CarbonX — 去中心化森林碳汇系统

推动全球可信碳交易

CarbonX 团队

2026/1

目录

1. 执行摘要

CarbonX 是一个可验证、可审计、注重隐私的平台，将经过验证的林业碳转化为可交易的数字资产（CAT），同时通过原生治理代币（FOX）和有限供应的碳汇智能体（CA）身份层协调去中心化治理和激励。

该平台结合了基于卫星的遥感、机器学习、隐私保护计算（MPC + ZKP + 可验证计算）以及无许可随机节点认证协议，能够生成高完整性、RWA 支持的碳代币。CarbonX 针对辖区和项目规模的森林碳供应，支持机构级资金建设（DAT 金融金库）、零售和机构市场，以及对不断变化的自愿和受监管碳市场的合规发行。

本白皮书记录了技术架构、核心算法、代币经济学、市场分析、合规方法、安全模型、团队以及生产的实用路线图。

---

2. 市场机会

全球对碳信用和自然解决方案的需求巨大，预计将在 2030 年及以后实现实质性增长。需求驱动因素包括企业净零承诺、司法管辖区 REDD+/司法管辖区项目的增长、公共融资工具以及创新的混合融资（公私合营和主权支持的远期购买计划）。

鉴于其目前自愿发行的份额、数字 MRV 的扩展机会以及现有的机构融资流，CarbonX 将林业和土地利用碳（基于自然的供应）列为优先事项。

（详见附录，了解详细假设和敏感性表。）

---

3. 关键要点

当前自愿性和管辖区森林碳市场受限于：

1）高成本、缓慢的 MRV 循环;

2）来源不明和完整性感知;

3）土地所有者和政府的隐私和主权关切;

4）分散的清理和定居基础设施;

5）长期买家和机构国债的金融产品不足。

CarbonX 通过提供更便宜、可重复的 MRV 来弥补这些空白;敏感原始数据的可证明隐私;去中心化认证，减少单点信任;符合标准的发行，且可与现有注册机构进行核对;以及用于流动性和资金管理的代币金融系统。

---

4. 平台愿景与定位

CarbonX 定位为高质量林业 RWA 的认证碳资产市场与协议。核心产品支柱：

- **认证并代币化。** 将经过验证的森林碳减排/移除转换为 CAT 代币，并实现一对一映射到链上支持的 RWA 元数据和审计证明。
- **隐私优先的 MRV。** 使用 MPC + ZKP + 可验证计算，允许利益相关者贡献敏感的测量数据，而无需泄露原始输入。
- **去中心化认证。**随机、质押安全节点选择用于认证;每次发行三节点共识以分配信任和经济奖励。
- **机构财政部。** DAT 金融金库将 CAT 与 BTC 及 PAXG 结合，打造多资产可持续的宝库。
- **治理与激励措施。** FOX 代币管理平台参数;CA 代理（5000 个终身供应）是稀缺的身份/参与名额和收入共享承载者。

---

5. 技术架构

高层架构分为分层：数据层、处理层、隐私层、共识/认证层、结算层和外部合规/预言机层。

5.1 数据层：遥感与地面真实化

数据来源：

- 多光谱卫星影像（Sentinel-2、Landsat、Planet、商业 VHR（合同））。

- 基于激光雷达的伞盖高度和结构（GEDI，空中激光雷达活动（如有）。

- 项目合作伙伴和本地核查团队提供的实地盘点（地块测量）。

- 辅助数据：土壤地图、土地利用地图、土地使用记录、社区报告输入。

设计原则：

- 利用多源聚变估算地上生物质（AGB）并进行变化检测。

- 维护来源：每次数据摄取都会存储一个签名元数据包（源、时间戳、传感器、预处理链）。

- 接受公共和商业资源;当使用商业数据时，平台会记录可验证的语句（哈希/承诺），同时在隐私层下保持原始文件私密。

5.2 处理层：人工智能 / 算法

核心算法组件：

1. **预处理与拼接。** 放射性和几何校正、大气校正、云遮蔽。

2. **树冠高度与生物量估计器。** 集成机器学习结合光学指标、SAR 反向散射（如有）和激光雷达推导的高度模型，估算带有不确定性带的每公顷 AGB。

3. **变化检测与基线建模。** 时间序列模型检测森林砍伐/退化事件，并利用历史趋势和管辖区政策建模反事实的基线排放。

4. **不确定性传播模块。**传感器和模型不确定性在最终碳估算和发行量中的蒙特卡洛传播。

5. **欺诈/异常检测。**时空异常评分，标记异常模式（例如，以该速率突然再生树冠不太可能），供人类审查。

输出：网格化 AGB 地图、发布窗口的 delta-AGB、每图置信区间，以及用于下游隐私计算和验证的签名摘要。

5.3 隐私层：MPC、ZKP、可验证计算

目标：允许贡献者（地方政府、项目开发者、测量员）保持原始数据私密，同时公开证明平台的发行数学对这些数据的正确运行。

模式：

1. **秘密共享/MPC 聚合。** 本地数据所有者将敏感测量拆分为秘密共享，提交给一组计算节点（从经过审核的 MPC 联盟中选出）。节点共同计算汇总统计数据（如平均生物量、变化总数），无需重建原始输入。

2. **可验证计算/简明 ZK 证明。** MPC 聚合后，节点生成零知识证明（如 zk-SNARK 或 STARK），证明协议中定义的规范发行函数 f（data） 在提交输入上正确执行，最终的发行量为 Q。证明非常简洁，可以链上发布。

3. **校样出版。** 证明+承诺摘要会发布到区块链;智能合约验证证明（或验证证明证明），并相应铸造 CAT 证书。

4. **可审计性与隐私。** 经许可的审计员可通过密码开口请求针对特定地块或时间窗口进行选择性披露。该系统支持在当地法律和政策允许的情况下进行基于角色的揭示。

- 平台运行轮换的 MPC 联合体;节点由可信运营商（研究合作伙伴、审计员、区域枢纽）运营，这些运营商需接受技术和法律的入职程序。

- 为了性能，重型机器学习任务在传统计算（GPU）链下运行，生成确定性摘要，然后输入 MPC/验证步骤。

5.4 共识与分散认证

认证模型（核心创新）：每个发行窗口随机选择 3 个认证节点，按质押加权。

流程：

- **质押。** 认证节点（可能包括 CA 持有者、机构合作伙伴、认证验证者）质押 FOX 或锁定在智能合约中的独立质押令牌。

- **随机选择。** 协议通过基于 VRF 的随机信标，在发行时选择 3 个节点，以证明 MPC/校样阶段准备的消化。

- **认证与奖励。** 被选中的 3 个节点验证证明，签署发行记录，并获得发行费用和部分 FOX 挖矿分配的分成。

- **削减。** 如果选定节点后来被发现恶意行为（例如签署无效发行），则该节点将受到切割（质押减少）并暂时从认证池中移除。

理由是：三节点选择既能保证每次发行信任的分布，又能控制运营成本。

5.5 结算与智能合约

高吞吐量的 L2 或兼容 EVM 链的智能合约将管理：

- CAT 铸造/销毁（RWA 支持的发行和退役）。

- FOX 治理质押和矿工排放计划。

- 加州身份签发与转移登记。

- DAT 财务保险库控制、多重签名托管和再平衡规则。

关键模式：

- **链上证明验证。** 智能合约在铸造 CAT 前验证链上证明/证明对象的存在。

- **RWA 元数据 CID。** 令牌元数据指向一个不可变的 CID（IPFS/分布式存储），包括发行摘要、总结 MRV 报告、治理数据以及第三方审计报告的引用。

- **抵消机制。** 买家可以销毁 CAT，创建链上退休收据和链下登记更新，以便管辖区对账。

5.6 预言机、审计与互作性

- **预言机** 提供外部数据：汇率、国库价格、登记册更新和监管事件。
- **第三方审计与** 证明流程集成：认证审计员可以将其报告锚定于发行的 CID，并发布独立的声明。

- **互作性**：为其他链的 CAT 交易提供跨链桥（乐观或信任最小化）;结算和托管模式遵循最佳实践以避免重复计数。

---

6. 代币设计与经济模型

6.1 双令牌原语（CAT / FOX）

CAT — 碳资产代币

- **目的：**1 ： 1 代币化表示已验证的林业碳 RWA 单位（根据发行政策;例如，根据平台定义的老年规则，1 CAT = 1 T CO_2当量）。

- **属性：**可转让、可燃烧、可作为抵押品使用、在交易所上市。

- **发行：**仅在成功验证 MRV、三节点认证和智能合约验证后铸造。每个 CAT 都关联到一个不可变的发行记录。

- **销毁：**链上烧毁 CAT 并产生不可撤销的抵消收据。

FOX — 治理与激励代币

- **目的：**平台治理、认证者权利质押，以及作为启动验证者/认证者生态系统的排放奖励。

- **供应与配置：**

总供应量 10,000,000,000 FOX。

配置：

20%用于基金会财库，

50%用于挖矿（发行/监控奖励），

10%用于早期投资者，

10%用于团队，

5%用于社区，

5%用于生态伙伴

- **实用性：**质押以成为认证者，保证发行 CAT（经济安全），治理投票，费用折扣和协议参数提案。

6.2 碳汇智能体（CA）

Carbon X 运营着一个由 10,000 个碳汇智能体组成的网络，负责：

一. 森林数据提交

二. 卫星与遥感验证

三. MRV 协调

四. 治理参与

节点是基础设施提供商，而非投机性挖矿者，必须满足严格的运营和合规要求。

6.3 FOX 代币概述（代币经济学）

基本参数

- 代币名称：FOX
- 代币类型：实用性与治理代币
- 总供应量：10,000,000,000 FOX（固定，无通胀）

FOX 不代表股权、收益权或资产索赔。它的存在仅是为了运营和管理 CarbonX 协议。

核心经济原则：烧成新品

Carbon X 严格执行“**燃烧**”机制：

每一次链上铸造森林碳资产（CAT）都需要不可逆燃烧 FOX 元素。

燃烧参数在链上受控，并可根据以下因素动态调整：

- 碳市场定价
- 网络利用
- 系统安全要求

该设计确保：

- FOX 的结构性长期通缩
- 实际碳活动与代币需求之间的直接关联
- 平台增长驱动的无象征性通胀

FOX 分配结构

类别	分配	关键原则
代理挖矿激励	50%	100 年排放下降
财政储备	20%	稳定性与生态系统支持
团队与顾问	10%	长期归属
战略合作伙伴	5%	里程碑式发行
社区与生态系统	5%	DAO 与公共利益激励
早期投资者	10%	长期归属
总计	**100%**	固定供给

不进行公开拍卖或 IDO。

代理采矿激励（50%）

发射模型

- 排放持续时间：100 年

- 排放曲线：显著下降
- 日排放量，逐年减少

这一超长的计划反映了森林碳资产的数十年生命周期。

早期代理激励措施

前 500 个激活节点根据激活顺序获得更高的奖励系数：

- 更早激活=更高的寿命分配
- 系数线性衰减
- 节点#500 之后，奖励趋于规范

这种方式提升了数据可靠性，同时不造成永久集中化。

TGE 循环控制

- TGE 前的奖励作为不可转移的积分累积
- 在 TGE，只有部分有上限的部分可转换
- 目标 TGE 流通供应： **< 5%**

财政储备（20%）

目的

国库作为**数字资产国库（DAT）**运作，不参与投机性市场活动。

主要用途：

- 协议安全与审计
- 法律与监管合规
- 基础设施升级
- 长期生态系统投资

治理

- 多重签名控制（5/9）
- DAO 与董事会监督
- 所有作均记录在链上

团队、顾问及早期投资者（20%）

团队	Cliff	释放
团队与顾问	12–24 个月	36–48 个月
早期投资者	12–24 个月	36–48 个月

不允许 TGE 解锁。

战略合作伙伴（5%）

仅在经过验证的里程碑后才发布，包括：

- 国家或区域森林入驻
- 国际碳协议
- MRV 或卫星验证突破

未达标将无法释放。

社区与生态系统激励（5%）

该配置基于行为驱动且非投机性，支持：

- DAO 治理参与
- 碳数据贡献
- 公共利益验证
- 开发者生态系统的增长

分布是连续的，每个地址有上限。

7. 安全与风险缓解

主要安全领域：

- **密码学正确性：** 经审计的 MPC/ZK 库、确定性机器学习流水线、可复现摘要。

- **智能合约安全：** 多阶段审计、关键模块的形式验证及分阶段主网部署。

- **运营安全：** 基于 HSM 的 MPC 节点密钥管理、冷/暖钱包分离、作节点的 SOC2 级进程。

- **经济安全性：** 设立了质押、切割和时间锁定窗口，以防止行为不当后立即撤资。

---

8. 合规与治理

管辖战略：项目总部设在新加坡，利用新加坡明确的数字支付代币监管框架和严格的反洗钱/反恐融资监管。平台将根据当地法律追求相关许可或与持牌合作伙伴合作。

关键合规支柱：

- **反洗钱/KYC：** 终端用户流程将根据 FATF 指导实施基于风险的 KYC。托管服务将遵循 MAS 关于资产分类和安全保管的规则。

- **登记对账：** 与现有注册系统（如管辖区 REDD+注册、国家 MRV 平台）整合，以避免重复计数。

- **标准对齐：** 发行和 MRV 流程将遵循 IPCC 原则和认可注册机构的方法论（如适用管辖区 REDD+时采用 TREES/ART），并采用第三方审计。

- **治理：** FOX 代币持有者选举或取消认证者;基金会（20% FOX）拥有管理权和紧急治理权力，支持多重签名和时间延迟检查。

---

9. 团队与组织结构

该团队总部设在新加坡，汇聚了森林碳、隐私计算、密码学、合规和数字金融领域的专家团队。团队角色和顾问的定义旨在确保技术交付、法规一致性和市场成功。

CarbonX 由世界级专家联盟推动，涵盖碳林业、区块链工程、隐私保护计算和机构金融领域。我们的主要人员包括：

- **陈伟博士（清华大学）：** 曾任中国碳交易试点项目专家。陈博士精通 CCER（认证自愿减排）方法论和生态补偿模型，专注于将自然碳汇转化为高质量数字资产。
- **刘洋（北京大学）：** 隐私保护计算领域的高级科学家。他的研究重点是将可信执行环境（TEE）应用于链上碳足迹追踪，有效解决了企业排放数据相关的隐私问题。
- **赵子涵（复旦大学）：** 曾任顶级投资基金 DeFi 研究负责人。她是动态利率和流动性激励模型的专家，专注于设计碳信用代币的二级市场经济驱动因素。
- **王朔（上海交通大学）：** 一位跨链协议架构师。他专注于零知识证明（ZKP）的技术实现，用于碳资产在异构链上的清算和结算，提升资产流通的安全性。
- **Benjamin Tan（新加坡国立大学）：** 曾任新加坡金融管理局（MAS）合规官员。他精通《支付服务法》（PSA），专注于构建碳交易平台的合规框架和反洗钱（AML）机制。
- **Sarah Jenkins（斯坦福大学）：** 美国领先气候技术基金的合伙人。凭借丰富的直接空气捕捉（DAC）投资后经验，她专注于碳资产的全球定价和对冲策略。
- **Marcus Müller（苏黎世联邦理工学院）：** 著名密码学家，专注于多方计算（MPC）。他为 CarbonX 提供机构级密钥管理和分布式数据主权解决方案。

- **Alistair Vance（牛津大学）：** ESG 定量分析专家，参与设计了欧洲主要碳排放指数。 她专注于构建绿色金融衍生品及其相应的经济估值模型。

---

10. 路线图与里程碑

2026 年第一季度 ——CA 向早期投资者开放（500 CA），进行 Alpha 测试及首次 CAT/FOX 发行测试。

2026 年第二季度——Alpha 启动，首个单项目 CAT 发布;基础搭建及 DAT 金库设计。

2026 年第三季度——FOX 代币上所，建立流动性。

2026 年第四季度——CORP31 公开发布，企业合作伙伴前 1000 名 CA 激活。

2027 年——FOX 和 CAT 在机构国库市场整合上市。

（详见附录 C 中的技术门时间线。）

---

11. 市场与财务预测

我们预测采用多情景：保守、基质和激进。预测包括已上线项目数量、年度 CAT 发行量、平台收入（费用）以及 DAT 保险库资产管理规模。

（详见附录，了解详尽的金融模型和敏感性分析。）

---

12. 风险与缓解措施

主要风险包括代币的监管分类、MRV 模型风险、数据访问限制以及平台治理攻击。缓解措施包括保守的合规优先推广、强有力的第三方审计、多元化数据供应商，以及通过质押和削减保障经济安全。

---

13. 附录

A. 核心算法（概述）

- **AGB 估计器：**集合回归栈（光学指标+SAR+激光雷达衍生特征），基于精心策划的田野图训练，并通过跨生态区迁移学习。
- **基线估计器：** 利用面板数据回归、政策指标和因果推断调整的管辖区及项目特定反事实模型。
- **不确定性传播：**利用传感器噪声模型和模型误差分布自力蒙特卡洛计算发行置信区间。

B. 智能合约示意图

- **铸造合同：** mintCAT（proofCID， sissueanceMetadata， certifierSigs） - > 验证证明和签名 - > mint CAT - > 更新注册表。
- **质押合同：** 锁定 FOX - >成为认证候选人 - >有资格被 VRF 选拔。

C. 词汇表

CAT：碳资产代币 CarbonX 生态系统的主要实用性和资产代币。每个 CAT 代表一公吨经验证的二氧化碳当量（CO_2e），由林业项目封存。它是一种完全担保的实物资产（RWA），用于碳抵消和绿色金融。

FOX：森林所有权执行代币 协议的原生治理和实用代币。FOX 用于质押以铸造 CAT、参与去中心化治理，并激励网络的长期可持续发展。它通过回购和销毁机制捕捉协议的价值。

CA：碳汇智能体 一种稀有且不可替代的数字身份（NFT），作为高性能的“验证节点”。CA 负责碳汇的去中心化验证。CA NFT 持有者通过参与 dMRV 过程，获得协议费用和挖矿奖励的分成。

MRV：测量、报告与验证 确保碳信用真实且永久的行业标准框架。CarbonX 将这一过程发展为 **dMRV（去中心化 MRV），**利用卫星影像、人工智能和物联网传感器实现验证过程的自动化和去中心化。

MPC：多方计算 这是一个密码学子领域，允许多方（CA 节点）在保持这些输入私密的情况下共同计算函数。在 CarbonX 中，MPC 用于汇总敏感森林数据，而不暴露具体的地理或专有信息。

ZKP：零知识证明 一种密码学方法，通过该方法，一方可以向另一方证明某个陈述为真，而不透露除陈述本身有效性之外的任何信息。CarbonX 使用 ZKP 验证链上碳封存数据的真实性，同时维护数据隐私。

RWA：现实世界资产 存在于物理世界中的有形资产（如木材、土地或树木中碳封存），通过代币化被带上链。CarbonX 专注于将基于林业的碳汇代币化为流动的可编程数字资产。
