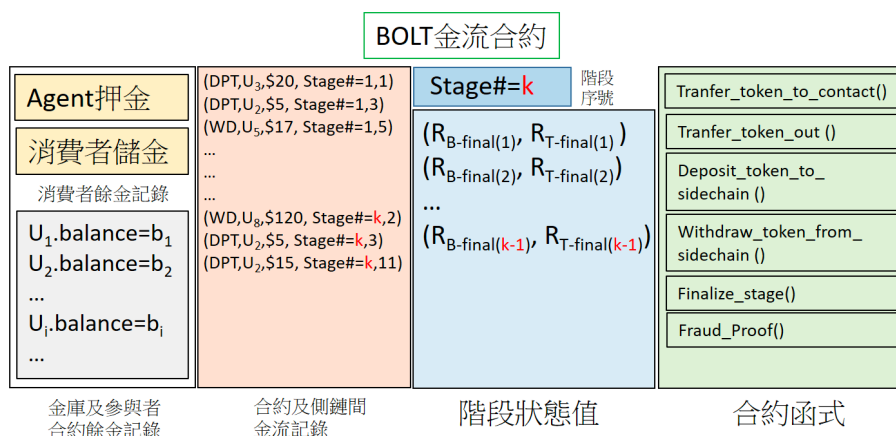


圖6：BOLT金流加速器運作圖

使用者隨時可以將加密貨幣或代幣³³存入合約（以下簡稱token），也可以提領出來。但是存入加速器合約的加密貨幣或代幣若流入加速器中交換，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。

³³ Token表示主鏈中共識決認可的有價加密貨幣。

見圖6，『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。加速器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加速器的交易記錄、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 為加速器參與者的地址、 a_i_bal 為 a_i 存入加速器Tokens的使用餘額。以加速器參與者的 a_i_adr 為索引，存到Balance tree中。參與者將加速器中的Tokens轉給加速器中其他參與者或是將加速器中的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6。MainMT為一索引模克樹，以加速器參與者的 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: 將自己加速器上的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加速器的Balance tree。
- Instant withdraw transaction: 將自己加速器的Balance tree上記錄的儲金小額且快速的移到主鏈地址。
- Withdraw transaction: 將自己加速器的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要將在加速器的Token轉X個單位給a_j)

- Step 1: 加速器參與者a_i將交易需求 $T_{rmit} = ((\text{Remittance}, \text{LSN}, a_i_adr, a_j_adr, X, SH), \text{SIG}_{PK(a_i)})$ 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_balance)。
- Step 3: 代理人將 $T_{receipt} = ((T_{rmit}, \text{Sender_balance}, \text{Receiver_balance}, \text{GSN}), \text{SIG}_{PK(\text{Agent})})$ 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 (加速器參與者a_i提出存幣申請X個單位的token移到加速器)

- Step 1: 加速器參與者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 $T_{receipt} = ((DPT, \text{LSN}, SH, a_i_adr, \text{Balance}, \text{GSN}), \text{SIG}_{PK(\text{Agent})})$ ，將 $T_{receipt}$ 傳給參與者a_i，並將其放入Receipt tree。

Instant Withdraw 交易協定 (加速器參與人a_i經由代理人將加速器 X個的tokens立即轉移到主鏈 帳戶address)

- Step 1: a_i將交易需求 $T_{InstantWithdraw} = ((WD, \text{LSN}, a_i_adr, X, SH), \text{SIG}_{PK(a_i)})$ 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 $T_{receipt} = ((T_{InstantWithdraw}, \text{Balance}, \text{GSN}), \text{SIG}_{PK(\text{Agent})})$ 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（加速器參與人 a_i 經由合約將加速器 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`Treceipt = ((WD, LSN, SH, a_i_adr , Balance, GSN), SIGPK(Agent))`，並呼叫`confirmWithdraw(Treceipt)`，log被改成`[WD, a_i_adr , X , SH, LSN, BKH, Granted]`，同時觸發合約事件將`Treceipt`回傳給加速器參與人 a_i 。
- Step 5: a_i 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]`。

加速器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 $R_{RTree}(k, init)$ ³⁴。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：

$$R_{BT}(k, init) \rightarrow R_{BT}(k, 1) \rightarrow R_{BT}(k, 2) \rightarrow R_{BT}(k, 3) \rightarrow \dots \rightarrow R_{BT}(k, final)$$

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 $R_{BT}(k, final)$ 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等交易協定使整個加速器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。以下說明加速器的挑戰機制。

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的帳本加速器，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

³⁴ 此為一個沒有任何`Treceipt`的Receipt tree。

核：

- 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 $R_{Tree}(k, final)$ 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。

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

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開始時於此加速器的餘額，假設這個Stage中參與者在加速器裡產生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 $R_{Tree}(k, final)$ 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BOLT金流加速器的安全協定架構，實際詳細協定及各式挑戰、自清的細節，請參考BOLT金流加速器白皮書。