BOLT

去中心化存證與應用平台

White Paper

v2.0.11 20230103

目錄

摘要

實現去中心式存證技術與稽核平台

隨著技術發展，我們有作為數位黃金般乘載價值的區塊鏈；也有作為雲端平台般承載服務的區塊鏈；Bolt 則是為了讓所有中心式服務擁抱開放式監管，設計作為乘載公信的區塊鏈技術。以鏈下壓縮資料、零揭露證明、分散式稽核、PoHCE 跨鏈證據之機制，實現兼顧隱私與公信的區塊鏈證據保存與稽核。

為了幫助區塊鏈系統與現有中心化應用場景融合，與加速推動區塊鏈應用落地，Bolt 發展出多項通用功能模組，運用模組化功能的易擴充性、易於接入的平台化服務介面，更容易與現有企業系統整合，創造適用於不同領域之解決方案，有效降低企業、開發者使用區塊鏈技術門檻。

本白皮書在應用案例章節列舉了商品防偽認證、產銷環節追訴、數位資產管理與儲備證明等應用場景，提供企業快速技術導入。Bolt 跨鏈架構不但實現更快速的且低成本的交易、注重數據隱私保障，同時能幫助項目方兼顧商業機密的場景下配合公共監管，打造出公部門與平台間、平台與用戶間、用戶與用戶間皆能彼此信任的應用生態系。

最後介紹了 Bolt 的通證經濟模型 – Bolt 的應用與發行計畫，說明未來如何透過 Bolt 的發行與運用，逐步發展實現 Bolt 之項目願景。

1

背景介紹

Bolt 推出的時期正值加密貨幣的雷曼時刻，數間龐大加密貨幣交易所沒有落實企業保管責任，挪用用戶資產並倒閉，造成廣大用戶的損失。我們觀察到區塊鏈相關產業的服務極度相似金融產業，但又不同於傳統金融產業受到大量的政府法規監管，在缺乏監督以及高額產值的誘惑下不停重現金融歷史曾發生的各種弊案。

Bolt 的設計理念期望使用特殊的驗證機制建立一個能保障隱私的公信平台，鼓勵各種中心式與去中心式服務在區塊鏈上提供各項數據供市場檢驗，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. 項目願景

突破區塊鏈既有限制，落實彼此信任之網路應用生態。

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。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。

然而當服務轉換為去中心化運作模式後，許多資訊無法受到公眾的檢視與監管，各種系統性與人因風險便隨之發生。以數位產品代理銷售為例，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。

另一方面，隨著更多的區塊鏈平台發展出來，並進入到各行業應用領域，如何避免異質區塊鏈間的閉鎖性阻礙創新應用，與協助跨鏈間的價值流通、建立跨鏈之間的可信任共識，也成為我們實現平等網路應用生態的必經關卡。因此，若有方法可突破上述限制，並與現有中心化系統良好地融合，能大大增加區塊鏈的應用價值，最終實現去中心化網路資訊平等的終極目標。如此我們才能真正迎來能彼此信任、安全又高效的網路應用生態。

1.2. Bolt 設計理念

Bolt 作為一新型公鏈，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，希望提出創新、高效運作、跨鏈連結的方法，建立無速度限制、高擴展性、受信任的去中心化架構，同時解決傳統區塊鏈的以下問題：

- 區塊鏈頻寬與承載空間不足
- 隱私權保護不足
- 異質區塊鏈間價值交換困難
- 難以和現有中心化應用融合，行業應用場景受限

Bolt 在架構設計上將以和主流公鏈平行的跨鏈模式，建立無速度限制、高瞬間交易量、更受信任的去中心化架構，此新型架構須具備以下優勢：

- 無交易速限：和主流公鏈平行的聯合運作模式，可達百萬級 TPS (每秒交易)。
- 確保交易隱私：在完成交易的過程中，確保消費者和數位資產擁有者之隱私。
- 跨鏈價值交換：在不同區塊鏈系統中能進行介接，並實現跨鏈資產轉換。
- 能與現有中心化商業場景融合：結合中心化代理人模式，同時保有去中心化資訊對等的價值。

我們提出的技術，將能有效的將實體資產對應至區塊鏈上，並永久詳細記載其包含所有權變化的歷史過程。在不遠的未來，將區塊鏈技術與 IoT 技術整合後可以經由智能合約對硬體進行管控，實現如智能租賃的應用，還可結合能將資產授權託管 AI 之技術，創造更高效的投資應用、自動化工程應用。

2

解決方案

為實現上述願景，我們提出多項技術支持

Bolt 發展，並同時提供多項即用的

服務模組，作為快速導入的解決方案：

2.1. 高速通訊協議

Bolt 使用特殊的通訊協議模式 Locutus，節點之間會定期根據共識定義出一張所有節點都可以互相連線的通訊樹狀網路 Borg-Tree。在這份網路中，從任何節點發出的資訊都會有一個最快速的傳遞模式，快速散佈至所有節點中。

2.2. 序列化壓縮存證技術

為了達到全球共識，Bolt 被設計成可以在陌生的節點與節點之間協同運行，且不需要中心化的伺服器控管權限，以區塊鏈上的智能合約來公布其運作協定。參與者在 Bolt 取得協定，遵循被公布的協定運作。

2.3. 即用服務模組

Bolt 的一大目標是打造企業級應用區塊鏈基礎設施，考量目前區塊鏈面對企業級場景的挑戰，如性能、通用性、擴展性、安全與可監管等，更重要的是易於理解和接入既有中心化資訊管理系統。歷經不斷的嘗試與挑戰，我們發展出平台化的服務架構。

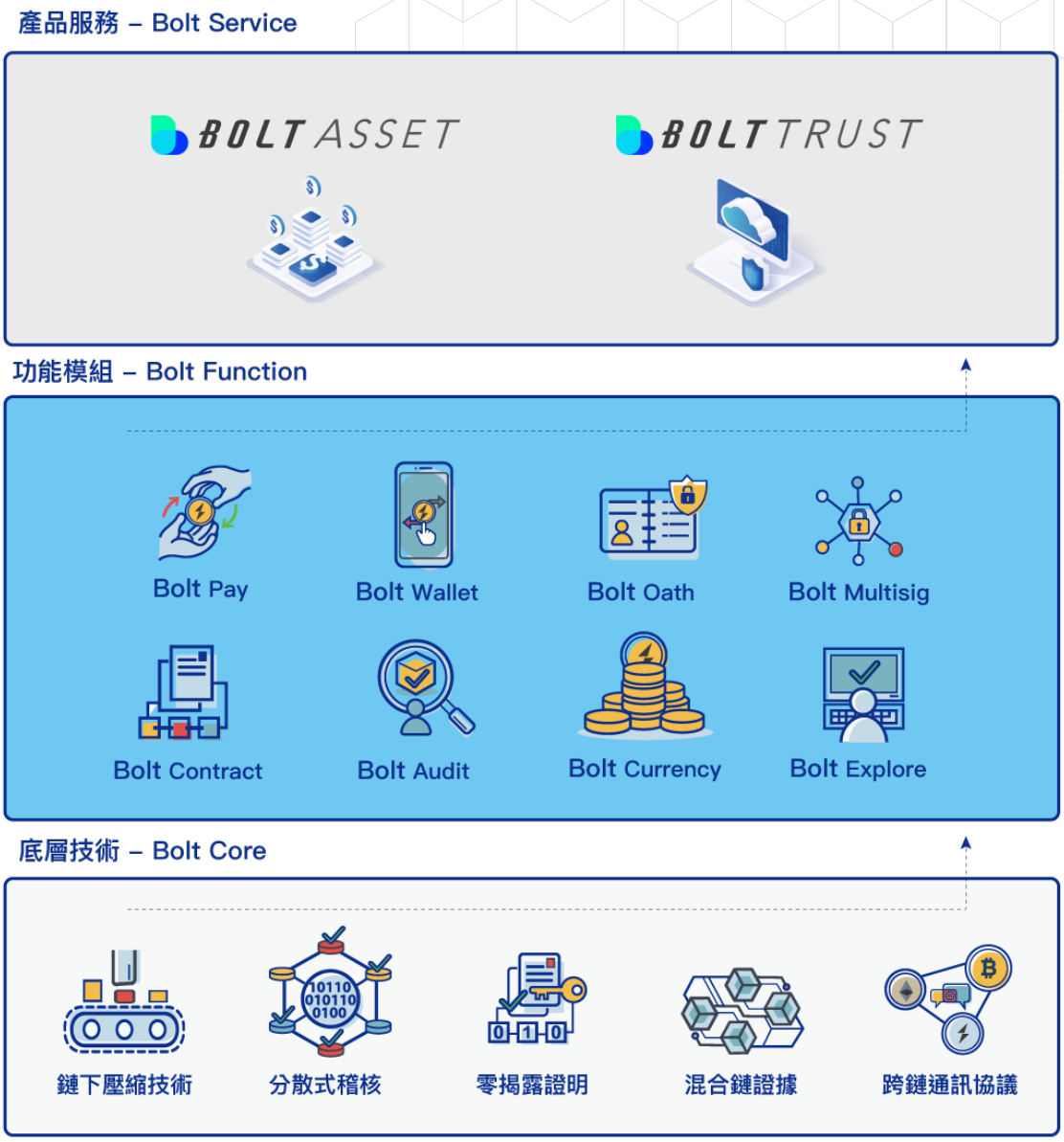


圖 2、Bolt 平台化服務架構圖

Bolt 平台化架構分為 Bolt Core（底層技術）、Bolt Function（功能模組）、Bolt Service（產品服務）三層架構。

底層技術 – Bolt Core

整個核心引擎以鏈下壓縮技術、分散式稽核、零揭露證明與混合鏈證據等技術為基礎，解決性能、安全、擴展等基礎和關鍵技術問題，建立創新的技術架構與應用。

功能模組 – Bolt Function

基於企業應用多樣性與複雜性，將基本需求模組化，可以帶來更好的擴展性，同時保證 BoltCHIAN 的核心邏輯穩定，達到低耦合高內聚。目前提供下列模組：

- **Bolt Pay 支付模組**

  數字貨幣支付功能，支援即時支付、即時到帳，用戶間可免手續費。

- **Bolt Wallet 錢包模組**

  管理多種數字貨幣，提供一個資產儲存、管理交易和兌換機制的錢包。

- **Bolt OAuth 身份認證與權限管理模組**

  提供便於外部系統與 Bolt 之間的的功能整合介面，可透過 API 密鑰映射角色權限與存取管控，並將操作轉譯為 Bolt 上的交易格式。

- **Bolt Multisig 多重簽署模組**

  支援多重簽署管理與驗證，並負責將用戶私鑰碎片化保管。

- **Bolt Currency 通證化模組**

  貨幣發行功能，透過智能合約支援各類資產的通證化。

- **Bolt Explore 帳本查詢模組**

  提供主鏈上帳本資料查詢，並顯示各筆交易於其他公鏈存證位址。

- **Bolt Contract 智能合約管理模組**

  合約註冊發行以及合約觸發和執行，用戶可依照自己商務邏輯開發合約。

- **Bolt Audit 稽核模組**

  可配合審計的服務，提供事後查核鏈上與鏈下證據，讓信任機制更完善。

產品服務 – Bolt Service

基於Bolt Function，我們已發展出兩種產品化服務，透過提供完善的 RESTful API 形式，提供企業用戶整合現有軟體服務或是中心化系統。

- **Bolt Trust 資料信任服務**

企業可將任何需要保存資訊放至多個公鏈存證，並可獲頒證書，提供使用者查詢與瀏覽，同時這些上鏈資訊經過壓縮與加密，讓安全與隱私性獲得保障。(詳細說明於5.1)

- **Bolt Asset 數位資產管理服務**

價值交換是區塊鏈的特性之一，Bolt Asset 可將資產數位化，轉換成區塊鏈的唯一資產，讓這資產的移轉、授權、取用都可以更安全簡單，並且可追溯。(詳細說明於5.2)

具備上述三層的基礎架構，企業可以快速且容易地透過服務介面與 Bolt 系統整合，建構出適用於企業的各種區塊鏈應用場景，目前我們已經與多家企業合作，分別導入應用區塊鏈技術的企業專屬解決方案。

3

核心技術

本節中，我們將先簡介 Bolt 可跨鏈的基本技術架構(圖3)，並依序介紹各層核心技術。Bolt 是以類似 Layer 2 protocal 機制，將所有於 Bolt 上的交易交易透過壓縮形成加密雜湊證據，再通過跨鏈協議將交易同步到 Ethereum、Bitcoin 等公鏈。因此 Bolt 支援的其他區塊鏈資產如 Ethereum、Bitcoin 都可以移轉到 Bolt 上運行，且在交易速度、延展性都有顯著的提升，同時因交易證據保留於其他區塊鏈的機制也讓 Bolt 本身的不可篡改特性大幅提升。

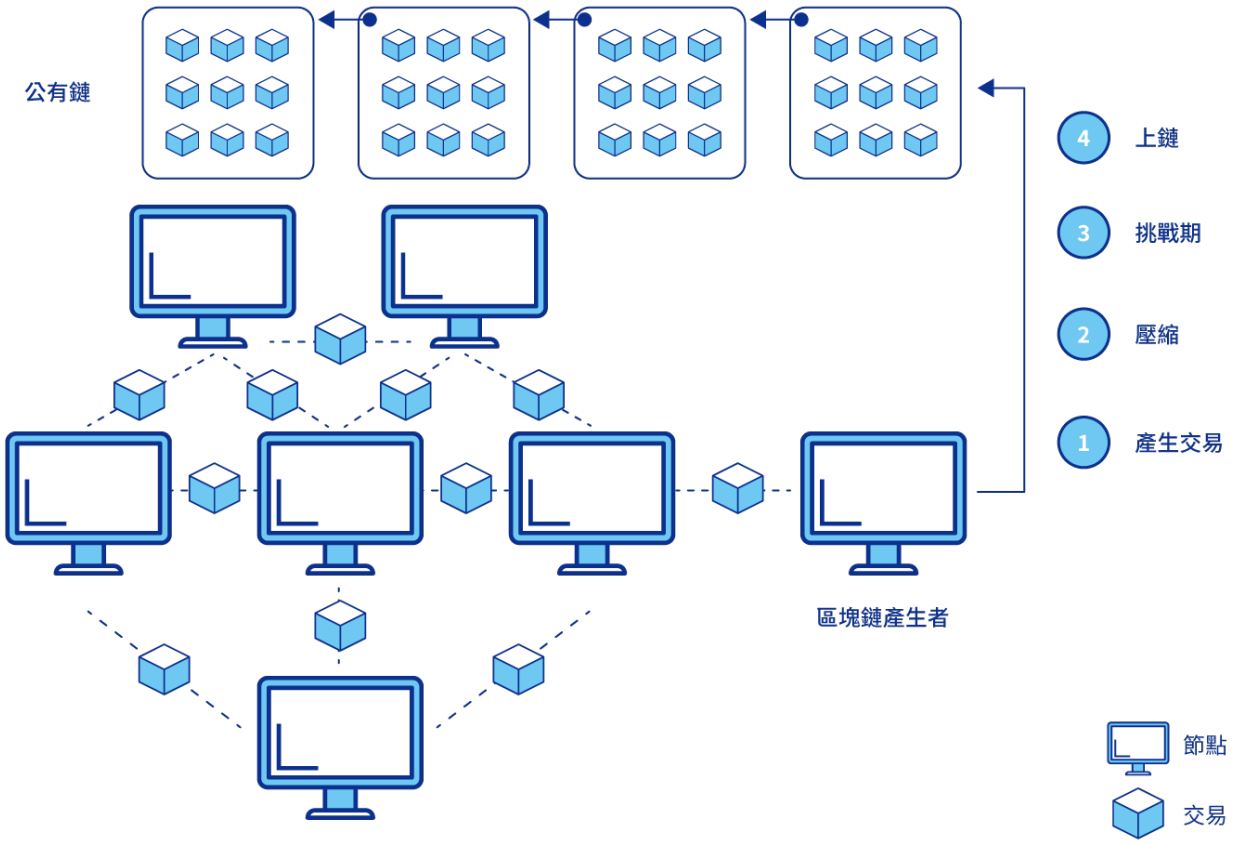
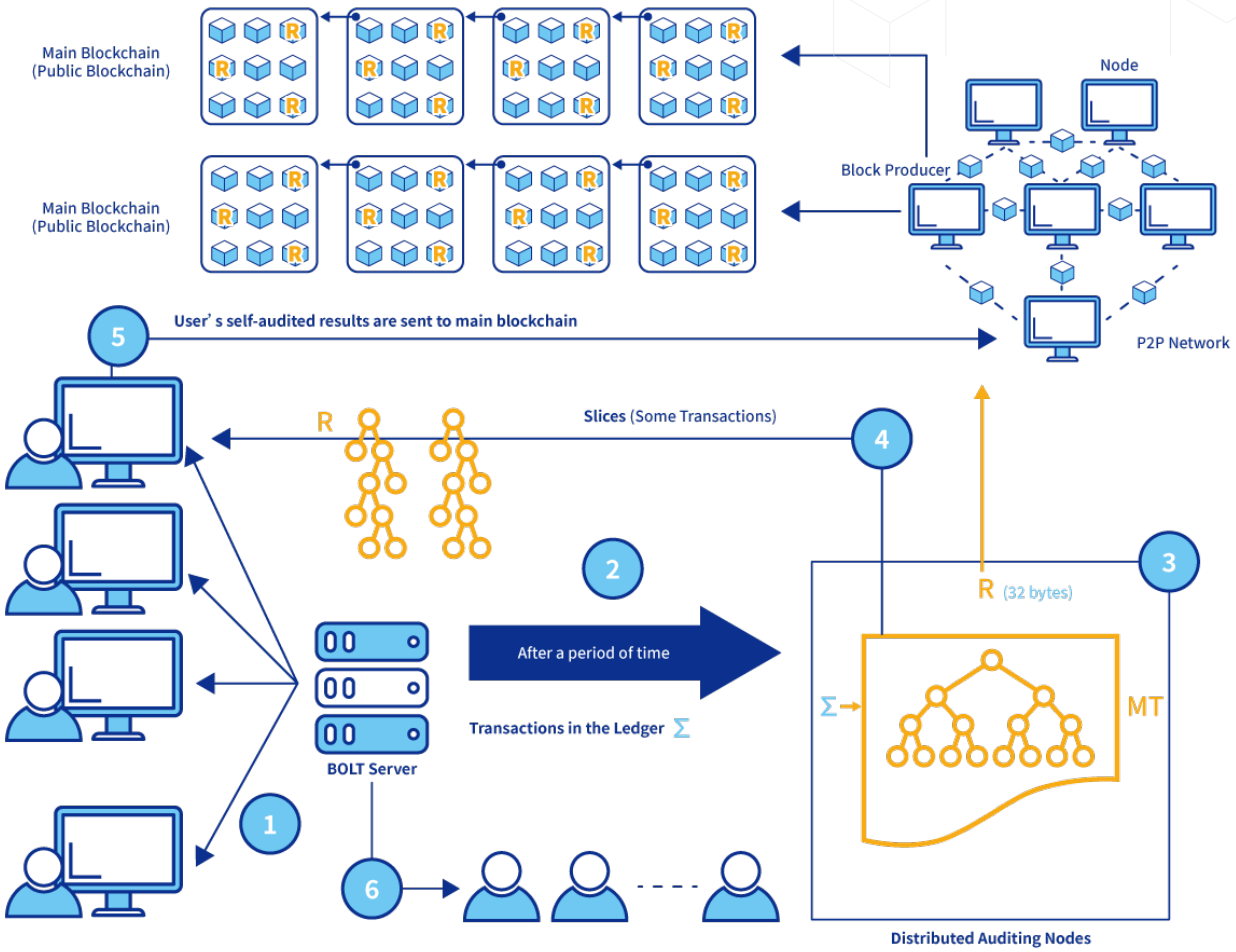


圖 3、Bolt跨鏈區塊鏈運作圖

3.1. 跨鏈協議 (Cross-chain channel)

Bolt 的跨鏈區塊鏈架構如圖4所示。所謂跨鏈就是多條平行的區塊鏈（Paralle Blockchain）之間組成的聯合運作模式。一般的區塊鏈交易，如加密貨幣交易或單一合約紀錄，用戶會直接將交易資訊送到該區塊鏈的 P2P 網路中，最後由成為區塊產生者的節點來固定到主鏈上，這樣的交易受限於該區塊鏈的特性，可能會帶來較高的



交易成本以及較慢的交易速度。因此當需要進行大量且高速交易時可以將交易送至 Bolt 上執行，Bolt 的運作高速，一段時間後累積大量數目的交易，由 Bolt 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，透過跨鏈協議固定在其他公有鏈。整個 Bolt 的跨鏈區塊鏈架構有『一般節點』（以下稱為節點）及『稽核節點』來組成整體系統的去中心化運作。

Bolt 採取多層次架構（Hierachy-Based），將共識系統中的一致性交由最上層主鏈來達成，而各自應用的交易有效性則是下層的資料結構來實現，而這些下層的側鏈（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 Bolt 所提供的特性中，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 的多鏈運作中，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 Bolt 所設計的側鏈運作，包含分散式稽核功能[1]。

圖 4、Bolt側鏈運作圖

側鏈運作由行業運用自行發起（如交易代理人平台、專業中介、投資銀行、證券公司、審計師、評估師、律師、衍生工具發行商等）按業務分類自行管理及營運不同的側鏈，並進行市場及業務推廣。側鏈需要定期將訊息同步到主鏈，避免側鏈訊息造假或者數據被竄改。主鏈和許多側鏈的運作並行，可以實現超過一千五百萬級TPS(每秒交易）。

依照以下的步驟可以完成一次側鏈的運作：

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，代理人將 Step (1) 中產生的交易Σ及需要支付分散式稽核的費用及押金 Token [2] 傳送給稽核節點。Token為加密貨幣，使用主鏈來傳送。

[1] 分散式稽核方法（Distributed Auditing Method），為 Bolt 確保混合鏈證據為安全且未經竄改之驗證機制。

[2] 押金亦可以先儲存於主鏈上。

Step（3）：稽核節點將交易Σ產生一個索引模克樹（Indexed Merkle Tree），稱為MT。同時產生MT的根雜湊值R[3]。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MT中：
根據取得的根雜湊值R，請求稽核節點送回自己交易的slices[4]，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MT的電子證據[5]。

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MT來稽核支付的權利金是否有誤。

跨鏈資產交換

基於跨鏈協議技術，Bolt 能提供另一項重要功能便是支援不同區塊鏈間的資產交換。Bolt 使用跨鏈通訊協議與 Layer 2 Protocol 將其他區塊鏈上的資產移轉至 Bolt

---

[3] 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。

[4] 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。

[5] 每個交易的稽核可以在1ms內完成。

系統運作，藉此達成多元區塊鏈價值流通。以 Ethereum 為例，用戶只需要將資產託管於 Bolt 於 Ethereum 建立的智能合約上，該資產便會在 Ethereum 上進行凍結，同時於 Bolt 產生相對應的資產，以進行低成本且高速的所有權移轉。藉由這項技術特色可以將 Bolt 作為一個資產交換的平台，將各種區塊鏈的資產移轉到此平台後進行各種轉換，如 ETH 兌換為 BTC，最後若有需要再將該資產移轉回其原生區塊鏈上進行處理，而這一系列操作過程中都受到區塊鏈技術完整的保障。

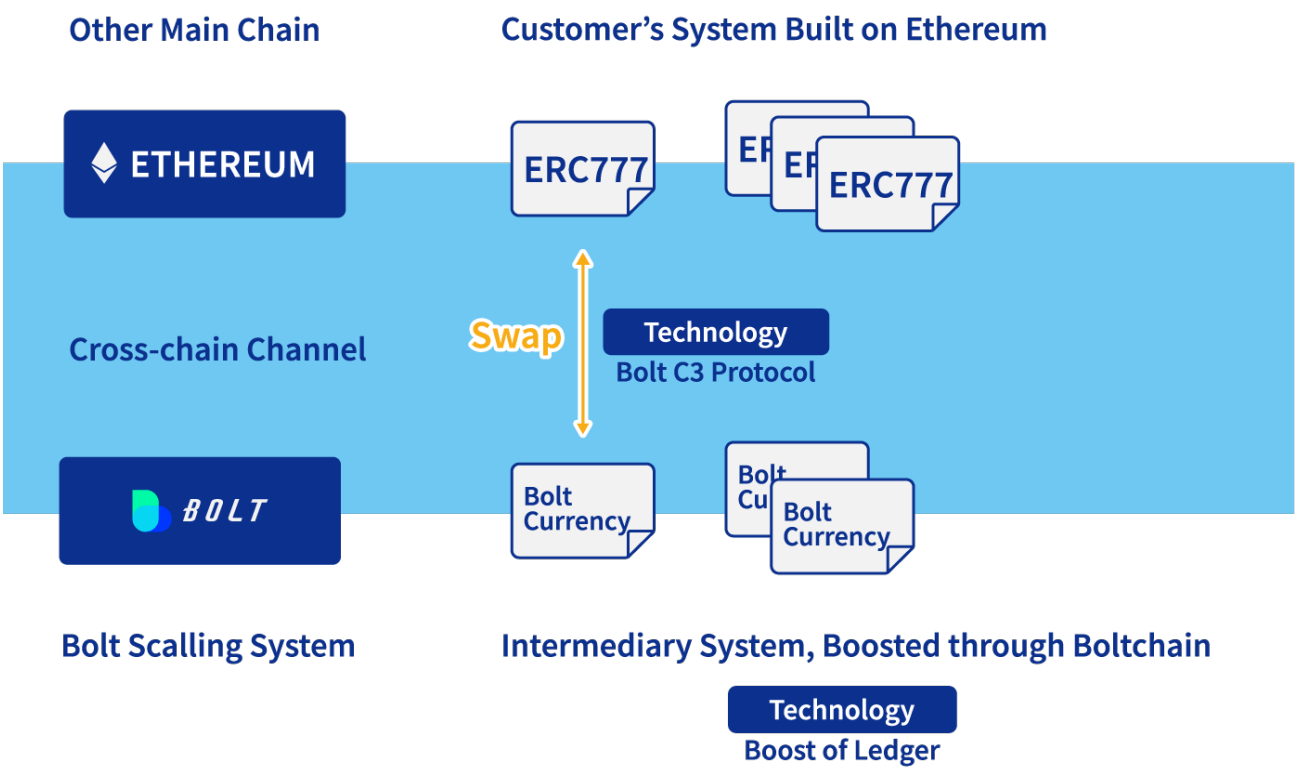


圖 5、Bolt 跨鏈資產交換示意圖

3.2. 鏈下壓縮技術

整個 Bolt 系統中會有很多的側鏈。每個側鏈進行不同的交易，通常是一個交易代理人負責的某個撮合服務的交易[6]。側鏈代理人處理的交易不用即時放上區塊鏈，最後將一個包含N個交易之帳本的根雜湊值放上區塊鏈時等同一次將N個交易放上區塊鏈，事實上將一個交易帳本的根雜湊值放上區塊鏈只佔用區塊鏈上一個交易的頻寬。如此可以幾乎無限的擴充區塊鏈的交易頻寬。每秒的交易數目不會受限於區塊鏈的限制，速度無限制，可達成『快速』的目標。

目前 Merialize 技術支持將一百萬個交易放在一個帳本中，分散式稽核可以在 100 milliseconds 以內完成一個其中交易的稽核，而且分散式稽核可以完全平行運作。以現存公有區塊鏈上每秒數十個交易的能力，可以輕易將一個區塊鏈的速度提升到每秒千萬個交易量。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）

×（平均每個Bolt帳本中包含的交易數）

以 Ethereum 作為上層主鏈為例，若其每秒交易量為10個，整個 Bolt 的每秒交易量＝10×1,000,000=10,000,000 TPS。可輕鬆達到每秒千萬的交易數。此技術將帶領區塊鏈進入另一個實用的境界。

[6] 如電子書販售、音樂販售、影片租閱、電子票卷販售、貨幣交換等。

3.3. 混合鏈證據

區塊鏈技術使用了分散式儲存的技術滿足其不可篡改的特性，在這樣的條件下每個節點除了會根據密碼學驗證其保存資料的正確性外，也會確認其承認的區塊是否與其他結點一致，因此即使單一節點被入侵並修改其資料也無法竄改區塊鏈上最終的結果。即便如此，當攻擊者的攻擊能力足夠強大，甚至可以同時入侵 51% 以上的節點時，區塊鏈的資料依舊會受到威脅。區塊鏈的交易資料隨著時間以及擴容方案的演進，其成長的速度愈來愈快，這個現象造成區塊鏈中有能力且願意保存完整交易資料的節點正在快速減少，加上 Sybil Attack 等攻擊技術的出現，使得區塊鏈上不可篡改的特性逐漸受到威脅。

Bolt 為了解決這個問題，研發了獨有的混和鏈證據技術（Hybrid-Chain Evidence，HCE），將 Bolt 上的證據使用上節鏈下壓縮技術壓縮為索引模克樹後，保存於包含 Bitcoin、Ethereum 等多條區塊鏈上，並將原始交易內容加密後保存於 IPFS 上，因此當攻擊者意圖竄改 Bolt 上的交易內容時，首先必須要同時篡改保存於區塊鏈上與 IPFS 的所有交易證據，其後再入侵 51% 以上的 Bolt 節點進行竄改，等同於攻擊者必須同時成功攻擊 Bitcoin、Ethereum、IPFS、Bolt 才有辦法實現其竄改目的，藉此極大幅提升其攻擊成本。

3.4. PoHCE 共識

在 Bolt 運作過程，如同其他的區塊鏈，每隔一段時間需要將鏈上交易證據進行封裝成一個區塊，並廣播至所有節點形成共識，由於 Bolt 使用了上節混和鏈證據（HCE）確保其不可篡改特性，因此結點間進行共識時需要仰賴比其他區塊鏈更加複雜的分工與處理，而所有參與整個 Bolt 共識過程的節點，根據其付出程度都能得到相對應的獎勵，下面條列出在 Bolt 共識機制中的節點角色與其負擔事項，每個節點可擔任多種不同的角色。

- **集群管理者**

在這個角色，節點有三項主要職責：維護節點成員清單、定期對成員進行評分並維護成員評價資訊、廣播與協調各項資訊，共識機制的通訊行為皆由此角色代理進行，同時也確保節點的評價必須達到一定程度才能執行特定角色。Bolt 使用改良後的 Raft 演算法管理集群，並在一致的節點名單下使用獨有的廣播演算法技術 Locutus 確保所有的協議能在最短的時間內完成。

- **區塊封裝者**

在這個角色，節點的主要職則便是將既有交易驗證後打包，再根據上述技術產生壓縮證據，節點之間根據證據確認彼此資料皆無誤便完成了封裝共識，其後便會繼續生成跨鏈證據，並將打包後的交易加密後上傳至 IPFS 上封存。

- **資料稽核者**

在這個角色，其需要在區塊封裝者完成工作後快速進行資料抽查，結點會根據演算法決定此區塊內自己所負責的稽核範圍，藉此在證據上傳至其他區塊鏈之前快速檢驗其都是正確無誤的，然後產生稽核共識。這個共識環節需要複雜的機制確保其即時性，詳細細節在下個章節會進行補充描述。

- **證據上鏈者**

擔任這個角色的節點會各自負責不同的區塊鏈，在達成稽核共識後，便將前面完成的跨鏈證據上傳到自身負責的區塊鏈上，同時也需要支出上鏈成本。

藉由這一系列的共識機制，除了可以確保攻擊者更加難以突破 Bolt 的保護，同時新節點的加入也只需要向其他區塊鏈及 IPFS 索取 Bolt 資料，讓系統整體的安全性極大幅度提升。

3.5.分散式稽核

承上節，在使用 PoHCE 共識機制後，驗證區塊與交易資料的行為變得更加複雜，同時又牽涉到需要與其他區塊鏈上的智能合約進行互動，時間成本也將大幅度的提升，因此我們需要一套機制將稽核作業進行分工，確保其不影響系統效能。

去中心化的系統，面對有代理人操作的運用，主要的問題是代理人是否將正確的交易記錄放上區塊鏈，Bolt 分散式稽核技術可以解決此問題。因為側鏈的代理人的運作還是經由分散式的方式來稽核，所以整個系統的依然維持去中心化的運作概念。關於先讓代理人處理一些交易，再放到區塊鏈來記錄，在早期比特幣發展期間有一些系統被提出，但是這些系統無法解決代理人黑箱作業的問題，這和區塊鏈去中心化的理念違背，因此無法被廣泛的接受。Bolt 的分散式稽核技術，已徹底解決此問題。

在側鏈運作中，所有交易都妥善儲存於索引莫克樹且其根雜湊值被公布後，參與者及數位資產提供人的某個交易可以經由索引函數立即定位出在索引莫克樹的那個底層節點。參與者要稽核自己的交易是否正確或是否有存在於交易帳本中，即對代理人提出某交易的稽核請求[7]，因為參與者本身有交易的序列號（此交易的完成有代理人的電子簽章，所以代理人不可否認），所以代理人必須呈現此交易的切片，消費者可以使用此帳本的根雜湊值及此交易的切片來驗證此交易是否正確或是否有存在於交易帳本中。

分散式稽核於側鏈運作和整個區塊鏈的生態系統結合，不僅區塊產生者有仲裁的能力，且因為產生區塊的工作及貢獻獲得加密貨幣的回饋，側鏈的消費者也可以因為參與稽核獲得系統的貨幣回饋。

[7] 經由開源程式自動運作，透過 Bolt Audit API 進行溝通稽核工作。

3.6. 零揭露證明

在 Bolt 中，所有交易都妥善儲存於索引莫克樹，同時交易細節以參與者及數位資產提供人的公鑰加密，因此只有參與者及數位資產提供人能使用自己的私鑰驗證自己的相關交易，過程中無需揭露參與者及數位資產提供人的隱私，更可確保資料正確性，由此方法完成零揭露的證明過程。透過零揭露證明，Bolt 實作之系統可滿足參與者與監管人事後的稽核需求，同時不侵害系統用戶的個人隱私。詳細的細節，可進一步參考附錄 A 。

4

應用場景

近年各行各業都在討論區塊鏈潛在的應用價值，在防偽領域，區塊鏈能協助商品原廠做認證，並導入系統追溯商品的流轉過程、生產履歷；在金融領域、交易、支付等也不斷發展，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、智能合約上有廣大的應用前景。

商品防偽認證

商品防偽溯源一直是區塊鏈技術落地的重要標的之一，也是 Bolt 能夠發揮技術優勢的應用領域。隨著仿冒商品與食安議題受到重視，消費者也開始重視購買商品的真偽，過去都是透過廠商的系統提供商品生產訊息，但中心化的資訊容易受到竄改或是假冒，而區塊鏈正是解決資料安全與可信的技術。透過 Bolt 的 Bolt Trust 服務，可協助廠商將商品生產資訊上鏈，目前已協助數家廠商如：蒲昌葡萄酒、帕米爾高原礦泉水、植物先盟環保吸管等，透過將商品資訊寫入區塊鏈，提供更可信的商品認證資訊給其消費者。

圖 10、Bolt Trust 應用於商品防偽認證

Bolt Trust 可保證商品資訊與生產履歷為不可篡改且可信任，同時上鏈的成本已大幅降低，提供商品價值之餘卻不會大幅影響營銷成本。同時，利用 Bolt Currency，Bolt 亦能提供合作廠商結合數位通證的營銷應用。

產銷環節追溯

用區塊鏈記錄品牌商品之完整資訊，從生產商、經銷商，以及物流運送，到後續的通路販售，每一處檢核點的產銷記錄，一旦產生及經過授權人員驗證後，透過客戶端App將該驗證訊息登錄到區塊鏈，消費者和機構裡的任何成員、任何節點，在 Bolt 上都可以追溯該筆記錄，透過信任機器，確定這筆生產履歷是不可篡改且可信任的，有效加強對於商品流轉資訊的可信度。

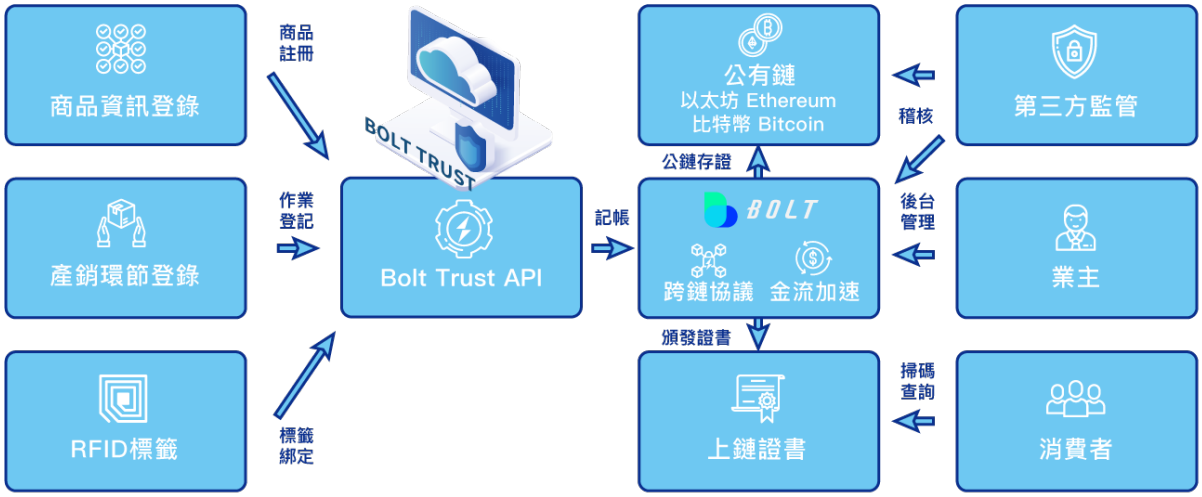


圖 11、Bolt Trust 商品追溯方案示意圖

Bolt Trust 不僅將數據紀錄在主鏈 Bolt 上，同時會將須存證之紀錄上到比特幣、以太坊等公有鏈存證，可大幅提高鏈上證據之可信度與安全性。在防止中間環節掉貨、篡貨上，透過私鑰授權才能寫入、分散式稽核技術，可以保證登錄資料的可靠性。

金融商品 / 儲備證明

以基金交易為例，買家購買後需要花費一段時間去追蹤基金申購的進度。對於基金公司，金融商品交易需要符合金融管理單位監管，必須投入大量成本在法律公司、

稽核員、顧問等等，以降低所有投資者的風險。善用區塊鏈的信任機制，可透過將交易紀錄、平台管理行為固定在區塊鏈上，增加平台運營的公正性、資訊透明度，並可能降低企業稽核的部分中間人成本，例如稽核員與文件管理員。

H公司為台灣的基金商品交易平台，其創新服務是將基金、股票、期貨等各式商品通證化，讓基金投資人可在平台上交換金融商品。其將交易記錄、平台管理紀錄寫在區塊鏈上，增加相關查詢的正確及可信度，這些紀錄需要能提供監管機關事後稽核，但現有公有鏈的交易頻寬不足以面對其龐大的交易紀錄數量。透過整合 Bolt Trust 資料信任服務，除了滿足紀錄大量交易的需求外，在隱私保護上讓每個交易者根據自己的權限，僅能查詢自己的相關記錄；對監管單位的事後稽核需求，則透過零揭露證明來完成稽核，協助平台被信任之虞，兼顧了交易速度與隱私性。

圖 12、Bolt 應用於金融商品交易

企業內控 / 法規遵循

善用公有區塊鏈的信任機器 (Trust machines) 可以實現企業內部控管、法規遵循的要求，例如銀行行員何時做何種交易業務行為，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。

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、訂立規範，以及事後的文件比對及人力稽核確認，運用 Bolt 的稽核技術，銀行和行員的業務記錄透明，行員可稽核自己的交易記錄是否正確，或對銀行提出某個區間紀錄的稽核請求，減少記錄出錯的可能。此種稽核方式，可省略大量稽核文件、查詢人力，我們為此設計 Bolt Auditor 稽核工具(如圖13)，幫助有相關需求稽核單位，能快速驗證透過 Bolt 上鏈之交易證據是否正確、未經竄改。

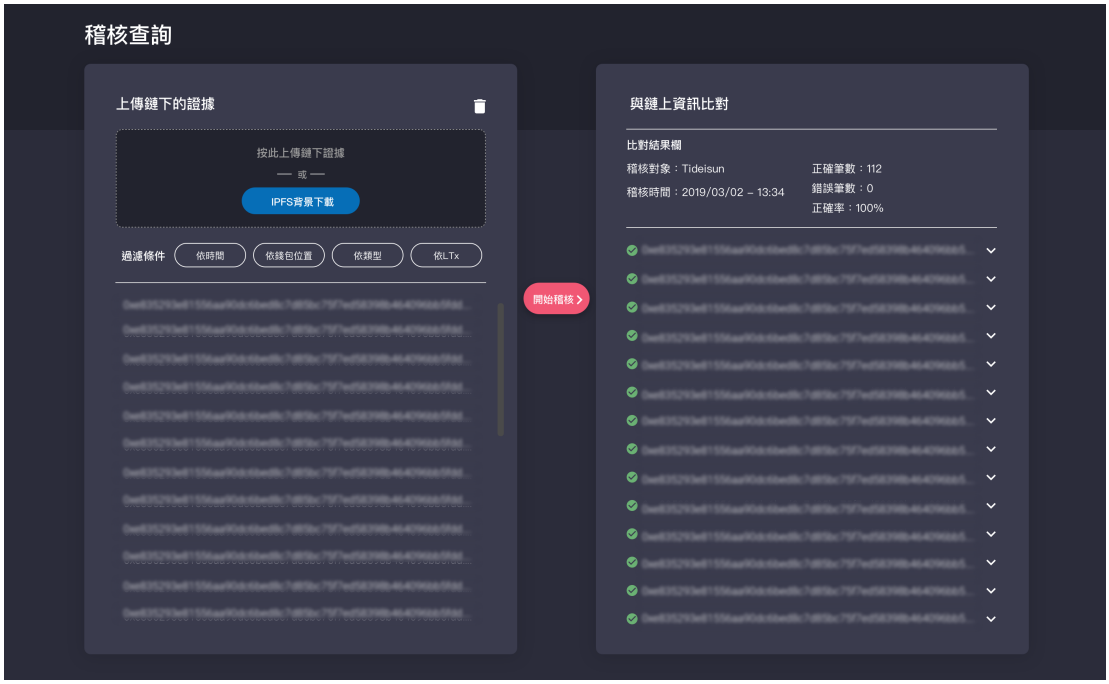


圖 13、Bolt Auditor 稽核介面示意圖

小額支付 / 交易上鏈

2016年中國第三方移動支付的規模擴大兩倍多，達 38 萬億元人民幣（合 5.5 萬億美元）[8]，而福雷斯特研究公司(Forrester Research)的數據顯示，全年美國移動支付規模增長為 39%，為 1120 億美元。以VISA為例，全球平均每秒的交易數量約為

[8] https://www.read321.com/182130.html

2000筆（最多每秒有58,000筆），然而比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[9]（每秒交易TPS、transactions per second）。

為了滿足越來越多人利用小額支付進行日常生活的瑣碎交易，像是買咖啡、繳水電費等等，利用 Bolt Trust 金流加速、多筆記錄壓縮上鏈的特性，更多小額支付也能快速完成並記錄到區塊鏈上。同時可利用 Bolt 的分散式稽核的功能，來保護個別消費者的隱私交易內容。不僅是 Bolt 上的虛擬貨幣可以記錄在平台上，一般傳統的信用卡、銀行轉帳、支票抑或是其他虛擬貨幣，一樣可以記錄在 Bolt 系統中，以更順利的與現有系統結合。

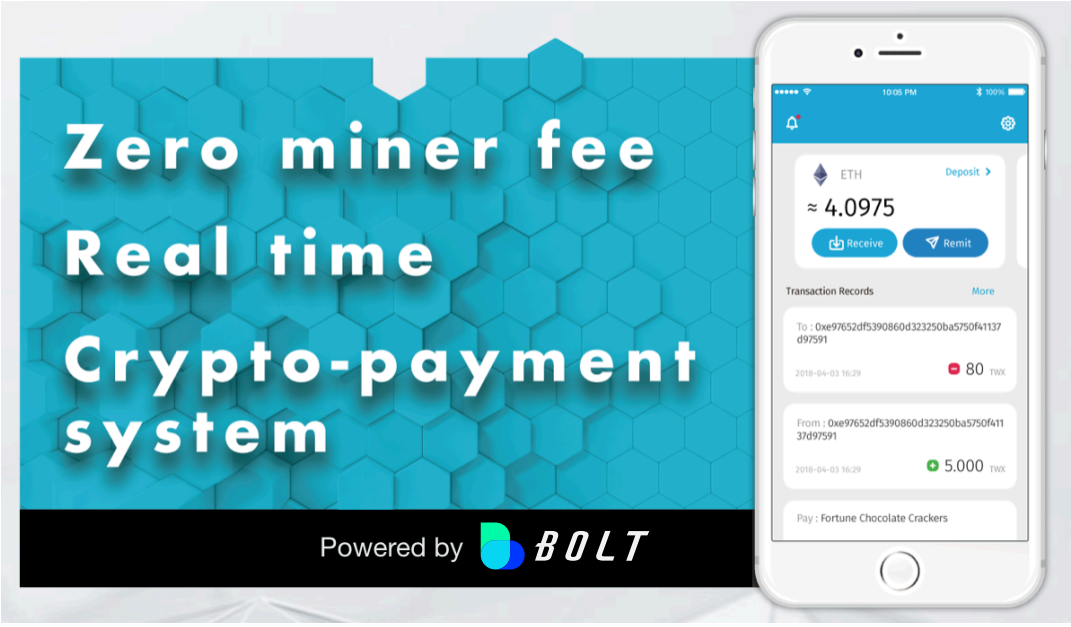


圖 14、Bolt 應用於微支付

數據資產 / 大數據應用

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

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

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 目前已提供主流公鏈資產轉換的方式，並預計提供資產交易管理應用，在交易的同時，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。

消費分潤

iSunTV 和區塊鏈結合，根據使用者實際的視頻觀看數量、比例，將權利金以加密貨幣分潤給內容提供商。消費者在iSunTV上的消費模式是訂閱制隨選隨看，若是每筆觀影記錄都要立即寫入區塊鏈會令成本過高。使用 Bolt Trust 的資料壓縮上鏈、分散式稽核技術，即使消費者的觀影記錄再分散，也可以準確地記錄到區塊鏈，並讓內容供應商能確實稽核帳本，促進內容商的合作意願。

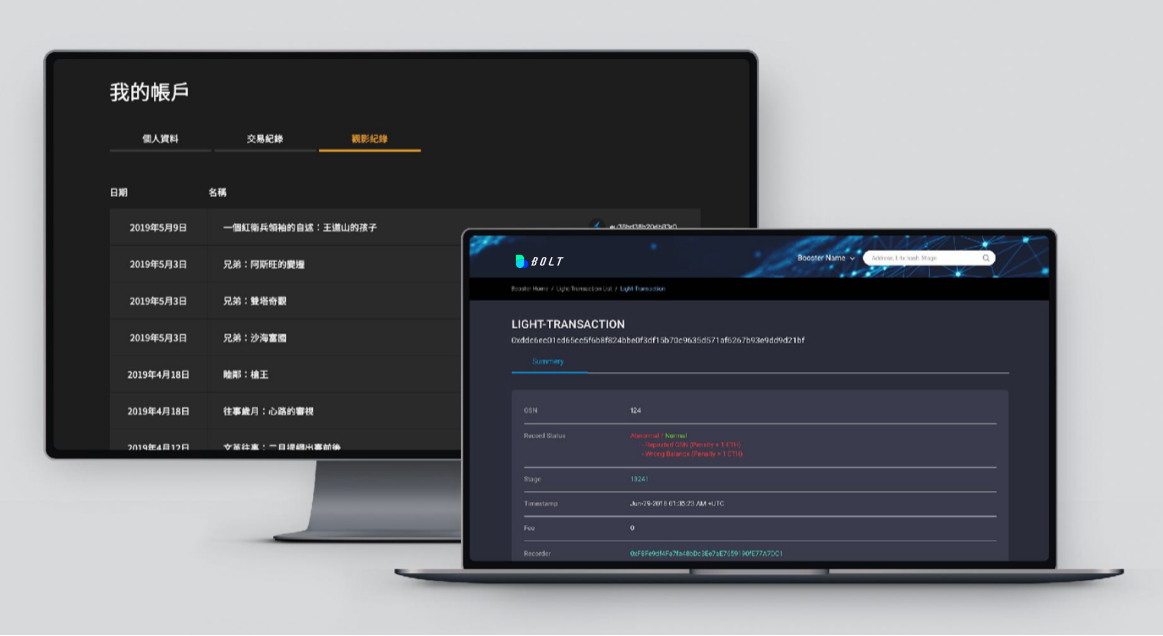


圖15、iSunTV 採用 Bolt Trust 記帳進行消費分潤

5

Bolt
通證模型與發行計畫

5.1. BOLT 挖礦獎勵

稽核即挖礦 – Auditing Is Mining

BOLT 作為節點用戶協助稽核上鏈資料的驗證獎勵，以激勵 Bolt 上參與驗證的用戶（礦工）。礦工可透過同步 Bolt 的所有交易，定期打包為區塊並提交，確保上鏈數據達成 PoHCE 共識，即可獲得相關獎勵。Bolt 遵循自由軟體精神，相關程式碼公開於網路上，任何人都能下載成為 Bolt 節點。

5.2. 權益委託證明與審計機制

除了作為礦工節點外，持有 BOLT 的用戶亦可藉由抵押支持稽核節點取得稽核獎勵。要成為驗證節點，可透過抵押不低於 100,000 枚 BOLT 作為保證成為稽核，稽核節點將針對所有打包的區塊進行解析與驗證，並取得對應的 BOLT 獎勵後分享給支持該節點的所有用戶。

由於 Bolt 的資料寫入與稽核上鏈是非同步進行，因此稽核驗證過程並不會影響資料寫入的 TPS，此設計能確保同時實現高效寫入與上鏈稽核機制，取得交易速度與公信力的平衡。

5.3. BOLT 回收機制

使用 Bolt 將資料上鏈需要消耗 BOLT，其中一定比例的 BOLT 將會永久銷毀以確保在發行總量限制下，後期生態能持續有足量的稽核獎勵。BOLT 銷毀比例計算依據和平均交易手續費 $f_{transation\ fee}$ 、匯率 $R_{target\ blockchain}$ 和壓縮筆數 C 有關，隨著壓縮資料筆數的增加，BOLT 銷毀比例最高達 50%，計算公式如下：

$$BOLT_{consume} = f_{transation\ fee} * R_{target\ blockchain} * \ln(C)$$

$BOLT_{consume}$：每次上鏈消耗的 BOLT 數量
$f_{transation\ fee}$：平均交易手續費
$R_{target\ blockchain}$：對目標公鏈匯率
ln(C)：壓縮資料量的係數

5.4. BOLT 發行規範

主網上線時間	2023-01-01 14:00:00 (UTC+8)
BOLT 發行總量	210,000,000,000 BOLT
初始區塊獎勵	10,000 BOLT
出塊時間	12 seconds
獎勵半衰期	10,500,000 blocks

表 2、BOLT 發行規範

5.5. BOLT Fundation

Bolt 為了實現企業化跨鏈技術解決方案的目標，BOLT 挖礦獎勵將有 10% 貢獻於 BOLT Fundation，用於實現 Bolt 生態開發與推廣。Bolt Foundation 採用去中心式治理原則，其運行根據持有 BOLT 所有成員共同決議。

5.6. BOLT 投資價值

Bolt 作為公信載體，致力於承載區塊鏈與區塊鏈間、區塊鏈與真實世界間的商務應用資料，並確保其隱私且易於授權應用，若成功連結主流公有鏈的大型應用場域，將創造極高價值。

BOLT 作為參與生態的重要媒介與抵押物，在市場上有一定程度的消耗需求，且因固定的發行總量，在 Bolt 創造的生態系中，無論企業資料上鏈、資產鏈上轉移都需要消耗，隨著 Bolt 涉入越來越多的行業領域，使用量會越來越多，隨著網路的擴張也將提升 BOLT 的持有價值。

附錄A Bolt 稽核與隱私保護技術

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 22ms ），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[10]。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[11]；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。

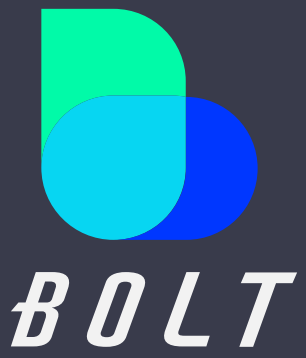
---

[10] 解不出的交易為其他數位資產提供人的相關交易。

[11] 此運算時間還未加上於索引莫克樹上的traversal 花費時間。

數位資產提供人要稽核自己所有相關交易時[12]，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，由此實現零揭露證明。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。

[12] 執行公布的開源程式，該程式透過 Bolt Audit API 與 Bolt 系統溝通。


BOLT