

第一章 OSN 做什麼事

1.1 業務定位

OSN 是面向持牌金融機構的跨境清算網路。它不面向公眾，不持有終端客戶，不提供外匯兌換，也不參與任何一方的支付執行。它承擔的是機構與機構之間的一件事：**把"誰應當向誰清算多少"這件事，變成一個各方都能獨立核驗、且事後無人可以修改的記錄。**

OSN 由兩層構成，職責嚴格分開。

QCC 層——價值與事實。 QCC 是一條無准入公開帳本，協議規則在正式版本釋出時凍結：沒有升級金鑰，沒有可修改的規則集入口，任何一方都無法單方變更已生效的規則。OSNB 結算憑證的發行、銷毀與每一次轉移都記錄在這一層，公開且任何人可重放核驗。OSN 不控制 QCC，也無法暫停它。

OSN 層——清算與協調。 OSN 運營核心服務節點，負責機構間清算請求的路由、同步、異常處理與審計重放。成員機構自行部署機構節點，持有自己的客戶資料與私鑰。這一層由 OSN 運營方協調，這是一個運營型網路所必需的，也是承擔牌照義務的主體所在。

這樣分層的結果是：**參與機構需要與 OSN 建立商業與合規關係，但不需要信任 OSN 的帳本。**資金對應的價值事實不在 OSN 的伺服器裡，而在一條 OSN 無權修改的公開帳本上。

與現有跨境清算模式的結構對比

	代理行網路	卡組織清算	匯款服務商	OSN
價值記錄持有者	各代理行各自帳本	清算組織	服務商	公開帳本，無單一持有者
參與方需要信任誰	鏈路上每一層代理行	清算組織	服務商	無需信任任何一方
記錄可否被持有方單方修改	可	可	可	否
爭議時的事實來源	雙方各自記錄後對帳	組織的記錄	服務商的記錄	同一份不可修改記錄
中間環節可見性	對發起方不可見	組織內可見	服務商內可見	全程可核驗
後量子簽名	未規劃	未規劃	未規劃	自創世起原生

這張表刻意不包含吞吐量與網路覆蓋。在這兩項上，執行數十年的全球清算體系具有 OSN 短期內不可比擬的規模，白皮書無意在此作不對等比較。OSN 主張的差異在記錄的性質上，不在規模上。

關於效能的分層說明

OSN 與 QCC 承擔不同的工作，效能指標也必須分開陳述。

層	承擔的工作	指標
QCC	價值轉移與終局性	公開測試環境約 1,000 TPS [已實現]
OSN	機構間清算報文同步與處理	架構設計目標 100,000 TPS [設計目標]

兩者量級不同，因為承擔的事不同。一份清算報文中可包含一批清算訂單，落到帳本上是一次淨額價值轉移——**跨境小額清算的真實瓶頸從來不在帳本寫入速度，而在報文傳遞與事後對帳。**

QCC 的 1,000 TPS 是一項主動取舍的結果，而非未經最佳化。後量子格簽名的驗證開銷顯著高於橢圓曲線簽名，而全量重放與執行層雜湊一致性要求每個節點重算全部歷史。這是為"任何人可獨立核驗"這一性質支付的成本。對於清算場景，這個價格是划算的：終局性每秒千筆已遠超實際淨額結算需求，而可驗證性無法事後補上。

OSN 層的清算報文採用 P2P 直連同步，報文之間互不依賴、不爭用全域性狀態，架構上不存在序列瓶頸。10 萬 TPS 是設計目標與最終測試目標，開發與壓測尚未完成，本白皮書不將其作為已具備的能力陳述。

1.2 小額跨境清算的實際場景

OSN 第一階段服務的是**小額、高頻、目的地集中的**跨境資金流動。典型來源包括：

- **勞務匯款**——東南亞區域內數千萬跨境務工人口的定期匯款，單筆金額小、頻次固定、走廊高度集中；
- **中小企業貨款**——區域內貿易的小額結算，金額通常在數百至數千美元；
- **平臺類結算**——電商、出行、內容平臺向境外收款方的批次結算。

這些場景的共同特徵是：**單筆金額遠低於代理行體系的經濟門檻，但筆數極大。**在現有體系中，一筆一百美元的跨境匯款可能經過兩到三層代理行，每一層收取固定費用並引入一段不可見的時間，最終成本佔比可達本金的百分之幾到百分之十幾，到賬時間從數小時到數日不等，且發起方無法回答客戶"現在錢在哪裡"。

OSN 的網路層單筆技術上限設定為 **5,000 美元**。這是網路層硬頂，用於將 OSN 界定在小額清算範圍內。終端客戶的實際單筆限額由發起機構依其自身的客戶分層政策決定（普通客戶與 VIP 客戶不同），OSN 不介入這一判斷。

參與角色共四類：

角色	職責	持有什麼
發起機構	收集客戶支付需求，構建清算請求	自有客戶 KYC 記錄、自有私鑰
清算機構	在本地完成實際付款，回寫清算事實	自有客戶記錄、自有私鑰
儲備銀行	持有 1:1 美元儲備	法幣儲備帳戶
監管機構	依授權部署觀察節點	對其所監管機構資料的可見性

OSN 自身不在這張表裡持有任何客戶資產，也不持有任何機構的私鑰。

1.3 現有體系的四個結構性問題

OSN 要解決的不是"跨境匯款有點貴有點慢"這一表象，而是四個結構性問題。它們都源於同一個根因：**清算事實分散記錄在各參與方各自控制的帳本中，且每一份都可被其持有方修改。**

其一，沒有共同的事實來源。 發起行、中間行、收款行各記一本賬。三本賬在正常情況下一致，在異常情況下不一致，而判斷哪一本正確需要人工對帳。跨境、跨法域、跨時區的對帳成本，是小額匯款高費率的主要構成之一，遠大於實際的資金移動成本。

其二，過程對參與方不可見。 發起機構把報文交給代理行之後即失去可見性。客戶問"錢到哪了"，發起機構只能查詢並等待。這不是技術缺陷，而是體系結構的必然——每一段的記錄都在別人的系統裡。

其三，記錄可被單方修改，因此爭議缺乏客觀依據。 任何一方的帳本都由該方的資料庫持有，技術上可以被修改、回滾或重建。絕大多數機構不會這樣做，但"不會"是承諾，不是可核驗的狀態。當爭議真的發生時，各方只能援引各自的記錄。

其四，後量子遷移是一筆尚未支付的賬。 現有跨境支付體系的身份認證與報文簽名普遍基於經典密碼學。當具備密碼分析能力的量子計算成為現實威脅時，這些體系需要完成一次涉及全部存量金鑰、全部歷史記錄與全部參與方的遷移。這項工程的成本尚未被計入任何一家機構的帳本，但它一定會到來。

OSN 對這四個問題的回應，構成本白皮書第二章與第三章的全部內容：**用一份任何人可獨立核驗、且無人可以修改的記錄，取代分散在各方手中的多份可修改記錄；並在建立這份記錄時，一開始就使用後量子簽名。**

1.4 一筆清算的完整生命週期

以下用一筆實際清算走完全程。參與方為發起機構 A（新加坡）與清算機構 B（馬來西亞），本輪共 312 筆終端客戶訂單，淨額約 48.25 萬美元。

第一步：訂單收集。機構 A 在其自有系統內完成客戶 KYC、反洗錢篩查與收款指令收集。這一步完全發生在 A 的內部，OSN 不介入，也不接收任何客戶身份資訊。開發期採用 30 秒收集視窗——此為執行引數而非不可變協議常量，由協議版本號對應的引數定義。

第二步：構建清算請求。A 將本輪訂單序列化為 `Request`，包含每筆訂單的編號、收款人、清算行、金額與時間。`Request` 以 A 的機構主金鑰派生金鑰加密。[已實現]

第三步：價值轉移上鍊。A 在 QCC 上將對應淨額的 OSNB 轉移至 B 的白名單地址。這一步產生一個公開的交易雜湊與確認高度，二者寫入報文物件的明文 `Header`。**價值轉移在此刻即已終局，且公開可核驗，不依賴後續任何環節。** [已實現]

第四步：固定建立雜湊。

```
CreationHash = SHA3-256( Request.toByteArray() + Header.toByteArray() )
```

此雜湊一經生成永久固定。任何驗證節點讀取 `Header` 與 `Request` 密文即可重算比對，**無需持有解密金鑰即可確認內容完整。**這是 OSN 報文模型中最重要的一項確定性。[已實現]

第五步：清算方執行。B 向金鑰服務申請一次性派生金鑰，解密 `Request`，在其本地系統中完成 312 筆實際付款。這一步同樣完全發生在 B 的內部。

第六步：回寫清算事實。B 將逐筆清算結果寫入 `Result`，以其機構白名單私鑰（ML-DSA-87）產生 `ResultSignature`。**`Result` 是追加的新資料段，`Request` 不被修改。** [已實現]

第七步：封存生命週期。完成雜湊繫結建立雜湊、結果摘要與清算方簽名，成為該報文物件的最終錨點，一經生成不可覆蓋。整個生命週期設計約 1 分鐘。

各方在事後能各自核驗什麼：

誰 無需任何人配合即可核驗

機構 A 價值轉移已終局；B 的清算事實由 B 的私鑰簽署，不可抵賴

機構 B A 的請求內容未被修改；A 的價值轉移真實存在於公開帳本

監管機構 經其所監管機構授權後，可見該機構全部明文與全部雜湊錨點

任意第三方 OSNB 總量、每一次增發銷毀、每一筆轉移——無需任何授權

1.5 清算、糾錯與退款

正常路徑即 1.4 所述。清算機構在本地完成付款後回寫事實，報文物件封存。

部分失敗是常態而非例外：一批 312 筆訂單中，可能有若干筆因收款帳戶狀態、當地合規篩查或資訊錯誤而無法完成。OSN 的處理方式是—— **Result** 逐筆記錄每一筆訂單的實際狀態，成功與失敗在同一份清算事實中並存。**clearingFact** 欄位可承載各機構不統一的本地回撥與支付憑證，OSN 不要求各國機構統一其內部憑證格式。[已實現]

退款不是對歷史的修改，而是一筆新的事實。這是 OSN 與傳統清算體系在處理邏輯上的根本差別。傳統體系中，衝正是對原記錄的狀態變更；在 OSN 中，原報文物件已被雜湊封存，任何一方都無法回頭修改它。退款表現為一筆新的清算，反向引用原訂單編號，形成一條完整且互相引用的事實鏈。任何人事後重放這條鏈，看到的都是"發生了什麼以及如何被糾正"，而不是一個被抹平的最終狀態。

淨額結算與費用。機構之間採用批次淨額結算，而非逐筆全額轉移，這是 OSN 能夠承載小額高頻場景的經濟基礎。費用分兩層：一是機構向其終端客戶收取的網路費率（0.1%），二是 OSN 向成員機構收取的服務費。當 OSN 不自行承擔轉帳業務時，僅收取後者。

白名單的定位。OSNB 僅可在白名單地址之間轉移，這是協議層規則，而非可被任何人升級或繞過的機制。需要明確的是：**白名單不是商業准入的篩選工具，而是最後的法律兜底條款。**機構備案後 10 個工作日內無監管異議即開通白名單資格；機構贖回結算憑證並申請退出後，10 個工作日公開期內無法律爭議即關閉資格。OSN 不在此環節做商業裁量。

關於凍結許可權的邊界，第三章將詳述一項協議層事實：**在 QCC 上，任何規則集都無法在沒有持有人簽名的情況下轉移其資產。**可用的最高許可權是凍結，不存在從持有人地址強制劃轉或銷毀的能力。

第一章完。第二章「OSN 如何實現全球轉帳網路」將展開可驗證帳本、結算憑證發行與儲備、報文物件與加密體系、節點同步、清算框架、糾錯退款與監管觀察節點的完整實現。

第二章 如何實現全球清算網路

本章描述業務場景、執行流程與實現框架。"為什麼可信、如何獨立核驗"是第三章的內容，兩章主題有意重疊，視角不同。

2.1 清算為什麼需要一個可驗證帳本

第一章指出的四個結構性問題，根因是同一個：**清算事實分散記錄在各參與方各自控制的資料庫中。**

要消除這個根因，只有兩條路。一是所有參與方共同承認一個權威帳本——這是現有清算體系的做法，它要求各方接受同一個中心機構的記錄為準。二是讓帳本本身不屬於任何人，任何參與方都能從原始資料獨立重算出同一個結果。

跨法域、跨監管轄區的機構之間，第一條路的前提往往不成立：沒有一個所有參與方都願意接受的權威。因此 OSN 選擇第二條。

這條路對底層帳本提出三項硬性要求，缺一不可：

1. **無准入**——任何一方都可以自行部署節點並核驗，不需要任何主體批准；
2. **規則不可被單方修改**——否則參與方只能驗證過去，無法確知未來；
3. **全量可重放**——重放所依據的規則集與資料是同一份，而不是歷次變更規則的集合。

滿足這三條的帳本，參與方不需要信任運營方，只需要信任數學。QCC 是為滿足這三條而構建的。

2.2 QCC：無准入、協議凍結、全量重放

QCC 是 OSN 的底層帳本。它與 OSN 公司在資產上無關，是一條獨立的開放協議公鏈，OSN 只是其上的一個應用。

無准入。任何人都可以部署 QCC 節點、參與共識、執行超級節點。入網條件只有兩條：地址符合 QCC 標準且不重複，執行層雜湊與全網一致。不需要任何主體批准，不存在成員名單。

協議凍結。QCC 第一個正式版本釋出即凍結底層共識協議。沒有升級金鑰，沒有治理主體，沒有可修改的規則集入口，也沒有"以後靠程式化執行層補"的退路。這是 QCC 正式釋出一再推遲的原因——**新增協議必須在凍結前完成**。任何新增協議須同時滿足三條：普惠使用、必須由底層協議實現、必須滿足全量重放與執行層雜湊一致性。

全量重放。每個節點從創世高度起，用同一份規則集重算全部歷史，得出同一個執行層雜湊。這與"按高度裝配不同版本規則"的重放有本質區別：後者的重放依據是規則的歷史序列，前者是同一份規則。

沒有治理主體。QCC 不保留任何治理機構、否決權或管理員。協議對所有參與者是同一份，加入之後沒有任何一方能單方改變它。這不是承諾，是協議中不存在該功能。

2.3 容器模型與"一切皆為交易"

QCC 的帳本單位是**容器**，而非固定節奏產出的區塊。

容器是執行時執行體，近似作業系統中的程序；容器內的區塊近似執行緒。每個容器繫結唯一資產 ID——一個 OSNB 容器內只有 OSNB 交易。**容器由交易觸發拉起，3 秒內無資料即銷毀且不上鍊；有資料才產出並上鍊。**

這意味著 QCC 上不存在空容器。與按固定節奏出塊（無論有無交易）的帳本相比，儲存中不含無謂資料。鏈是單條的，容器按實際發生順序串成雜湊鏈，相鄰容器可以是不同資產。

"一切皆為交易"是 QCC 的第一原則：轉帳是交易，規則變更是交易，白名單更新是交易，凍結是交易，人工操作也是交易。不存在繞過交易管道的特權路徑——白名單規則更新與普通轉帳走同一條單執行緒准入佇列。這一點對清算網路的意義在於：**任何管理動作都留下與普通交易同等強度的公開記錄，不存在"後臺操作"。**

2.4 規則集，而非可程式化執行層

QCC 沒有任何形式的可程式化執行層。資產的能力由**系統規則集**定義，而規則集是協議的一部分，隨協議一同凍結。

這是 OSN 選擇 QCC 的決定性原因。在可程式化執行層上發行的資產，其轉移限制、凍結能力、增發許可權都由部署者編寫的程式碼決定，而這些程式碼通常可被其部署者升級、替換或重新定義。**參與方要信任的不是協議，而是部署者今天寫了什麼、明天會不會改。**

在 QCC 上，轉移限制是帳本自身規則的一部分。它不能被升級，不能被繞過，也不能被任何人重新定義——包括 OSN。

由此產生一條協議層事實，第三章將展開論證：**任何規則集都無法在沒有持有人簽名的情況下轉移其資產。**除持有人自身明確授權的機制（如繼承交易、去中心化撮合）外，不存在從持有人地址強制劃轉的能力。

2.5 OSNB：結算憑證的定位

OSNB 是 OSN 成員機構之間使用的結算憑證，由 QCC 的白名單資產機制承載，與美元 1:1 對應。

需要明確其邊界：

持有人範圍	僅白名單內的持牌金融機構
公眾可否持有	否
用途	機構間清算的記帳與結算單位
單筆網路層上限	5,000 美元
是否用於投機或流通	否，不在任何公開市場交易

OSNB 不是面向公眾的支付工具，也不是投資標的。它是機構之間清算的記帳媒介，其全部意義在於讓"誰應當向誰清算多少"這件事有一個公開可核驗的記錄。

發行門檻。 QCC 協議對穩定幣類資產的發行設有強制門檻：發行必須由多籤地址完成（單籤地址不能發行穩定幣）、固定發行費用、以及大額原生代幣質押且長期不可解押。這些門檻在協議層強制執行，目的是使穩定幣發行不能是隨意行為。

2.6 發行與銷毀：3-of-3 聯合簽署

OSNB 的增發與銷毀由 QCC 的多籤地址控制，採用 **3-of-3 聯合簽署**。

這裡必須澄清一個常被混淆的概念：**QCC 的多籤不是門限多籤（m-of-n），而是聯合簽署**。簽名人數量在地址建立時確定，一經確定，此後該地址發起的每一筆交易都必須由全部簽名人簽署，缺一不可。協議層的 threshold 恆等於簽名人總數，不存在"多數透過"這一檔。

恰當的類比不是董事會表決，而是**刑事陪審團的一致裁決**：不是多數說了算，是任何一位都能否決。

三個簽名分屬不同主體、不同託管路徑：兩個由業務經理崗位持有，第三個由業務執行總裁在其本人裝置上獨立完成，不經過任何共享服務。**公司內部不存在任何單一人員能夠完成一次增發或銷毀**。具體託管機制不在本白皮書披露範圍內，相關細節僅向監管機構提交。

一次增發的完整路徑：

1. 法幣進入已備案的儲備銀行帳戶；
2. 三名簽名人分別獨立簽署增發交易，交易描述關聯該筆儲備入金；
3. 交易上鍊，OSNB 總量變更成為公開記錄；
4. 任何人可在鏈上查得該次增發的時間、數量與描述。

銷毀路徑與之對稱。**每一次總量變更都是永久且公開的鏈上事實，不存在鏈下增發。**

簽名人失聯的處理。聯合簽署的代價是真實的：任一簽名人永久失聯，該地址即無法再發起交易。OSN 對此有兩條路徑——一是 QCC 協議層的繼承機制，二是企業內部金鑰管理制度。後者不屬於公鏈層問題，前者是協議原生能力。這一點在 2.14 與第三章進一步展開。

2.7 儲備金：多家儲備銀行與 1:1 對應

OSNB 與美元儲備 1:1 對應。儲備採用**多家儲備銀行分散託管**，避免單一銀行構成單點風險。

儲備帳戶為專項帳戶，性質接近專項資金託管而非理財產品。儲備銀行設在新加坡、受 MAS 監管——這意味著**監管機構對儲備帳戶餘額本就具有查詢能力，無需 OSN 提供任何介面或授權。**

由此形成一個可對帳的閉環：

鏈上 OSNB 總餘額 ↔ 各儲備銀行帳戶餘額合計

左側任何人可隨時自行計算，無需任何授權；右側由監管隨時查詢。兩側應當始終相等，任何偏差都可被立即發現。

這一模型與"周度披露 + 月度第三方鑑證"的驗證方式有本質區別，第三章將以"同步驗證與非同步驗證"為題展開。此處只陳述事實邊界：**儲備銀行是否提供餘額查詢介面由銀行決定，OSN 無法強制；OSN 能決定的是選擇哪家銀行作為儲備行——向監管機構與成員機構提供只讀餘額查詢，是 OSN 選擇儲備銀行的前提條件。**在儲備行安排落定之前，OSN 能做的是存入並自行查詢；對監管機構而言，查詢受其監管銀行的帳戶餘額本就不需要 OSN 授權。

2.8 白名單：協議層機制與法律兜底定位

OSNB 僅可在白名單地址之間轉移。這是**協議層機制**，不是應用層策略，也不是可被任何人升級的程式碼。

開啟不可逆。白名單由發行地址在資產發行後發起白名單交易開啟。**一經開啟，該資產永久僅支援白名單流通，無法恢復自由流通。**同樣，凍結與銷毀能力必須在資產發行時選擇，未選擇則該資產永久無法發起對應交易。這些能力的開啟機制不同，但共同點是：**都不可逆。**

發行到開啟之間存在空窗期。從資產發行到白名單交易上鍊之間，理論上存在一個短暫視窗。OSN 的立場是不必消除這個視窗——該期間的任何轉帳都是永久的鏈上事實，任何人可自行重放核驗。OSNB 發行地址的首筆轉出即為向白名單地址轉移，這一事實本身公開可查。

定位是法律兜底，不是商業篩選。這一點必須明確：

- 機構備案後 **10 個工作日內無監管異議即開通白名單資格**；
- 機構贖回結算憑證並申請退出後，**10 個工作日公開期內無法律爭議即關閉資格**；

- OSN 在此環節**不做商業裁量**，不以商業關係、費率談判或競爭關係為由拒絕或延遲。

白名單存在的理由是：當出現法律要求時，需要有一個可執行的手段。它不是 OSN 用來選擇客戶的工具。

2.9 白名單的規模與更新方式

機構發行的穩定幣面向其自身客戶時，白名單可能達到千萬級地址規模。QCC 的處理方式是將規模問題分解為兩個獨立的問題。

其一，鏈下對映。客戶身份與地址的對應關係由發行機構自行維護在鏈下。QCC 只強制執行鏈上白名單成員資格，不承載任何身份資訊。

其二，單筆更新有上限。客戶端每筆白名單更新交易所能攜帶的地址數受協議約束（當前設定為 1,000–5,000 個），因此單筆交易的體積與費用可預測，不隨白名單總長度變化。這是一項刻意的設計：如果不設上限，白名單越長則單筆更新越貴，最終導致大規模白名單在經濟上不可行。

規模驗證：QCC 測試網已完成 1 億個白名單地址的測試，超過千萬級的設計目標。測試參數可應機構及其顧問要求提供；正式基準測試報告將隨協議規範一同公佈。

2.10 凍結的邊界：能凍結，不能劃轉

在資產控制能力上，QCC 與部分現有穩定幣實現存在一項結構性差異，值得單獨說明。

QCC 上可用的最高許可權是凍結。發行方可以凍結某個地址的資產，使其無法轉出。發行方**不能**從持有人地址強制劃轉資產到第三方地址，也不能銷毀持有人地址內的資產。

據公開資訊，部分基於可程式化執行層發行的穩定幣，其發行方保留了從黑名單地址銷毀或轉移資產的能力。這兩類能力的差別在實務中很大：凍結是可恢復的、不改變歸屬的保全措施；強制劃轉與銷毀則直接改變了資產歸屬。

OSN 將凍結與解凍視為**公示義務**——每一次凍結與解凍都是鏈上公開事實，任何人可查得其時間與物件。

2.11 OSNMesObject：報文物件的三段結構

清算指令在機構之間以 **OSNMesObject** 傳遞。其結構為：

```
OSNMesObject = Header + Request + Result  
               + CreationHash + CompletionHash + ResultSignature
```

段	明文/密文	寫入方	內容
Header	明文	發起方	路由、幣種、匯率與清算規則雜湊、QCC 交易雜湊與確認高度、請求摘要、型別、建立時間、協議版本
Request	密文	發起方	清算訂單列表：編號、收款人、清算行、金額、時間、可選支付憑證
Result	密文	清算方	逐筆清算事實：訂單編號、狀態、清算時間、本地清算憑證

核心約束：歷史內容不存在編輯操作。發起方建立 Request 之後不能修改它；清算方不能修改 Request，只能追加 Result；Result 一經寫入亦不可改。**報文物件的生命週期不透過可變的狀態欄位表達，而透過兩個不可變階段的雜湊證明。**

`clearingFact` 欄位接受 JSON 或位元組附件，用於容納不同商業銀行與支付機構互不統一的本地回撥與支付憑證格式。**OSN 不要求各法域機構統一其內部憑證格式**——這是跨境清算網路能否被實際採用的關鍵之一。

2.12 兩階段密碼學完整性模型

這是 OSN V1 最重要的一項協議確定性。

建立階段：

```
CreationHash = SHA3-256( Request.toByte() + Header.toByte() )
```

拼接順序在協議中明確規定為 Request 在前、Header 在後。CreationHash 一經生成永久固定。

其價值在於驗證順序：驗證節點讀取 Header → 讀取 Request **密文** → 重算雜湊 → 與 CreationHash 比對。**全過程無需解密金鑰即可確認內容完整**。只有在完整性確認之後，才需要決定是否獲取解密金鑰。這使得完整性驗證與資料訪問許可權徹底解耦。[已實現]

完成階段：

```
ResultHash      = SHA3-256( Result.toByte() )
CompletionHash = SHA3-256( CreationHash + ResultHash + ResultSignature.toByte() )
```

CompletionHash 繼承發起方的建立事實、繫結清算方的結果摘要與機構簽名，成為完整生命週期的最終錨點，一經生成不允許重新計算後覆蓋。

ResultSignature 由清算方以其機構白名單私鑰（ML-DSA-87）產生，證明該清算結果確實來源於該授權機構，且事後不可抵賴。

全鏈雜湊演算法統一為 **SHA3-256**，包括創世容器錨定雜湊。

2.13 加密體系與主金鑰派生

報文業務資料由發起方派生金鑰體系加密。

- 派生主金鑰由機構自身持有，**不直接用於業務資料加密**；
- 每個報文物件使用一次性派生金鑰；
- 清算方收到報文後，依報文身份向金鑰服務申請該次的一次性派生金鑰；
- 機構可用自身主金鑰還原任意派生金鑰，從而解密其全部歷史報文。

資料加密層的最高許可權歸屬機構，不歸 OSN。 OSN 傳輸與同步的是密文，不具備解密能力，也不提供跨轄區直接讀取客戶明文的許可權。這一設計的目的是保護終端客戶隱私：即便 OSN 的伺服器被完全攻破，攻擊者取得的也只是無法解密的密文。

機構間 TCP 通訊幀以機構對應的 ML-DSA-87 私鑰簽名，實現節點身份認證與安全通訊；斷網後支援自動重連與同步。

2.14 金鑰輪換

機構金鑰輪換不依賴任何協議變更或協調視窗，而是利用 QCC 的資產轉移能力完成：

1. 機構生成新的 ML-DSA-87 金鑰對；
2. 將其持有的 OSNB 轉移至新地址；
3. 更新白名單地址。

建議輪換週期為 1–5 年，由機構自行決定。**整個過程不需要 OSN 參與金鑰生成，不需要停機，也不需要其他機構配合。**

這一點與傳統體系形成對照：在共享金鑰或中心簽發證書的體系中，金鑰輪換通常需要協調視窗與中心方配合。在 OSN 中，輪換隻是一筆普通的資產轉移加一次白名單更新。

2.15 節點架構與同步

網路形態。OSN 第一階段採用 S/C (Server / Client-Node) 組織方式：OSN 運營方提供核心服務節點（規劃全球 6 個，主備容災），成員機構自行部署機構節點並經授權加入。預期機構規模 1,000 以上。

節點型別	職責	持有資料
OSN 核心服務節點	網路服務、同步、授權	全網密文報文
機構節點	本機構清算執行與資料持有	僅本機構明文與金鑰
監管觀察節點	依授權對其監管物件的可見性	授權範圍內資料

同步機制。節點之間以狀態憑證替代單純心跳包，可由定時或狀態變化觸發。本地儲存採用標準檔案盒子方式，透過 API 拉取實現冗餘與恢復。**節點恢復以不可變物件與可重放歷史為基礎**——網路故障不刪除任何業務事實，恢復後透過同步重建本地狀態與索引。

QCC 層的一項後量子工程分層，值得單獨說明。後量子簽名的體積顯著大於經典簽名。QCC 的處理方式是：**公鑰與簽名都不進入容器，而是各自作為獨立的內容定址快照庫同步。**簽名庫以簽名的 SHA3-256 作為定址鍵，分片儲存，新節點透過分片逐片下載後重建索引，增量同步透過尾分片體積核對完成。

每個節點必須強制同步這兩個庫，否則無法完成重放執行。這一分層是後量子簽名能夠在實際帳本中落地的關鍵工程決策之一——它把"簽名很大"這個成本從容器體積中移出，同時不損失任何可驗證性。

2.16 清算框架與淨額結算

機構之間採用批次淨額結算，而非逐筆全額轉移。這是 OSN 能夠承載小額高頻場景的經濟基礎：312 筆終端訂單在鏈上只表現為一次淨額價值轉移。

一輪清算的完整流程：

```
發起方收集訂單 → 構建 Request → 計算請求摘要 → 完成 Header  
→ 計算 CreationHash → 在 QCC 轉移淨額 OSNB → 傳送報文物件  
→ 清算方獲取一次性派生金鑰 → 解密 Request → 本地非同步清算  
→ 構建逐筆清算事實 → 構建 Result → ResultHash  
→ ML-DSA-87 簽名 → CompletionHash → 報文完成 → 節點廣播同步
```

報文物件的生命週期設計約 **1 分鐘**。開發期採用 30 秒訂單收集視窗——此為執行引數而非不可變協議常量，由協議版本號對應的引數定義。**已建立物件的解釋不因未來版本變化而被重新解釋**，這是協議版本管理的基本原則。

費用結構分兩層：

層	收取方	說明
網路費率 0.1%	機構向其終端客戶	OSN 前期自行承擔機構轉帳業務時由 OSN 收取；OSN 不做轉帳業務後不收此項
成員機構服務費	OSN 向成員機構	OSN 的長期收入來源

這一結構對應 OSN 的分階段定位：**前期自己持牌下場做支付業務以驗證系統，驗證成功後退出交易支付業務，改由成員機構承擔支付，OSN 只做儲備金管理與技術維護。**

2.17 糾錯與退款

部分失敗是常態。一批訂單中總有若干筆因收款帳戶狀態、當地合規篩查或資訊錯誤而無法完成。Result 逐筆記錄每筆訂單的實際狀態，成功與失敗在同一份清算事實中並存，不需要整批迴滾。

退款是一筆新的事實，不是對歷史的修改。這是 OSN 與傳統清算體系在處理邏輯上的根本差別。

傳統體系中衝正是對原記錄的狀態變更：原記錄被改寫為"已衝正"，最終狀態被抹平。在 OSN 中，原報文物件已被雜湊封存，任何一方——包括 OSN——都無法回頭修改它。退款表現為一筆新的清算，反向引用原訂單編號，形成一條完整且互相引用的事實鏈。

任何人事後重放這條鏈，看到的是"發生了什麼以及如何被糾正"，而不是一個被整理過的最終狀態。對爭議處理、審計與監管調查而言，這兩者的價值差別很大。

2.18 全量同步驗證與監管觀察節點

審計重放。OSN 的審計不依賴 OSN 提供的報表，而依賴重放：從不可變的報文物件與公開的鏈上交易出發，任何具備資料訪問權的一方都能重建全部清算曆史，並與自己的記錄比對。

監管觀察節點。OSN 提供統一的觀察節點技術框架，任何成員機構在其監管要求時均可配置。

其許可權模型有一條關鍵約束，必須明確陳述：**觀察節點由成員機構授權開通，不由 OSN 開通，也不由監管自行開通。**

原因是技術性的，而非政策選擇。一個接入網路的節點，本身不攜帶任何機構證明、機構資訊或機構金鑰。**OSN 無法認定某個節點是否真的屬於某個監管機構**——OSN 也不會為監管機構生成機構金鑰。在無法自證來訪方身份的前提下開通明文訪問許可權，本身就是一個資料安全缺口。因此技術上繞不開由成員機構授權這一條路徑。

需要同時說明的是：技術上是機構向監管授權，**行政上監管有權要求機構必須配合**。兩者並不衝突——機構既有權授權監管，技術上也可能授權他方，OSN 無法阻擋也無權阻擋。

協議層限制：每個白名單機構節點只能授權一個觀察節點，不能授權第二個。這項限制寫在技術框架中，而不是寫在協議條款裡——它使"授權範圍被無限擴散"在技術上不可能發生。

監管觀察節點能看到什麼：

	可見範圍
其所監管機構的報文明文	是（經該機構授權後）
其他機構的報文明文	否
全網雜湊錨點與完整性證明	是
OSNB 總量、每一次增發銷毀與轉移	是——且無需任何授權，公開可查

最後一行值得強調：**監管機構核驗 OSNB 總量與儲備對應關係，完全不需要 OSN 授權，也不需要部署任何節點。**這部分事實是公開的。

第二章完。第三章「OSN 創新要點」將從"如何獨立核驗"的角度，重新論證本章描述的實現——包括同步驗證與非同步驗證的區別、聯合簽署的權力結構、資產控制權轉移、以及原生後量子的工程含義。

第三章 創新要點

第二章描述"怎麼做"，本章論證"憑什麼可信"。兩章內容有意重疊，視角不同。本章每一節按四個層次組織：**主張** → **依據** → **如何獨立核驗** → **當前狀態**。

3.1 協議事實與權威事實

主張。 跨機構、跨法域的清算，其記帳層不能建立在權威事實之上，只能建立在協議事實之上。

依據。 一份清算記錄要被所有參與方接受為"事實"，只有兩條路徑。

權威事實——各方共同承認某個主體的記錄為準。這是現有全球清算體系的做法，執行了數十年，規模遠超任何帳本技術。它成立的前提是存在一個各方都願意接受的權威。

協議事實——記錄的真偽由規則與資料決定，任何人用同一份規則重算同一份資料都得到同一個結論，不需要承認任何主體。

參與方越多、越分散、越跨法域，第一條路徑的前提越難成立：不是效率問題，而是那個"共同承認的權威"可能根本不存在，或者曾經存在而現在不被所有人接受。當這個前提失效時，清算的記帳層只剩下第二條路。

這不意味著權威消失。 現實中的清算權威不只是記錄者，還是違約時的兜底者。協議事實能取代記錄職能，不能取代救濟職能。因此實際形態是：**協議事實做帳本層，法律與持牌主體做兜底層**。OSN 正是這個結構——白名單是法律兜底條款，QCC 是帳本層。

如何獨立核驗。 部署一個 QCC 節點，從創世高度重放全部歷史，比對執行層雜湊。這個過程不需要 OSN、不需要任何機構、也不需要任何人的許可。

當前狀態。 架構原則，已在 QCC 中實現。

3.2 核心命題：規則不可篡改 + 全量獨立重放

主張。 一個能夠承載全球化清算的底層帳本，必須同時滿足兩項性質：**規則不可被任何單方修改，且任何人可以對全量資料獨立重放核驗**。這兩項缺一，"無需信任"就不成立。

依據。 拆開看這兩項各自不足：

- 只有**獨立重放**而規則可變——參與方能驗證昨天，無法確知明天。今天驗證得再幹淨，也推不出明天的規則不變。

- 只有**規則凍結**而資產單一——帳本只能服務它自己那一種資產，無法承載多機構、多幣種的清算。

現有帳本大多落在這個二維平面的某一側：可程式化執行層豐富但規則可升級，或規則近乎不可變但只服務單一資產。**同時滿足兩項，是 QCC 的設計出發點。**

必須說明的是，規則可變的一方並非疏忽，而是主動取捨——可升級意味著 bug 可修、功能可加。OSN 選擇了另一端，代價是真實的：**協議凍結後，共識層缺陷沒有"發補丁"這條路**。處理方式見 3.3 與 3.16。

如何獨立核驗。閱讀 QCC 原始碼，確認其中不存在升級金鑰、治理入口或可修改的規則集介面。這是程式碼事實，不是承諾——不需要相信任何人的話。

當前狀態。協議規格與原始碼將於主網釋出時公開。[路線圖節點]

3.3 技術上不可篡改，與事實上不可篡改

主張。這是兩項不同的性質，多數關於"區塊鏈不可篡改"的討論把它們混為一談。

依據。

技術上不可篡改是密碼學性質：雜湊鏈完整，任何對歷史的修改都會被檢測出來。這是協議屬性，讀程式碼即可確認。

事實上不可篡改是網路性質：實際上不存在任何主體有能力協調足夠多的節點重寫歷史。它不由程式碼保證——聯盟鏈與許可鏈的雜湊鏈同樣完好，但成員協商即可回滾。**技術屬性在治理面前不作數。**

這項區分對 OSN 的意義在於誠實：

	技術上不可篡改	事實上不可篡改
性質	協議屬性	網路屬性
何時成立	主網上線即成立	隨節點數量與部署方分散度增長而增強
如何核驗	讀程式碼	數節點、看部署方
QCC 現狀	滿足	演進中

任何帳本在啟動初期都不滿足第二項，比特幣最初兩年同樣如此。區別在於路徑是否存在：**無准入設計使這條路徑存在，許可制設計使這條路徑根本不存在**。許可鏈的回滾能力是結構性內建的，它不在這條演進路徑上。

如何獨立核驗。第一項讀程式碼；第二項查詢當前節點數量與部署方分佈——這項資料任何人可隨時自行採集。

當前狀態。技術不可篡改 [已實現] ；事實不可篡改 [演進中，隨網路增長] 。

3.4 為什麼凍結協議必須原生後量子

主張。 對一個承諾規則凍結的協議，後量子簽名不是可選項，而是必須在創世前完成的一次性決定。

依據。 這不是效能論證，而是邏輯封閉性論證，分兩步：

第一步。 更換籤名演算法是共識規則的變更。一個能夠隨時完成該變更的系統，按定義就是規則可被修改的系統——3.2 的第一項當場破產。**凍結與遷移不能同時成立。**

第二步。 獨立重放要求籤名驗證規則從創世到永遠是同一份。若簽名規則在某個高度變更，重放依據就從"一份規則"變成"按高度裝配的規則序列"，這正是 3.2 判定強度較低的那一類。

因此：**一個協議若承諾凍結，其簽名方案必須在第一個區塊之前定案。**這條推論同時給出一個篩選標準——所有把後量子留到日後解決的帳本，連"凍結"那一條都不滿足。

一個可觀察的旁證：現有主流帳本的後量子遷移路徑普遍是"帳戶可選升級到抗量子金鑰"這類方案，必然要經過一次協議變更。這不是它們的缺陷，而是它們選擇了可升級那一端的必然結果。

如何獨立核驗。 檢查該帳本創世塊使用的簽名演算法，以及是否存在協議升級機制。這兩項都是公開可查的事實。

當前狀態。 ML-DSA-87 自創世起使用。[已實現]

3.5 原生 ML-DSA-87 與遷移成本

主張。 OSN 的參與機構不會從這套基礎設施繼承任何後量子遷移義務。

依據。 體系中的每一處簽名——QCC 上的價值轉移、清算結果簽名、機構間節點身份認證、結算憑證的增發與銷毀——統一使用 ML-DSA-87，即 NIST 標準化模格簽名方案（FIPS 204）的最高引數集。內容完整性統一使用 SHA3-256（FIPS 202）。

所有權路徑上不存在任何橢圓曲線金鑰，在任何歷史時點都不存在。

正在推進後量子準備計劃的機構，通常要為所接入的每一套帳本規劃三項工作：經典金鑰材料清點、含切換點的遷移路徑、切換前所生成金鑰與記錄的處理政策。**在 OSN 上這三項都不產生**，因為不存在需要清點的經典金鑰。

金鑰輪換仍是常規運維事項，但它與"遷移"是兩回事——輪換隻是生成新金鑰對、轉移資產、更新白名單，不涉及協議變更，不需要協調視窗。

範圍宣告。 本節所述限於簽名與內容完整性。節點間傳輸層機密性及其所用金鑰封裝機制另行推進，本白皮書不作主張。

如何獨立核驗。 檢視任意一筆鏈上交易的簽名結構與演算法標識。

當前狀態。 [已實現]

3.6 同步驗證與非同步驗證

主張。 現有主流結算憑證的儲備驗證是**非同步**的；OSN 的是**同步**的。這是本白皮書最重要的一項論點。

依據。

非同步驗證的典型形態是：發行方定期披露儲備構成，第三方會計師事務所定期出具鑑證報告。使用者在兩次披露之間處於資訊空白，且必須信任披露方與鑑證方。**驗證的時點由發行方決定。**

同步驗證的形態是：任何時刻都可以取得兩側的資料並比對。

鏈上 OSNB 總餘額 ↔ 各備案儲備銀行帳戶餘額合計

- **左側：**任何人任何時刻可自行計算，不需要任何授權、不需要 OSN 配合、不需要部署任何節點。總量、每一次增發與銷毀的時間與數量、每一筆轉移，全部公開。
- **右側：**儲備銀行設在新加坡、受 MAS 監管。**監管機構對受其監管銀行的帳戶餘額本就具有查詢能力**，不需要 OSN 提供任何介面或授權。

兩側應當始終相等。任何偏差可被立即發現，而不是等到下一次披露。

左側既可由鏡像節點即時跟蹤，也可透過全量重放從創世起獨立重建。結算憑證僅在儲備資金到帳後增發、在資金劃出前銷毀，因此鏈上總量在任何時刻都不應超過儲備餘額。

邊界要說明白。 OSN 無法強制儲備銀行向第三方提供餘額查詢介面，但可以把它作為選擇儲備銀行的前提條件：只有向監管機構與成員機構提供只讀餘額查詢的銀行，才會被選為儲備行。因此嚴格地說：

- **絕大部分主張不依賴任何人配合**——鏈上側的全部事實、報文完整性、執行層重放一致性；
- **僅法幣側餘額需要配合**——而對金融機構與監管機構而言，取得受監管銀行的帳戶餘額確認並非難事。

這是 OSN 的啟動期門檻，不是驗證體系的缺口。

與審計的關係。 同步驗證不取代審計。餘額無法證明的事項——儲備資產的法律權屬、是否存在質押等權利負擔、託管條款——仍由定期審計覆蓋。改變的是：餘額本身不再需要等待審計，審計工作從“確認過去某一時點的餘額”轉向“核實餘額背後的法律安排”。

如何獨立核驗。 鏈上側：任何人立即可做。法幣側：監管機構或經授權的審計方向儲備銀行核實。

當前狀態。 鏈上側 [已實現]；儲備行安排 [進行中]。

3.7 無需解密的完整性驗證

主張。 驗證一份清算報文的內容是否完整，不需要有權讀取它的內容。

依據。 CreationHash 對 Request 的**密文位元組**與 Header 計算。因此驗證節點的流程是：讀取 Header → 讀取 Request 密文 → 重算 SHA3-256 → 比對。全程不觸碰解密金鑰。

這把兩件通常被綁在一起的事徹底解耦：

	傳統做法	OSN
確認內容未被修改	需要讀取內容	不需要
誰能做完整性驗證	有資料訪問權的一方	任何持有密文的節點
客戶隱私	驗證方看得見	驗證方看不見

對跨境清算的實際意義：**一個不該看到某國客戶明文的節點，仍然能夠證明該報文未被篡改**。資料保護要求與可驗證性要求在此不再衝突。

如何獨立核驗。官方網站提供了瀏覽器內的演示：修改任意欄位，觀察 CreationHash 與已存錨點失配。演示使用自包含的 SHA3-256（FIPS 202）實現，不向外傳輸任何資料。

當前狀態。〔已實現〕

3.8 不可編輯的報文物件，與可變狀態記錄

主張。報文物件的生命週期由兩個不可變階段的雜湊表達，而不是由一個可變的狀態欄位表達。

依據。傳統清算報文通常帶有一個 `status` 欄位，隨流程推進被反覆改寫：待處理 → 處理中 → 已完成。這種設計的問題是**最終只留下最後一個狀態**——中間發生了什麼，取決於日誌是否被完整保留，而日誌由記錄方控制。

OSN 的做法是：發起方建立 Request 後不可修改；清算方不修改 Request，只追加 Result；兩個階段各自被雜湊封存。**"這份記錄現在處於什麼階段"由哪些雜湊已經生成來回答，而不是由某個欄位的當前值回答**。

由此產生的性質：**任何一方，包括 OSN 本身，都不具備修改已封存內容的能力**。這不是許可權設定，是結構——修改後雜湊即不匹配，而雜湊已經被對方持有。

如何獨立核驗。對任意歷史報文物件重算兩個雜湊並比對。

當前狀態。CreationHash 〔已實現〕；CompletionHash 的最終位元組拼接與編碼規則屬協議凍結項，Java 實現前最終確認。〔測試中〕

3.9 退款作為新事實：對審計與爭議的價值

主張。在 OSN 中不存在"衝正"這一動作。糾錯表現為一筆新的、反向引用原訂單的清算事實。

依據。傳統體系中，衝正改寫原記錄，最終狀態被抹平為"已衝正"。審計時看到的是整理過的結果，而整理過程由記錄方控制。

在 OSN 中，原報文物件已被雜湊封存，無法回頭修改。退款是一筆新的清算，反向引用原訂單編號，形成互相引用的事實鏈。

任何人事後重放這條鏈，看到的是"發生了什麼，以及如何被糾正"。

對三類場景的價值：

- **爭議處理**——雙方援引的是同一份記錄，而不是各自的記錄；
- **審計**——審計物件是事實鏈本身，不是發行方提供的報表；
- **監管調查**——糾錯行為本身也是永久記錄，無法事後消除。

如何獨立核驗。沿訂單編號的引用關係重放整條事實鏈。

當前狀態。 [已實現]

3.10 聯合簽署：不是多數表決，是一致裁決

主張。QCC 的多籤是**聯合簽署**，不是門限多籤（m-of-n）。協議層的 threshold 恆等於簽名人總數。

依據。多籤地址在建立時確定簽名人數量，此後該地址發起的每一筆交易都必須由**全部**簽名人簽署，缺一不可。協議中不存在"多數透過"這一檔。

恰當的類比不是董事會表決，而是**刑事陪審團的一致裁決**：不是多數說了算，是任何一位都能否決。

這項設計對結算憑證發行的直接含義：

- **不存在"多數合謀即可增發"的攻擊面**——需要全部簽名人同時失守；
- **每一位簽名人都持有真實的否決權**，而不是形式上的會籤；
- **公司內部不存在任何單一人員能夠完成一次增發或銷毀。**

代價是真實的，必須一併說明。任一簽名人永久失聯，該地址即無法再發起交易，其控制的資產隨之鎖定。這不是可以迴避的問題，處理路徑有二：QCC 協議層的繼承機制（3.12），以及企業內部的金鑰管理制度。後者不屬於公鏈層問題。

如何獨立核驗。查詢該多籤地址的簽名人配置與歷史交易的簽名數量。

當前狀態。 [已實現]

3.11 凍結的邊界：能凍結，不能劃轉

主張。 在 QCC 上，任何規則集都無法在沒有持有人簽名的情況下轉移其資產。可用的最高許可權是凍結。

依據。 發行方可以凍結某個地址的資產，使其無法轉出。發行方**不能**：

- 從持有人地址強制劃轉資產至第三方地址；
- 銷毀持有人地址內的資產。

據公開資訊，部分基於可程式化執行層發行的結算憑證，其發行方保留了從特定地址銷毀或轉移資產的能力。這兩類能力在實務中差別很大：

	凍結	強制劃轉 / 銷毀
是否改變資產歸屬	否	是
是否可恢復	是	否
性質	保全措施	處分行為

這項差別對持有機構的意義直接：**持有 OSNB 的機構，其資產的歸屬不可能在沒有其簽名的情況下發生變化。**最壞情況是資產被凍結，而凍結是可恢復的、留有公開記錄的保全措施。

如何獨立核驗。 檢視 QCC 規則集中定義的資產操作型別。

當前狀態。 [已實現]

3.12 資產控制權轉移：所有權與控制權的分離

主張。 在 QCC 上，資產的**發行控制權**可以整體轉移，而持有人的資產一枚都不需要移動，且轉移過程留下永久可核驗的公開記錄。

依據。 考慮一個真實場景：一家發行了結算憑證的機構被全資收購，或進行重大股權變更、治理結構調整。

在現有體系中通常有兩條路：把全部持有人遷移到新的發行合約（成本高、且需要每一位持有人配合），或者把控制權在鏈下私下移交給新股東（鏈上毫無痕跡，持有人無從得知誰在控制這項資產）。

在 QCC 上，這是一筆**資產控制權轉移交易**：原控制地址簽名，新控制地址生效，鏈上留下永久且任何人可核驗的記錄。持有人的餘額不變，地址不變，無需任何操作。

真正的論點不是"資產可以被收購"，而是：所有權與控制權在協議層是分離的，且控制權的變更是公開可核驗的事實。這一結構同時回答了發行方最實際的幾個焦慮：

- 簽名人離職或長期失聯 → 控制權可依既定路徑轉移；
- 公司重組、被收購、股東變更 → 一筆交易完成，持有人無感；

- 治理結構升級（如從單籤升級為多籤）→ 協議原生支援。

單籤地址與多籤地址之間的控制權轉移路徑均已實現並測試。

關於同類能力的說明。 這一能力在現有公鏈中少見，但本白皮書不主張唯一性——我們未對全部現有帳本作系統性核查。可以確認的是：在可程式化執行層上，這類能力通常由發行方自行編寫的程式碼實現，因而同樣可被其升級或重新定義；在 QCC 上，它是協議的一部分。

如何獨立核驗。 查詢該資產的控制權變更交易歷史。

當前狀態。 [已實現]

3.13 白名單：法律兜底，不是商業篩選

主張。 OSNB 的白名單機制是最後的法律兜底條款，不是 OSN 用來選擇客戶或施加商業影響的工具。

依據。 一個由單一主體控制准入的清算網路，無論其技術如何，最終仍然是一個權威事實體系——因為那個主體可以決定誰能參與。OSN 透過三項安排使這件事在制度上被約束：

1. **開通標準是監管異議，不是商業判斷。** 機構備案後 10 個工作日內無監管異議即開通；
2. **退出同樣有明確路徑。** 機構贖回結算憑證並申請退出後，10 個工作日公開期內無法律爭議即關閉資格；
3. **OSN 不做商業裁量。** 不以商業關係、費率談判或競爭關係為由拒絕或延遲。

同時必須承認邊界：**白名單確實是一項權力。** OSN 對它的立場不是“我們不會濫用”（那是承諾），而是把行使條件寫成可被觀察和檢驗的規則，且每一次白名單變更都是公開的鏈上交易——**行使記錄本身無法隱藏。**

如何獨立核驗。 白名單更新是普通鏈上交易，與轉帳走同一條准入佇列，任何人可查得每一次變更的時間與物件。

當前狀態。 協議機制 [已實現] ；准入制度 [隨牌照程序確立] 。

3.14 監管觀察節點：OSN 無法自行開通

主張。 監管觀察節點由成員機構授權開通，OSN 無法代為開通。這不是政策選擇，是技術必然。

依據。 一個接入網路的節點本身不攜帶任何機構證明、機構資訊或機構金鑰。**OSN 無法認定某個節點是否真的屬於某個監管機構**，也不會為監管機構生成機構金鑰。在無法自證來訪方身份的前提下開通明文訪問許可權，本身就構成資料安全缺口。

因此技術上繞不開由成員機構授權這一條路徑。

技術與行政並不衝突：技術上是機構向監管授權；行政上監管有權要求機構必須配合。機構既有權授權監管，技術上也可能授權他方，OSN 無法阻擋也無權阻擋。

協議層限制：每個白名單機構節點只能授權一個觀察節點。這項限制寫在技術框架中而非條款裡——它使"授權範圍被無限擴散"在技術上不可能發生。

同時說明：監管核驗 OSNB 總量與儲備對應關係，完全不需要觀察節點，也不需要任何授權。那部分事實是公開的。觀察節點解決的是明文報文可見性，不是帳本可見性。

如何獨立核驗。檢視觀察節點的授權機制與數量限制的實現。

當前狀態。技術框架 [已實現] ；實際部署 [隨沙盒程序] 。

3.15 成本可確定性：非圖靈完備的經濟後果

主張。OSN 的單筆清算成本是事先可精確計算的，而不是估算的。

依據。QCC 沒有可程式化執行層。資產操作由規則集定義，每一種操作的執行路徑是確定的，因此其費用可以在交易發起前精確算出，且不隨網路狀態變化。

在圖靈完備的執行環境中，一筆交易的執行成本依賴執行時路徑與鏈上擁堵，事前只能估計。這不是最佳化問題，而是圖靈完備本身的性質。

對清算機構的實際意義：**一筆跨境轉帳的成本必須能寫進產品定價，不能是浮動的。**可預測性在這裡比絕對值更重要。

同時要說清楚成本的分層。技術成本只是機構採用一套清算基礎設施總成本中很小的一部分——合規評估、法律意見、系統改造、內部審批、對手方協調才是大頭。OSN 對此的應對不在技術側：持牌降低合規不確定性，免費培訓降低學習成本，公開規範降低整合成本。**這些不是技術最佳化，但按採用成本決定勝負這一規律，它們才是關鍵。**

如何獨立核驗。在測試網上對同一操作反覆發起交易，比對費用。

當前狀態。QCC 層 [已實現] ；OSN 層費率結構 [隨牌照程序確立] 。

3.16 當前階段與路線圖

本白皮書對每一項主張標註了狀態。此處集中說明當前階段。

已實現並可核驗：

- QCC 容器模型、規則集、執行層雜湊一致性、全量重放
- 原生 ML-DSA-87 與 SHA3-256
- 多籤聯合簽署、資產控制權轉移、白名單、凍結邊界
- 白名單規模：測試網 1 億地址測試已完成（正式基準報告待發布）
- OSNMesObject 三段結構、CreationHash、金鑰派生體系

- 簽名庫與公鑰庫的分層同步

測試中：

- CompletionHash 的最終位元組拼接與規範編碼
- OSN 層清算框架與節點同步
- 永久測試網

設計目標，尚未壓測：

- OSN 層 100,000 TPS

路線圖節點：

階段 內容

- | | |
|---|--|
| 一 | QCC 永久測試網上線；協議凍結前的最後新增協議完成 |
| 二 | 主網釋出，協議規格與原始碼公開 |
| 三 | OSN 取得牌照，首批成員機構接入，跑通真實清算 |
| 四 | OSN 退出交易支付業務，改由成員機構承擔支付，OSN 只做儲備金管理與技術維護 |

關於協議凍結後的缺陷處理。 3.2 指出凍結的代價是共識層缺陷沒有"發補丁"這條路。OSN 與 QCC 的立場是明確的：**協議中不包含任何修改歷史執行結果的機制**。任何規則變更都無法作用於既有歷史；若出現必須處理的致命共識缺陷，唯一路徑是停止當前鏈、以缺陷發生前的狀態為創世快照啟動新鏈。

這不是"我們保證不改"這樣的承諾，而是協議裡沒有那個功能——**任何人，包括 QCC 的作者，都不具備修改已生效歷史的能力**。

第三章完。第四章為常見問題，按公司與牌照、資金與儲備、反洗錢與合規、技術與安全、持續經營五組編排。

第四章 常見問題

本章回應監管機構與金融機構在評估階段最常提出的問題，按五組編排。回答力求直接。凡涉及尚未實現的部分，均明確標註。

一、公司與牌照

Q1 OSN 是什麼主體？股權結構如何？

Open Settlement Network Pte. Ltd.，新加坡註冊，**沒有母公司**，股權直接由四名股東持有，不存在多層控股或離岸架構。公司分技術、運營、融資、業務四個團隊。技術架構由公司自行設計與實現，未採用第三方現成方案。

Q2 申請哪一類牌照？為什麼是這一類？

OSN 正在準備向 MAS 申請**標準支付機構（SPI）牌照**。選擇 SPI 而非大型支付機構牌照，是因為第一階段的業務規模、機構數量與交易量都刻意控制在有限範圍內，目標是先驗證系統而非追求規模。

需要明確：**截至本白皮書釋出，OSN 尚未取得任何 MAS 牌照，不向公眾提供支付服務。**

Q3 OSN 與 QCC 是什麼關係？是同一個主體嗎？

不是。**QCC 是一條獨立的開放協議公鏈，與 OSN 公司在資產上無關**。OSN 是 QCC 之上的一個應用，與任何其他使用 QCC 的機構地位相同。

OSN 不控制 QCC，無法暫停它，也無法修改它的規則——QCC 協議中不存在任何變更入口或治理主體。這一分離是刻意的：如果 OSN 能夠控制底層帳本，本白皮書關於獨立可驗證性的全部主張都不成立。

Q4 OSN 是否向公眾發行數字資產？

否。OSNB 是機構間結算憑證，**僅可在白名單內的持牌金融機構地址之間轉移，公眾不可持有**，不在任何公開市場交易，不作為投資標的推廣。這一限制由帳本的協議規則強制執行，不是商業政策。

Q5 OSN 是否提供外匯兌換？

否。OSN 不做外匯兌換、不持有終端客戶、不參與任何一方的支付執行。匯率由參與機構之間約定，其協議雜湊記錄在報文物件的明文頭部，用於事後核驗，OSN 不定價也不撮合。

Q6 沙盒與牌照兩條路徑是什麼關係？

兩條路徑**獨立推進，互不構成前提**。牌照申請是常規監管路徑；Sandbox Plus 申請的目的是在受控環境中與金融機構聯合驗證系統。任一路徑的進展不依賴另一路徑。

截至本白皮書釋出，**兩項申請均在籌備中，均未獲批**。

二、資金與儲備

Q7 OSNB 的法律性質是什麼？

OSNB 是機構間清算的記帳與結算憑證，與美元 **1:1** 對應，由全額儲備支援。它的全部意義在於讓"誰應當向誰清算多少"有一個公開可核驗的記錄，不承擔價值儲藏或投資功能。網路層單筆上限 5,000 美元，用於將 OSN 界定在小額清算範圍內。

Q8 儲備資金如何持有？

採用**多家儲備銀行分散託管**，避免單一銀行構成單點風險。儲備帳戶為專項帳戶，性質接近專項資金託管，不投入任何理財或收益類產品。儲備銀行設在新加坡、受 MAS 監管。

Q9 誰有權增發或銷毀 OSNB？

由多籤地址控制，採用 **3-of-3 聯合簽署**——不是門限多籤，協議層的 threshold 恆等於簽名人總數，缺一不可。三個簽名分屬不同主體、不同託管路徑，其中一個由業務執行總裁在其本人裝置上獨立完成，不經過任何共享服務。

公司內部不存在任何單一人員能夠完成一次增發或銷毀。具體託管機制不在白皮書披露範圍內，相關細節單獨向監管提交。

Q10 監管如何驗證儲備與發行總量的對應關係？

分兩段，兩段都不需要 OSN 配合：

- **鏈上側**：OSNB 總量、每一次增發與銷毀、每一筆轉移，公開可查。任何人任何時刻可自行計算，不需要向 OSN 申請任何許可權，也不需要部署節點。
- **法幣側**：儲備帳戶餘額。儲備行受 MAS 監管，監管對帳戶餘額本就具有查詢能力。

兩側應當始終相等。與"周度披露 + 月度第三方鑑證"的驗證方式相比，此模型**不存在披露間隔**——任意時點均可比對。

需要誠實說明：OSN 無法控制儲備銀行是否提供餘額查詢介面。對監管機構與金融機構而言，取得受監管銀行的帳戶餘額確認並非難事；對 OSN 自身而言，這是啟動期的商業門檻。

Q11 終端客戶的資金是否經過 OSN 的帳戶？

否。客戶付款由發起機構在其本地收取，實際付款由清算機構在其本地完成。OSN 不接觸任何一方的客戶資金，只承載清算指令與清算事實的記錄。儲備帳戶中的資金對應的是機構間結算憑證，不是終端客戶資金。

Q12 如果某家儲備銀行出現問題怎麼辦？

這正是採用多家儲備銀行的原因。單一銀行的問題不會導致全部儲備不可用。同時，儲備為專項帳戶而非投資產品，不承擔市場風險。

需要說明的是，**銀行破產風險不是 OSN 能夠消除的風險**，任何持有法幣儲備的機構都面對同一問題。OSN 能做的是分散、選擇受監管機構、並使儲備與發行量的對應關係隨時可查——**使問題能夠被及早發現，而不是聲稱問題不會發生。**

三、反洗錢與合規

Q13 KYC 由誰執行？

由參與機構對其自身客戶執行。OSN 不持有終端客戶，不執行客戶層面的 KYC。客戶身份記錄、以及客戶與地址的對映關係，全部留在發行機構側。

帳本本身不承載任何身份資訊，只承載地址與交易。

Q14 OSN 如何執行制裁名單篩查？

制裁名單篩查在**機構側**執行——由發起機構在收集客戶指令時完成，由清算機構在本地付款前再次執行。這與機構現有的合規流程一致，OSN 不要求機構改變其篩查工具或流程。

在 OSN 層面，機構准入本身受白名單約束，非白名單地址無法接收 OSNB。

Q15 白名單與制裁名單是什麼關係？

兩者層次不同。**制裁名單針對終端客戶，由機構執行；白名單針對機構地址，由協議執行。**

白名單的定位是最後的法律兜底條款，不是商業篩選工具：機構備案後 10 個工作日內無監管異議即開通；贖回退出後 10 個工作日公開期內無法律爭議即關閉。**OSN 在此環節不做商業裁量**，不以商業關係或競爭關係為由拒絕或延遲。

Q16 可疑交易如何報告？

由參與機構依其所在法域的義務報告。OSN 作為持牌主體，就其自身可觀察到的機構間清算行為承擔相應報告義務。

OSN 可觀察的是密文報文的路由與頻次，**不可觀察終端客戶身份與交易明細**——這部分資料 OSN 不具備解密能力。

Q17 個人資料保護（PDPA）如何處理？

終端客戶的個人資料從不進入帳本，也不以明文形式進入 OSN 的系統。報文業務資料以發起機構派生金鑰體系加密，OSN 傳輸與同步的是密文，不具備解密能力。

即便 OSN 的伺服器被完全攻破，攻擊者取得的也只是無法解密的密文。這一點是 OSN 資料保護方案的核心，而不是附加措施。

Q18 跨境資料傳輸如何處理？

報文以密文形式在機構節點之間同步，**解密能力僅在資料所屬機構手中**。OSN 不提供跨轄區直接讀取客戶明文的許可權——技術上 OSN 也不具備該能力。

對於監管訪問，路徑是機構授權的觀察節點，範圍限於該機構自身資料（見 Q26）。

四、技術與安全

Q19 為什麼使用公鏈，而不是許可鏈或聯盟鏈？

因為許可鏈無法提供本方案所依賴的那一項性質。

許可鏈可以具備完好的雜湊鏈，同時具備成員協商回滾的能力——技術上不可篡改，事實上可篡改。回滾能力是其結構性內建的屬性，不是配置選項。如果帳本可以被其運營者協商回滾，那麼參與方要信任的仍然是運營者，獨立可驗證性不成立。

QCC 是無准入公鏈：任何人可自行部署節點核驗，不需要任何主體批准。這是"任何人可獨立核驗"這句話成立的前提。

Q20 資產記錄在公鏈上，是否意味著任何人都能取得這些資產？

不。**公開的是記錄，不是控制權**。任何人可以看到 OSNB 的總量與每一筆轉移，但資產的轉移必須由持有人的私鑰簽名。

可以進一步陳述一條協議層事實：**任何規則集都無法在沒有持有人簽名的情況下轉移其資產**。QCC 上可用的最高許可權是凍結——發行方可以凍結某地址使其無法轉出，但不能將其轉移至第三方，也不能銷毀。

Q21 如果 QCC 出現共識層缺陷怎麼辦？

協議凍結意味著沒有"發個補丁修復"這條路，因此必須事先說明處理原則。

歷史執行結果不可修改是硬約束。任何規則變更都無法作用於既有歷史。若出現致命共識缺陷（定義限於憑空增發或憑空轉移他人資產這一類），唯一路徑是停止舊鏈、以缺陷發生前的狀態快照啟動新鏈——而不是修補舊鏈的歷史。舊鏈的參與者不會被任何人拖入新鏈。

這一處理方式的代價是真實的。OSN 的應對是：**極簡協議、反覆測試、以及在協議凍結前完成第三方安全審計**，而不是聲稱不會出錯。

Q22 機構私鑰丟失或簽名人失聯怎麼辦？

對機構自身的資產地址：私鑰由機構持有，金鑰輪換隻是生成新金鑰對、轉移結算憑證、更新白名單地址，不需要 OSN 參與、不需要停機、不需要其他機構配合。建議輪換週期 1-5 年。

對多籤地址：**聯合簽署的代價是真實的**——任一簽名人永久失聯，該地址即無法再發起交易。處理路徑有兩條：QCC 協議層的繼承機制（協議原生能力），以及企業內部的金鑰管理制度。後者不屬於公鏈層問題。

Q23 為什麼後量子安全在現在就重要？

因為**協議凍結與演算法遷移不能同時成立**。

更換籤名演算法是共識規則的變更。一個能夠隨時完成這一變更的系統，按定義就是規則可被單方修改的系統。反過來，一個已經凍結的協議若籤名方案不是原生的，未來就沒有任何合法路徑更換它。因此對一個承諾凍結的帳本而言，後量子不是可選項，而是**必須在創世之前完成的一次性決定**。

實際部署：全部簽名點統一使用 ML-DSA-87（FIPS 204 最高引數集），雜湊統一使用 SHA3-256（FIPS 202），**所有權路徑上不存在任何橢圓曲線金鑰**。

對參與機構的含義是：接入 OSN 不會帶來新的後量子遷移義務——沒有經典金鑰清點、沒有切換點規劃、沒有歷史金鑰處理政策。

Q24 系統被攻破的最壞情況是什麼？

分三層回答：

- **OSN 伺服器被完全攻破**：攻擊者取得的是無法解密的密文。OSN 不持有機構私鑰，不具備解密能力。
- **某家機構節點被攻破**：影響限於該機構自身的資料與資產，不擴散至其他機構——每個機構節點只處理自己的流量與資料，不復制其他機構的明文。
- **帳本層**：資產轉移必須由持有人私鑰簽名，攻破 OSN 或任何機構節點都不產生轉移他人資產的能力。

Q25 效能是否足以支撐實際業務？

兩層指標必須分開陳述：

層	承擔的工作	指標
QCC	價值轉移與終局性	公開測試環境約 1,000 TPS [已實現]
OSN	機構間清算報文同步與處理	架構設計目標 100,000 TPS [設計目標，開發與壓測未完成]

兩者量級不同，因為承擔的事不同：一份清算報文包含一批訂單，落到帳本上是一次淨額價值轉移。**跨境小額清算的瓶頸不在帳本寫入速度，而在報文傳遞與事後對帳。**

QCC 的 1,000 TPS 是主動取舍的結果——後量子簽名驗證開銷高於橢圓曲線，全量重放要求每節點重算全部歷史。這是為可驗證性支付的成本。

Q26 監管觀察節點如何工作？

由成員機構授權開通，不由 OSN 開通，也不由監管自行開通。

原因是技術性的：一個接入網路的節點本身不攜帶任何機構證明或機構金鑰，**OSN 無法認定某個節點是否真的屬於某個監管機構**，也不會為監管機構生成機構金鑰。在無法自證來訪方身份的前提下開通明文訪問，本身就是資料安全缺口。

技術上是機構向監管授權，**行政上監管有權要求機構必須配合**，兩者並不衝突。協議層另有一項限制：**每個白名單機構節點只能授權一個觀察節點。**

觀察節點可見其所監管機構的報文明文與全網雜湊錨點，不可見其他機構的明文。而 OSNB 總量與每一次增發銷毀，本就公開可查，不需要任何授權。

五、持續經營

Q27 如果 OSN 停止運營，機構的資產會怎樣？

機構持有的 OSNB 記錄在 QCC 上，不在 OSN 的伺服器上。OSN 停止運營不影響這些記錄的存在與可驗證性——帳本是無准入公鏈，OSN 無權也無法刪除或凍結整條鏈。

贖回路徑依賴儲備安排與公司的清算程式，屬於常規的公司退出問題，將在向 MAS 提交的材料中詳述。這裡要強調的是二者的區別：**記錄的存續不依賴 OSN 是否存在；法幣贖回則依賴 OSN 的持續經營與儲備安排。**

Q28 公司對個別人員的依賴程度如何？

技術架構目前由創始人主導設計與實現，這是現階段的真實情況，也是早期深科技公司的常態。緩解措施包括：技術文件化、協議規範公開、以及第三方安全審計——**目標是使系統不依賴任何單一人員的記憶或判斷即可被理解、驗證與維護。**

在結算憑證的控制權上，這一依賴已經被結構性消除：3-of-3 聯合簽署下，公司內部無任何單一人員可完成增發或銷毀。

Q29 資本與預算安排？

公司已為牌照與沙盒申請安排專項預算，用於合規顧問、審計、系統建設與監管申請。具體金額與資本充足安排屬於向 MAS 提交的材料範圍，不在本白皮書披露。

Q30 分階段目標是什麼？

第一階段（SPI 首年）：機構成員控制在 5 家以下，業務量刻意限制，目標是"3 個 0"——零安全事故、零合規違規、零資金損失。此階段 OSN 自行持牌下場承擔機構轉帳業務，目的是驗證系統而非追求規模。

第二階段：系統驗證成功後，**OSN 退出交易支付業務**，改由成員機構承擔支付執行，OSN 只做儲備金管理與技術維護。屆時 OSN 的收入來源為成員機構服務費，不再收取網路費率。

這一安排的含義是：**OSN 的長期定位是基礎設施提供方，而不是支付業務的參與者**。前期下場是為了證明它能用，不是為了佔據它。

第四章完。

附：本白皮書未涵蓋的內容

為避免誤解，以下內容有意不在本白皮書中披露或主張：

- **多籤金鑰的具體託管機制**——僅向監管機構提交。
- **股東身份與資本充足的詳細材料**——屬於牌照申請範圍。
- **各項技術主張的基準測試資料**——將隨協議規範一同公佈。
- **對其他帳本或支付網路的唯一性主張**——本白皮書未對全部現有系統作系統排查，只主張 OSN 滿足所述特徵，不主張唯一。