Ontomir

Ontomir 白皮书 v1.2

April 4, 2025

First published January 29, 2020

中文翻译版

Adam Dossa

Graeme Moore

Jesse Lancaster

Michael Buchanan

Pablo Ruiz

Ontomir

执行摘要

安全代币有能力改变金融格局，释放数万亿美元的资产价值和投资潜力，通过可编程的方式自动化操作，并开辟新的流动性路径。以太坊区块链在安全代币方面是一个很好的起点，但它缺乏发行者和投资者所需的基础元素，也缺乏机构和监管机构所要求的元素。在利用以太坊创建了150多个代币之后，我们的研究和经验表明，机构需要一个从底层基于安全代币监管要求构建的区块链。

Ontomir通过一个针对安全代币而设计的企业级区块链来满足这一需求。Ontomir的基础集中于最关键的监管元素，这些元素通过四个关键设计原则来解决，以满足监管机构和机构的需求，同时释放安全代币的真正潜力：

•**保密性**：在提供准确的报告和审计机制的同时，保护信息和所有权隐私。

•**身份**：确保没有个人或实体能够在没有经过验证的身份的情况下创建、获取或出售安全代币。

•**治理**：提供Ontomir的操作和治理结构，以便对其进行管理，保护资产免受网络升级期间的硬分叉影响，并提供处理和执行提案的方法。

•**合规性**：提供金融原语和智能扩展，用于在一个或多个管辖区跨管理安全代币，执行创建、发行和交易安全代币的适当规则，并提供管理必要的复杂限制和分发的能力。

Ontomir将使用诺姆伯证明权益（Nominated Proof-of-Stake）共识机制，并结合GRANDPA最终性装置，支持其原生协议代币OTM。Ontomir上的验证者将抵押OTM并运行authoring节点，提名者将抵押OTM给验证者，验证者和提名者都将根据其角色和区块的添加情况受到奖励或罚款。当前在以太坊上存在的所有OTM代币都将能够以1:1的比例升级为OTM。

我们相信，通过这样一种结构，Ontomir将填补安全代币技术与发行者、投资者、机构和监管机构需求之间的空白。

Ontomir

目录

1.0 简介 1

2.0 架构 2

2.1金融原语 2
2.1.1 监管资产 2
2.1.2 身份 3
2.1.3 记录保存 3
2.1.4 资本分配 3
2.1.5 企业治理 3
2.1.6 稳定币 3
2.2 经济 4
2.2.1 启用经济 4
2.2.2 内部经济 6
2.2.3 启用经济 7
2.2.4 代币 7
2.2.5 代币分配方案 8
2.2.6 21个节点分配机制 9
2.3智能扩展 10
2.4第三方扩展性 10

3.0 身份 11

4.0 保密性 12

4.1 保密交易工作流程 12
4.2 可审计性与隐私 13
4.3 发行人报告和控制 13
4.4 谁能看到什么 13

5.0 治理 14

5.1 网络更新 14

6.0 合规性 15

7.0 标准与互操作性 16

7.1ERC-1400 16
7.2 接力链 16
7.3 封装资产 16
7.4 迁移的安全令牌 17

8.0 甲骨文和市场数据 18

8.1 验证器市场数据(链下工作者) 16
8.2 一般市场数据(已签署数据) 16

2.0 架构

2.1 金融原语

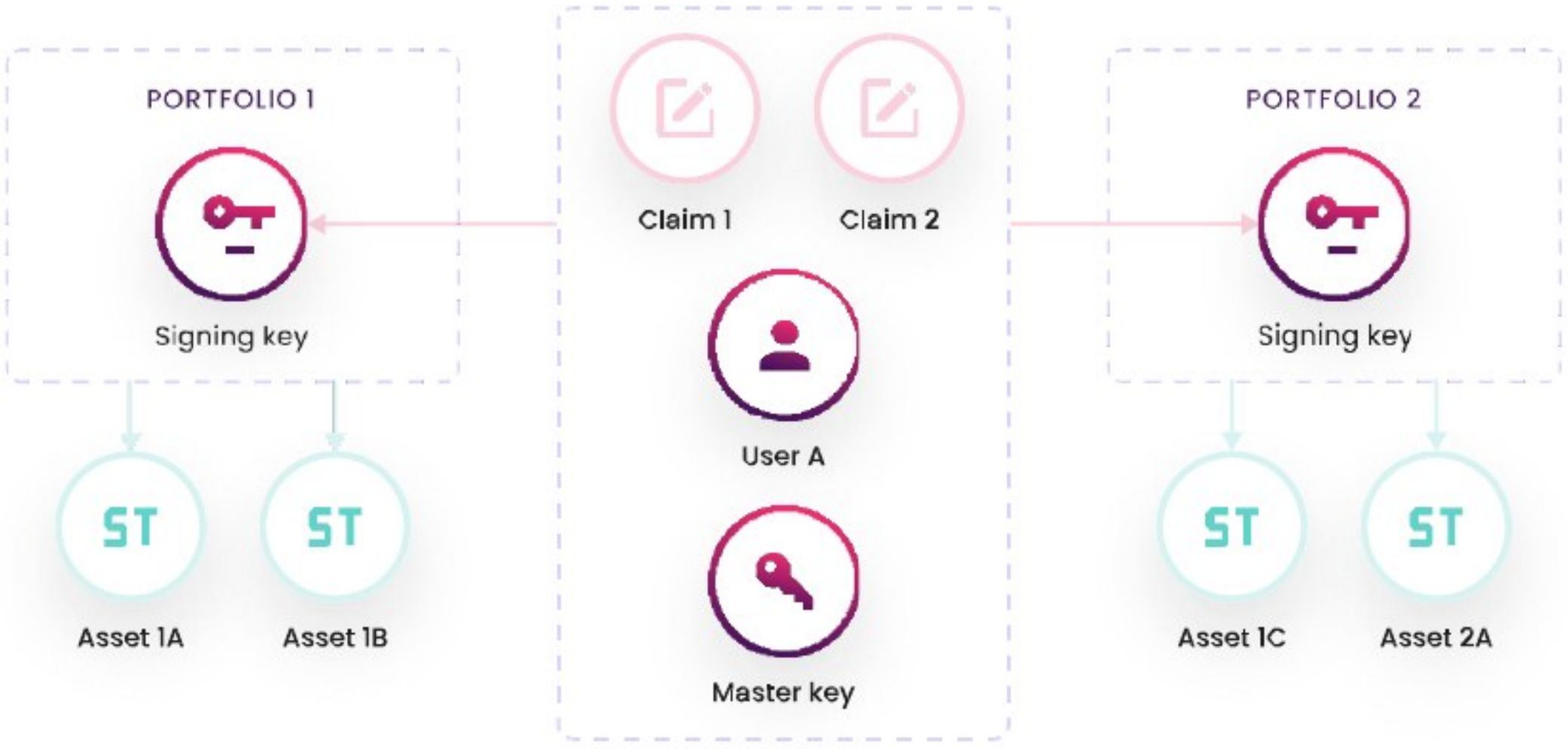
通用目的的区块链通常只有少数几个原语，即在区块链核心内置的功能。相反，包括安全代币及其相关的所有权、转让和其他限制在内的元素都是在区块链之上以智能合约的形式实现的，这导致了可扩展性和性能方面的挑战。然而，Ontomir的金融原语是内置于链的基础中的。Ontomir的金融原语允许用户以低预定的成本操作区块链，同时允许第三方开发人员在链上部署创新去中心化应用程序（dApps）。

2.1.1 监管资产

监管资产是Ontomir的基石。我们的初始团队在行业领先的专业知识推动了ERC-1400标准的创建，以帮助平衡开放、透明和可访问的全球系统与管辖区合规性之间的挑战。

2.1.2 身份

身份对于处理监管证券的每一个操作都至关重要。为了呈现一个灵活且全球化的身份系统，我们使其成为Ontomir　功能的核心。与大多数公共区块链仅使用公共密钥不同，Ontomir上的所有操作都通过身份进行中介。这些身份既是通用的（即可以在整个Ontomir中访问），又是有权限的——它们收集了一组由网络批准的权威机构或发行者特定的权威机构发出的声明或证明。这些声明然后可以用来管理资产所有权、转让和其他限制，以及区块链基础共识的操作。



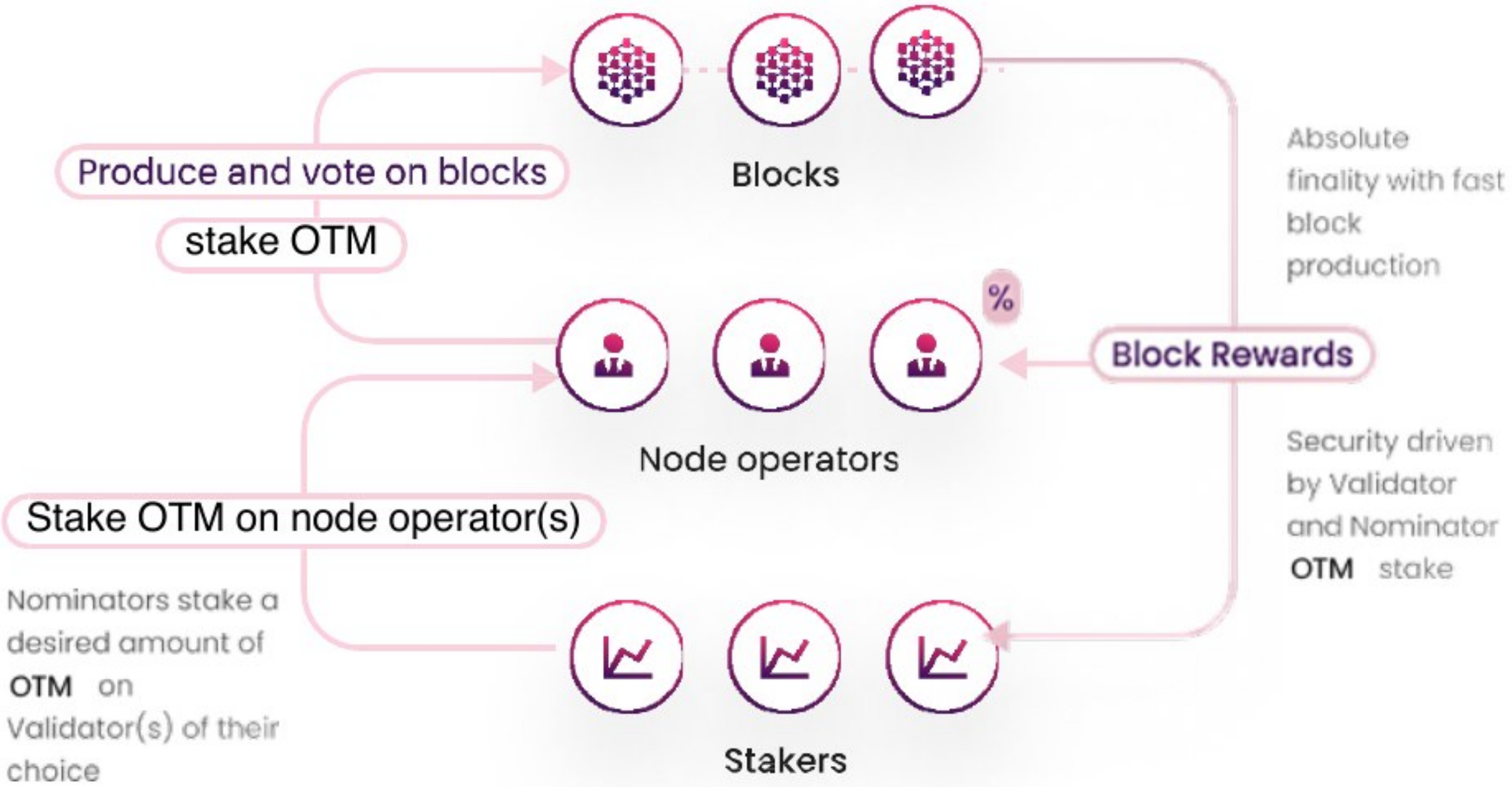
区块奖励由所有遵守协议规则的验证者均分。验证者会保留一定比例的奖励，其余部分按比例分配给提名者。

锁定期是指OTM代币在验证者或提名者撤回请求后被锁定的时间。一旦请求撤回，抵押的OTM代币将在锁定期结束后解锁。锁定期可能通过治理过程进行调整。

最终性

提名权益证明（Nominated Proof-of-Stake）提供确定性的最终性，能够被立即信任。验证者对生成的区块进行投票，一旦超过三分之二的验证者投票支持一个区块，该区块即被最终确认。

区块链的一个共同特征是，每一个新的区块包含对所有前一区块的详细信息。如果一个区块被最终确认，则其之前的所有区块也被最终确认。这一特征允许在一次投票中对多个区块进行最终确认，而不需要对每个区块进行投票。批量处理使链在保证秒级最终确认的同时保持实时和可扩展。



3. Alistair Stewart, 2019, "Extended Abstract: GRANDPA Finality Gadget," Research at W3F, Web3 Foundation, November 20, https://research.web3.foundation/en/latest/polkadot/GRANDPA.html

2.2.5 OTM代币分配方案

以下是 Ontomir公链项目（21个节点） 的100亿代币分配方案，结合节点激励、生态发展与去中心化治理，分为核心分配框架与节点运行机制两部分：

一、代币分配总框架

分配模块	比例	代币数量	核心逻辑
节点质押与奖励	20%	20亿	激励节点长期维护网络安全（按年释放）
生态发展基金	20%	20忆	DApp开发补助、跨链合作、技术升级
社区激励	20%	20亿	空投、开发者赏金、治理提案奖励
团队与顾问	15%	15亿	4年线性解锁，绑定长期利益
基金会储备	10%	10亿	用于合规、市场扩张、突发事件应对
私募与公募	10%	10亿	5%早期私募（机构）、5%公募（社区）
流动性储备	5%	5亿	交易所做市、稳定币池初始化

4.0 保密性

保密性是管辖合规资产的重要环节。Ontomir 的保密和隐私特性专为金融行业设计，关注以下三方面：

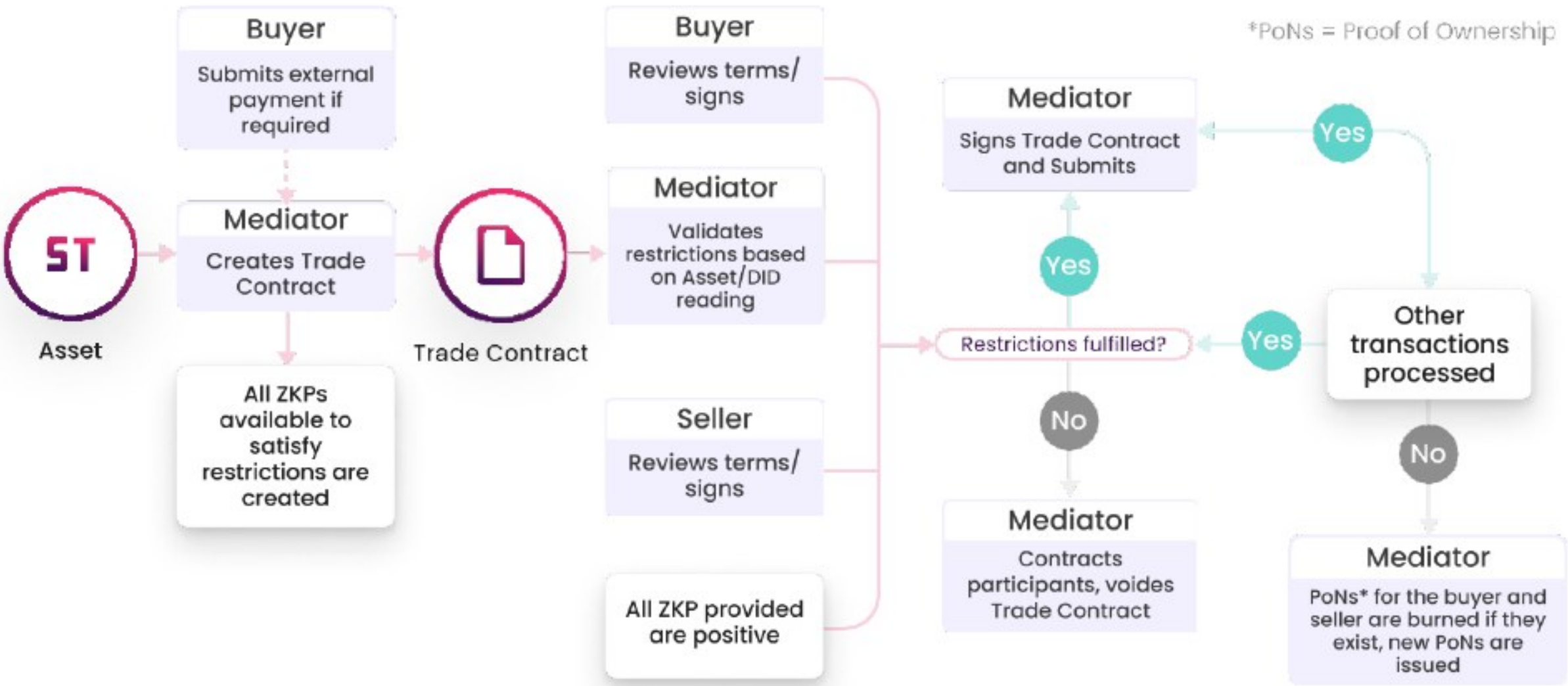
1.在不泄露机密信息的情况下，执行所有权、转让及其他限制。
2.保护代币持有人的隐私。
3.在满足前两点的同时，确保发行者能够报告、审计其资产持仓。

通过保密交易工作流程实现Ontomir的保密性。

4.1 保密交易工作流

Ontomir的保密交易工作流通过结合零知识证明和链下声明，安全地实现交易隐私。例如，双方进行交易时：

1.发行者或受信任的第三方在链上创建交易合约，设定需满足的限制条件。
2.可用零知识证明替代部分限制条件。
3.对于其他限制，中介方在链下验证并签署确认。
4.双方数字签署交易。
5.交易在链上完成。
6.加密交易详情记录在资产数据存储，供报告或其他转让限制参考。



4. Trusted third parties/mediators are companies like exchanges, broker-dealers, etc. who handle anything from a single transaction to a raise, all on behalf of the issuer.

5.0 Ontomir 治理

Ontomir 是一个去中心化的区块链网络，拥有完善的治理机制。治理结构主要由主委员会（Governing Council）和若干专门的子委员会组成。

主委员会的职责：

•监督所有子委员会的运作。
•有权创建或解散子委员会。
•协调各子委员会的活动。
•确保治理过程的透明性和有效性。

子委员会的职责：

•**技术委员会**：负责网络升级和技术开发。

•**经济委员会**：管理网络经济，包括 OTM 的发行政策和费用设置。

•**公司治理与提名委员会**：监管主委员会和各子委员会的运作，制定治理框架、行为准则和道德政策。

•**咨询委员会（特别项目委员会）**：负责处理技术委员会和经济委员会以外的特别项目和活动。

5.1 网络升级

传统公有区块链在升级过程中存在硬分叉的问题，可能导致区块的重复实例化，对于网络资产来说是严重的问题。Ontomir 通过链上治理机制实现无分叉升级，避免了这一问题。

Ontomir的 WASM 运行时直接存储在区块链上，节点在接到升级通知时，会从链上自行拉取最新版本。这种机制确保所有节点使用相同的运行时版本，降低了升级过程中需要的协调开销。通过链上治理管理网络升级，所有链上观察者均能明确区块的官方版本，减少了用户和节点在分叉情况下的不确定性。