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。

免责声明

本文件仅供信息目的，不对Ontomir产生任何义务。本文件概述了Ontomir的产品开发计划，所含信息是选择性的、前瞻性的，可能会根据技术发展和行业条件等风险和不确定性因素进行更新、扩展、修订或修改。Ontomir不承担任何义务向收件人提供额外信息或更新、扩展、修订本文件中的信息，也不保证本文件中的信息准确无误。

本文件不构成出售或购买OTM或OTM的要约或邀请，也不构成Ontomir的承诺或意图。它不构成一份招股说明书，也不构成任何形式的法律或财务建议。收件人应进行自己的调查和分析，并寻求专业的法律、财务、税务、技术等方面的建议。

Ontomir对本文件中的任何信息不承担任何责任。

Ontomir

目录

1.0 简介

安全代币是使用区块链技术创建的金融证券。与传统证券类似，它们代表资产的所有权利（如股权、债务、房地产等），但以数字化形式（代币化）创建，能够通过区块链技术提升效率和功能。安全代币为市场带来诸多好处，例如通过自动化操作提高效率、增加全球流动性池、创建新的金融资产。

以太坊区块链是创建、发行和管理安全代币最广泛使用的平台。通过智能合约，以太坊可以高效管理嵌入发行者安全代币的监管规则，从而解锁非传统资产并提高流动性。最初选择在以太坊上发布初始平台是一个明显的选择——可信且安全的基础设施使我们能够验证安全代币市场的可行性。

然而，我们在一个通用区块链上的经验帮助我们理解，以太坊缺乏一些关键元素，而这些元素对于行业和机构接受安全代币至关重要。例如：

身份：以太坊的核心原则是匿名性和分散化，这与身份验证的法律和合规要求相冲突。

保密性：以太坊上的交易和持仓信息公开可见。

治理：以太坊的硬分叉在升级期间对发行者构成重大风险。

合规性：必要的安全代币功能受到交易限制的阻碍。

通过一个专为安全代币设计的特定领域区块链，这些元素可以从底层就被纳入其中，从而提高可用性并优化共识机制，推动安全代币行业的采用。

2.0 架构

2.1 金融原语

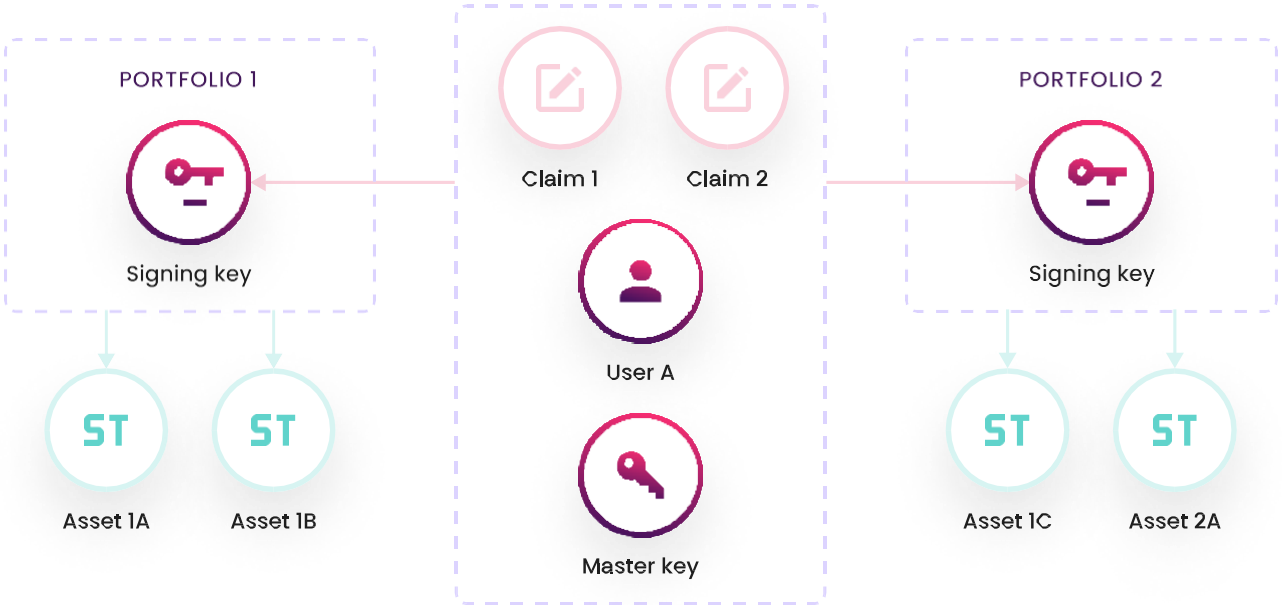
通用目的的区块链通常只有少数几个原语，即在区块链核心内置的功能。相反，包括安全代币及其相关的所有权、转让和其他限制在内的元素都是在区块链之上以智能合约的形式实现的，这导致了可扩展性和性能方面的挑战。然而，Ontomir的金融原语是内置于链的基础中的。Ontomir的金融原语允许用户以低预定的成本操作区块链，同时允许第三方开发人员在链上部署创新去中心化应用程序（dApps）。

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。



每个身份都有一个唯一的管理密钥，可用于从身份中添加或删除签名密钥。签名密钥可用于通过身份执行操作，以及为身份和Ontomir内的相关功能提供粒度角色和权限。作为去中心化身份基金会的成员，以及多个标准化机构的参与者，我们在身份方面的方法反映了这些合作。

2.1.3 记录保存

Ontomir区块链捕获所有一级市场和二级市场的安全代币转让，允许信任地在链上捕获代币所有权数据，从而减少发行者与代币持有人之间的信息不对称。Ontomir以多种形式记录发行的安全代币的转让，从链上原子结算到来自链下第三方服务提供商的付款收据。

2.1.4 资本分配

许多资产都有相关的现金流。Ontomir允许发行者通过在固定时间点捕获所有权分发数据来分发这些现金流。发行者可以根据身份或其他标准来确定分发的受益人。他们可以使用智能扩展（见2.3部分）来执行复杂的计算，确定分发金额，在链上使用稳定币（见2.1.6部分）进行分发，或者使用付款收据在链下分发，或者通过链上和链下交易的组合来分发。

2.1.5 公司治理

Ontomir上的公司治理允许发行者利用公共区块链的力量，结合透明度和令代币持有人能够在隐私保护下对发行者的公司行动进行投票，同时减轻对投票操纵的激励。

2.1.6 稳定币

除了安全代币，Ontomir还支持稳定币，以便在链上进行活动（如现金分配）时降低传统成本。Ontomir上的稳定币可以与任何货币挂钩，并由具有适当许可证和资本的第三方发行。

2.2 经济

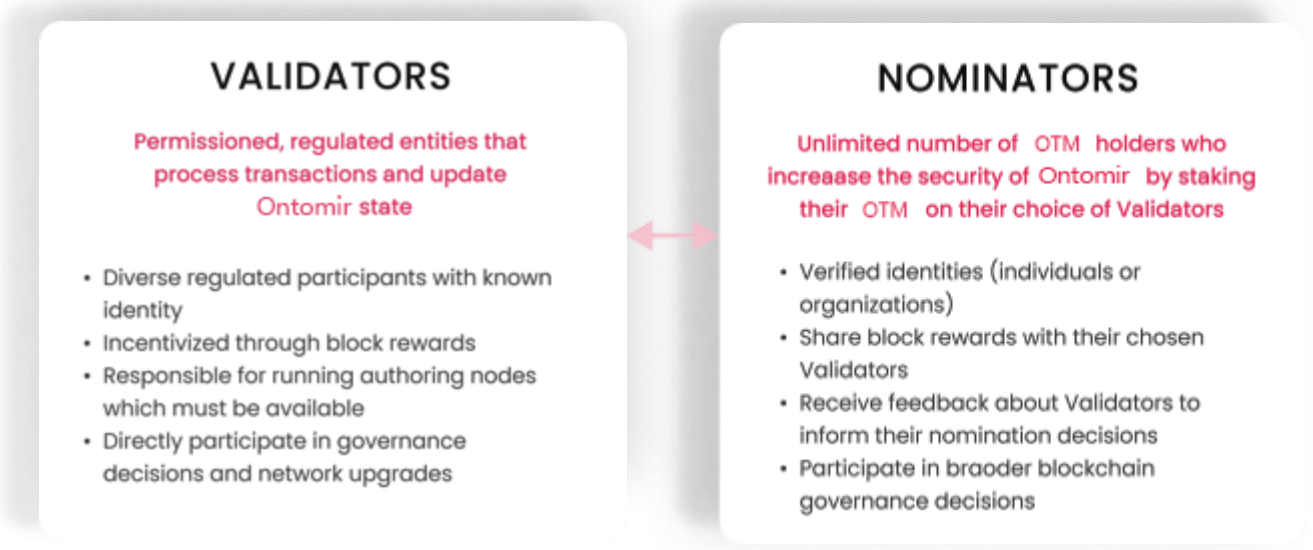
通过与领先的经济、博弈论和运营流程专家进行广泛的研究和咨询，为Ontomir建立了代币经济，旨在为该链提供效用、安全性和可持续性。该经济的核心是原生协议代币，即OTM，它既保护又运营区块链。在Ontomir上进行的任何交易或使用智能合约都需要用OTM支付。

2.2.1 启用经济

Ontomir的共识机制是提名权益证明（Nominated Proof-of-Stake）。验证者和提名者通过在网络中抵押并根据共识规则行事，为Ontomir的启用经济提供动力。参与者根据协议规则成功验证区块后获得奖励。验证者和提名者不负责确保交易合规，只负责确保交易按照协议规则正确完成。

验证者运行授权节点，以确保区块链的安全和操作正常。Ontomir上的验证者是具有权限的实体，并在各自管辖区受到监管。它们在区块生成和最终确认时获得区块奖励，并可能因恶意、闲置或错误的活动受到以罚款形式表现的处罚。预期的验证者可以将他们的申请提交给经济委员会审查和批准。（见5.0部分更多关于治理的信息）。

提名者选择并抵押验证者，以表明信任。它们的抵押分散在其选择的验证者上，使用一种算法来尽量均匀分配所有抵押的OTM代币。任何经过验证的OTM代币持有人都可以成为提名者。如果被提名的验证者按照协议规则表现良好，验证者和提名者都会获得区块奖励。同样，提名者可能因提名验证者的不当行为受到处罚。



1. Web3 Foundation, "Intro to Nominated Proof-of-Stake," Research at W3F. https://research.web3.foundation/en/latest/polkadot/NPoS/index.html
2. Web3 Foundation, 2019, "Sequential Phragmen Method," October 30. https://wiki.polkadot.network/docs/en/learn-phragmen

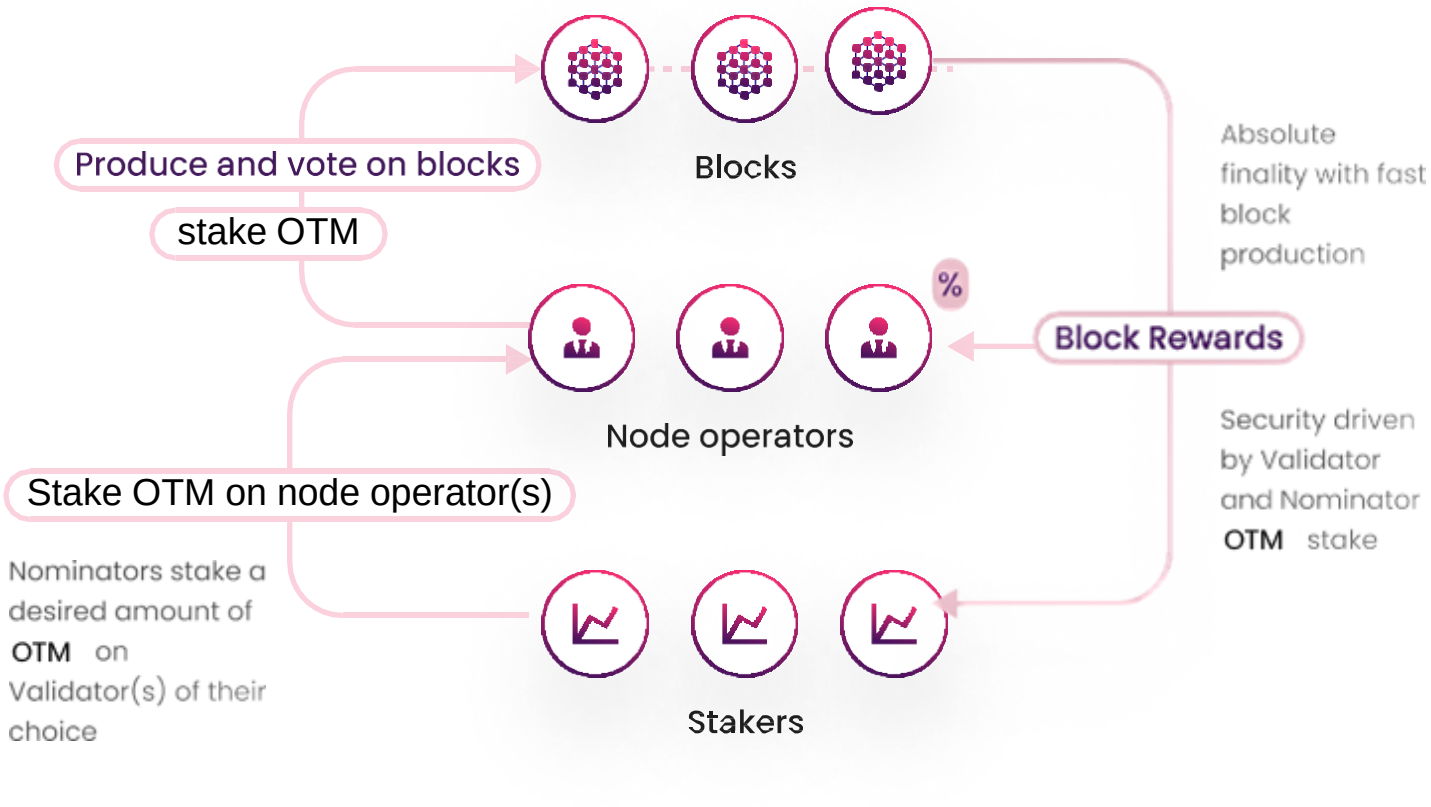
区块奖励由所有遵守协议规则的验证者均分。验证者会保留一定比例的奖励，其余部分按比例分配给提名者。

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

2.2.2 内部经济

Ontomir的内部经济是由提供绝对最终性、激励正确生产区块和建设可持续和安全网络的客观目标驱动的。

Ontomir网络的财政部已在2025的Q3季度OTMT到OTM桥接关闭时完成资助。财政部不从协议交易中获得任何费用，所有交易费用流向协议的运营商。OTM代币从网络储备中分配，基于治理过程，这将随着Ontomir的发展而可能演变。从网络储备中支出资金的请求将最初由Ontomir治理委员会管理，并最终可能由OTM代币持有人治理，具体取决于治理委员会的决定。网络储备资金将用于以下用途：向开发者提供赠款和补贴，并以这些赠款和补贴来扩展Ontomir生态系统。

在2025年Q3季度Ontomir桥接关闭后，Ontomir总代币供应约为100亿代币。OTM代币的总供应20%以资助区块奖励。区块奖励机制的设计将确保在任何时候有一足够比例的OTM代币被抵押以支持Ontomir的基于证明权益的共识机制。除了通过创建新的OTM代币以外，区块奖励也将通过网络费用来提供资金。

2.2.3 启用经济中的费用

OTM费用是Ontomir核心中的关键要素，主要用于两方面：

1.防止服务拒绝（DoS）或垃圾攻击：通过收取费用，防止网络被滥用和拥塞。
2.奖励开发者或机构：鼓励开发者在Ontomir 上构建应用，并为特定资产类别和管辖区提供定制合规规则。

Ontomir共有三类费用，所有费用均由交易发起者承担：

•交易费用（GAS费用）：所有在Ontomir上的交易均需支付此费用。费用基于交易的字节大小和复杂程度，但无论交易功能如何，费用都会统一收取。
•协议费用：具体用于某些原生功能，如保留代币名称 OTM。费用由Ontomir治理委员会设定。
•开发者费用：由智能合约和智能扩展的开发者自行设定。该功能目前尚未在Ontomir中激活，具体机制、费用分成比例等细节将通过链上治理过程确定并公布。

2.2.4 OTM代币

OTM代币专为Ontomir链设计，主要用于以下几个方面：
•为网络提供动力：类似于以太坊上的ETH，OTM作为燃料在Ontomir上使用，用于支付交易费用（如提交交易、运行智能合约）和覆盖系统运营开支。
•提升系统价值：OTM代币持有者可以通过质押代币来提名验证节点并获得区块奖励中的分成，从而参与 blockchain 的安全保障。
•防止垃圾信息：为每笔交易设置OTM成本，有助于避免网络的垃圾信息泛滥。
•资助生态系统：通过OTM代币，拨款资助促进生态系统增长和维护的项目。
•治理升级：OTM代币可用于质押和投票网络升级决策。

OTMT 到 OTM 代币升级机制

Ontomir主网上线后，Ontomir治理委员会可自主决定至少在25年Q4季度开启OTMT到OTM的桥接上线。持有OTMT代币的用户可1:20的比例升级为OTM代币。此外，Ontomir公司的部分OTM代币储备也将通过相同的桥接进行迁移。进行任何OTM代币交易的用户需通过授权的身份验证服务提供商进行身份验证，以确保合规性与安全性。

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

2.2.6 21个节点分配方案分配方案

一、节点资格与质押
最低质押门槛：每个节点需质押 1%总代币（1亿），防止女巫攻击。
动态轮换机制：每季度根据 节点贡献度排名 淘汰末位3节点，新节点需重新质押。

二、节点奖励分配（20亿代币）
基础奖励（50%）：按出块数量平均分配，确保基础运维动力。
绩效奖励（50%）：根据 三项指标加权：
技术贡献（40%）：代码提交、漏洞修复（GitHub数据挂钩）
治理参与（30%）：提案投票率、社区提案发起数量
生态增长（30%）：引入DApp数量、链上TVL增量

三、防中心化设计
质押上限：单个实体最多控制 2个节点，且总质押量≤3%。
惩罚机制：节点作恶（双签、宕机）则扣除 50%质押代币，注入生态基金。

四、代币释放周期
释放规则：

节点质押奖励	每年释放20%（持续5年），首年启动后第6个月开始
团队与顾问	6个月锁定期，后按月线性解锁
生态发展基金	社区投票决定释放节奏（每年最高释放30%）
私募投资者	6个月锁定期，后按月释放25%

五、治理模型补充
节点治理权：每个节点拥有 1票，重大提案需≥15票通过。
社区对冲机制：普通用户可质押代币（≥10万）发起「节点弹劾提案」，获得51%社区支持即可强制替换节点。

六、风险控制
冷启动阶段：前3个月由基金会临时托管5个节点，确保链稳定运行。
极端情况熔断：若超过7个节点同时故障，自动启用备用链并冻结转账48小时。

七、分配方案优势
激励兼容：节点收益与生态增长强绑定，避免躺平。
去中心化平衡：通过轮换+质押上限降低巨头垄断风险。
抗波动性：逐年释放的代币减少市场抛压，提升长期价值。

2.3 智能扩展

智能扩展极大拓展了Ontomir上安全代币的功能。发行者可通过智能扩展根据监管机构和投资者的定制需求，扩展其代币的功能，同时依然保持基础协议中标准化的生命周期事件执行。以下四个金融原语可通过智能扩展进行个性化配置：

- 隐私资产（Regulated Asset）
- 资本分配（Capital Distribution）
- 记录保存（Record Keeping）
- 公司治理（Corporate Governance）

2.4 第三方可扩展性

智能扩展的功能还可根据具体领域进行限制。此外，Ontomir允许第三方公司开发智能扩展，部署链上去中心化应用程序（dApps），以利用Ontomir的金融原语，提供创新型开源金融协议和其他相关服务，从而丰富生态系统。

3.0 身份验证

用户在首次接入Ontomir时，需通过授权的身份验证服务提供商验证身份。这一验证身份是Ontomir体系的核心，它虽增加了用户接入的复杂性，但带来了诸多长期的优势，包括提升合规性、防止欺诈、支持机构用户的快速接入等。

身份验证服务提供商需确保用户的身份声明持续有效（持续合规性）。部分发行者和代币持有者需接受额外持续检查，视具体资产和管辖区而定，部分情况下需进行资质鉴别。

身份验证在初始接入中的另一个关键作用是提高对付 Sybil 攻击的抵抗力，即阻止用户随意创建多个虚假身份。通过将身份验证置于底层协议中，用户可基于单一身份和相互声誉进行交易，大幅降低了复杂开源金融协议的使用门槛。

身份认证带来的其他优势：

•**OTM代币来源追踪**：法规合规的实体（包括机构）可通过可追溯的代币来源，确信其获取和使用OTM代币的合法性和合规性。

•**身份验证**：所有验证节点和提名节点在身份验证后，网络可有效防范与限制或制裁国家、机构或个人进行交易的风险。

•**监管资产的身份验证**：通过分层客户尽职调查（CDD）方法，发行者可结合验证身份和补充调查，达到自身需求的合规保障水平。

所有用户在正式接入Ontomir前，需通过Ontomir授权的身份验证服务商验证身份。服务商名单将通过Ontomir治理机制维护更新。初始身份验证为Ontomir内部的业务风险管理目的，发行者、开发者等其他实体需自行进行更严谨的合规调查，切勿依赖Ontomir的验证结果。

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：

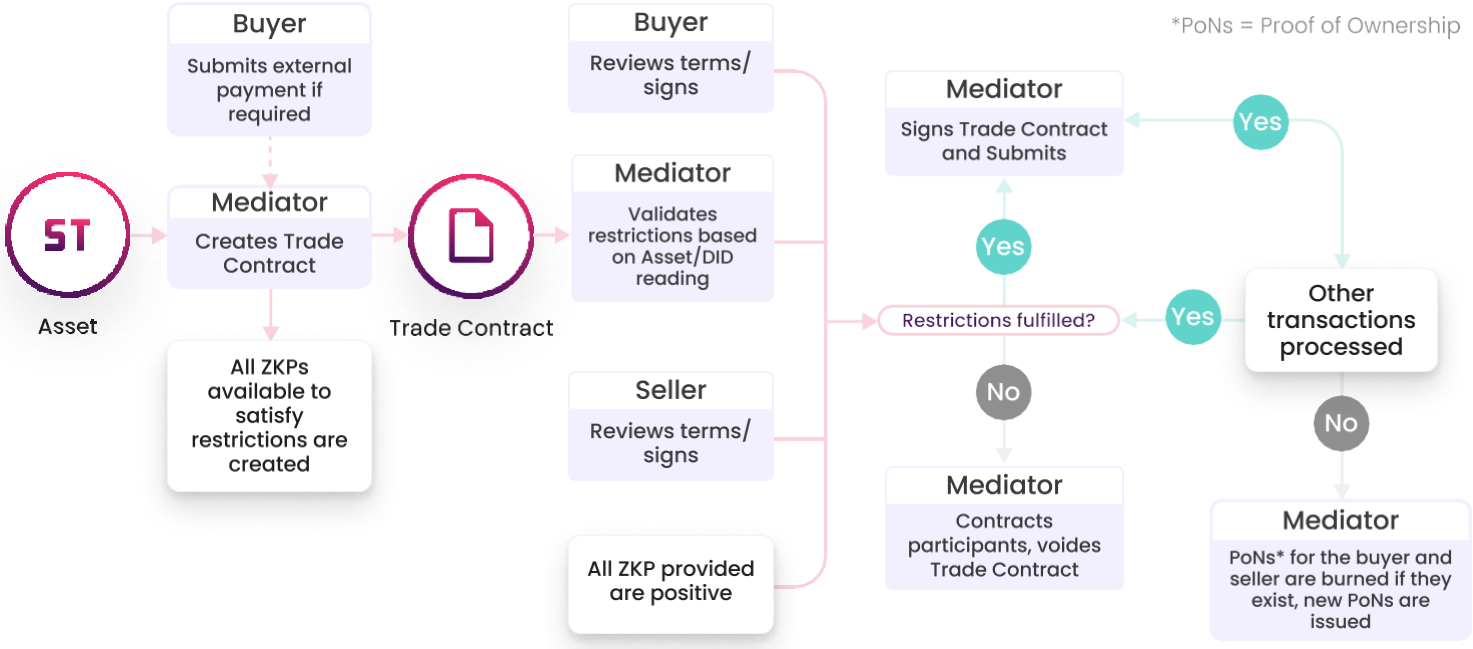
1.在不泄露机密信息的情况下，执行所有权、转让及其他限制。
2.保护代币持有人的隐私。
3.在满足前两点的同时，确保发行者能够报告、审计其资产持仓。

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.

4.2 审计与隐私的平衡

当涉及到所有权隐私时，Ontomir面临的一个挑战是它使用账户模型而不是UTXO模型，这使得许多在转移过程中保护隐私的现有方案对Ontomir来说不可行。[5] 这个挑战通过使用各种加密技术来解决。关于这些技术的更多细节将在专门讨论隐私的单独白皮书中讨论。

4.3 发行者报告与管控

正如4.1中提到的，由于贸易合同和交易工作流程设计，无论参与方或调解人是谁发行方的资产交易细节始终可以被发行方解密。在链上，它将记录为加密的blob，因此所有报告和审计都可以完全由发行方完成。

4.4 观察权限

	CAN SEE	CANNOT SEE
Issuers[6]	• All transactions and details relating to their own assets	• Transaction data for other issuers' assets • Investor ownership of unrelated assets
Mediators	• Details for transactions they have mediated • Asset data required to verify trade restrictions	• Transaction data for transactions they did not mediate, unless an issuer has made this information available for satisfying transfer restrictions • Investor ownership of other assets
Investors	• Their own wallet balances • May be able to deduce when other parties are trading an asset they previously held, but not the quantity traded	• Transaction data relating to the asset outside their own transactions • Other investor ownership of other assets
Validators/ Nominators/Public	• That a transaction has occurred between two parties	• Transaction amounts or assets

5. Rui Zhang, Rui Xue, Ling Liu, 2019, "Security and Privacy on Blockchain," Association for Computing Machinery, August 16, 7-9, https://arxiv.org/pdf/1903.07602.pdf

6. Regulators can request details from issuers directly.

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。

6.0 合规性

在Ontomir上，资产的自动化合规既透明又实时，有助于简化资产的监管报告，消除使用复杂系统跟踪和授权资产转移的需要，降低运营成本，并降低流动性障碍。

在Ontomir上管理资产分配和代币所有权意味着发行者有实时执行合规性的能力，通过代表不同合规规则的智能扩展来实现。这些智能扩展用于验证资产转移，并在以标准化方式管理资产类型、司法管辖区和提供类型组合的合规性时提供灵活性。智能扩展由第三方开发人员提供，并可供所有Ontomir发行者使用。发行者负责为其代币发行选择、配置和实施适当的智能扩展套件，以满足特定的监管、合同或其他要求。

智能扩展如何运作的一个例子:

创建一项资产，最多可由1,000名投资者持有，任何单一投资者持有的资产不得超过10%。·

两个独立的智能扩展将分别管理一条规则(最大投资者数量和最大所有权百分比)，根据这些规则批准或拒绝转让。

Ontomir还通过身份原语对资产合规管理进行了标准化。发行者可以根据投资者的身份声明创建规则，以控制谁可以持有资产以及在何种条件下持有资产。例如，发行者可以将资产所有权限制在完成特定客户身份识别和反洗钱的投资者手中，或者可以管理适用于其员工或附属机构的转让限制。

7.0 标准与互操作性

虽然Ontomir是一个独立的区块链，但在某些情况下，将资产从其他区块链带到Ontomir的优势可以非常强大。

7.1 ERC-1400标准：

在以太坊上，Ontomir团队领导了安全令牌标准(ERC-1400)的创建，以满足金融机构对资产创建和处理一致性的需求。ERC-1400是一个标准库，用于指导合规安全令牌的高效和有效创建。具体来说，它包括:ERC-1594，核心安全令牌标准;ERC-1643，文档管理标准;ERC-01644，控制器令牌标准;ERC-2258，托管所有权标准;以及ERC-1410，部分可互换代币标准。Ontomir的资产和合规模型受到ERC-1400规范的启发，并进一步增强，为原生在Ontomir上创建的资产提供完整的资产生命周期功能。

7.2 Relay Chains（转接链）：

实现互操作性的一个途径是通过中继链。像Polkadot这样的中继链旨在提供一个去中心化的互操作层，使不同的网络能够以原子的方式通信和交换状态。它们在安全性、用户体验和必要的验证者方面有不同的权衡，验证者可以监控中继链及其交互的区块链。目前没有立即计划将Polymesh运行在中继网络上。然而，该架构的设计是为了在未来考虑这一选项。

7.3 Wrapped Assets（包装资产）：

Ontomir无缝支持各种类型的封装代币，以及其他开放金融协议。对于这些在其他区块链上的资产，可以迁移资产至Ontomir。通过桥接机制将资产锁定在原链并在Ontomir上重铸为包装代币。包装代币可按需在Ontomir上销毁以解锁原链上的资产。

7.4 迁移已监管的安全代币

Ontomir 提供了一个简化的流程，允许已存在的监管资产发行者将其资产迁移到 Ontomir，以利用其独特功能和优化。然而，对于拥有大量投资者的先前存在的资产，这一过程可能较为复杂，因为需要对每一位投资者进行单独迁移。为了减轻这一疑虑，Ontomir 提供了占位身份和账户，供尚未迁移到该链的现有投资者使用。这些占位身份可以由投资者在他们希望与自己拥有资产进行交互时无缝领取。

8.0 数据来源与市场数据

Ontomir采用行业标准来定义如何引用或检索各种类型的市场数据。它依赖于一个联邦式的安全模型，通过验证节点或市场数据提供商作为可信的数据来源。

8.1 验证节点的市场数据

（离链工作者）

Ontomir 通过一组经过许可和信誉良好的验证节点，整合了主要市场数据提供商。这些验证节点使用称为“离链工作者”的方法，从外部（非区块链）来源检索和提供数据。这一方法处理超过单个区块的任务。

8.2 一般市场数据

（已签名数据）

市场数据也可以通过特定的数据提供商以相同的流程请求。这一数据使用提供商的已知公钥进行签名，并在链上进行验证后，再使数据可供使用。此方法依赖于信任单一数据提供商来共享正确数据并保护其私钥。

进一步阅读

加密资产的制度化

链接：https://assets.kpmg/content/dam/kpmg/us/pdf/2018/11/institutionalization-cryptoassets.pdf

保密性

- Aztec隐私协议：https://www.aztecprotocol.com
- Zether：实现智能合约中的隐私：https://crypto.stanford.edu/~buenz/papers/zether.pdf
- 匿名Zether：https://github.com/jpmorganchase/anonymous-zether
- ZkVM：快速、隐私、灵活的区块链智能合约：https://github.com/stellar/slingshot/blob/main/zkvm/docs/zkvm-design.md
- Lelantus：基于标准假设的区块链交易保密性和匿名性：https://eprint.iacr.org/2019/373.pdf

参考文献

加密资产的制度化：https://assets.kpmg/content/dam/kpmg/us/pdf/2018/11/institutionalization-cryptoassets.pdf

斯图尔特，阿利斯泰尔（Alistair Stewart）。2019年11月20日。“GRANDPA最终确定器：扩展摘要。”W3F基金会研究。链接：https://research.web3.foundation/en/latest/polkadot/GRANDPA.html

W3F基金会的“提名权益证明简介”：链接：https://research.web3.foundation/en/latest/polkadot/NPoS/index.html

W3F基金会。“顺序法格门方法”。Polkadot Wiki。2019年10月30日。链接：https://wiki.polkadot.network/docs/en/learn-phragmen

张瑞（Rui Zhang）、薛瑞（Rui Xue）、刘玲（Ling Liu）。2019年8月16日。“区块链上的安全性与隐私性。”美国计算机学会。链接：https://arxiv.org/pdf/1903.07602.pdf