

第一章 OSN 做什么事

1.1 业务定位

OSN 是面向持牌金融机构的跨境清算网络。它不面向公众，不持有终端客户，不提供外汇兑换，也不参与任何一方的支付执行。它承担的是机构与机构之间的一件事：**把"谁应当向谁清算多少"这件事，变成一个各方都能独立核验、且事后无人可以修改的记录。**

OSN 由两层构成，职责严格分开。

QCC 层——价值与事实。 QCC 是一条无准入公开账本，协议规则在正式版本发布时冻结：没有升级密钥，没有可修改的规则集入口，任何一方都无法单方变更已生效的规则。OSNB 结算凭证的发行、销毁与每一次转移都记录在这一层，公开且任何人可重放核验。OSN 不控制 QCC，也无法暂停它。

OSN 层——清算与协调。 OSN 运营核心服务节点，负责机构间清算请求的路由、同步、异常处理与审计重放。成员机构自行部署机构节点，持有自己的客户数据与私钥。这一层由 OSN 运营方协调，这是一个运营型网络所必需的，也是承担牌照义务的主体所在。

这样分层的结果是：**参与机构需要与 OSN 建立商业与合规关系，但不需要信任 OSN 的账本。**资金对应的价值事实不在 OSN 的服务器里，而在一条 OSN 无权修改的公开账本上。

与现有跨境清算模式的结构对比

	代理行网络	卡组织清算	汇款服务商	OSN
价值记录持有者	各代理行各自账本	清算组织	服务商	公开账本，无单一持有者
参与方需要信任谁	链路上每一层代理行	清算组织	服务商	无需信任任何一方
记录可否被持有方单方修改	可	可	可	否
争议时的事实来源	双方各自记录后对账	组织的记录	服务商的记录	同一份不可修改记录
中间环节可见性	对发起方不可见	组织内可见	服务商内可见	全程可核验
后量子签名	未规划	未规划	未规划	自创世起原生

这张表刻意不包含吞吐量与网络覆盖。在这两项上，运行数十年的全球清算体系具有 OSN 短期内不可比拟的规模，白皮书无意在此作不对等比较。OSN 主张的差异在记录的性质上，不在规模上。

关于性能的分层说明

OSN 与 QCC 承担不同的工作，性能指标也必须分开陈述。

层	承担的工作	指标
QCC	价值转移与终局性	公开测试环境约 1,000 TPS [已实现]
OSN	机构间清算报文同步与处理	架构设计目标 100,000 TPS [设计目标]

两者量级不同，因为承担的事不同。一份清算报文中可包含一批清算订单，落到账本上是一次净额价值转移——**跨境小额清算的真实瓶颈从来不在账本写入速度，而在报文传递与事后对账。**

QCC 的 1,000 TPS 是一项主动取舍的结果，而非未经优化。后量子格签名的验证开销显著高于椭圆曲线签名，而全量重放与执行层哈希一致性要求每个节点重算全部历史。这是为"任何人可独立核验"这一性质支付的成本。对于清算场景，这个价格是划算的：终局性每秒千笔已远超实际净额结算需求，而可验证性无法事后补上。

OSN 层的清算报文采用 P2P 直连同步，报文之间互不依赖、不争用全局状态，架构上不存在串行瓶颈。10 万 TPS 是设计目标与最终测试目标，开发与压测尚未完成，本白皮书不将其作为已具备的能力陈述。

1.2 小额跨境清算的实际场景

OSN 第一阶段服务的是**小额、高频、目的地集中**的跨境资金流动。典型来源包括：

- **劳务汇款**——东南亚区域内数千万跨境务工人员人口的定期汇款，单笔金额小、频次固定、走廊高度集中；
- **中小企业货款**——区域内贸易的小额结算，金额通常在数百至数千美元；
- **平台类结算**——电商、出行、内容平台向境外收款方的批量结算。

这些场景的共同特征是：**单笔金额远低于代理行体系的经济门槛，但笔数极大。**在现有体系中，一笔一百美元的跨境汇款可能经过两到三层代理行，每一层收取固定费用并引入一段不可见的时间，最终成本占比可达本金的百分之几到百分之十几，到账时间从数小时到数日不等，且发起方无法回答客户"现在钱在哪里"。

OSN 的网络层单笔技术上限设定为 **5,000 美元**。这是网络层硬顶，用于将 OSN 界定在小额清算范围内。终端客户的实际单笔限额由发起机构依其自身的客户分层政策决定（普通客户与 VIP 客户不同），OSN 不介入这一判断。

参与角色共四类：

角色	职责	持有什么
发起机构	收集客户支付需求，构建清算请求	自有客户 KYC 记录、自有私钥
清算机构	在本地完成实际付款，回写清算事实	自有客户记录、自有私钥
储备银行	持有 1:1 美元储备	法币储备账户
监管机构	依授权部署观察节点	对其所监管机构数据的可见性

OSN 自身不在这张表里持有任何客户资产，也不持有任何机构的私钥。

1.3 现有体系的四个结构性问题

OSN 要解决的不是"跨境汇款有点贵有点慢"这一表象，而是四个结构性问题。它们都源于同一个根因：**清算事实分散记录在各参与方各自控制的账本中，且每一份都可被其持有方修改。**

其一，没有共同的事实来源。 发起行、中间行、收款行各记一本账。三本账在正常情况下一致，在异常情况下不一致，而判断哪一本正确需要人工对账。跨境、跨法域、跨时区的对账成本，是小额汇款高费率的主要构成之一，远大于实际的资金移动成本。

其二，过程对参与方不可见。 发起机构把报文交给代理行之后即失去可见性。客户问"钱到哪了"，发起机构只能查询并等待。这不是技术缺陷，而是体系结构的必然——每一段的记录都在别人的系统里。

其三，记录可被单方修改，因此争议缺乏客观依据。 任何一方的账本都由该方的数据库持有，技术上可以被修改、回滚或重建。绝大多数机构不会这样做，但"不会"是承诺，不是可核验的状态。当争议真的发生时，各方只能援引各自的记录。

其四，后量子迁移是一笔尚未支付的账。 现有跨境支付体系的身份认证与报文签名普遍基于经典密码学。当具备密码分析能力的量子计算成为现实威胁时，这些体系需要完成一次涉及全部存量密钥、全部历史记录与全部参与方的迁移。这项工程的成本尚未被计入任何一家机构的账本，但它一定会到来。

OSN 对这四个问题的回应，构成本白皮书第二章与第三章的全部内容：**用一份任何人可独立核验、且无人可以修改的记录，取代分散在各方手中的多份可修改记录；并在建立这份记录时，一开始就使用后量子签名。**

1.4 一笔清算的完整生命周期

以下用一笔实际清算走完全程。参与方为发起机构 A（新加坡）与清算机构 B（马来西亚），本轮共 312 笔终端客户订单，净额约 48.25 万美元。

第一步：订单收集。 机构 A 在其自有系统内完成客户 KYC、反洗钱筛查与收款指令收集。这一步完全发生在 A 的内部，OSN 不介入，也不接收任何客户身份信息。开发期采用 30 秒收集窗口——此为运行参数而非不可变协议常量，由协议版本号对应的参数定义。

第二步：构建清算请求。 A 将本轮订单序列化为 `Request`，包含每笔订单的编号、收款人、清算行、金额与时间。`Request` 以 A 的机构主密钥派生密钥加密。 [已实现]

第三步：价值转移上链。 A 在 QCC 上将对应净额的 OSNB 转移至 B 的白名单地址。这一步产生一个公开的交易哈希与确认高度，二者写入报文对象的明文 `Header`。**价值转移在此刻即已终局，且公开可核验，不依赖后续任何环节。** [已实现]

第四步：固定创建哈希。

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

此哈希一经生成永久固定。任何验证节点读取 `Header` 与 `Request` 密文即可重算比对，**无需持有解密密钥即可确认内容完整。**这是 OSN 报文模型中最重要的一项确定性。 [已实现]

第五步：清算方执行。 B 向密钥服务申请一次性派生密钥，解密 `Request`，在其本地系统中完成 312 笔实际付款。这一步同样完全发生在 B 的内部。

第六步：回写清算事实。 B 将逐笔清算结果写入 `Result`，以其机构白名单私钥（ML-DSA-87）产生 `ResultSignature`。**`Result` 是追加的新数据段，`Request` 不被修改。** [已实现]

第七步：封存生命周期。 完成哈希绑定创建哈希、结果摘要与清算方签名，成为该报文对象的最终锚点，一经生成不可覆盖。整个生命周期设计约 1 分钟。

各方在事后能各自核验什么：

谁	无需任何人配合即可核验
机构 A	价值转移已终局；B 的清算事实由 B 的私钥签署，不可抵赖
机构 B	A 的请求内容未被修改；A 的价值转移真实存在于公开账本
监管机构	经其所监管机构授权后，可见该机构全部明文与全部哈希锚点
任意第三方	OSNB 总量、每一次增发销毁、每一笔转移——无需任何授权

1.5 清算、纠错与退款

正常路径即 1.4 所述。清算机构在本地完成付款后回写事实，报文对象封存。

部分失败是常态而非例外：一批 312 笔订单中，可能有若干笔因收款账户状态、当地合规筛查或信息错误而无法完成。OSN 的处理方式是—— **Result** 逐笔记录每一笔订单的实际状态，成功与失败在同一份清算事实中并存。 **clearingFact** 字段可承载各机构不统一的本地回调与支付凭证，OSN 不要求各国机构统一其内部凭证格式。 [已实现]

退款不是对历史的修改，而是一笔新的事实。 这是 OSN 与传统清算体系在处理逻辑上的根本差别。传统体系中，冲正是对原记录的状态变更；在 OSN 中，原报文对象已被哈希封存，任何一方都无法回头修改它。退款表现为一笔新的清算，反向引用原订单编号，形成一条完整且互相引用的事实链。任何人事后重放这条链，看到的都是"发生了什么以及如何被纠正"，而不是一个被抹平的最终状态。

净额结算与费用。 机构之间采用批量净额结算，而非逐笔全额转移，这是 OSN 能够承载小额高频场景的经济基础。费用分两层：一是机构向其终端客户收取的网络费率（0.1%），二是 OSN 向成员机构收取的服务费。当 OSN 不自行承担转账业务时，仅收取后者。

白名单的定位。 OSNB 仅可在白名单地址之间转移，这是协议层规则，而非可被任何人升级或绕过的机制。需要明确的是：**白名单不是商业准入的筛选工具，而是最后的法律兜底条款。** 机构备案后 10 个工作日内无监管异议即开通白名单资格；机构赎回结算凭证并申请退出后，10 个工作日公开期内无法律争议即关闭资格。OSN 不在此环节做商业裁量。

关于冻结权限的边界，第三章将详述一项协议层事实：**在 QCC 上，任何规则集都无法在没有持有人签名的情况下转移其资产。** 可用的最高权限是冻结，不存在从持有人地址强制划转或销毁的能力。

第一章完。第二章「OSN 如何实现全球转账网络」将展开可验证账本、结算凭证发行与储备、报文对象与加密体系、节点同步、清算框架、纠错退款与监管观察节点的完整实现。

第二章 如何实现全球清算网络

本章描述业务场景、执行流程与实现框架。"为什么可信、如何独立核验"是第三章的内容，两章主题有意重叠，视角不同。

2.1 清算为什么需要一个可验证账本

第一章指出的四个结构性问题，根因是同一个：**清算事实分散记录在各参与方各自控制的数据库中。**

要消除这个根因，只有两条路。一是所有参与方共同承认一个权威账本——这是现有清算体系的做法，它要求各方接受同一个中心机构的记录为准。二是让账本本身不属于任何人，任何参与方都能从原始数据独立重算出同一个结果。

跨法域、跨监管辖区的机构之间，第一条路的前提往往不成立：没有一个所有参与方都愿意接受的权威。因此 OSN 选择第二条。

这条路对底层账本提出三项硬性要求，缺一不可：

1. **无准入**——任何一方都可以自行部署节点并核验，不需要任何主体批准；
2. **规则不可被单方修改**——否则参与方只能验证过去，无法确知未来；
3. **全量可重放**——重放所依据的规则集与数据是同一份，而不是历次变更规则的集合。

满足这三条的账本，参与方不需要信任运营方，只需要信任数学。QCC 是为满足这三条而构建的。

2.2 QCC：无准入、协议冻结、全量重放

QCC 是 OSN 的底层账本。它与 OSN 公司在资产上无关，是一条独立的开放协议公链，OSN 只是其上的一个应用。

无准入。任何人都可以部署 QCC 节点、参与共识、运行超级节点。入网条件只有两条：地址符合 QCC 标准且不重复，执行层哈希与全网一致。不需要任何主体批准，不存在成员名单。

协议冻结。QCC 第一个正式版本发布即冻结底层共识协议。没有升级密钥，没有治理主体，没有可修改的规则集入口，也没有"以后靠可编程执行层补"的退路。这是 QCC 正式发布一再推迟的原因——**新增协议必须在冻结前完成**。任何新增协议须同时满足三条：普惠使用、必须由底层协议实现、必须满足全量重放与执行层哈希一致性。

全量重放。 每个节点从创世高度起，用同一份规则集重算全部历史，得出同一个执行层哈希。这与"按高度装配不同版本规则"的重放有本质区别：后者的重放依据是规则的历史序列，前者是同一份规则。

没有治理主体。 QCC 不保留任何治理机构、否决权或管理员。协议对所有参与者是同一份，加入之后没有任何一方能单方改变它。这不是承诺，是协议中不存在该功能。

2.3 容器模型与"一切皆为交易"

QCC 的账本单位是**容器**，而非固定节奏产出的区块。

容器是运行时执行体，近似操作系统中的进程；容器内的区块近似线程。每个容器绑定唯一资产 ID——一个 OSNB 容器内只有 OSNB 交易。**容器由交易触发拉起，3 秒内无数据即销毁且不上链；有数据才产出并上链。**

这意味着 QCC 上不存在空容器。与按固定节奏出块（无论有无交易）的账本相比，存储中不含无谓数据。链是单条的，容器按实际发生顺序串成哈希链，相邻容器可以是不同资产。

"一切皆为交易"是 QCC 的第一原则：转账是交易，规则变更是交易，白名单更新是交易，冻结是交易，人工操作也是交易。不存在绕过交易管道的特权路径——白名单规则更新与普通转账走同一条单线程准入队列。这一点对清算网络的意义在于：**任何管理动作都留下与普通交易同等强度的公开记录，不存在"后台操作"。**

2.4 规则集，而非可编程执行层

QCC 没有任何形式的可编程执行层。资产的能力由**系统规则集**定义，而规则集是协议的一部分，随协议一同冻结。

这是 OSN 选择 QCC 的决定性原因。在可编程执行层上发行的资产，其转移限制、冻结能力、增发权限都由部署者编写的代码决定，而这些代码通常可被其部署者升级、替换或重新定义。**参与方要信任的不是协议，而是部署者今天写了什么、明天会不会改。**

在 QCC 上，转移限制是账本自身规则的一部分。它不能被升级，不能被绕过，也不能被任何人重新定义——包括 OSN。

由此产生一条协议层事实，第三章将展开论证：**任何规则集都无法在没有持有人签名的情况下转移其资产。**除持有人自身明确授权的机制（如继承交易、去中心化撮合）外，不存在从持有人地址强制划转的能力。

2.5 OSNB：结算凭证的定位

OSNB 是 OSN 成员机构之间使用的结算凭证，由 QCC 的白名单资产机制承载，与美元 1:1 对应。

需要明确其边界：

持有人范围	仅白名单内的持牌金融机构
公众可否持有	否
用途	机构间清算的记账与结算单位
单笔网络层上限	5,000 美元
是否用于投机或流通	否，不在任何公开市场交易

OSNB 不是面向公众的支付工具，也不是投资标的。它是机构之间清算的记账媒介，其全部意义在于让"谁应当向谁清算多少"这件事有一个公开可核验的记录。

发行门槛。 QCC 协议对稳定币类资产的发行设有强制门槛：发行必须由多签地址完成（单签地址不能发行稳定币）、固定发行费用、以及大额原生代币质押且长期不可解押。这些门槛在协议层强制执行，目的是使稳定币发行不能是随意行为。

2.6 发行与销毁：3-of-3 联合签署

OSNB 的增发与销毁由 QCC 的多签地址控制，采用 **3-of-3 联合签署**。

这里必须澄清一个常被混淆的概念：**QCC 的多签不是门限多签（m-of-n），而是联合签署**。签名人数量在地址创建时确定，一经确定，此后该地址发起的每一笔交易都必须由全部签名人签署，缺一不可。协议层的 threshold 恒等于签名人总数，不存在"多数通过"这一档。

恰当的类比不是董事会表决，而是**刑事陪审团的一致裁决**：不是多数说了算，是任何一位都能否决。

三个签名分属不同主体、不同托管路径：两个由业务经理岗位持有，第三个由业务执行总裁在其本人设备上独立完成，不经过任何共享服务。**公司内部不存在任何单一人员能够完成一次增发或销毁**。具体托管机制不在本白皮书披露范围内，相关细节仅向监管机构提交。

一次增发的完整路径：

1. 法币进入已备案的储备银行账户；
2. 三名签名人分别独立签署增发交易，交易描述关联该笔储备入金；
3. 交易上链，OSNB 总量变更成为公开记录；
4. 任何人可在链上查得该次增发的时间、数量与描述。

销毁路径与之对称。**每一次总量变更都是永久且公开的链上事实，不存在链下增发。**

签名人失联的处理。联合签署的代价是真实的：任一签名人永久失联，该地址即无法再发起交易。OSN 对此有两条路径——一是 QCC 协议层的继承机制，二是企业内部密钥管理制度。后者不属于公链层问题，前者是协议原生能力。这一点在 2.14 与第三章进一步展开。

2.7 储备金：多家储备银行与 1:1 对应

OSNB 与美元储备 1:1 对应。储备采用**多家储备银行分散托管**，避免单一银行构成单点风险。

储备账户为专项账户，性质接近专项资金托管而非理财产品。储备银行设在新加坡、受 MAS 监管——这意味着**监管机构对储备账户余额本就具有查询能力，无需 OSN 提供任何接口或授权。**

由此形成一个可对账的闭环：

链上 OSNB 总余额 ↔ 各储备银行账户余额合计

左侧任何人可随时自行计算，无需任何授权；右侧由监管随时查询。两侧应当始终相等，任何偏差都可被立即发现。

这一模型与“周度披露 + 月度第三方鉴证”的验证方式有本质区别，第三章将以“同步验证与异步验证”为题展开。此处只陈述事实边界：**储备银行是否提供余额查询接口由银行决定，OSN 无法强制；OSN 能决定的是选择哪家银行作为储备行——向监管机构与成员机构提供只读余额查询，是 OSN 选择储备银行的前提条件。**在储备行安排落定之前，OSN 能做的是存入并自行查询；对监管机构而言，查询受其监管银行的账户余额本就不需要 OSN 授权。

2.8 白名单：协议层机制与法律兜底定位

OSNB 仅可在白名单地址之间转移。这是**协议层机制**，不是应用层策略，也不是可被任何人升级的代码。

开启不可逆。白名单由发行地址在资产发行后发起白名单交易开启。**一经开启，该资产永久仅支持白名单流通，无法恢复自由流通。**同样，冻结与销毁能力必须在资产发行时选择，未选择则该资产永久无法发起对应交易。这些能力的开启机制不同，但共同点是：**都不可逆。**

发行到开启之间存在空窗期。从资产发行到白名单交易上链之间，理论上存在一个短暂窗口。OSN 的立场是不必消除这个窗口——该期间的任何转账都是永久的链上事实，任何人可自行重放核验。OSNB 发行地址的首笔转出即为向白名单地址转移，这一事实本身公开可查。

定位是法律兜底，不是商业筛选。这一点必须明确：

- 机构备案后 **10 个工作日内无监管异议即开通白名单资格**；
- 机构赎回结算凭证并申请退出后，**10 个工作日公开期内无法律争议即关闭资格**；

- OSN 在此环节**不做商业裁量**，不以商业关系、费率谈判或竞争关系为由拒绝或延迟。

白名单存在的理由是：当出现法律要求时，需要有一个可执行的手段。它不是 OSN 用来选择客户的工具。

2.9 白名单的规模与更新方式

机构发行的稳定币面向其自身客户时，白名单可能达到千万级地址规模。QCC 的处理方式是把规模问题分解为两个独立的问题。

其一，链下映射。客户身份与地址的对应关系由发行机构自行维护在链下。QCC 只强制执行链上白名单成员资格，不承载任何身份信息。

其二，单笔更新有上限。客户端每笔白名单更新交易所能携带的地址数受协议约束（当前设定为 1,000–5,000 个），因此**单笔交易的体积与费用可预测，不随白名单总长度变化**。这是一项刻意的设计：如果不设上限，白名单越长则单笔更新越贵，最终导致大规模白名单在经济上不可行。

规模验证：QCC 测试网已完成 1 亿个白名单地址的测试，超过千万级的设计目标。测试参数可应机构及其顾问要求提供；正式基准测试报告将随协议规范一同公布。

2.10 冻结的边界：能冻结，不能划转

在资产控制能力上，QCC 与部分现有稳定币实现存在一项结构性差异，值得单独说明。

QCC 上可用的最高权限是冻结。发行方可以冻结某个地址的资产，使其无法转出。发行方**不能**从持有人地址强制划转资产到第三方地址，也不能销毁持有人地址内的资产。

据公开信息，部分基于可编程执行层发行的稳定币，其发行方保留了从黑名单地址销毁或转移资产的能力。这两类能力的差别在实务中很大：冻结是可恢复的、不改变归属的保全措施；强制划转与销毁则直接改变了资产归属。

OSN 将冻结与解冻视为**公示义务**——每一次冻结与解冻都是链上公开事实，任何人可查得其时间与对象。

2.11 OSNMesObject：报文对象的三段结构

清算指令在机构之间以 **OSNMesObject** 传递。其结构为：

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

段	明文/密文	写入方	内容
Header	明文	发起方	路由、币种、汇率与清算规则哈希、QCC 交易哈希与确认高度、请求摘要、类型、创建时间、协议版本
Request	密文	发起方	清算订单列表：编号、收款人、清算行、金额、时间、可选支付凭证
Result	密文	清算方	逐笔清算事实：订单编号、状态、清算时间、本地清算凭证

核心约束：历史内容不存在编辑操作。 发起方创建 Request 之后不能修改它；清算方不能修改 Request，只能追加 Result；Result 一经写入亦不可改。**报文对象的生命周期不通过可变的字段表达，而通过两个不可变阶段的哈希证明。**

`clearingFact` 字段接受 JSON 或字节附件，用于容纳不同商业银行与支付机构互不统一的本地回调与支付凭证格式。**OSN 不要求各法域机构统一其内部凭证格式**——这是跨境清算网络能否被实际采用的关键之一。

2.12 两阶段密码学完整性模型

这是 OSN V1 最重要的一项协议确定性。

创建阶段：

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

拼接顺序在协议中明确规定为 Request 在前、Header 在后。CreationHash 一经生成永久固定。

其价值在于验证顺序：验证节点读取 Header → 读取 Request **密文** → 重算哈希 → 与 CreationHash 比对。**全过程无需解密密钥即可确认内容完整。**只有在完整性确认之后，才需要决定是否获取解密密钥。这使得完整性验证与数据访问权限彻底解耦。[已实现]

完成阶段：

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

CompletionHash 继承发起方的创建事实、绑定清算方的结果摘要与机构签名，成为完整生命周期的最终锚点，一经生成不允许重新计算后覆盖。

ResultSignature 由清算方以其机构白名单私钥（ML-DSA-87）产生，证明该清算结果确实来源于该授权机构，且事后不可抵赖。

全链哈希算法统一为 **SHA3-256**，包括创世容器锚定哈希。

2.13 加密体系与主密钥派生

报文业务数据由**发起方派生密钥体系**加密。

- 派生主密钥由机构自身持有，**不直接用于业务数据加密**；
- 每个报文对象使用一次性派生密钥；
- 清算方收到报文后，依报文身份向密钥服务申请该次的一次性派生密钥；
- 机构可用自身主密钥还原任意派生密钥，从而解密其全部历史报文。

数据加密层的最高权限归属机构，不归 OSN。 OSN 传输与同步的是密文，不具备解密能力，也不提供跨辖区直接读取客户明文的权限。这一设计的目的是保护终端客户隐私：即便 OSN 的服务器被完全攻破，攻击者取得的也只是无法解密的密文。

机构间 TCP 通讯帧以机构对应的 ML-DSA-87 私钥签名，实现节点身份认证与安全通信；断网后支持自动重连与同步。

2.14 密钥轮换

机构密钥轮换不依赖任何协议变更或协调窗口，而是利用 QCC 的资产转移能力完成：

1. 机构生成新的 ML-DSA-87 密钥对；
2. 将其持有的 OSNB 转移至新地址；
3. 更新白名单地址。

建议轮换周期为 1-5 年，由机构自行决定。**整个过程不需要 OSN 参与密钥生成，不需要停机，也不需要其他机构配合。**

这一点与传统体系形成对照：在共享密钥或中心签发证书的体系中，密钥轮换通常需要协调窗口与中心方配合。在 OSN 中，轮换只是一笔普通的资产转移加一次白名单更新。

2.15 节点架构与同步

网络形态。OSN 第一阶段采用 S/C (Server / Client-Node) 组织方式：OSN 运营方提供核心服务节点（规划全球 6 个，主备容灾），成员机构自行部署机构节点并经授权加入。预期机构规模 1,000 以上。

节点类型	职责	持有数据
OSN 核心服务节点	网络服务、同步、授权	全网密文报文
机构节点	本机构清算执行与数据持有	仅本机构明文与密钥
监管观察节点	依授权对其监管对象的可见性	授权范围内数据

同步机制。节点之间以状态凭证替代单纯心跳包，可由定时或状态变化触发。本地存储采用标准文件盒子方式，通过 API 拉取实现冗余与恢复。**节点恢复以不可变对象与可重放历史为基础**——网络故障不删除任何业务事实，恢复后通过同步重建本地状态与索引。

QCC 层的一项后量子工程分层，值得单独说明。后量子签名的体积显著大于经典签名。QCC 的处理方式是：**公钥与签名都不进入容器，而是各自作为独立的内容寻址快照库同步。**签名库以签名的 SHA3-256 作为寻址键，分片存储，新节点通过分片逐片下载后重建索引，增量同步通过尾分片体积核对完成。

每个节点必须强制同步这两个库，否则无法完成重放执行。这一分层是后量子签名能够在实际账本中落地的关键工程决策之一——它把“签名很大”这个成本从容器体积中移出，同时不损失任何可验证性。

2.16 清算框架与净额结算

机构之间采用批量净额结算，而非逐笔全额转移。这是 OSN 能够承载小额高频场景的经济基础：312 笔终端订单在链上只表现为一次净额价值转移。

一轮清算的完整流程：

```
发起方收集订单 → 构建 Request → 计算请求摘要 → 完成 Header  
→ 计算 CreationHash → 在 QCC 转移净额 OSNB → 发送报文对象  
→ 清算方获取一次性派生密钥 → 解密 Request → 本地异步清算  
→ 构建逐笔清算事实 → 构建 Result → ResultHash  
→ ML-DSA-87 签名 → CompletionHash → 报文完成 → 节点广播同步
```

报文对象的生命周期设计约 **1 分钟**。开发期采用 30 秒订单收集窗口——此为运行参数而非不可变协议常量，由协议版本号对应的参数定义。**已创建对象的解释不因未来版本变化而被重新解释**，这是协议版本管理的基本原则。

费用结构分两层：

层	收取方	说明
网络费率 0.1%	机构向其终端客户	OSN 前期自行承担机构转账业务时由 OSN 收取；OSN 不做转账业务后不收此项
成员机构服务费	OSN 向成员机构	OSN 的长期收入来源

这一结构对应 OSN 的分阶段定位：**前期自己持牌下场做支付业务以验证系统，验证成功后退出交易支付业务，改由成员机构承担支付，OSN 只做储备金管理与技术维护。**

2.17 纠错与退款

部分失败是常态。一批订单中总有若干笔因收款账户状态、当地合规筛查或信息错误而无法完成。Result 逐笔记录每笔订单的实际状态，成功与失败在同一份清算事实中并存，不需要整批回滚。

退款是一笔新的事实，不是对历史的修改。这是 OSN 与传统清算体系在处理逻辑上的根本差别。

传统体系中冲正是对原记录的状态变更：原记录被改写为"已冲正"，最终状态被抹平。在 OSN 中，原报文对象已被哈希封存，任何一方——包括 OSN——都无法回头修改它。退款表现为一笔新的清算，反向引用原订单编号，形成一条完整且互相引用的事实链。

任何人事后重放这条链，看到的是"发生了什么以及如何被纠正"，而不是一个被整理过的最终状态。对争议处理、审计与监管调查而言，这两者的价值差别很大。

2.18 全量同步验证与监管观察节点

审计重放。OSN 的审计不依赖 OSN 提供的报表，而依赖重放：从不可变的报文对象与公开的链上交易出发，任何具备数据访问权的一方都能重建全部清算历史，并与自己的记录比对。

监管观察节点。OSN 提供统一的观察节点技术框架，任何成员机构在其监管要求时均可配置。

其权限模型有一条关键约束，必须明确陈述：**观察节点由成员机构授权开通，不由 OSN 开通，也不由监管自行开通。**

原因是技术性的，而非政策选择。一个接入网络的节点，本身不携带任何机构证明、机构信息或机构密钥。**OSN 无法认定某个节点是否真的属于某个监管机构**——OSN 也不会为监管机构生成机构密钥。在无法自证来访方身份的前提下开通明文访问权限，本身就是一个数据安全缺口。因此技术上绕不开由成员机构授权这一条路径。

需要同时说明的是：技术上是机构向监管授权，**行政上监管有权要求机构必须配合**。两者并不冲突——机构既有权授权监管，技术上也可能授权他方，OSN 无法阻挡也无权阻挡。

协议层限制：每个白名单机构节点只能授权一个观察节点，不能授权第二个。这项限制写在技术框架中，而不是写在协议条款里——它使"授权范围被无限扩散"在技术上不可能发生。

监管观察节点能看到什么：

	可见范围
其所监管机构的报文明文	是（经该机构授权后）
其他机构的报文明文	否
全网哈希锚点与完整性证明	是
OSNB 总量、每一次增发销毁与转移	是——且无需任何授权，公开可查

最后一行值得强调：**监管机构核验 OSNB 总量与储备对应关系，完全不需要 OSN 授权，也不需要部署任何节点。**这部分事实是公开的。

第二章完。第三章「OSN 创新要点」将从"如何独立核验"的角度，重新论证本章描述的实现——包括同步验证与异步验证的区别、联合签署的权力结构、资产控制权转移、以及原生后量子的工程含义。

第三章 创新要点

第二章描述"怎么做"，本章论证"凭什么可信"。两章内容有意重叠，视角不同。本章每一节按四个层次组织：**主张** → **依据** → **如何独立核验** → **当前状态**。

3.1 协议事实与权威事实

主张。 跨机构、跨法域的清算，其记账层不能建立在权威事实之上，只能建立在协议事实之上。

依据。 一份清算记录要被所有参与方接受为"事实"，只有两条路径。

权威事实——各方共同承认某个主体的记录为准。这是现有全球清算体系的做法，运行了数十年，规模远超任何账本技术。它成立的前提是存在一个各方都愿意接受的权威。

协议事实——记录的真伪由规则与数据决定，任何人用同一份规则重算同一份数据都得到同一个结论，不需要承认任何主体。

参与方越多、越分散、越跨法域，第一条路径的前提越难成立：不是效率问题，而是那个"共同承认的权威"可能根本不存在，或者曾经存在而现在不被所有人接受。当这个前提失效时，清算的记账层只剩下第二条路。

这不意味着权威消失。 现实中的清算权威不只是记录者，还是违约时的兜底者。协议事实能取代记录职能，不能取代救济职能。因此实际形态是：**协议事实做账本层，法律与持牌主体做兜底层**。OSN 正是这个结构——白名单是法律兜底条款，QCC 是账本层。

如何独立核验。 部署一个 QCC 节点，从创世高度重放全部历史，比对执行层哈希。这个过程不需要 OSN、不需要任何机构、也不需要任何人的许可。

当前状态。 架构原则，已在 QCC 中实现。

3.2 核心命题：规则不可篡改 + 全量独立重放

主张。 一个能够承载全球化清算的底层账本，必须同时满足两项性质：**规则不可被任何单方修改，且任何人可以对全量数据独立重放核验**。这两项缺一，"无需信任"就不成立。

依据。 拆开看这两项各自不足：

- 只有**独立重放**而规则可变——参与方能验证昨天，无法确知明天。今天验证得再干净，也推不出明天的规则不变。

- 只有**规则冻结**而资产单一——账本只能服务它自己那一种资产，无法承载多机构、多币种的清算。

现有账本大多落在这个二维平面的某一侧：可编程执行层丰富但规则可升级，或规则近乎不可变但只服务单一资产。**同时满足两项，是 QCC 的设计出发点。**

必须说明的是，规则可变的一方并非疏忽，而是主动取舍——可升级意味着 bug 可修、功能可加。OSN 选择了另一端，代价是真实的：**协议冻结后，共识层缺陷没有"发补丁"这条路。**处理方式见 3.3 与 3.16。

如何独立核验。阅读 QCC 源代码，确认其中不存在升级密钥、治理入口或可修改的规则集接口。这是代码事实，不是承诺——不需要相信任何人的话。

当前状态。协议规格与源代码将于主网发布时公开。[路线图节点]

3.3 技术上不可篡改，与事实上不可篡改

主张。这是两项不同的性质，多数关于"区块链不可篡改"的讨论把它们混为一谈。

依据。

技术上不可篡改是密码学性质：哈希链完整，任何对历史的修改都会被检测出来。这是协议属性，读代码即可确认。

事实上不可篡改是网络性质：实际上不存在任何主体有能力协调足够多的节点重写历史。它不由代码保证——联盟链与许可链的哈希链同样完好，但成员协商即可回滚。**技术属性在治理面前不作数。**

这项区分对 OSN 的意义在于诚实：

	技术上不可篡改	事实上不可篡改
性质	协议属性	网络属性
何时成立	主网上线即成立	随节点数量与部署方分散度增长而增强
如何核验	读代码	数节点、看部署方
QCC 现状	满足	演进中

任何账本在启动初期都不满足第二项，比特币最初两年同样如此。区别在于路径是否存在：**无准入设计使这条路径存在，许可制设计使这条路径根本不存在。**许可链的回滚能力是结构性内建的，它不在这条演进路径上。

如何独立核验。第一项读代码；第二项查询当前节点数量与部署方分布——这项数据任何人可随时自行采集。

当前状态。技术不可篡改 [已实现] ；事实不可篡改 [演进中，随网络增长] 。

3.4 为什么冻结协议必须原生后量子

主张。 对一个承诺规则冻结的协议，后量子签名不是可选项，而是必须在创世前完成的一次性决定。

依据。 这不是性能论证，而是逻辑封闭性论证，分两步：

第一步。 更换签名算法是共识规则的变更。一个能够随时完成该变更的系统，按定义就是规则可被修改的系统——3.2 的第一项当场破产。**冻结与迁移不能同时成立。**

第二步。 独立重放要求签名验证规则从创世到永远是同一份。若签名规则在某个高度变更，重放依据就从“一份规则”变成“按高度装配的规则序列”，这正是 3.2 判定强度较低的那一类。

因此：**一个协议若承诺冻结，其签名方案必须在第一个区块之前定案。**这条推论同时给出一个筛选标准——所有把后量子留到日后解决的账本，连“冻结”那一条都不满足。

一个可观察的旁证：现有主流账本的后量子迁移路径普遍是“账户可选升级到抗量子密钥”这类方案，必然要经过一次协议变更。这不是它们的缺陷，而是它们选择了可升级那一端的必然结果。

如何独立核验。 检查该账本创世块使用的签名算法，以及是否存在协议升级机制。这两项都是公开可查的事实。

当前状态。 ML-DSA-87 自创世起使用。 [已实现]

3.5 原生 ML-DSA-87 与迁移成本

主张。 OSN 的参与机构不会从这套基础设施继承任何后量子迁移义务。

依据。 体系中的每一处签名——QCC 上的价值转移、清算结果签名、机构间节点身份认证、结算凭证的增发与销毁——统一使用 ML-DSA-87，即 NIST 标准化模格签名方案（FIPS 204）的最高参数集。内容完整性统一使用 SHA3-256（FIPS 202）。

所有权路径上不存在任何椭圆曲线密钥，在任何历史时点都不存在。

正在推进后量子准备计划的机构，通常要为所接入的每一套账本规划三项工作：经典密钥材料清点、含切换点的迁移路径、切换前所生成密钥与记录的处理政策。**在 OSN 上这三项都不产生**，因为不存在需要清点的经典密钥。

密钥轮换仍是常规运维事项，但它与“迁移”是两回事——轮换只是生成新密钥对、转移资产、更新白名单，不涉及协议变更，不需要协调窗口。

范围声明。 本节所述限于签名与内容完整性。节点间传输层机密性及其所用密钥封装机制另行推进，本白皮书不作主张。

如何独立核验。 检视任意一笔链上交易的签名结构与算法标识。

当前状态。 [已实现]

3.6 同步验证与异步验证

主张。 现有主流结算凭证的储备验证是**异步**的；OSN 的是**同步**的。这是本白皮书最重要的一项论点。

依据。

异步验证的典型形态是：发行方定期披露储备构成，第三方会计师事务所定期出具鉴证报告。使用者在两次披露之间处于信息空白，且必须信任披露方与鉴证方。**验证的时点由发行方决定。**

同步验证的形态是：任何时刻都可以取得两侧的数据并比对。

链上 OSNB 总余额 ↔ 各备案储备银行账户余额合计

- **左侧：**任何人任何时刻可自行计算，不需要任何授权、不需要 OSN 配合、不需要部署任何节点。总量、每一次增发与销毁的时间与数量、每一笔转移，全部公开。
- **右侧：**储备银行设在新加坡、受 MAS 监管。**监管机构对受其监管银行的账户余额本就具有查询能力**，不需要 OSN 提供任何接口或授权。

两侧应当始终相等。任何偏差可被立即发现，而不是等到下一次披露。

左侧既可由镜像节点实时跟踪，也可通过全量重放从创世起独立重建。结算凭证仅在储备资金到账后增发、在资金划出前销毁，因此链上总量在任何时刻都不应超过储备余额。

边界要说明白。 OSN 无法强制储备银行向第三方提供余额查询接口，但可以把它作为选择储备银行的前提条件：只有向监管机构与成员机构提供只读余额查询的银行，才会被选为储备行。因此严格地说：

- **绝大部分主张不依赖任何人配合**——链上侧的全部事实、报文完整性、执行层重放一致性；
- **仅法币侧余额需要配合**——而对金融机构与监管机构而言，取得受监管银行的账户余额确认并非难事。

这是 OSN 的启动期门槛，不是验证体系的缺口。

与审计的关系。 同步验证不取代审计。余额无法证明的事项——储备资产的法律权属、是否存在质押等权利负担、托管条款——仍由定期审计覆盖。改变的是：余额本身不再需要等待审计，审计工作从“确认过去某一时点的余额”转向“核实余额背后的法律安排”。

如何独立核验。 链上侧：任何人立即可做。法币侧：监管机构或经授权的审计方向储备银行核实。

当前状态。 链上侧 [已实现]；储备行安排 [进行中]。

3.7 无需解密的完整性验证

主张。 验证一份清算报文的内容是否完整，不需要有权读取它的内容。

依据。 CreationHash 对 Request 的**密文字节**与 Header 计算。因此验证节点的流程是：读取 Header → 读取 Request 密文 → 重算 SHA3-256 → 比对。全程不触碰解密密钥。

这把两件通常被绑在一起的事彻底解耦：

	传统做法	OSN
确认内容未被修改	需要读取内容	不需要
谁能做完整性验证	有数据访问权的一方	任何持有密文的节点
客户隐私	验证方看得见	验证方看不见

对跨境清算的实际意义：一个不该看到某国客户明文的节点，仍然能够证明该报文未被篡改。数据保护要求与可验证性要求在此不再冲突。

如何独立核验。 官方网站提供了浏览器内的演示：修改任意字段，观察 CreationHash 与已存锚点失配。演示使用自包含的 SHA3-256（FIPS 202）实现，不向外传输任何数据。

当前状态。 [已实现]

3.8 不可编辑的报文对象，与可变状态记录

主张。 报文对象的生命周期由两个不可变阶段的哈希表达，而不是由一个可变的字段表达。

依据。 传统清算报文通常带有一个 `status` 字段，随流程推进被反复改写：待处理 → 处理中 → 已完成。这种设计的问题是**最终只留下最后一个状态**——中间发生了什么，取决于日志是否被完整保留，而日志由记录方控制。

OSN 的做法是：发起方创建 Request 后不可修改；清算方不修改 Request，只追加 Result；两个阶段各自被哈希封存。**"这份记录现在处于什么阶段"由哪些哈希已经生成来回答，而不是由某个字段的当前值回答。**

由此产生的性质：**任何一方，包括 OSN 本身，都不具备修改已封存内容的能力。**这不是权限设置，是结构——修改后哈希即不匹配，而哈希已经被对方持有。

如何独立核验。 对任意历史报文对象重算两个哈希并比对。

当前状态。 CreationHash [已实现]；CompletionHash 的最终字节拼接与编码规则属协议冻结项，Java 实现前最终确认。[测试中]

3.9 退款作为新事实：对审计与争议的价值

主张。 在 OSN 中不存在"冲正"这一动作。纠错表现为一笔新的、反向引用原订单的清算事实。

依据。传统体系中，冲正改写原记录，最终状态被抹平为"已冲正"。审计时看到的是整理过的结果，而整理过程由记录方控制。

在 OSN 中，原报文对象已被哈希封存，无法回头修改。退款是一笔新的清算，反向引用原订单编号，形成互相引用的事实链。

任何人事后重放这条链，看到的是"发生了什么，以及如何被纠正"。

对三类场景的价值：

- **争议处理**——双方援引的是同一份记录，而不是各自的记录；
- **审计**——审计对象是事实链本身，不是发行方提供的报表；
- **监管调查**——纠错行为本身也是永久记录，无法事后消除。

如何独立核验。沿订单编号的引用关系重放整条事实链。

当前状态。 [已实现]

3.10 联合签署：不是多数表决，是一致裁决

主张。QCC 的多签是**联合签署**，不是门限多签（m-of-n）。协议层的 threshold 恒等于签名人总数。

依据。多签地址在创建时确定签名人数量，此后该地址发起的每一笔交易都必须由**全部**签名人签署，缺一不可。协议中不存在"多数通过"这一档。

恰当的类比不是董事会表决，而是**刑事陪审团的一致裁决**：不是多数说了算，是任何一位都能否决。

这项设计对结算凭证发行的直接含义：

- **不存在"多数合谋即可增发"的攻击面**——需要全部签名人同时失守；
- **每一位签名人都持有真实的否决权**，而不是形式上的会签；
- **公司内部不存在任何单一人员能够完成一次增发或销毁。**

代价是真实的，必须一并说明。任一签名人永久失联，该地址即无法再发起交易，其控制的资产随之锁定。这不是可以回避的问题，处理路径有二：QCC 协议层的继承机制（3.12），以及企业内部的密钥管理制度。后者不属于公链层问题。

如何独立核验。查询该多签地址的签名人配置与历史交易的签名数量。

当前状态。 [已实现]

3.11 冻结的边界：能冻结，不能划转

主张。在 QCC 上，任何规则集都无法在没有持有人签名的情况下转移其资产。可用的最高权限是冻结。

依据。发行方可以冻结某个地址的资产，使其无法转出。发行方**不能**：

- 从持有人地址强制划转资产至第三方地址；
- 销毁持有人地址内的资产。

据公开信息，部分基于可编程执行层发行的结算凭证，其发行方保留了从特定地址销毁或转移资产的能力。这两类能力在实务中差别很大：

	冻结	强制划转 / 销毁
是否改变资产归属	否	是
是否可恢复	是	否
性质	保全措施	处分行为

这项差别对持有机构的意义直接：**持有 OSNB 的机构，其资产的归属不可能在没有其签名的情况下发生变化。**最坏情况是资产被冻结，而冻结是可恢复的、留有公开记录的保全措施。

如何独立核验。检视 QCC 规则集中定义的资产操作类型。

当前状态。 [已实现]

3.12 资产控制权转移：所有权与控制权的分离

主张。在 QCC 上，资产的**发行控制权**可以整体转移，而持有人的资产一枚都不需要移动，且转移过程留下永久可核验的公开记录。

依据。考虑一个真实场景：一家发行了结算凭证的机构被全资收购，或进行重大股权变更、治理结构调整。

在现有体系中通常有两条路：把全部持有人迁移到新的发行合约（成本高、且需要每一位持有人配合），或者把控制权在链下私下移交给新股东（链上毫无痕迹，持有人无从得知谁在控制这项资产）。

在 QCC 上，这是一笔**资产控制权转移交易**：原控制地址签名，新控制地址生效，链上留下永久且任何人可核验的记录。持有人的余额不变，地址不变，无需任何操作。

真正的论点不是"资产可以被收购"，而是：所有权与控制权在协议层是分离的，且控制权的变更是公开可核验的事实。这一结构同时回答了发行方最实际的几个焦虑：

- 签名人离职或长期失联 → 控制权可依既定路径转移；
- 公司重组、被收购、股东变更 → 一笔交易完成，持有人无感；

- 治理结构升级（如从单签升级为多签）→ 协议原生支持。

单签地址与多签地址之间的控制权转移路径均已实现并测试。

关于同类能力的说明。 这一能力在现有公链中少见，但本白皮书不主张唯一性——我们未对全部现有账本作系统性核查。可以确认的是：在可编程执行层上，这类能力通常由发行方自行编写的代码实现，因而同样可被其升级或重新定义；在 QCC 上，它是协议的一部分。

如何独立核验。 查询该资产的控制权变更交易历史。

当前状态。 [已实现]

3.13 白名单：法律兜底，不是商业筛选

主张。 OSNB 的白名单机制是最后的法律兜底条款，不是 OSN 用来选择客户或施加商业影响的工具。

依据。 一个由单一主体控制准入的清算网络，无论其技术如何，最终仍然是一个权威事实体系——因为那个主体可以决定谁能参与。OSN 通过三项安排使这件事在制度上被约束：

1. **开通标准是监管异议，不是商业判断。** 机构备案后 10 个工作日内无监管异议即开通；
2. **退出同样有明确路径。** 机构赎回结算凭证并申请退出后，10 个工作日公开期内无法律争议即关闭资格；
3. **OSN 不做商业裁量。** 不以商业关系、费率谈判或竞争关系为由拒绝或延迟。

同时必须承认边界：**白名单确实是一项权力。** OSN 对它的立场不是“我们不会滥用”（那是承诺），而是把行使条件写成可被观察和检验的规则，且每一次白名单变更都是公开的链上交易——**行使记录本身无法隐藏。**

如何独立核验。 白名单更新是普通链上交易，与转账走同一条准入队列，任何人可查得每一次变更的时间与对象。

当前状态。 协议机制 [已实现]；准入制度 [随牌照进程确立]。

3.14 监管观察节点：OSN 无法自行开通

主张。 监管观察节点由成员机构授权开通，OSN 无法代为开通。这不是政策选择，是技术必然。

依据。 一个接入网络的节点本身不携带任何机构证明、机构信息或机构密钥。**OSN 无法认定某个节点是否真的属于某个监管机构**，也不会为监管机构生成机构密钥。在无法自证来访方身份的前提下开通明文访问权限，本身就构成数据安全缺口。

因此技术上绕不开由成员机构授权这一条路径。

技术与行政并不冲突： 技术上是机构向监管授权；行政上监管有权要求机构必须配合。机构既有权授权监管，技术上也可能授权他方，OSN 无法阻挡也无权阻挡。

协议层限制：每个白名单机构节点只能授权一个观察节点。这项限制写在技术框架中而非条款里——它使"授权范围被无限扩散"在技术上不可能发生。

同时说明：监管核验 OSNB 总量与储备对应关系，完全不需要观察节点，也不需要任何授权。那部分事实是公开的。观察节点解决的是明文报文可见性，不是账本可见性。

如何独立核验。检视观察节点的授权机制与数量限制的实现。

当前状态。技术框架 [已实现] ；实际部署 [随沙盒进程] 。

3.15 成本可确定性：非图灵完备的经济后果

主张。OSN 的单笔清算成本是事先可精确计算的，而不是估算的。

依据。QCC 没有可编程执行层。资产操作由规则集定义，每一种操作的执行路径是确定的，因此其费用可以在交易发起前精确算出，且不随网络状态变化。

在图灵完备的执行环境中，一笔交易的执行成本依赖运行时路径与链上拥堵，事前只能估计。这不是优化问题，而是图灵完备本身的性质。

对清算机构的实际意义：**一笔跨境转账的成本必须能写进产品定价，不能是浮动的。**可预测性在这里比绝对值更重要。

同时要说清楚成本的分层。技术成本只是机构采用一套清算基础设施总成本中很小的一部分——合规评估、法律意见、系统改造、内部审批、对手方协调才是大头。OSN 对此的应对不在技术侧：持牌降低合规不确定性，免费培训降低学习成本，公开规范降低集成成本。**这些不是技术优化，但按采用成本决定胜负这一规律，它们才是关键。**

如何独立核验。在测试网上对同一操作反复发起交易，比对费用。

当前状态。QCC 层 [已实现] ；OSN 层费率结构 [随牌照进程确立] 。

3.16 当前阶段与路线图

本白皮书对每一项主张标注了状态。此处集中说明当前阶段。

已实现并可核验：

- QCC 容器模型、规则集、执行层哈希一致性、全量重放
- 原生 ML-DSA-87 与 SHA3-256
- 多签联合签署、资产控制权转移、白名单、冻结边界
- 白名单规模：测试网 1 亿地址测试已完成（正式基准报告待发布）
- OSNMesObject 三段结构、CreationHash、密钥派生体系

- 签名库与公钥库的分层同步

测试中：

- CompletionHash 的最终字节拼接与规范编码
- OSN 层清算框架与节点同步
- 永久测试网

设计目标，尚未压测：

- OSN 层 100,000 TPS

路线图节点：

阶段 内容

- | | |
|---|--|
| 一 | QCC 永久测试网上线；协议冻结前的最后新增协议完成 |
| 二 | 主网发布，协议规格与源代码公开 |
| 三 | OSN 取得牌照，首批成员机构接入，跑通真实清算 |
| 四 | OSN 退出交易支付业务，改由成员机构承担支付，OSN 只做储备金管理与技术维护 |

关于协议冻结后的缺陷处理。 3.2 指出冻结的代价是共识层缺陷没有"发补丁"这条路。OSN 与 QCC 的立场是明确的：**协议中不包含任何修改历史执行结果的机制。**任何规则变更都无法作用于既有历史；若出现必须处理的致命共识缺陷，唯一路径是停止当前链、以缺陷发生前的状态为创世快照启动新链。

这不是"我们保证不改"这样的承诺，而是协议里没有那个功能——**任何人，包括 QCC 的作者，都不具备修改已生效历史的能力。**

第三章完。第四章为常见问题，按公司与牌照、资金与储备、反洗钱与合规、技术与安全、持续经营五组编排。

第四章 常见问题

本章回应监管机构与金融机构在评估阶段最常提出的问题，按五组编排。回答力求直接。凡涉及尚未实现的部分，均明确标注。

一、公司与牌照

Q1 OSN 是什么主体？股权结构如何？

Open Settlement Network Pte. Ltd.，新加坡注册，**没有母公司**，股权直接由四名股东持有，不存在多层控股或离岸架构。公司分技术、运营、融资、业务四个团队。技术架构由公司自行设计与实现，未采用第三方现成方案。

Q2 申请哪一类牌照？为什么是这一类？

OSN 正在准备向 MAS 申请**标准支付机构（SPI）牌照**。选择 SPI 而非大型支付机构牌照，是因为第一阶段的业务规模、机构数量与交易量都刻意控制在有限范围内，目标是先验证系统而非追求规模。

需要明确：**截至本白皮书发布，OSN 尚未取得任何 MAS 牌照，不向公众提供支付服务。**

Q3 OSN 与 QCC 是什么关系？是同一个主体吗？

不是。**QCC 是一条独立的开放协议公链，与 OSN 公司在资产上无关**。OSN 是 QCC 之上的一个应用，与任何其他使用 QCC 的机构地位相同。

OSN 不控制 QCC，无法暂停它，也无法修改它的规则——QCC 协议中不存在任何变更入口或治理主体。这一分离是刻意的：如果 OSN 能够控制底层账本，本白皮书关于独立可验证性的全部主张都不成立。

Q4 OSN 是否向公众发行数字资产？

否。OSNB 是机构间结算凭证，**仅可在白名单内的持牌金融机构地址之间转移，公众不可持有**，不在任何公开市场交易，不作为投资标的推广。这一限制由账本的协议规则强制执行，不是商业政策。

Q5 OSN 是否提供外汇兑换？

否。OSN 不做外汇兑换、不持有终端客户、不参与任何一方的支付执行。汇率由参与机构之间约定，其协议哈希记录在报文对象的明文头部，用于事后核验，OSN 不定价也不撮合。

Q6 沙盒与牌照两条路径是什么关系？

两条路径**独立推进，互不构成前提**。牌照申请是常规监管路径；Sandbox Plus 申请的目的是在受控环境中与金融机构联合验证系统。任一路径的进展不依赖另一路径。

截至本白皮书发布，**两项申请均在筹备中，均未获批**。

二、资金与储备

Q7 OSNB 的法律性质是什么？

OSNB 是机构间清算的记账与结算凭证，与美元 **1:1** 对应，由全额储备支持。它的全部意义在于让"谁应当向谁清算多少"有一个公开可核验的记录，不承担价值储藏或投资功能。网络层单笔上限 5,000 美元，用于将 OSN 界定在小额清算范围内。

Q8 储备资金如何持有？

采用**多家储备银行分散托管**，避免单一银行构成单点风险。储备账户为专项账户，性质接近专项资金托管，不投入任何理财或收益类产品。储备银行设在新加坡、受 MAS 监管。

Q9 谁有权增发或销毁 OSNB？

由多签地址控制，采用 **3-of-3 联合签署**——不是门限多签，协议层的 threshold 恒等于签名人总数，缺一不可。三个签名分属不同主体、不同托管路径，其中一个由业务执行总裁在其本人设备上独立完成，不经过任何共享服务。

公司内部不存在任何单一人员能够完成一次增发或销毁。具体托管机制不在白皮书披露范围内，相关细节单独向监管提交。

Q10 监管如何验证储备与发行总量的对应关系？

分两段，两段都不需要 OSN 配合：

- **链上侧**：OSNB 总量、每一次增发与销毁、每一笔转移，公开可查。任何人任何时刻可自行计算，不需要向 OSN 申请任何权限，也不需要部署节点。
- **法币侧**：储备账户余额。储备行受 MAS 监管，监管对账户余额本就具有查询能力。

两侧应当始终相等。与"周度披露 + 月度第三方鉴证"的验证方式相比，此模型**不存在披露间隔**——任意时点均可比对。

需要诚实说明：OSN 无法控制储备银行是否提供余额查询接口。对监管机构与金融机构而言，取得受监管银行的账户余额确认并非难事；对 OSN 自身而言，这是启动期的商业门槛。

Q11 终端客户的资金是否经过 OSN 的账户？

否。客户付款由发起机构在其本地收取，实际付款由清算机构在其本地完成。OSN 不接触任何一方的客户资金，只承载清算指令与清算事实的记录。储备账户中的资金对应的是机构间结算凭证，不是终端客户资金。

Q12 如果某家储备银行出现问题怎么办？

这正是采用多家储备银行的原因。单一银行的问题不会导致全部储备不可用。同时，储备为专项账户而非投资产品，不承担市场风险。

需要说明的是，**银行破产风险不是 OSN 能够消除的风险**，任何持有法币储备的机构都面对同一问题。OSN 能做的是分散、选择受监管机构、并使储备与发行量的对应关系随时可查——**使问题能够被及早发现，而不是声称问题不会发生。**

三、反洗钱与合规

Q13 KYC 由谁执行？

由参与机构对其自身客户执行。OSN 不持有终端客户，不执行客户层面的 KYC。客户身份记录、以及客户与地址的映射关系，全部留在发行机构侧。

账本本身不承载任何身份信息，只承载地址与交易。

Q14 OSN 如何执行制裁名单筛查？

制裁名单筛查在**机构侧**执行——由发起机构在收集客户指令时完成，由清算机构在本地付款前再次执行。这与机构现有的合规流程一致，OSN 不要求机构改变其筛查工具或流程。

在 OSN 层面，机构准入本身受白名单约束，非白名单地址无法接收 OSNB。

Q15 白名单与制裁名单是什么关系？

两者层次不同。**制裁名单针对终端客户，由机构执行；白名单针对机构地址，由协议执行。**

白名单的定位是最后的法律兜底条款，不是商业筛选工具：机构备案后 10 个工作日内无监管异议即开通；赎回退出后 10 个工作日公开期内无法律争议即关闭。**OSN 在此环节不做商业裁量**，不以商业关系或竞争关系为由拒绝或延迟。

Q16 可疑交易如何报告？

由参与机构依其所在法域的义务报告。OSN 作为持牌主体，就其自身可观察到的机构间清算行为承担相应报告义务。

OSN 可观察的是密文报文的路由与频次，**不可观察终端客户身份与交易明细**——这部分数据 OSN 不具备解密能力。

Q17 个人资料保护（PDPA）如何处理？

终端客户的个人资料从不进入账本，也不以明文形式进入 OSN 的系统。报文业务数据以发起机构派生密钥体系加密，OSN 传输与同步的是密文，不具备解密能力。

即便 OSN 的服务器被完全攻破，攻击者取得的也只是无法解密的密文。这一点是 OSN 数据保护方案的核心，而不是附加措施。

Q18 跨境数据传输如何处理？

报文以密文形式在机构节点之间同步，**解密能力仅在数据所属机构手中。**OSN 不提供跨辖区直接读取客户明文的权限——技术上 OSN 也不具备该能力。

对于监管访问，路径是机构授权的观察节点，范围限于该机构自身数据（见 Q26）。

四、技术与安全

Q19 为什么使用公链，而不是许可链或联盟链？

因为许可链无法提供本方案所依赖的那一项性质。

许可链可以具备完好的哈希链，同时具备成员协商回滚的能力——技术上不可篡改，事实上可篡改。回滚能力是其结构性内建的属性，不是配置选项。如果账本可以被其运营者协商回滚，那么参与方要信任的仍然是运营者，独立可验证性不成立。

QCC 是无准入公链：任何人可自行部署节点核验，不需要任何主体批准。这是“任何人可独立核验”这句话成立的前提。

Q20 资产记录在公链上，是否意味着任何人都能取得这些资产？

不。**公开的是记录，不是控制权。**任何人可以看到 OSNB 的总量与每一笔转移，但资产的转移必须由持有人的私钥签名。

可以进一步陈述一条协议层事实：**任何规则集都无法在没有持有人签名的情况下转移其资产。**QCC 上可用的最高权限是冻结——发行方可以冻结某地址使其无法转出，但不能将其转移至第三方，也不能销毁。

Q21 如果 QCC 出现共识层缺陷怎么办？

协议冻结意味着没有“发个补丁修复”这条路，因此必须事先说明处理原则。

历史执行结果不可修改是硬约束。任何规则变更都无法作用于既有历史。若出现致命共识缺陷（定义限于凭空增发或凭空转移他人资产这一类），唯一路径是停止旧链、以缺陷发生前的状态快照启动新链——而不是修补旧链的历史。旧链的参与者不会被任何人拖入新链。

这一处理方式的代价是真实的。OSN 的应对是：**极简协议、反复测试、以及在协议冻结前完成第三方安全审计**，而不是声称不会出错。

Q22 机构私钥丢失或签名人失联怎么办？

对机构自身的资产地址：私钥由机构持有，密钥轮换只是生成新密钥对、转移结算凭证、更新白名单地址，不需要 OSN 参与、不需要停机、不需要其他机构配合。建议轮换周期 1-5 年。

对多签地址：**联合签署的代价是真实的**——任一签名人永久失联，该地址即无法再发起交易。处理路径有两条：QCC 协议层的继承机制（协议原生能力），以及企业内部的密钥管理制度。后者不属于公链层问题。

Q23 为什么后量子安全在现在就重要？

因为**协议冻结与算法迁移不能同时成立**。

更换签名算法是共识规则的变更。一个能够随时完成这一变更的系统，按定义就是规则可被单方修改的系统。反过来，一个已经冻结的协议若签名方案不是原生的，未来就没有任何合法路径更换它。因此对一个承诺冻结的账本而言，后量子不是可选项，而是**必须在创世之前完成的一次性决定**。

实际部署：全部签名点统一使用 ML-DSA-87（FIPS 204 最高参数集），哈希统一使用 SHA3-256（FIPS 202），**所有权路径上不存在任何椭圆曲线密钥**。

对参与机构的含义是：接入 OSN 不会带来新的后量子迁移义务——没有经典密钥清点、没有切换点规划、没有历史密钥处理政策。

Q24 系统被攻破的最坏情况是什么？

分三层回答：

- **OSN 服务器被完全攻破**：攻击者取得的是无法解密的密文。OSN 不持有机机构私钥，不具备解密能力。
- **某家机构节点被攻破**：影响限于该机构自身的数据与资产，不扩散至其他机构——每个机构节点只处理自己的流量与数据，不复制其他机构的明文。
- **账本层**：资产转移必须由持有人私钥签名，攻破 OSN 或任何机构节点都不产生转移他人资产的能力。

Q25 性能是否足以支撑实际业务？

两层指标必须分开陈述：

层	承担的工作	指标
QCC	价值转移与终局性	公开测试环境约 1,000 TPS [已实现]
OSN	机构间清算报文同步与处理	架构设计目标 100,000 TPS [设计目标, 开发与压测未完成]

两者量级不同，因为承担的事不同：一份清算报文包含一批订单，落到账本上是一次净额价值转移。**跨境小额清算的瓶颈不在账本写入速度，而在报文传递与事后对账。**

QCC 的 1,000 TPS 是主动取舍的结果——后量子签名验证开销高于椭圆曲线，全量重放要求每节点重算全部历史。这是为可验证性支付的成本。

Q26 监管观察节点如何工作？

由成员机构授权开通，不由 OSN 开通，也不由监管自行开通。

原因是技术性的：一个接入网络的节点本身不携带任何机构证明或机构密钥，**OSN 无法认定某个节点是否真的属于某个监管机构**，也不会为监管机构生成机构密钥。在无法自证来访方身份的前提下开通明文访问，本身就是数据安全缺口。

技术上是机构向监管授权，**行政上监管有权要求机构必须配合**，两者并不冲突。协议层另有一项限制：**每个白名单机构节点只能授权一个观察节点。**

观察节点可见其所监管机构的报文明文与全网哈希锚点，不可见其他机构的明文。而 OSNB 总量与每一次增发销毁，本就公开可查，不需要任何授权。

五、持续经营

Q27 如果 OSN 停止运营，机构的资产会怎样？

机构持有的 OSNB 记录在 QCC 上，不在 OSN 的服务器上。OSN 停止运营不影响这些记录的存在与可验证性——账本是无准入公链，OSN 无权也无法删除或冻结整条链。

赎回路径依赖储备安排与公司的清算程序，属于常规的公司退出问题，将在向 MAS 提交的材料中详述。这里要强调的是二者的区别：**记录的存续不依赖 OSN 是否存在；法币赎回则依赖 OSN 的持续经营与储备安排。**

Q28 公司对个别人员的依赖程度如何？

技术架构目前由创始人主导设计与实现，这是现阶段真实情况，也是早期深科技公司的常态。缓解措施包括：技术文档化、协议规范公开、以及第三方安全审计——**目标是使系统不依赖任何单一人员的记忆或判断即可被理解、验证与维护。**

在结算凭证的控制权上，这一依赖已经被结构性消除：3-of-3 联合签署下，公司内部无任何单一人员可完成增发或销毁。

Q29 资本与预算安排？

公司已为牌照与沙盒申请安排专项预算，用于合规顾问、审计、系统建设与监管申请。具体金额与资本充足安排属于向 MAS 提交的材料范围，不在本白皮书披露。

Q30 分阶段目标是什么？

第一阶段（SPI 首年）：机构成员控制在 5 家以下，业务量刻意限制，目标是"3 个 0"——零安全事故、零合规违规、零资金损失。此阶段 OSN 自行持牌下场承担机构转账业务，目的是验证系统而非追求规模。

第二阶段：系统验证成功后，**OSN 退出交易支付业务**，改由成员机构承担支付执行，OSN 只做储备金管理与技术维护。届时 OSN 的收入来源为成员机构服务费，不再收取网络费率。

这一安排的含义是：**OSN 的长期定位是基础设施提供方，而不是支付业务的参与者**。前期下场是为了证明它能用，不是为了占据它。

第四章完。

附：本白皮书未涵盖的内容

为避免误解，以下内容有意不在本白皮书中披露或主张：

- **多签密钥的具体托管机制**——仅向监管机构提交。
- **股东身份与资本充足的详细材料**——属于牌照申请范围。
- **各项技术主张的基准测试数据**——将随协议规范一同公布。
- **对其他账本或支付网络的唯一性主张**——本白皮书未对全部现有系统作系统排查，只主张 OSN 满足所述特征，不主张唯一。