Climate Action Data Trust®

SERVICE LAYER
Data User Connectivity Deck

Climate Warehouse
End-to-End Digital Ecosystem for Carbon Markets

The Service Layer represents a robust connection to the CAD Trust metadata layer, primarily leveraging an API. This connection type is particularly advantageous for large-scale users who require regular and intensive access to data. It facilitates seamless integration, ensuring efficient and reliable data retrieval and management. Ideal for organisations seeking to maximise their interactions with CAD Trust metadata, the Service Layer offers a scalable and secure solution for handling extensive data requirements with ease.

Common taxonomy of data facilitates communication between entities

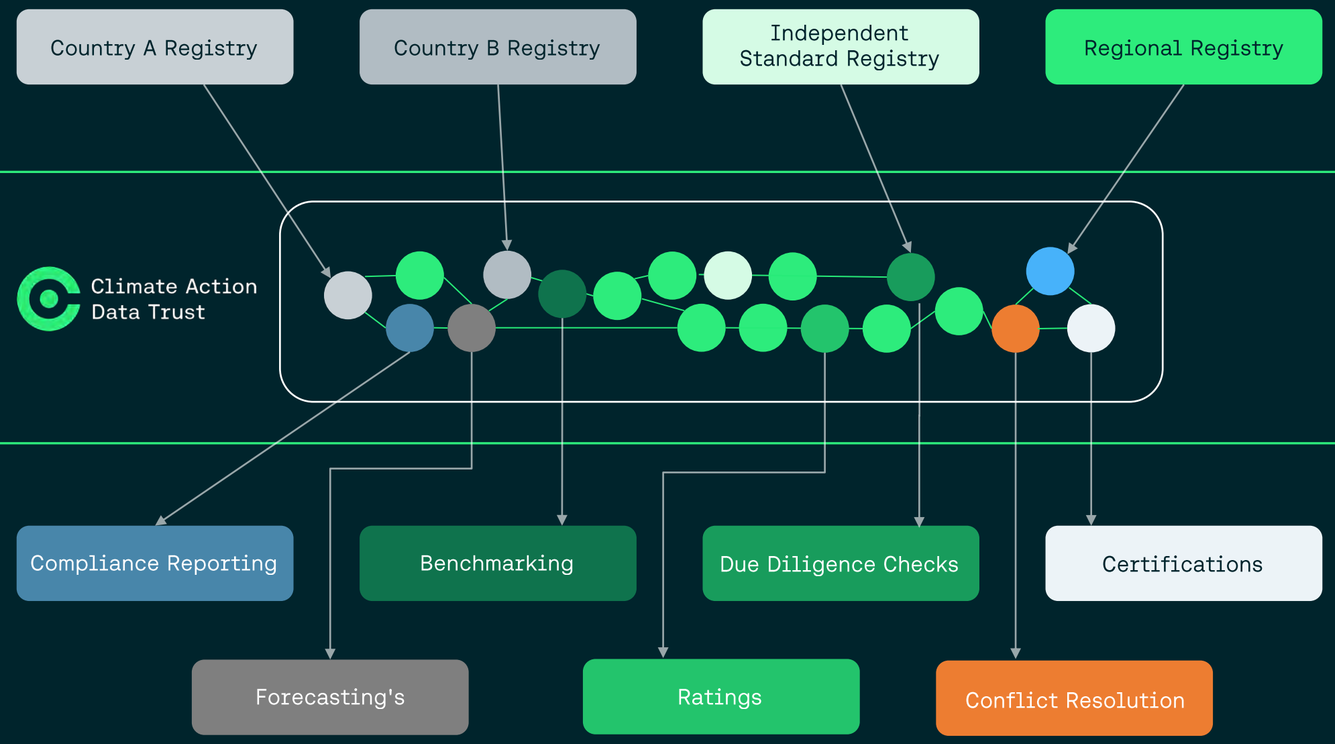
REGESTRY LAYER

Registry service providers and countries share data to CAD Trust

METADATA LAYER

Public and private sector market players can host a node and build out the service layer

SERVICE LAYER

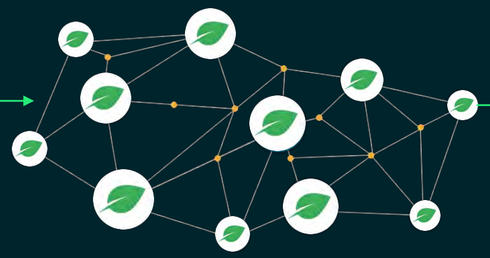


Data Flow

Registry's Existing Database

(Independent standards, sovereign registries, UNFCCC registries)

CAD Trust Node
(Hosted by Registry)



Chia Blockchain Network

Climate Warehouse
End-to-End Digital Ecosystem for Carbon Markets

- Compliance reporting
- Forecasting
- Benchmarking
- Ratings
- DD Checks
- Conflict Resolution
- Certifications

Registry Layer

Metadata Layer

Service Layer

Data Model

PROJECT LOCATION

- CAD Trust Project ID* (FK)
- Project Location ID (PK)
- Country*
- In Country Region
- Geographic Identifier*

PROJECT RATING

- CAD Trust Project ID* (FK)
- Project Rating ID (PK)
- Rating Type*
- Rating Range Lowest*
- Rating Range Highest*
- Rating*
- Rating Link*

CO-BENEFITS

- CAD Trust Project ID* (FK)
- Co-Benefit ID (PK)
- Co-Benefit

ESTIMATIONS

- CAD Trust Project ID* (FK)
- Estimations ID (PK)
- Crediting Period Start*
- Crediting Period End*
- Unit Count*

PROJECTS

- CAD Trust Project ID* (PK)
- Current Registry*
- Project ID*
- Registry of Origin*
- Program
- Project Name*
- Project Description
- Project Link*
- Project Developer*
- Sector*
- Project Type*
- Project Tags
- Covered by NDC*
- NDC Information
- Project Status*
- Project Status Date*
- Unit Metric*
- Methodology*
- Validation Body
- Validation Date

Each ID is global unique, meaning no organisations will generate the same ID for any table.

RELATED PROJECTS

- CAD Trust Project ID* (FK)
- Related Project ID (PK)
- Relationship Type
- Registry

ISSUANCES

- CAD Trust Project ID* (FK)
- Issuance ID (PK)
- Issuance Start Date*
- Issuance End Date*
- Verification Approach*
- Verification Report Date*
- Verification Body*

LABELS

- CAD Trust Project ID* (FK)
- Label ID (PK)
- Label Type*
- Label*
- Crediting Period Start Date*
- Crediting Period End Date*
- Validity Start Date*
- Validity End Date*
- Unit Quantity*
- Label Link*

UNITS

- Issuance ID* (FK)
- CAD Trust Unit ID* (PK)
- Unit Issuance Location* (FK to project loc ID)
- Label ID* (FK)
- Unit Owner
- Country Jurisdiction of Owner*
- In-Country Jurisdiction of Owner*
- Unit Block Start*
- Unit Block End*
- Unit Count*
- Vintage Year*
- Unit Type*
- Marketplace
- Marketplace Link
- Marketplace Identifier
- Unit Tags
- Unit Status*
- Unit Status Reason
- Unit Registry Link*
- Corresponding Adjustment Declaration*
- Corresponding Adjustment Status*

Fields with an ***** are required form fields

PK donates primary key for a specific table

FK denotes foreign key which links tables together

GOVERNANCE (PICKLIST VALUES)

- Registry values
- Project Sector values
- Project Status values
- Project Type values
- Methodology values
- Unit Metric values
- Validation Body values
- Country values
- Rating Type values
- Unit Type Values
- Unit Status values
- Corresponding Adjustment Declaration values
- Corresponding Adjustment Status values
- Related Project
- Relationship type values
- Label Type values
- Verification Body values
- Tag values
- Co-benefit values

Data Model Explanation

CAD Trust will provide the data model Excel sheet—a business-oriented document that describes the expected fields in the data layer.

Below are some of the key data attributes:

Organisation data

The organisation ID is the unique identifier generated by CAD Trust App. Registries will update their organisation using the CADT APIs.

Project

Organisation will post project data they host, such as project names, types, owner, status, etc.
Each Project gets assigned a unique project ID

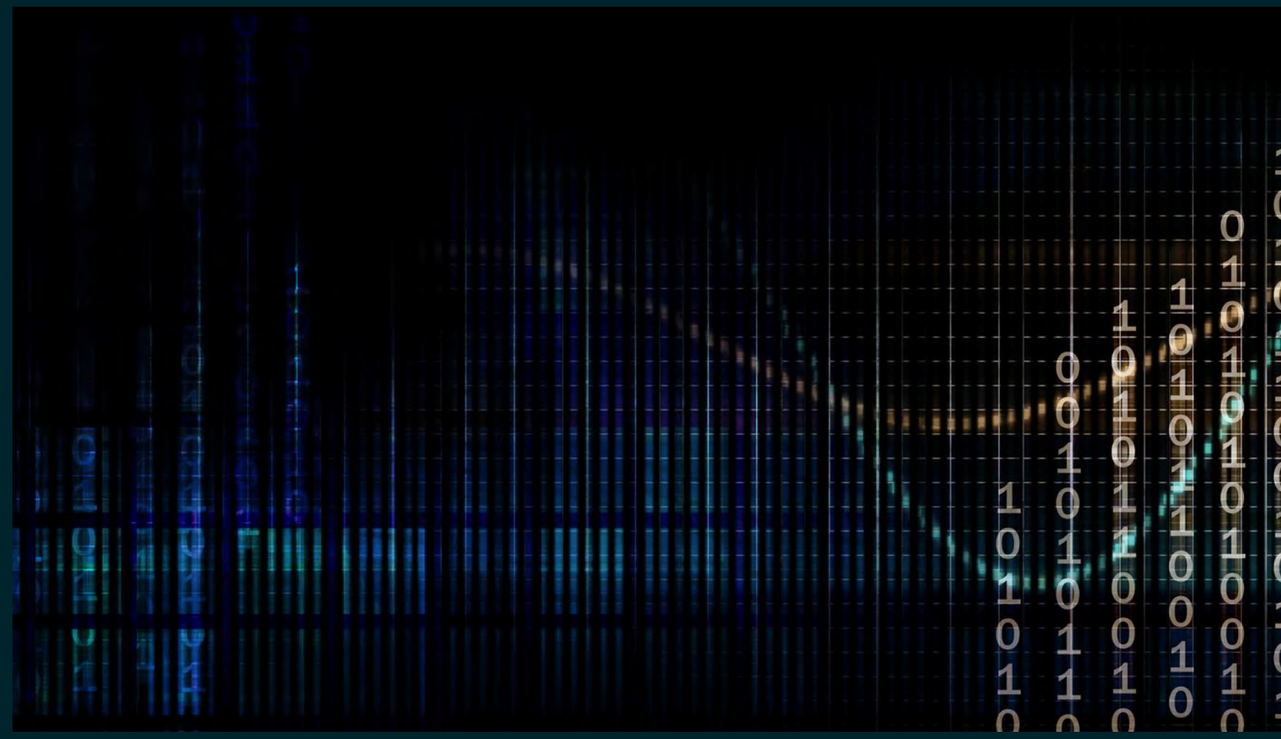
Units (Carbon Credit Data)

It is connected to specific projects through the project ID. Organisation will input information denoting the issuances, amount, status, etc.

Governance (Picklist values)

CAD Trust governance node will maintain the values in certain data fields (picklists); data providers are expected to match their data accordingly to the various picklist values maintained within CAD Trust

Installation



Deployment Methods

Server Based

On-Prem Hosted

Runs in a secure environment inside an organisation's network.

This is the lowest-cost secure deployment model.

Private / Hybrid Cloud Hosted

Minimises cloud hosting costs while still providing a robust deployment of CAD Trust.

It is anticipated to be the most common model for service providers that consume data from the CAD Trust.

Public Cloud

This is anticipated to be the most common model for Participants and the Governor node.

All components other than the CAD Trust API and Chia are provided by the cloud service provider.

User Type: Registry Layer + Service Layer

Local Install

The most common model for observers will be to simply install the CAD Trust App on their local computers.

Observers do not require cryptographic keys and cannot change data in the CAD Trust, so the reduced security of this model is acceptable.

User Type: Service Layer + Public

System Requirements

Server Based

On-Prem Hosted

Private / Hybrid Cloud Hosted

Public Cloud

Deploying the CAD Trust requires installing both the Chia blockchain software and the CAD Trust API server software.

For Hosted deployments, both pieces of software are typically installed on the same machine, but can be installed on different machines and pointed to one another. The machine should have at the least the following minimum specs:

- Dual core 1.5Ghz CPU (64 bit) x86
- 8 GB ram
- 250 GB SSD disk space
- Python version 3.8+

Ubuntu is the preferred OS to use as the Chia and CAD Trust software is packaged and tested primarily with Ubuntu. Other Linux distributions should run Chia and CAD Trust just fine, but may not be extensively tested or have packages routinely built. Windows or Mac systems can be used to host a remote CAD Trust instance.

Local Install

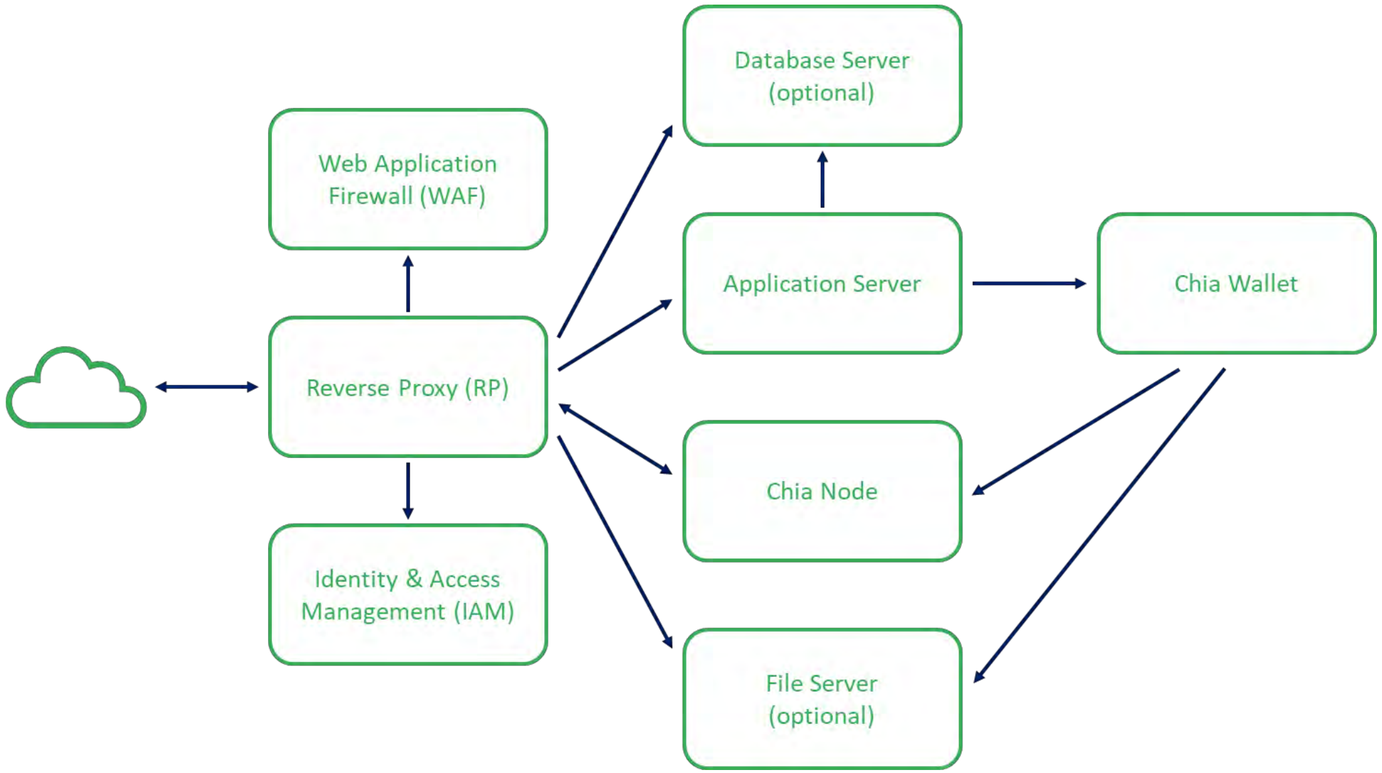
Deploying the CAD Trust requires installing both the Chia blockchain software and the CAD Tust API server software.

For local deployments, both pieces of software are always installed on the same machine. The machine should have at the least the following minimum specs:

- Quad core 1.5Ghz CPU (64 bit)
- 4 GB ram
- 500 GB disk space
- Python version 3.8+

Architectural Components

The primary components of a CAD Trust deployment will include



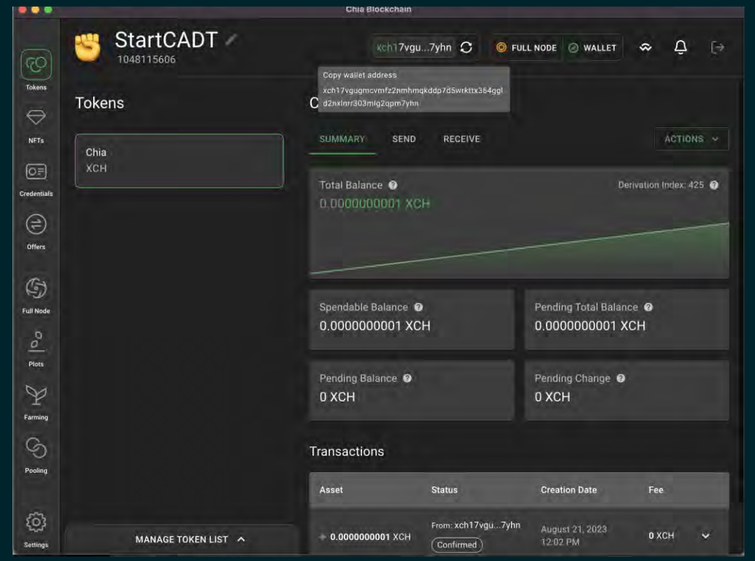
Component	Description
Reverse Proxy	The reverse proxy is responsible for providing a secure SSL access endpoint, and routing requests through the IAM module and WAF before providing authenticated access to the CAD Trust API, the File Server, the Database Server or the Chia Node. The reverse proxy does not provide inbound access to the Chia Wallet.
Web Application Firewall	The WAF is responsible for ensuring the requests made to the CAD Trust API are well-formed and for blocking many common kinds of attacks.
Identity & Access Management	The IAM module is responsible for authenticating the user and verifying the authenticated user has been granted access to the application. Not required if no interactive access is to be provided.
Application Server	This is the CAD Trust API, which provides all of the business logic for the CAD Trust.
Database Server	The database server is optional. If available, the CAD Trust API will maintain a complete copy of all of the CAD Trust in the database for easy access by standard reporting and analytics tools.
Chia Wallet	The Chia Wallet stores the cryptographic keys and the assets controlled by those keys, such as Chia DataLayer data tables and chia cryptocurrency (XCH) for use in paying transaction fees.
Chia Node	The Chia Node is a full validator node on the Chia blockchain and always keeps an up-to-date and validated copy of the blockchain. The Chia node is optionally capable of farming chia cryptocurrency (XCH) to pay for transaction fees.
File Server	Chia DataLayer sends the data from peer to peer through a http protocol. The Chia node has a built-in http file server for basic use, making a stand-alone file server optional. Use of a more robust file server is recommended for most participants. In some cases, the reverse proxy may have a robust http file server built-in.

Steps to install CAD Trust

1. Download Software

Setting Up Chia Node / Wallet

Official GUI Installation Download Page
- Reference : Installation Documentation



Setting Up CAD Trust API Server Software

Main CADT Public GitHub repository

Server Based

Server / Remote Installation Guide

Local Install

Local Installation Guide

Setting Up CAD Trust UI App (Optional)

The CAD Trust UI is useful for visualising the data that is entered into the CAD Trust, but presumably the data will be visible on the public observer node.

The CAD Trust UI is a javascript application that connects to the CAD Trust API. It is offered as a desktop application packaged with Electron, or as a web application. If running as a web application, most organizations will host the UI on the same server as the CAD Trust API or in a public S3 bucket. Alternatively, each user can run the desktop application on their workstation and connect to the single CAD Trust API. In either scenario, the CAD Trust API must be connectable from the user's workstation, which usually means making it publicly available on port 31310.

CADT UI Installation

Steps to install CAD Trust

2. Additional Setup / Config

Setting Up Mirror Database (Optional)

One additional server can be added to this setup in order to mirror the CAD Trust DB structure into a multi-user access database such as mySQL.

This is useful for analytics on the data that is reported to the CAD Trust ecosystem - this database will have both the data the registry owns, along with the data other registries have provided.

We recommend the machine for the MySQL instance to have at least:

- Single core CPU
- 2 GB ram
- 50gb diskspace

Configuration Details

Postman API Collection

CADT API Collection

GET Examples

List all subscribed organizations

```
// Request
curl --location --request GET 'localhost:31310/v1/organizations' --header 'Content-Type: application/json'

// Response
{
    "77641db780adc6c74f1ff357804e26a799e4a09157f426aac588963a39bdb2d9":{
        "orgUid":"77641db780adc6c74f1ff357804e26a799e4a09157f426aac588963a39bdb2d9",
        "name":"Org Test",
        "icon":"https://climate-warehouse.s3.us-west-2.amazonaws.com/public/orgs/me.svg",
        "isHome":true,
        "subscribed":true
    }
}
```

API Connectivity

Observers / Subscribers:

- Anyone can download and run the open-source CAD Trust software
- The CAD Trust software can find and download the published data based on the registry ID

User Type: Registry Layer + Service Layer + Public

- The CAD Trust software creates encoded data files representing the data entered by the registry
- The Registry makes those files available on the internet
    - Can use cloud services like AWS, Azure, GCP, etc
    - Can use CAD Trust built-in server
    - Can use 3rd party hosting service
- The Registry announces the location of the files for its ID to all other users of CAD Trust

Observers / Subscribers: Subscribing to Data in CAD Trust

- Subscriber looks up the registry ID for the registry they want to subscribe to

  CAD Trust governance body publishes a list of known registries

- Subscriber's CAD Trust software:

  Finds a location to access the data files, which may or may not be directly from the Publisher.

  May also get the files from another Subscriber.

  Downloads the files.

  Decodes them to make the data available to the subscriber/user

- Subscribers can subscribe to many registries at once

- By default, the CAD Trust software automatically subscribes to all the registries on the list of known registries published by the CAD Trust governance body
- Users of the CAD Trust software can decide not to subscribe to certain registries, even if they are on the list provided by the CAD Trust governance body
- Users of the CAD Trust software can subscribe to registries not on the list provided by the CAD Trust governance body by entering that registry's ID manually

Observers / Subscribers: Subscribing to Public Data in CAD Trust

Observer Node: Public Data Access

- The Observer Node is an instance of the CAD Trust open-source software that is operated by the CAD Trust governance body
- It runs the exact same software that any other instance of CAD Trust runs
- It automatically subscribes to all registries recognised by the governance body
- It allows the public to access raw CAD Trust data via the web
- It offers both API access and a simple user interface

UI: https://data.climateactiondata.org/

API: https://observer.climateactiondata.org/api/v1/

Reference of links / documents

Setting Up Chia Node / Wallet

Official GUI Installation Download Page
- Reference : Installation Documentation

Setting Up CAD Trust UI App (Optional)

CAD Trust UI Installation

Setting Up CAD Tust API Server Software

Main CAD Trust Public GitHub repository

Server Based

Server / Remote Installation Guide

Local Install

Local Installation Guide

Setting Up Mirror Database (Optional)

Configuration Details

Postman API Collection

CAD Trust API Collection

Appendix

Threat Analysis

The CAD Trust is unique in that it is a fully-decentralised application. There is no central server that can be attacked by a malicious actor to cause system-wide failures. Instead, it is a true peer-to-peer network with each participant running a node that acts as a peer to all of the other participants' nodes.

Identified potential attacks on the CAD Trust fall into a few broad categories:

- Changing data - a threat actor attempts to either change data without permission, or causes the data to appear to be changed when other users view it.
- Denial of service - a threat actor attempts to prevent legitimate users from accessing the system.
- Malicious code injection - a threat actor attempts to cause the system to distribute malicious payloads.
- Stealing cryptocurrency - there is a small amount of chia cryptocurrency (XCH) required to publish data using the Chia blockchain that a threat actor could attempt to steal.
- Blockchain attacks - a threat actor attempts to change data previously confirmed on the blockchain, or stops the blockchain entirely.

The CAD Trust is designed to allow nodes to be deployed in a wide range of environments:

- Public cloud hosted
- Hybrid / private cloud hosted
- On-prem hosted
- Local install

The local install deployment model is only intended for observer nodes, which do not have cryptographic keys to change data. The effect of an attack on observer nodes installed locally would be limited to the experience of the local user.

All of the hosted deployment models mitigate most attacks using industry-standard technologies including:

- Isolated and secured subnet deployment
- Reverse proxy with SSL/TLS
- Web application firewall (WAF)
- Identity and access management system (IAM)
- Local firewall on the application server

Threat Analysis

Exogenous factors such as compromised client computers or networks, leaked credentials, phishing and zero-day vulnerabilities are outside the scope of the CAD Trust and must be mitigated through good security hygiene practices among users and node administrators.

Blockchain attack vectors and their mitigating factors are thoroughly described in documentation published by Chia Network, Inc.

As a truly decentralized system, DDoS attacks would have very limited effectiveness and can only disable access to a single node. Users of all other nodes would be unaffected.

A number of additional potential attack vectors are considered and mitigations addressed, including malicious source code commits, malicious upstream library releases, poisoned installers and leaked or lost cryptographic keys, among others.

In summary, the application can be fully secured through the use of correct deployment and maintenance practices by node administrators, good security practices by users and good source code control and upstream monitoring by code maintainers.

Technical FAQ

Q: Why was it important to use a public blockchain instead of a private blockchain?

A: Public blockchain is within the spirit of the Paris Agreement's decentralised bottom-up approach. It does not rely on the trust of any central authority, including the company managing the chain. It is a truly decentralised tool that democratises access and cannot be manipulated by any authority or owner.

Q: More validators (nodes) on a blockchain network make it more decentralised and secure. Are there adequate incentives to ensure Chia's 200,000+ validators continue? Have there been any reductions in the hype leading to a decrease in validators?

A: Chia's Proof of Space & Time consensus mechanism rewards the storage ecosystem effectively and incentivises validators. If validators start to leave the Chia ecosystem, that creates a higher rate of return for new validators allocating storage to Chia and thus incentivises more validators to add space to the network.

Q: Carbon offset project data is often very high volume. Is this costly? Are all participants expected to store all the data in order to participate with the CADTrust?

A: Chia's blockchain was designed to be simple, extremely resource-efficient and functional. Chia's unique Data Layer is a decentralised database that is calculable on-chain and secured by Chia's entire network. The CADTrust Data Model is limited to critical fields to ensure fast and ultra-low-cost datasync on blockchain. Although uniquely "calculable on-chain" the blockchain only stores proofs (hashes) of the transactional data, so each node is not required to store every other node's data, but rather proofs that the other nodes' data are all provable, calculable, and correct.

Technical FAQ

Q: What are transaction fee projections? How are the projections calculated?

A: Settling transactions on the blockchain can incur a fee when block-space is limited. This fee to secure block-space accrues to validators (nodes), not to Chia. Today blocks are below capacity, so no fees are charged and there is enough excess capacity that the Chia Network does not expect fees of even 1 US cent to be required for a long time to come. Although the Chia Network cannot control when small fees could be required, Chia has been developed to easily add layer 2 functionality that would exponentially increase Chia's data capacity while still executing all smart contracts.

Q: How is Chia addressing the complications other blockchains are having in terms of regulatory problems?

A: Chia is recognised as one of a few blockchains that never did an Initial Coin Offering (ICO) and is not at risk of being classified as an illegal security. Chia Network has never sold XCH, the currency associated with the Chia blockchain, ensuring that the token cannot be considered a security in the company. In order to assure long-term regulatory compliance, the Chia Network intends to become a publicly-traded company on an accelerated timeline with all of the board and shareholder oversight that entails.

W www.climateactiondata.org

E evan@climateactiondata.org

Climate Action Data Trust®