CarbonX — Decentralized Forestry Carbon System

POWERING CARBON TRADE FOR THE FUTURE

CarbonX Team

2026/1

Table of Contents

1. Executive Summary

CarbonX is a provable, auditable, privacy-first platform that converts verified forestry carbon into tradeable digital assets (CAT) while coordinating decentralized governance and incentives via a native governance token (FOX) and a limited-supply Carbon Agent (CA) identity layer.

The platform combines satellite-based remote sensing, machine learning, privacy-preserving computation (MPC + ZKP + verifiable compute), and a permissionless random-node certification protocol to produce high-integrity, RWA-backed carbon tokens. CarbonX targets jurisdictional and project-scale forest carbon supply, enabling institutional-grade treasury construction (DAT financial vault), retail and institutional markets, and compliant issuance for evolving voluntary and regulated carbon markets.

This whitepaper documents the technical architecture, core algorithms, tokenomics, market analysis, compliance approach, security model, team, and a practical roadmap to production.

2. Market Opportunity

Global demand for carbon credits and nature-based solutions is large and expected to grow materially through 2030 and beyond. Demand drivers include corporate net-zero commitments, growth in jurisdictional REDD+/jurisdictional programs, public finance instruments, and innovative blended finance (public-private partnerships and sovereign-backed forward purchase programs).

CarbonX targets forestry and land-use carbon (nature-based supply) as a priority given its current share of voluntary issuance, opportunity to scale with digital MRV, and existing institutional financing flows.

(See Appendix for detailed assumptions and sensitivity tables.)

3. Problem Statement

Current voluntary and jurisdictional forest carbon markets are limited by:

1) high-cost, slow MRV cycles;

2) uncertain provenance and integrity perceptions;

3) privacy and sovereignty concerns from landholders and governments;

4) fragmented clearing and settlement infrastructure;

5) insufficient financial products for long-term buyers and institutional treasuries.

CarbonX addresses these gaps by delivering: cheaper, repeatable MRV; provable privacy for sensitive raw data; decentralized certification that reduces single-point trust; standard-compliant issuance that is reconcilable with existing registries; and token-native financial primitives for liquidity and treasury management.

4. Platform Vision & Positioning

CarbonX is positioned as a Verified Carbon Assets Market & Protocol for high-quality forestry RWA. Core product pillars:

- **Certify & Tokenize.** Convert verified forest carbon reductions/removals into CAT tokens with a one-to-one mapping to on-chain-backed RWA metadata and audit proofs.
- **Privacy-first MRV.** Use MPC + ZKP + verifiable computation to allow stakeholders to contribute sensitive measurement data without revealing raw inputs.
- **Decentralized Certification.** Randomized, stake-secured node selection for attestations; 3-node consensus per issuance to distribute trust and economic rewards.
- **Institutional Treasury.** DAT financial vault combining CAT with BTC and PAXG to create a multi-asset sustainable treasury.
- **Governance & Incentives.** FOX token governs platform parameters; CA agents (5000 lifetime supply) are scarce identity/participation slots and revenue share carriers.

5. Technical Architecture

High-level architecture is layered: Data Layer, Processing Layer, Privacy Layer, Consensus/Certification Layer, Settlement Layer, and External Compliance/Oracle Layer.

5.1 Data Layer: Remote Sensing & Ground Truthing

Data sources:

- Multi-spectral satellite imagery (Sentinel-2, Landsat, Planet, commercial VHR where contracted).

- LiDAR-derived canopy height and structure (GEDI, airborne LiDAR campaigns where available).

- On-the-ground inventory (plot measurements) from project partners and local verification teams.

- Auxiliary data: soil maps, land use maps, tenure records, community-reported inputs.

Design principles:

- Use multi-source fusion to estimate above-ground biomass (AGB) and change detection.

- Maintain provenance: every data ingestion stores a signed metadata packet (source, timestamp, sensor, preprocessing chain).

- Accept both public and commercial sources; when commercial data are used, the platform records the verifiable statement (hash / commitment) while keeping raw files private under the privacy layer.

5.2 Processing Layer: AI / Algorithms

Core algorithmic components:

1. **Preprocessing & Tile Stitching.** Radiometric and geometric corrections, atmospheric correction, cloud masking.

2. **Canopy Height & Biomass Estimator.** Ensemble ML combining optical indices, SAR backscatter where available, and LiDAR-derived height models to estimate AGB per hectare with uncertainty bands.

3. **Change Detection & Baseline Modeling.** Time-series models detect deforestation/degradation events and model counterfactual baseline emissions using historical trends and jurisdictional policies.

4. **Uncertainty Propagation Module.** Monte Carlo propagation of sensor and model uncertainties into the final carbon estimate and issuance quantity.

5. **Fraud / Anomaly Detection.** Spatial-temporal anomaly scoring that flags unusual patterns (e.g., sudden canopy regrowth improbable at that rate) for human review.

Outputs: gridded AGB maps, delta-AGB for issuance windows, per-plot confidence intervals, and a signed digest for downstream privacy computation and verification.

5.3 Privacy Layer: MPC, ZKP, Verifiable Computation

Goals: allow contributors (local governments, project developers, surveyors) to keep raw data private while producing public proofs that the platform’s issuance math ran correctly on that data.

Pattern:

1. **Secret-sharing / MPC aggregation.** Local data owners split sensitive measurements into secret shares and submit to a set of computation nodes (chosen from a vetted MPC federation). The nodes jointly compute aggregated statistics (e.g., average biomass, change totals) without reconstructing raw inputs.

2. **Verifiable Computation / Succinct ZK Proof.** After the MPC aggregation, nodes produce a zero-knowledge proof (e.g., zk-SNARK or STARK) attesting that a canonical issuance function f(data) (defined in the protocol) was executed correctly over the committed inputs, and the resulting issuance quantity is Q. The proof is compact and publishable on-chain.

3. **Proof Publishing.** The proof + commitment digest is posted to the blockchain; smart contract verifies the proof (or verifies a proof attestation) and mints CAT accordingly.

4. **Auditability & Privacy.** Auditors with permission can request selective disclosures (via cryptographic openings) for specific plots or time windows. The system supports role-based reveal where permitted by local laws and policy.

Operational notes:

- The platform operates a rotating MPC federation; nodes are run by trusted operators (research partners, auditors, regional hubs) that are subject to technical and legal onboarding.

- For performance, heavy ML tasks run off-chain in conventional compute (GPU), producing deterministic digests that are then input into MPC/verification steps.

5.4 Consensus & Decentralized Certification

Certification model (core innovation): a randomized staking-weighted selection of 3 certifier nodes per issuance window.

Process:

- **Staking.** Certifier nodes (which may include CA holders, institutional partners, accredited verifiers) stake FOX or a separate stake token locked in a smart contract.

- **Random Selection.** Using a VRF-based randomness beacon, the protocol selects 3 nodes at issuance time to attest to the digest prepared by the MPC/proof stage.

- **Attestation & Reward.** The 3 selected nodes validate proofs, sign the issuance record, and receive a split of the issuance fees and a portion of minted FOX mining allocation for their role.

- **Slashing.** If a selected node is later found to have acted maliciously (e.g., signing an invalid issuance), it is subject to slashing (stake reduction) and temporary removal from the certifier pool.

Rationale: 3-node selection keeps per-issuance trust distributed while keeping operational costs manageable.

5.5 Settlement & Smart Contracts

Smart contracts on a high-throughput L2 or EVM-compatible chain will manage:

- CAT minting/burning (RWA-backed issuance and retirement). - FOX governance staking and miner emission schedules.

- CA identity issuance and transfer registry.

- DAT financial vault controls, multi-sig custody, and rebalancing rules.

Key patterns:

- **On-chain proof verification.** Smart contracts verify that an on-chain attestation/proof object exists before minting CAT.

- **RWA metadata CID.** Token metadata points to an immutable CID (IPFS / distributed store) that includes the issuance digest, summary MRV report, governance data, and references to third-party audit reports.

- **Retirement mechanism.** Buyers can retire CAT, creating on-chain retirement receipts and off-chain registry updates for jurisdictional reconciliation.

5.6 Oracles, Audits, and Interoperability

- **Oracles** provide external data: exchange rates, treasury prices, registry updates, and regulatory events.
- **Third-party audits** integrate with the proof pipeline: accredited auditors can anchor their report to the issuance CID and publish independent attestations.
- **Interoperability**: cross-chain bridges (optimistic or trust-minimized) for CAT trading on other chains; settlement and custody patterns follow best practices to avoid double-counting.

6. Token Design & Economic Model

6.1 Dual-token primitives (CAT / FOX)

CAT — Carbon Asset Token

- **Purpose:** 1:1 tokenized representation of a verified forestry carbon RWA unit (per issuance policy; e.g., 1 CAT = 1 tCO_2e equivalent under platform-defined vintage rules).

- **Properties:** transferable, burnable, can be used as collateral, listed on exchanges.

- **Issuance:** minted only after successful MRV proof and smart-contract verification. Each CAT ties to an immutable issuance record.

- **Retirement:** on-chain retirement burns the CAT and produces an irrevocable retirement receipt.

FOX — Governance & Incentive Token

- **Purpose:** platform governance, staking for certifier rights, and as the emission reward to bootstrap the validator/certifier ecosystem.

- **Supply & Allocation:** total supply 10,000,000,000 FOX. Allocation: 20% Treasury Reserve, 50% mining (issuance/monitoring rewards), 10% early investors, 10% team, 5% community, 5% strategic partners.

- **Utility:** staking to become a certifier, bonding to issue CAT (economic security), governance voting, fee discounts, and protocol parameter proposals.

6.2 Carbon Agent (CA) NFTs

Carbon X operates a capped network of 10,000 Carbon Agent Nodes responsible for:

1. Forest data submission
2. Satellite and remote-sensing validation
3. MRV coordination
4. Governance participation

Nodes are infrastructure providers, not speculative miners, and must meet strict operational and compliance requirements.

6.3 FOX Token Overview (Tokenomics)

Basic Parameters

- Token Name: FOX
- Token Type: Utility & Governance Token
- Total Supply: 10,000,000,000 FOX (fixed, no inflation)
- Decimals: 18

FOX does not represent equity, revenue rights, or claims on assets. It exists solely to operate and govern the Carbon X protocol.

Core Economic Principle: Burn-on-Mint

Carbon X enforces a strict **Burn-on-Mint** mechanism:

Every on-chain minting of a forest carbon asset (CAT) requires the irreversible burning of FOX.

Burn parameters are governed on-chain and may dynamically adjust based on:

- Carbon market pricing
- Network utilization
- System security requirements

This design ensures:

- Structural long-term deflation of FOX
- Direct linkage between real carbon activity and token demand
- No token inflation driven by platform growth

FOX Allocation Structure

Category	Allocation	Key Principles
Agent Mining Incentives	50%	100-year declining emission
Treasury Reserve	20%	Stability & ecosystem support
Team & Advisors	10%	Long-term vesting
Strategic Partners	5%	Milestone-based release
Community & Ecosystem	5%	DAO & public-good incentives
Early Investors	10%	Long-term vesting
Total	**100%**	Fixed supply

No public sale or IDO is conducted.

Agent Mining Incentives (50%)

Emission Model

- Emission Duration: 100 years
- Emission Curve: Strongly declining
- Daily emission, decreasing annually

This ultra-long schedule reflects the multi-decade lifecycle of forest carbon assets.

Early Agent Incentives

The first 500 activated nodes receive higher reward coefficients based on activation order:

- Earlier activation = higher lifetime allocation
- Coefficients decay linearly
- After node #500, rewards normalize

This bootstraps data reliability without creating permanent centralization.

TGE Circulation Control

- Pre-TGE rewards accrue as non-transferable points
- At TGE, only a capped portion is convertible
- Target TGE circulating supply: **< 5%**

Treasury Reserve (20%)

Purpose

The Treasury functions as a **Digital Asset Treasury (DAT)** and does not engage in speculative market activity.

Primary uses:

- Protocol security and audits
- Legal and regulatory compliance
- Infrastructure upgrades
- Long-term ecosystem investment

Governance

- Multi-signature control (5/9)
- DAO and board oversight
- All actions recorded on-chain

Team, Advisors & Early Investors (20%)

Group	Cliff	Vesting
Team & Advisors	12–24 months	36–48 months
Early Investors	12–24 months	36–48 months

No TGE unlocks are permitted.

Strategic Partners (5%)

Released only upon verified milestones, including:

- National or regional forest onboarding
- International carbon agreements
- MRV or satellite verification breakthroughs

Failure to meet milestones results in no release.

Community & Ecosystem Incentives (5%)

This allocation is behavior-driven and non-speculative, supporting:

- DAO governance participation
- Carbon data contribution
- Public-good verification
- Developer ecosystem growth

Distribution is continuous, capped per address, and Sybil-resistant.

---

7. Security & Risk Mitigation

Major security domains: - **Cryptographic correctness:** audited MPC/ZK libraries, deterministic ML pipelines, reproducible digests. - **Smart contract security:** multi-stage audits, formal verification for critical modules, and staged mainnet rollouts. - **Operational security:** HSM-based key management for MPC nodes, cold/warm wallet separation, SOC2-level processes for operator nodes. - **Economic security:** staking, slashing, and timelock windows to prevent immediate withdrawal after misbehavior.

Red-team exercises and bug-bounty programs will be standard practice prior to and after launch.

---

8. Compliance & Governance

Jurisdictional strategy: the project is based in Singapore for operational headquarters to benefit from Singapore’s clear regulatory framework for digital payment tokens and robust AML/CFT supervision. The platform will pursue relevant licenses or engage licensed partners according to local laws.

Key compliance pillars: - **AML / KYC:** end-user flows will implement risk-based KYC consistent with FATF guidance. Custodial services will follow MAS rules for asset segregation and safekeeping. - **Registry reconciliation:** integrate with existing registry systems (e.g., jurisdictional REDD+ registries, national MRV platforms) to avoid double-counting. - **Standards alignment:** issuance and MRV processes will adhere to IPCC principles and recognized registries’ methodologies (e.g., TREES/ART where jurisdictional REDD+ applies) and adopt third-party audits. - **Governance:** FOX token holders elect or remove certifiers; the

Foundation (20% FOX) holds stewardship rights and emergency governance powers with multi-sig and time-delay checks.

9. Team & Organizational Structure

The team is headquartered in Singapore and combines domain experts in forest carbon, privacy computation, cryptography, compliance, and digital finance. Team roles and advisers are defined to ensure technical delivery, regulatory alignment, and go-to-market success.

CarbonX is driven by a world-class coalition of experts spanning carbon forestry, blockchain engineering, privacy-preserving computation, and institutional finance. Our key personnel include:

- **Dr. Chen Wei (Tsinghua University):** A former expert in China's Carbon Trading Pilot programs. Dr. Chen is a master of CCER (Certified Voluntary Emission Reduction) methodologies and ecological compensation models, specializing in the conversion of natural carbon sinks into high-quality digital assets.
- **Liu Yang (Peking University):** A senior scientist in privacy-preserving computation. His research focuses on the application of TEE (Trusted Execution Environments) for on-chain carbon footprint tracing, effectively resolving privacy concerns regarding corporate emission data.
- **Zhao Zihan (Fudan University):** Formerly the Head of DeFi Research at a top-tier investment fund. She is an expert in dynamic interest rates and liquidity incentive models, specializing in designing secondary market economic drivers for carbon credit tokens.
- **Wang Shuo (Shanghai Jiao Tong University):** A cross-chain protocol architect. He focuses on the technical implementation of Zero-Knowledge Proofs (ZKP) for the clearing and settlement of carbon assets across heterogeneous chains, enhancing the security of asset circulation.
- **Benjamin Tan (National University of Singapore):** A former compliance officer at the Monetary Authority of Singapore (MAS). He is highly proficient in the Payment Services Act (PSA) and specializes in building compliance frameworks and Anti-Money Laundering (AML) mechanisms for carbon trading platforms.

- **Sarah Jenkins (Stanford University):** A partner at a leading U.S. Climate Tech fund. With extensive post-investment experience in Direct Air Capture (DAC), she specializes in global pricing and hedging strategies for carbon assets.
- **Marcus Müller (ETH Zurich):** A renowned cryptographer specializing in Multi-party Computation (MPC). He provides CarbonX with institutional-grade key management and distributed data sovereignty solutions.
- **Alistair Vance (University of Oxford):** An ESG quantitative analysis expert who participated in the design of major European carbon emission indices. She specializes in constructing green financial derivatives and their respective economic valuation models.

---

10. Roadmap & Milestones

2026 Q1 — CA open to early investors (500 CA), alphas and first CAT/FOX issuance testing.

2026 Q2 — Alpha launch, first single-project CAT issuance; foundation setup and DAT vault design.

2026 Q3 — The FOX token is scheduled to be listed.

2026 Q4 — CORP31 public launch, onboarding of top 1000 CA for enterprise partners.

2027 — Exchange listings for FOX, CAT integration into institutional treasuries, CA secondary markets.

(See detailed timeline with technical gates in Appendix C.)

---

11. Market & Financial Projections

We project multi-scenario adoption: conservative, base-case, and aggressive. Projections include number of projects onboarded, annual CAT issuance volumes, platform revenue (fees), and DAT vault AUM.

(See Appendix for exhaustive financial models and sensitivity analysis.)

---

12. Risks & Mitigations

Principal risks include regulatory classification of tokens, MRV model risk, data access limitations, and platform governance attacks. Mitigations include conservative compliance-first rollout, strong third-party auditing, diversified data suppliers, and economic security via staking and slashing.

---

13. Appendix

A. Core Algorithms (overview)

- **AGB Estimator:** ensemble regression stack (optical indices + SAR + LiDAR-derived features) trained on curated field plots and transfer-learned across ecoregions.
- **Baseline Estimator:** jurisdictional and project-specific counterfactual model leveraging panel-data regressions, policy indicators, and causal inference adjustments.
- **Uncertainty Propagation:** bootstrapped Monte Carlo using sensor noise models and model error distributions to compute issuance confidence intervals.

B. Smart Contract Schematics

- **Minting contract:** `mintCAT(proofCID, issuanceMetadata, certifierSigs)` -> verify proofs & signatures -> mint CAT -> update registry.
- **Staking contract:** lock FOX -> become certifier candidate -> eligible for selection by VRF.

C. Glossary

CAT: Carbon Asset Token The primary utility and asset token of the CarbonX ecosystem. Each CAT represents one metric ton of verified carbon dioxide equivalent (CO_2e) sequestered by forestry projects. It is a fully collateralized RWA (Real-World Asset) used for carbon offsetting and green finance.

FOX: Forest Ownership eXecution Token The native governance and utility token of the protocol. FOX is used for staking to mint CAT, participating in decentralized governance, and incentivizing the network's long-term sustainability. It captures the protocol's value through buy-back and burn mechanisms.

CA: Carbon Agent A scarce, non-fungible digital identity (NFT) that serves as a high-performance "validation node." CAs are responsible for the decentralized verification of carbon sinks. Owners of CA NFTs earn a share of protocol fees and mining rewards through their participation in the dMRV process.

MRV: Measurement, Reporting, and Verification The industry-standard framework for ensuring carbon credits are real and permanent. CarbonX evolves this into **dMRV (Decentralized MRV)**, utilizing satellite imagery, AI, and IoT sensors to automate and decentralize the validation process.

MPC: Multi-Party Computation A subfield of cryptography that allows multiple parties (CA nodes) to jointly compute a function over their inputs while keeping those inputs private. In CarbonX, MPC is used to aggregate sensitive forest data without exposing precise geographic or proprietary information.

ZKP: Zero-Knowledge Proof A cryptographic method by which one party can prove to another that a statement is true without revealing any information beyond the validity of the statement itself. CarbonX uses ZKPs to verify the authenticity of carbon sequestration data on-chain while maintaining data privacy.

RWA: Real-World Asset Tangible assets that exist in the physical world (such as timber, land, or carbon sequestered in trees) which are brought on-chain via tokenization. CarbonX specializes in the tokenization of forestry-based carbon sinks into liquid, programmable digital assets.

CarbonX — Decentralized Forestry Carbon System (v1.2)