

Libra 1.0 和技術實現

Table of Contents

Libra 1.0 和技術實現.....	1
背景.....	2
白皮書.....	3
Libra 聯盟鏈	4
交易的生命週期.....	7
帳本歷史	9
應用：LibraBridge: 連接 Libra 與 Ethereum	11
問題描述	11
情況一	11
情況二	12
參考.....	13

背景

今年六月，全球最大社群網站之一的臉書 (Facebook) 宣布其區塊鏈計畫 — Libra，旨在打造一個實現普惠金融 (Inclusive Financing) 的全球支付系統，臉書夾帶著分佈世界各國 20 億用戶的優勢，並組織一個 Libra 聯盟，28 個聯盟創始成員，如圖一，有來自支付、電信、科技、創投，與非營利組織等不同領域，例如 MasterCard, Visa, eBay, Uber, Lyft, Spotify, Coinbase, Kiva 等企業與組織，要打造一個新的全球貨幣。而該宣佈立即衝擊了各國金融以及數位貨幣市場，頓時使得世界各國不得不重視區塊鏈技術，也讓這個產業再度躍上檯面，從方方面面思考金融體系該如何立法監管與規範。



圖一：Libra 聯盟成員

按臉書原先的計畫，系統預計在 2020 正式上線，而在 Libra 的官方網站上，臉書也同時發佈 Libra 白皮書¹ (White paper) 描述其願景，技術白皮書描述系統的架構與設計，並且開源 Libra 的原始碼以及上線公開的測試網路 (Testnet)，讓開發者可以先嘗鮮。截至筆者撰寫本文，Libra 的開源項目仍在持續開發，而程式碼也不停在更新，甚至有系

統設計上的變動，開發者的討論區也是相當活躍。足見臉書在這個項目上，不但是野心勃勃，更是有備而來。

過去一段時間，Libra 飽受各界批評，有國家表達拒絕 Libra 在該國發行，也有國家設立特別工作小組進行審查，研擬如何監管與 Libra 對未來的衝擊，而美國國會也舉辦一連串的聽證會，考量臉書過去在資料保護與隱私問題的疑慮，要求臉書停止 Libra 專案，當然各界最重視的還是，Libra 可能侵犯隱私及動搖現有的貨幣系統。而這樣的一套系統，到底是如何實現與運行，我們將聚焦在技術上，一窺其奧妙。

白皮書

首先，我們先來理解，Libra 項目的願景與任務是什麼？以下是白皮書的描述。

Libra's mission is to enable a simple global currency and financial infrastructure that empowers billions of people.

由白皮書的描述與內容，得知 Libra 的任務是發行全球貨幣，而希冀這套新的金融系統可讓數以億計的人們受惠，實現普惠金融。而這又是透過何種方式來實現呢？臉書首先在瑞士設立 Libra 聯盟 (Libra Association)，目前已知的 28 個創始成員分別來自不同領域，有支付、科技、電信、區塊鏈、創投與非營利組織等不同背景成員，聯盟預計在全球招募 100 位成員，共同維護 Libra 驗證節點 (Validator Node)，打造一個許可制區塊鏈 (Permissioned Blockchain)，或稱聯盟鏈 (Consortium Blockchain)。

目前，較為人熟知的比特幣 (Bitcoin) 或是 Ethereum (以太坊)，都是屬於公有鏈 (Public Chain)，意味著任何人都能夠參與區塊鏈網路的交易與驗證，而通常能夠參與帳本驗證的角色稱作礦工 (Miner)；相較於公有鏈，許可制區塊鏈，顧名思義，則是只有受允許的驗證節點能夠維護帳本。在 Libra 聯盟的規定上，驗證節點將由聯盟成員來維護，共同建立一個聯盟區塊鏈，每位聯盟成員若允諾加入，則必須提供 1000 萬美金，作為 Libra 基金會的儲備金，而未來聯盟理事會的治理與討論下，則擁有一票的權利。而聯盟成員的選擇條件相當嚴苛，若是企業必須市值或用戶數超過一定門檻，或是具備有影響力的非營利組織或學術機構。

由於 Libra 目標是成為全球貨幣，用於支付系統，因此必須保持價格的穩定與低波動性，換言之，Libra 是一種穩定貨幣 (Stable Coin)，其價格將由一籃子的真實資產來進行掛鉤，

根據白皮書，目前包含的資產有美元、歐元、日圓、英鎊與新幣，甚至不排除信譽良好的政府短期公債，而每位聯盟成員提交的 1000 萬美金將用於儲備金，作為真實資產擔保的一部分。而 Libra 上也會發行證券型代幣 (Security Token) - Libra Investment token，作為獎勵運營和投票治理機制的一部分。未來，Libra 的發行將由使用者透過等值的法幣 1:1 交換進行購買，每增發 (Mint) 一枚 Libra 代幣，就要有相對應的法幣資產支撐，而當要將 Libra 兌換成法幣，則相當於燒毀 (Burn) 等值的 Libra 代幣。目前對於 Libra 的購買管道尚不明確，可能會透過 Libra 的專用手機錢包應用程式 - Calibra²，或其他 app 來進行購買。

到此，我們先做個簡單的小結。Libra 項目確實有備而來，而且隱含了許多數位貨幣的影子，像是分散式治理 (Distributed Governance)，聯盟鏈的設計並不會使臉書有一家獨大的情況，而每位聯盟成員都有投票權，作為治理的話語權，成員的加入與離開有相對應的規範，並且設計有證券型代幣來激勵成員維護聯盟鏈的系統。而在代幣的設計上，透過與一籃子貨幣的價格掛鉤，確保價格維持在低波動的情況，並有儲備金做為最後的擔保，隱約可見 MakerDAO³ 的治理與代幣模型，與 Terra⁴ 的穩定幣設計概念。下圖二是 Libra 主網上線的里程碑，針對主網的技術實現，將由臉書的開發團隊來進行，預計在 2020 年上線。下節我們將來看 Libra 聯盟鏈採用何種技術來進行實現。



圖二：主網里程碑

Libra 聯盟鏈

在 Libra 的技術白皮書之中，我們發現 Libra 聯盟鏈的設計，參考許多近期與早期的文獻，內容涵蓋共識協定 (Consensus Protocol)、可驗證隨機函數 (Verifiable Random Function, VDF)、簽章聚合 (Aggregation Signature)、資料結構儲存方法與 P2P 路由設計

等，透過分析既有設計的優缺點，試圖結合理論與實務，打造一個實際可用的聯盟鏈。不同於 J.P. Morgan 的 Quorum 聯盟鏈，系統是從以太坊的原始碼修改而來，Libra 是一套全新的區塊鏈設計，吸收各家設計的精華，並選用 Rust 語言來編寫，希冀達到高效與安全。

另外，由於 Libra 是聯盟鏈，在安全模型的設計上，條件不如公有鏈來的嚴苛，因此在共識協定的設計上，並非採用工作量證明 (Proof of Work)，即一般俗稱挖礦 (Mining) 的方式來記帳，而是採用自家修改自 HotStuff 協定的共識演算法，稱作 LibraBFT。拜占庭容錯問題算法 (Byzantine Fault Tolerance, BFT)，乃是源自拜占庭將軍問題 (Byzantine Generals Problem)，是討論在分散式系統中，錯誤資訊如何在通訊過程中，擁有容錯的過程。問題描述如下：一群將軍計畫要攻下某座城，但其中有些將軍是叛徒，目標是要達到：

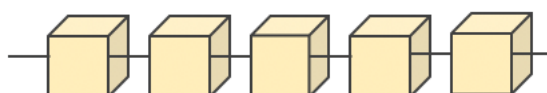
1. 忠誠的將軍會如實地執行既有計畫
2. 小部分叛將不應該影響既有決定

該問題在設計上，可以透過多個回合的交互步驟，保證在最多有 F 個叛將的情況下，若滿足 $2F+1$ 個忠誠的將軍如實執行計畫，就能夠確保計畫正確執行，在共識演算法上，既有計畫可能是指操作或是交易的執行順序。對應到聯盟鏈上，將軍就是聯盟鏈中的驗證節點，在最多有 F 個惡意或是非正常節點 (例如：故障、網路延遲等) 下，只要誠實節點忠實遵循協定，就能夠確保帳本的一致性。但假若共識協定設計的不好，也有可能導致系統無法運作，例如無法取得 $2F+1$ 個節點同意，將無法進行決策，影響到系統的活性 (Liveness)；同理，若有超過 F 的惡意節點在網路之中，也會影響到整體系統的安全性 (Security)。而 LibraBFT 基本上就是一套共識演算法，為了解決上述問題，以及為求帳本一致性所設計。Libra 在既有的文獻基礎上，優化網路層的通訊協議，簡化回合需要交互的溝通次數，並且在提案者 (Proposer) 的設計上，引入了可驗證隨機函數，降低在提案者選擇上的偏差，可能會導致提案者可對交易進行審查攻擊，或是與其他驗證者共謀的可能性。

Libra 預計在上線前招募 100 個驗證節點，若效能有所突破，則預期在未來擴展到 500-1000 個驗證節點。目前在效能上，交易速度約為每秒 1000 筆交易，而每筆交易預計在 10 秒內被確認。不同於公有鏈上的共識設計，通常我們會說以太坊交易需要等待 25 個區塊來進行確認，這是因為公有鏈挖礦的設計，可能會導致區塊在增長時會有分叉的

狀況，因此需要透過機率式的檢定，確認交易在未來不會被反轉或撤銷，但在 LibraBFT 的設計下，由於交易必須獲得至少 $2F+1$ 的驗證節點同意，因此確保了鏈的一致性，進而達到最終性 (Finality)，而這也是 BFT 類共識演算法所帶來的好處。

雖然 Libra 宣稱其為區塊鏈，不過從他的資料結構來看，Libra 並不像一般區塊鏈如圖三，具有連結串列 (Linked list) 的結構設計，由後一個區塊連結前一個區塊。Libra 的設計中並沒有區塊的概念，相反，比較像是一個帶版號的分散式資料庫 (Versioned Database)。



圖三：區塊鏈

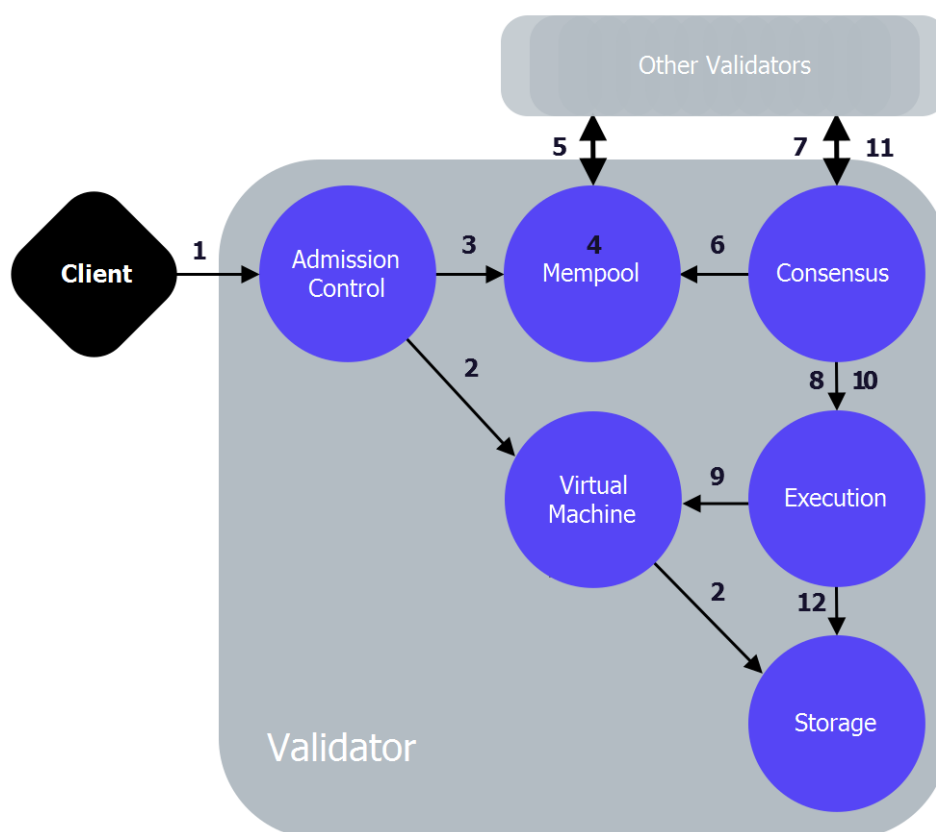
此外，在 Libra 目前的系統中，可以看出很大一部分的概念設計與以太坊相近，像 Libra 支持智能合約 (Smart Contract) 的功能，且重新設計一套新的合約語言 Move，有自己的虛擬機，而 Libra 的狀態 (State) 是由有序性的交易 (Ordered Transaction) 計算所維護的狀態而組成，並且可以被驗證。在帳戶的設計上，也採用 Account-Based 的方式，由每個帳戶維護一組自己的狀態，且每個帳戶會記有一個序列號，做為交易的執行順序。同時，在交易上也需要指定 gas 的單位價格與 gas 的使用量，作為預防 DDoS 攻擊的防禦措施，不同的是，gas 在此並不作為交易手續費。不過在雜湊函數上，則選用 SHA3-256，在簽章演算法上，選用 EdDSA，不同於多數主流區塊鏈選用的 ECDSA，而未來也考慮採用 BLS 簽章演算法來做簽名的聚合。表一為 Libra 與 Ethereum 的簡易系統比較：

	Libra	Ethereum
Consensus	LibraBFT	Ethash (PoW)
Address	Account-based	Account-based
Hash function	SHA3-256	KECCAK-256
Signature Algorithm	EdDSA (ed25519-dalek)	ECDSA (secp256k1)
Transaction Per Second (TPS)	~1000 Tx/s	~10 Tx/s
Finality	10 secs	n/a
Smart Contract	Move	Solidity, Vyper
Type	Permissioned	Permissionless
Ledger structure	Versioned Database	Blockchain
Serialization	LCS	RLP

表一：Libra vs. Ethereum

交易的生命週期

前面我們介紹過 Libra 的架構與系統設計，這節我們來看一筆交易從發送到寫入帳本的生命週期。從 Libra 白皮書，Libra 代幣的發送需要透過 Calibra，或者是經授權的相關應用程式，下圖四是 Libra 白皮書中針對交易在 Libra Core 中的工作流程：



圖四：Libra Core 中的交易生命週期

首先，要發送一筆交易，客戶端的錢包，會透過 Libra 定義好的交易格式，產生原始交易內容 (Raw Transaction)，再經由錢包的私鑰簽名後，得到簽名後的交易。接著再由錢包將這筆交易發送給驗證節點，等待進入聯盟網路寫入帳本，而關於交易的内容格式，Libra 與以太坊交易格式非常相近，如表二的格式比較。主要會發現 Libra 多了發送方地址與公鑰的欄位，且沒有收款方與數量，其他則大同小異，這是因為在以太坊中利用 (v, r, s) 的部分，讓送方地址可被還原；至於沒有收款方與數量，則是因為在 Libra 中，交易基本上都屬合約交易，包含 Libra Coin 與 Validator 皆屬於智能合約，因此交易邏輯的執行，實際上是發生在 Program 的部分，相當於以太坊中 data 的欄位。其他欄位除了命名有些許不同，概念上大致是相近的。簽名的部分，則是透過 EdDSA 演算法來進行，但在 Libra Core 的原始碼部分，我們可以看到除了 EdDSA 之外，還有 BLS 簽章演算

法，雖然目前是使用 EdDSA，但相信未來等 BLS 簽章規格成熟後，採用 BLS，對於共識算法的簽名聚合也會相對有幫助，節省更多簽名的資料量。

Libra	Ethereum
Sender address	(v, r, s)
Sender public key	
Program	data
Gas Price	gasPrice
Maximum gas amount	gasLimit
Sequence number	nonce
Transaction expiration	-
-	to
-	value

表二：交易格式 Libra vs Ethereum

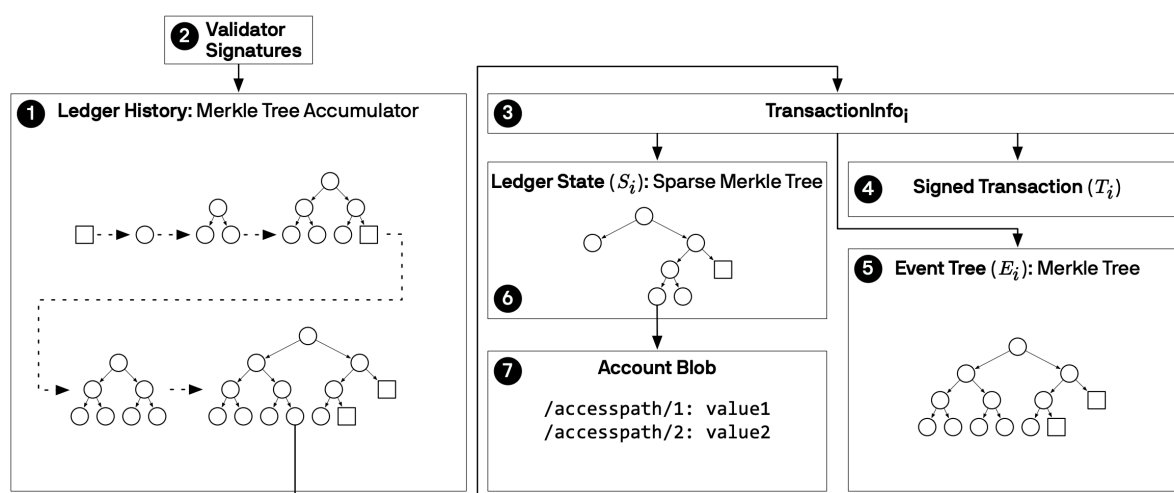
接著，我們來看交易進入到驗證節點的步驟：

1. Admission Control: 當驗證節點收到交易後，會先經過准入控制，由節點檢查交易的合法性後，再決定是否接收該筆交易，避免惡意的交易進入到網路形成 Spam 攻擊。
2. Virtual Machine & Storage: 為了讓准入控制進行驗證，節點會存取虛擬機與儲存單元以取得帳號相關的資訊，來驗證簽名的正確性，帳號序列號是否正確與連續，發送的金額是否足夠等等。
3. Mempool: 通過准入控制檢查的交易，將會進到驗證節點中的一塊記憶體位置，類似存放等待打包的交易的倉庫，並且這個專于搜集待驗證交易的交易池，會與其他驗證節點共享與同步這些交易。
4. Consensus: 當某個驗證節點被選為提案節點時，將會從其記憶體池中選出交易，利用 LibraBFT 演算法與其他驗證節點互動，進行提案投票，若有足夠的有效票 ($2F+1$)，則該交易被接受，並成為帳本的一部分。
5. Execution: 而共識流程的一部分是交易會被執行，而執行後的狀態將由其他驗證節點來驗證，若交易被接受，則牽涉到資料與帳本的更新。

由上述的設計，可以看出 Libra 在效能與安全方面的考量，通過准入機制確保不會有垃圾交易，之所以這麼嚴謹，也才能確保聯盟鏈上的流量可以被管控，當然另一方面驗證節點的處理能力與複雜度也會相對較高。

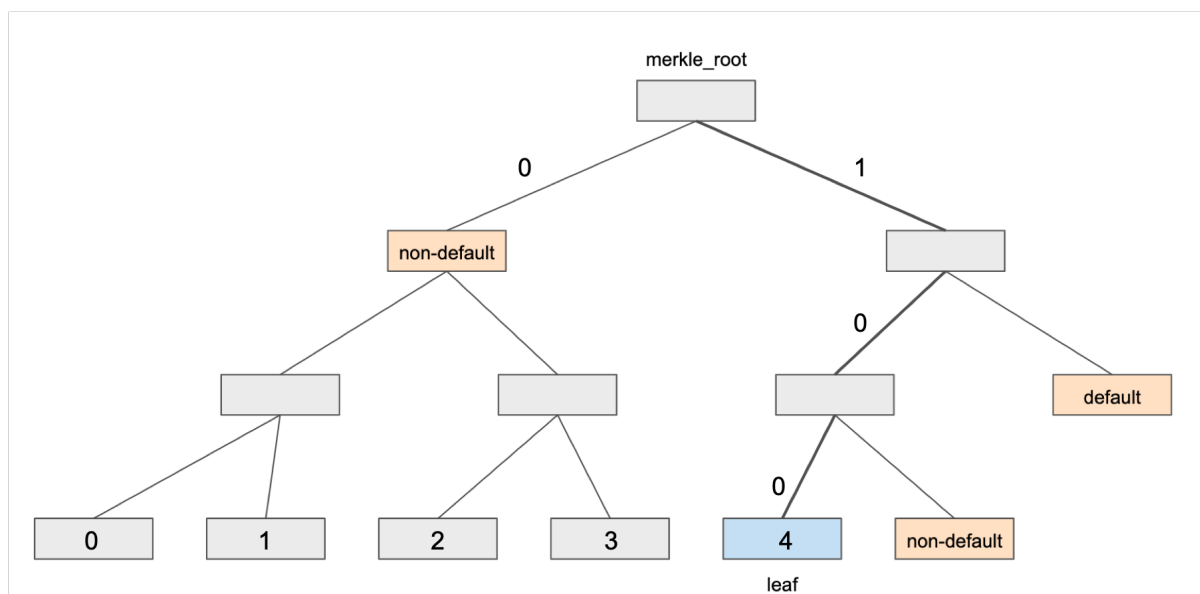
帳本歷史

關於帳本的紀錄與資料結構，看似與以太坊相似但實質上又不太相同。同樣的，帳本都會維護一個 Ledger History (以太坊上是 Global State)，如圖五所示，當一筆新的交易被寫入時，該交易涉及的帳戶與資料因為更新，涉及帳本狀態的改變，以及合約執行時產生的相關事件 (Event) 的紀錄。



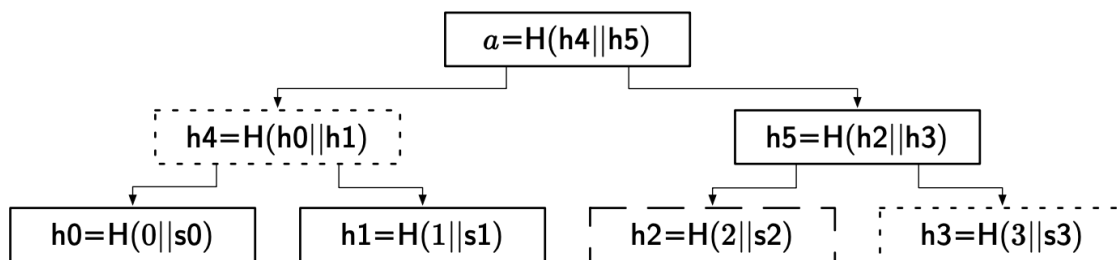
圖五：Ledger History (取自 Libra 1.0 白皮書)

首先，我們先來看 Merkle Tree Accumulator 的部分，而這個結構事實上就是前面談及的帶交易版號的資料庫。每當一筆新的交易被寫入帳本，就會成為樹的葉節點 (Leaf node)。舉例來說，當第 5 筆交易被寫入時，一個新的葉節點產生，而其版本號碼則為 4，對應到二進位表示的 100，這樣的方式，讓交易的搜尋可以透過交易流水號，快速地被搜尋。而新的葉節點不足以成為二元樹的部分，則由定義好的替代字符來取代成為葉節點。換言之，Libra 上每筆交易都會有流水號，並不像一般區塊鏈的交易序列號，是由交易的雜湊值所計算而成。另外，也沒有區塊的概念，整個帳本就是一個有序性交易的帳本歷史，如圖六所示：



圖六：Merkle Tree Accumulator

由於 Accumulator 採用 Merkle Tree 資料結構的設計方式，除了具備有效率搜尋資料的特性，也兼具了可驗證的特性。下圖是一個 Merkle Tree 的例子，假設要證明 s_2 是否存在於資料庫之中，我們可以利用 Merkle Root (a) 與 Merkle Branch (h_3, h_4) 來進行檢驗。在葉節點的部分，由每筆交易的版本號與狀態計算的雜湊值而定。透過比對 $a \stackrel{?}{=} H(h_4 || H(h_2 || s_2) || h_3)$ 是否等於 a ，即可得知 s_2 是否在資料庫中。



圖七：Merkle Tree

通常這類交易的驗證又稱作 SPV (Simplified Payment Verification)，主要是設計給一些輕量級的客戶端使用，例如手機或是計算能力較弱的終端。誠如其名，簡單支付驗證，表示客戶端僅需要轉帳的功能以及確認交易是否完成，這意味著客戶端能夠將交易簽完名後，並傳送交易到第三方具有驗證節點功能的節點上，進行交易廣播，並等待交易上鏈後完成交易確認。這樣的方式特別適合於 Calibra 類型的手機應用程式，由於手機本身不具備交易同步與驗證的能力，但通過 SPV 即可檢驗交易是否已經完成。

應用：LibraBridge: 連接 Libra 與 Ethereum

在前面的小節中，我們介紹 Libra SPV，這個小節我們將來看一個簡單的應用，透過 Libra SPV 搭建 Libra 與 Ethereum 之間的橋樑，姑且稱做 LibraBridge。本小節，我們將利用 SPV validation 實作跨鏈的代幣交換，SPV 是一種用於輕節點驗證交易的方法，透過智能合約的協助，我們可以在合約上驗證來自 Libra 的交易。我們將介紹如何在 Libra 與 Ethereum 上搭建一個無需信任的託管服務 (Trustless Custodian)。

問題描述

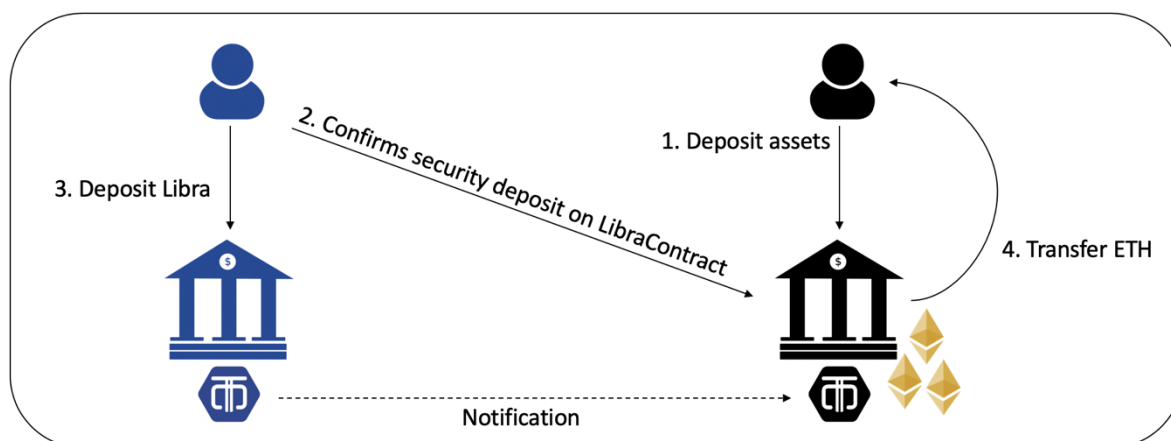
由於在現有的 Libra 測試網上，尚無法部署智能合約，或與智能合約進行互動，僅能夠在本機端單機執行合約。在僅有一條鏈 (以太坊) 支持智能合約的情況下，我們無法直接執行原子代幣交換 (Atomic Swap)，但實際上，透過協定的設計，我們是能夠實現無需信任的託管服務。舉例來說，假設我手中只有 Libra 代幣，而 MAX 交易所賣 ETH，我想與其幣幣交換。最簡單的作法就是從 MAX¹ 入金 Libra 並與之交換 ETH，而前提是相信 MAX 會出金。

如果問題變成，同樣要做幣幣交換，是否可在不完全信任 MAX 交易所的情況下來實現呢？

情況一

正常的情況下，首先 MAX 會在 LibraContract 中放入保證金，作為履約保證，而合約內的保證金僅能在一定時間後才能由 MAX 取回，其他時間保證金則由非受第三方控制的合約鎖定與保管。而當用戶想與 MAX 進行幣幣交換時，會先查詢合約上是否有足夠的保證金，如果有的話，則將手上的 Libra 資產傳送到 MAX 的 Libra 地址，而當 MAX 確認後，則會在以太鏈上傳送等值的 ETH 給用戶，以完成本次交易。

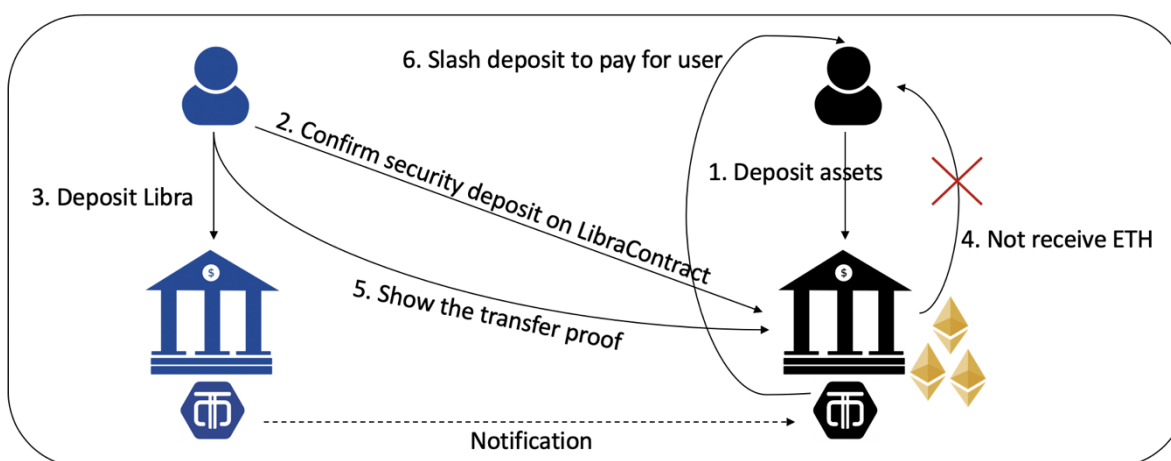
¹ MAX (<https://max.maicoi.com/>) 是一間中心化交易所，圖八的交易指鏈上交易，而非資料庫資料更新。



圖八：正常出入金

情況二

同樣的，MAX 會抵押保證金，以取得用戶的信任，相信可與之幣幣交換。但若 MAX 收到 Libra 後卻沒轉送 ETH 給用戶，即違約，由於合約內含一個違約挑戰的功能，若用戶可以出示在 Libra 上的轉帳證明，則可遞交證明作為憑據。而鏈外轉帳的證明可由 Libra SPV 來進行交易驗證，當能夠證明某筆交易已經被核定，而這正是 SPV 的既有功能。另一方面，MAX 作為違約的一方，將由公正第三方的合約，削減合約上的押金作為給用戶的歸還，甚至再由保證金多付出該筆交易 $x\%$ 的罰金來補償用戶。



圖九：異常出金的狀況

SPV 驗證與協定設計讓我們能夠實現無需信任的託管服務，並無需仰賴區塊鏈都支持智能合約。此外，一個可受信任的託管服務，相較於點對點的直接交易，資金池在流

通性上來的更有優勢，但相對也有一些挑戰需要克服。畢竟未來若 Libra 真的成為全球貨幣，讓 Libra 在不同鏈之間進行流通將有助於市場流動，加上 Ethereum 目前在 DeFi 應用的發展，這將會是相當大的優勢。

總結

Libra 是個具有野心與前瞻性的項目，技術上，透過在不同區塊鏈技術上的截長補短，試圖打造高效與安全的聯盟鏈，並且在設計上，同時考慮區塊鏈的自理與可續性，這是其他項目相對欠缺的部分。而在願景上，透過打造全球貨幣與無國界的金融設施，並夾帶臉書自身 20 億的用戶數與其他聯盟成員的規模度，是非常有希望將服務帶入一般用戶的生活當中，而這也是區塊鏈應用落地最有希望的一環。同時，成為全球貨幣也挑動了世界各國在金融貨幣上的敏感神經，紛紛開始成立研究小組或是研擬如何監管與規範，也將區塊鏈技術推到各國面前，使得數位貨幣再次被重視。Libra 項目有許多的創新，雖然距離其宣稱要走到公有鏈，可能有不少路要走，但是這樣大膽的概念與做法，縱使 Libra 項目失敗了，Libra 的概念或精神，也可以由其他區塊鏈或聯盟來實施與推行。作為公有鏈的支持者，仍是樂見 Libra 的發展與延續。

參考

1. Libra Whitepaper: <https://libra.org/en-US/white-paper/>
2. Calibra: <https://calibra.com/>
3. MakerDAO: <https://makerdao.com/>
4. Terra: <https://terra.money/>