Carbon Trading Network | THALLO

For Human, For Earth

全球领先的碳交易市场

数实融合 | 链通两岸

目录

Carbon Trading Network

摘 要

Carbon Trading Network，是基于区块链+隐私计算的碳交易网络，旨在利用区块链技术来构建一个去中心化的碳交易平台，以解决全球气候变化和温室气体排放的问题。该网络将建立一个透明、安全和可追溯的碳交易系统，通过智能合约和分布式账本技术记录和验证碳排放权的交易，同时采用多方安全计算和零知识证明确保双边交易的隐私安全。

CTN 为助力碳达峰和碳中和的实行，通过激励企事业单位和个人用户减少碳排放，并购买碳排放权来实现该愿景。我们采用拜占庭共识算法（BFT）和 CPoE 技术，使得 CTN 在稳定共识机制中确保交易的透明性和不可篡改性，同时降低交易成本，并提高交易效率。

我们使用 ToG、ToB、ToC 的商业模式与其他利益相关者合作，建立起全球碳交易平台。旨在打造去中心化碳交易网络，增强市场流动性与交易可信度，从而推动碳减排目标的实现，为“ 3060 ”碳达峰、碳中和提供一站式解决方案。

中国和美国是世界上最大的两个经济体，同时也是最大的能源消费国和碳排放国，是应对气候变化进程中影响最大的两国。

2023 年 11 月 15 日，中美元首会晤前夕，两国发表共同声明宣布加强气候合作，因为中美两国认识到，气候危机对世界各国的影响日益显著，面对政府间气候变化专门委员会（IPCC）第六次评估报告等现有最佳科学发现的警示。

中美能够克服重大差异，共同应对气候变化。这向世界其他地区发出了明确的信号 在联合声明中，中国首次誓言在 21 世纪 20 年代这关键十年，“可预期电力行业排放在达峰后实现有意义的绝对减少”，这比中国此前承诺的“碳排放力争于 2030 年前达到峰值”更进了一步。 两国的声明意味着“中国的煤电厂将很快实现减排”。

两国致力于有效实施联合国气候变化框架公约和巴黎协定，体现公平以及共同但有区别的责任和各自能力的原则，考虑不同国情，根据巴黎协定第二条所述将全球平均气温上升控制在低于 2℃之内并努力限制在 1.5℃之内，包括努力保持 1.5℃可实现，达成该协定的目的。

两国强调，公约第 28 次缔约方大会（COP28）对于在这关键十年及其后有意义地应对气候危机至关重要。两国认识到，两国无论是在国内应对措施还是共同合作行动方面对于落实巴黎协定各项目标、推动多边主义均具有重要作用。为了人类今世后代，两国将合作并与公约和巴黎协定其他缔约方一道直面当今世界最为严峻的挑战之一。

一、 背景与开发动机

其行业主要背景，CT 是指企业对温室气体（二氧化碳）排放权的交易，其原理是科斯定理。碳排放权分配可以视为一种资源配置方式，在这样的情况下，以市场机制对交易进行调节是最有效的，实现 Pareto Efficiency。我们建立的 CTN 是作为一种通过买卖二氧化碳排放配额的方式来减少温室气体排放的网络模式。这种模式的背后是应对气候变化和减少温室气体排放的全球共识和努力。

在传统碳交易市场中存在一些问题和挑战。其中之一是多个碳交易平台的存在，这导致了碳交易市场的分散和不透明。同时，由于数据难以追溯和验证，存在着潜在的欺诈和不合规行为风险。此外，传统碳交易市场还面临着高昂的交易成本和低效率问题。

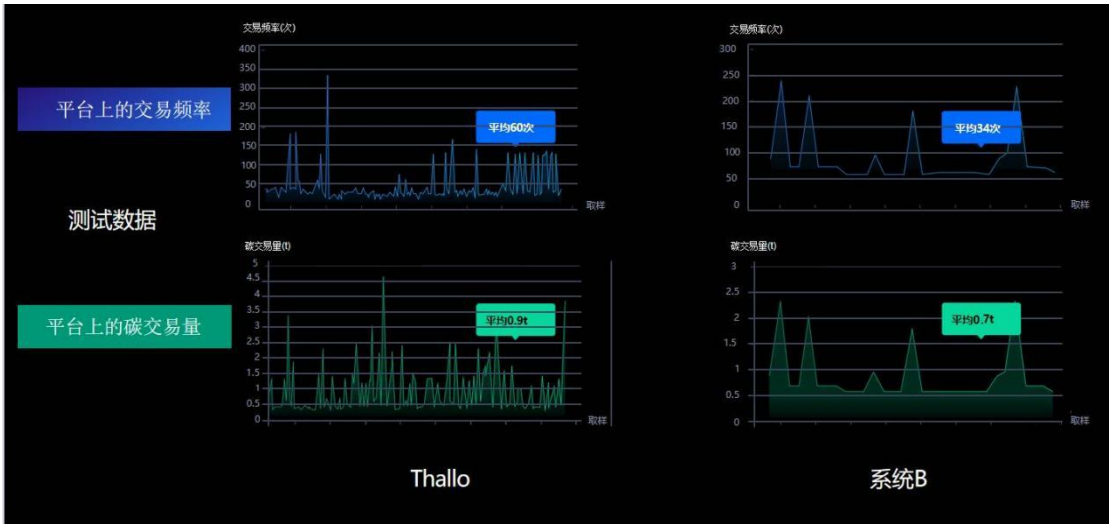
因此，基于区块链技术的 CTN 可以解决这些问题。区块链技术的分布式账本和智能合约可以提供更高的透明度和数据可追溯性，从而增加碳交易市场信任度。通过将所有参与方的交易记录和验证信息存储在区块链上，可以防止潜在欺诈行为和不合规行为。此外，区块链可以提供更高的交易效率和降低交易成本，从而促进碳交易市场发展和扩大。

区块链碳交易网络项目设计理念是基于碳交易行业的背景和动机，旨在解决传统碳交易市场存在的问题，提高交易透明性、可信度和效率。

二、平台与平台模型

2.1 平台

Thallo 平台采用 P2P 交易机制，从用户使用数据中进行对比，可知我们的交易频率比系统 B 提高近一倍，Thallo 平台交易机制比系统 B 更具有优势，无论是从碳交易频率还是碳交易量上都比系统 B 多出 1.76 倍，所以 Thallo 平台更适用于当前碳交易趋势，更好响应国家政策，跟紧时代步伐，从而实现人类共同体，维护地球生态平衡。

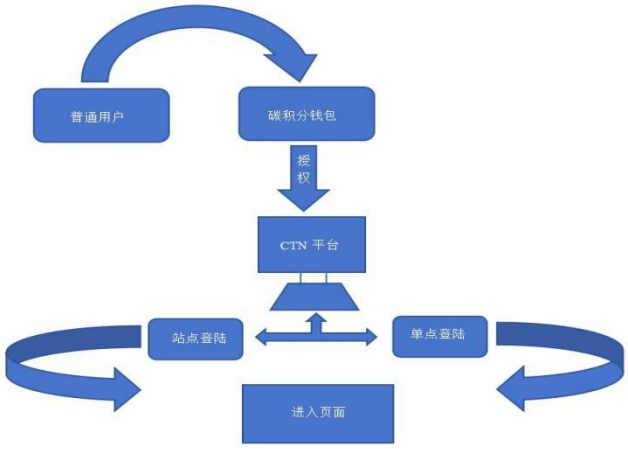


【图 1-平台对比图】

Thallo 是 CTN 中提供内容存储、用户交互、授权登陆等服务的智能解决方案，第三方可通过抵押碳积分，来获取到更多权益，同时若有在平台违反社区共识/条例则吊销平台资格并处以其他处罚。普通用户通过碳积分钱包对平台进行授权，可授权平台代理使用其鉴权权限，利用该权限可进行跨站点登陆、单点登陆，由于这是一个受限权限，无法对用户主

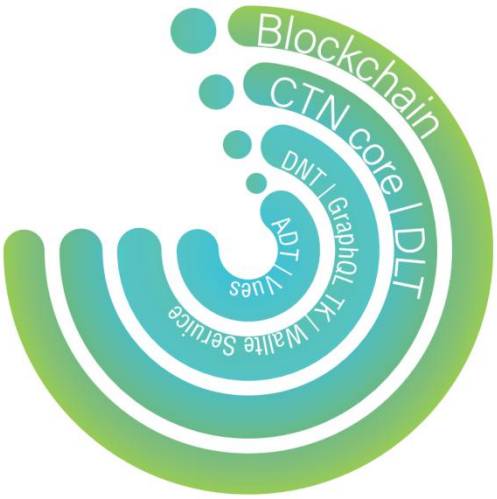
钱包进行关键性操作。同时平台也无法获取用户私钥，保证用户资产安全同时，确保系统开放性。普通用户也可随时撤销授权进行账号注销，这使平台不断为用户提供更好的服务。

CTN 网络本身不存储碳权或者碳量，只存储用户所拥有的储存值。而平台依赖用户交易中的佣金来获取回报，考虑到目前存储设备的费用极其低廉，我们预期 Thallo 平台提供的一般性交易方便性对最终用户来说应该是免费或者只收取极低廉的费用，而对于有去中心化内容交易需求用户来说，可以借助不同备份平台提供同步/备份服务来实现，用户通过使用碳积分可以将内容放置在多个备份平台中进行托管保存，而这些备份平台也可将内容放置到其他去中心化的内容存储区块链网络中进行备份（比如将内容放置到 Sia 或者 IPFS 中）。由于数据的散列值已经保存在 CTN 中，平台也无法擅自篡改内容而不被发现。



【图 2-进入页面】

2.2 平台模型



【图 3-平台模型】

CTN 主要由 4 个层次组成： 最底层为大赛提供的海峡链。在海峡链的基础上构建我们的核心层 CTN Core、DLT。CTN Core 作为核心层，实现评分逻辑、统一授权登陆、收益分配算法、社群平台等核心业务逻辑。提 T 供统一内容、评分以及用户管理等外部程序开发接口，拥有雄厚开发能力平台可以直接使用该接口进行深度开发。DLT 同为核心层之一，分布式账本技术原理是智能合约、分布式计算和储存技术、共识机制等。它分散存储在多个节点上，每个节点都有一份完整账本副本。所有节点通过共识机制达成一致，确保账本完整

性和安全性。分布式账本可以记录和存储各种类型数据，包括交易记录、身份信息、物品所有权等等。 拥有分权是 DLT 整个概念基础。这些网络更加安全，因为它们删除了任何集中式攻击媒介。在 DLT 网络中，风险从一个集中目标转移到数千个较小的媒介。由于这些较小的节点没有中央管理机构等大量有价值资产，因此它们遭受重大攻击可能性较小。 此外，DLT 利用高科技安全性来确保其网络保持纯净。输入恶意或错误数据节点将立即从网络中驱逐。该策略有助于简化整个共识过程。

Archive 之上的是 DNT、GraphQL TK、Wallet Seruice，这些工具的使用使平台可以采用新技术来提高系统可扩展性，还可以让每个人均可参与数据库记录。最早是积分的基础技术，目前世界各地均在研究，可广泛应用于金融等各领域。用于提供如区块格式、共识算法、网络、数据库、用户 以及权限管理等底层区块链服务。

DNT：动态网络用于描述各种复杂系统的动力学，在处理不同测试样本时，能够动态地调节自身的结构/参数，从而在推理效率、表达能力、自适应性等方面展现出卓越优势。它参与固定网络架构，初始化网络参数；在训练集上优化网络参数；在推理阶段：固定网络架构与参数，输入测试样本进行前向传播，得到预测结果。DNT 提高模型的泛化能力，减少计算量。DLT 具有不信任性质，使它们成为寻求安全网络解决方案的公司有吸引力的替代方案。诸如区块链网络之类的 DLT 消除了对第三方验证系统需求。由于这些系统中每一个都会为每次交易增加更多成本和时间，因此消除它们会大大提高效率。公司了解这些网络点对点性质使它们比集中式系统更易于运行。

GraphQL TK：旨在让 API 变得快速、灵活并且为开发人员提供便利。出色的是它可以部署在名为 GraphiQL 集成开发环境（IDE）中。作为 REST 替代方案，GraphQL 允许开发人员构建相应请求，从而通过单个 API 调用从多个数据源中提取数据。此外，GraphQL 还可让 API 维护人员灵活地添加或弃用字段，而不会影响现有查询。开发人员可以使用自己喜欢的方法来构建 API，并且 GraphQL 规范将确保它们以可预测方式在客户端发挥作用。除了为 API 查询定义和验证语法外，GraphQL 把大部分决策权都留给了 API 设计人员。开发人员可以使用 PHP（graphql-php）、Scala（Sangria）、Python（Graphene Python）、Ruby（graphql-ruby）、JavaScript（graphql.js）等高级程序设计语言。而且 GraphQL 对网络、授权或分页没有任何要求。以从客户端的角度看，GraphQL 最惯用的操作是查询和修改。按照创建、读取、更新和删除（CRUD）模型来审视这些操作，使查询等同于读取，大大加快了查询和修改速率。其他所有操作（创建、更新和删除）均视+为修改。

这样的模式使 GraphQL 有以下优点：

GraphQL 模式会在 GraphQL 应用中设置单一事实来源。它为企业提供了一种整合其整个 API 方法。

一次往返通讯可以处理多个 GraphQL 调用。客户端可得到自己所请求的内容，不会超量。

严格定义数据类型可减少客户端与服务器之间通信错误。

GraphQL 具有自检功能。客户端可以请求一个可用数据类型列表。这非常适合文档自动生成。

GraphQL 允许应用 API 进行更新优化，而无需破坏现有查询。

许多开源 GraphQL 扩展可提供 REST API 所不具备的功能。

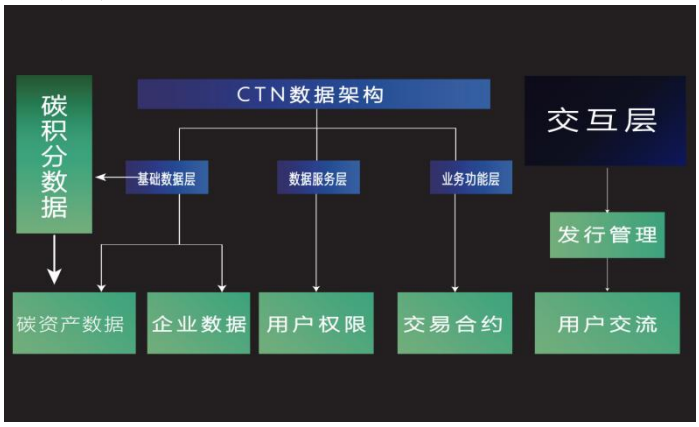
GraphQL 不指定特定应用架构。它能够以现有的 REST API 为基础，并与现有的 API 管理工具配合使用。

Wallet Seruice：此模块里包含区块链低碳钱包系统是一种基于区块链技术低碳经济应用，旨在为用户提供一个可靠数字化平台，记录和跟踪其对减少碳排放贡献。该系统采用去中心化的方式记录碳减排证书，安全、透明、可靠，有效解决了传统碳减排监管和核算问题，并

为环保和可持续发展提供了新手段和机会。 区块链低碳钱包系统运作原理如下：用户通过智能合约记录其低碳行为，例如骑自行车代替开车、使用可再生能源、购买环保产品等。这些行为将被记录在区块链系统上，每次记录都会生成一份碳减排证书，代表相应减排效果。这些碳减排证书可以存储在用户数字钱包中，并在需要时用于交易和奖励。

三、Thallo 平台架构介绍

3.1 Thallo 系统架构



【图 4-Thallo 系统架构图】

该系统架构由基础数据层、数据服务层、业务功能层、交互层由四层组成。基础数据层是由企业数据、碳资产数据、能源数据、碳积分数据组成，数据来源系统。数据服务层由系统提供用户权限、碳积分来支撑业务功能，数据服务层与业务功能层起相互支撑作用。保证用户在交互层有良好的功能体验，用户通过本系统完成碳排放权交易达成数额进行碳资产发行管理、碳资产即碳积分等功能实现 CTN 平台碳交易辅助和分析服务的业务路径。

3.2 Thallo 的透明性

Thallo 对于碳排放量和碳排放权交易数据是对外开放，除了系统成员加密数据外，任何人均可以通过公开接口进行对 Thallo 的访问，进行最新数据查询（列如碳量和碳权价格涨跌），提供给卖家与买家提供方便快捷的交易。

3.3 Thallo 登录权限与安全

透明可验证性：用户可随时查看验证权限和登记，数据确保可追溯其历史记录和所有权变更的流程。

管理和监督性：Thallo 可提供实时数据更新和监督，帮助用户有效地追踪和控制低碳排放权限分配和使用。

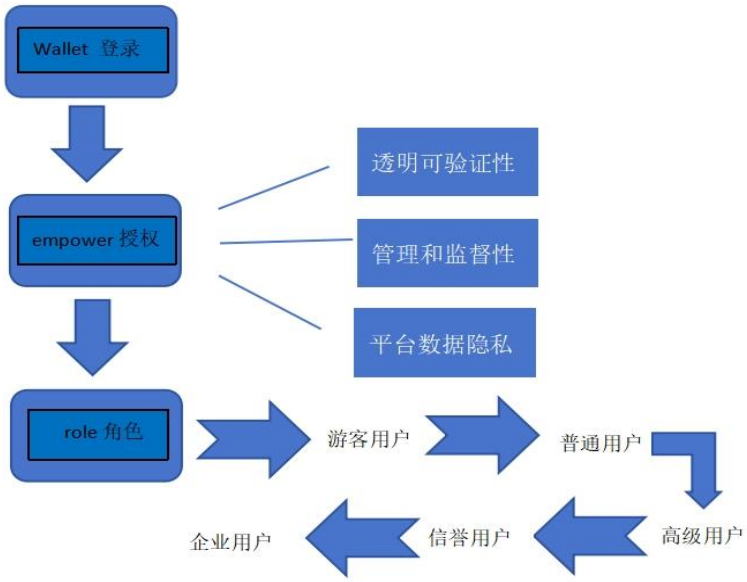
平台数据隐私：Thallo 用于构建去中心化的网络平台，用户拥有自身账号数据的使用权，有目的选择性共享数据，从而保护用户数据隐私。

3.4 Thallo 隐私计算

Thallo 隐私计算是在完成计算任务基础上，需要对全供应链数据进行管理，数据不能离开本地的存储节点，同时还对数据流通有规范性要求。确保数据安全与数据流通的平衡，使数据计算过程得到隐私保护。实现对数据隐私保护，并可以在不离开本地存储节点情况下，

进行跨组织数据计算和分析，数据就可以进行加密和处理，从而保护数据的隐私和安全更好的让碳排放和碳交易数据具有安全性。

3.5 用户角色



【图 5-用户角色】

游客用户：没进行 KYC 验证的为游客账户，不可进行任何形式的交易或碳积分领取，只允许浏览界面。

普通用户：可以买卖额度，进行积分兑换，额度或积分可用来进行抽奖或兑换奖励。通过节能减排例如乘坐公共交通、绿色低碳出行获取积分、兑换额度。

高级用户：交易额度足够多，或者积分足够多，将在普通用户的基础上升级高级用户，降低交易手续费，还有额外福利如优先与高评分信誉用户进行交易。

信誉用户：在交易中获取高评分的用户（包括普通与高级）将被评为信誉用户，在交易匹配时，获得优先权。

企业用户：通过企业认证成为企业用户，可以进行积分兑换，同时企业用户可以将自身商品或服务上架积分商城，共同建设平台生态。

3.6 评价系统

1. 所有卖家全部发货的订单，在交易结束天内买卖双方均可评价。

2. 对于信用评价，买家评价即生效;若双方都未给出评价，则该订单则产生不任何记录。

3. 商品/商家好评率(Positive Feedback Ratings)商家信用积分(Feedback Score)计算方法：

(一)相同买家在同一个自然旬内对同一个卖家只做出一个评价的，该买家订单评价星级则为当笔评价星级;

(二)相同买家在同一个自然旬内对同一个卖家做出多个评价，按照评价类型(好评、中评、差评)分别汇总计算，即好中差评数都只各计一次(包括 1 个订单里有多个产品情况);

(三)在卖家分项评分中，同一买家在一个自然旬内对同一卖家的商品描述准确性、沟通质量及回应速度、物品运送时间合理性三项中某一项的多次评分只算一个，该买家在该自然旬对某一项的评分计算方法如下：平均评分=买家对该分项评分总和/评价次数(四舍五入);

(四)成交金额过低订单不论买家留差评或好评，仅展示留评内容，不进行计算好评率及评价积分;

所有评价都会正常计算商品/商家好评率和商家信用积分。

3.6.1 智能推送系统

(一)推送系统基于评价系统，由评价系统的评分进行排列提高高分信誉用户的交易优先权。我们的推送系统通过大数据来研究用户喜好爱好，对用户提供个性化推送，给用户推送优质碳权和碳量交易。通过该推送系统使被撮合双方都能够提高交易满意度，来提高交易质量从而增加用户黏度。

(二)内容评价与价值体系

碳交易为 CTN 平台核心内容之一，其评价与价值体系至关重要。我们制定一套全面评价标准，以衡量碳积分质量、持久性和实用。

3.6.2 Thallo 的激励机制

筛选出用户主体碳排放量的活跃度（活跃度包括日常登录、成交数额等）进行商家好评率(Positive Feedback Ratings)商家信用积分(Feedback Score)计算，高分信誉用户交易优先权。

CTN 数据库对成交数额用户进行排名，对成交额大，信誉好的用户，给予优惠福利，如采用阶梯式将其分配给更加活跃的节点。

对与个人或企业在 Thallo 平台表现突出给予碳减排项目支持和开发，如：“植树造林绿色项目、火力发电转换水力发电项目、与绿色能源产品电能公交车或共享单车商合作”。

3.7 非对称算法密钥交换

使用各自的公钥和私钥，用户可以生成一个共享密钥，用于在双方之间建立保密的通信通道，对我们钱包用户进行加密形式，去保护用户隐私，非对称加密算法可用于验证用户身份并控制访问权限。通过使用公钥和私钥，用户证明自己身份并获得相应权限，必须跟私钥和公钥相互匹配，才可以获得解密权限。就算被拦截加密数据也无法解密，实现数据传输安全性。

3.8 非对称性加密算法的应用

1、CTN 用户身份的注册及应用验证：CTN 采用 Wallet 来进行登录，Wallet 由 Address＋Privacy key 组成。在达成交易时，用户需要使用 Wallet 记录并验证碳排放量数据认证，确保交易真实性和可信度。

2、在 CTN 数据传输中数据需要在节点之间进行传输。Thallo 采用 RSA 算法、DSA 算法、ECC 算法对传输数据进行加密，确保数据不可篡改性和安全性。

3、在用户最终确定成交数额时，Thallo 使用 ElGamal 算法、ElGamal 算法来生成数字签名，用于验证交易合法性。

四、去中心化与 CTN 钱包

4.1 去中心连接

在 CTN 中，每个用户可通过 Wallet Address 连接后来享受 CTN 上的服务。使用去中心连接取代单点连接将不再依赖于不同企业各自中心化账户体系，而是通过 DID 来实现自主身份。可以有效保护数据拥有者人生安全和财产安全。自主身份可以解决传统中心化身份带来的问题。去中心化连接它是一种用户个人拥有完全控制权的自我主权身份，与用户身份相关数据被安全、私密地存储，用户可以决定如何访问和使用这些身份数据，也能有效地用这些身份数据进行身份验证。在这种情况下，我们可以在不重复构建账户、不暴露身份数据情况下用一种身份连接不同服务。

4.2 碳积分的用途

Thallo，以碳积分形式完成平台交易。

【图 6-碳积分的用途】

4.3 评价权重和积分分配

4.3.1 CTN 主要利用 CBFT 去实现共识机制，通过零知识证明算法在保证数据安全和隐私前提下，提供可验证数据.采用 AMM 算法实现整体自动化交易，例如:当用户想要交易碳权或碳量时，交易信息被打包进区块，在交易过程中，采用智能合约实现法币和碳权或碳量直接交易，当投票结果达到预设条件时，系统会自动执行智能合约中的事件，从而完成交易。其价格由恒定的常数积公式确定，也就是:

$$T_A(p) * T_B(p) = K$$

其中，$T_A(p)$ 和 $T_B(p)$是两种 Token 的余额，K 是一个恒定值。这种价格确定方式可以避免恶意操纵价格，保证交易公平性和透明度。

4.3.2 CTN 平台还采用动态价值分配机制，根据碳积分的质量、价值和实用程度，将碳积分分配给不同用户。这种分配机制可以激励用户积极参与碳权交易，促进碳市场繁荣和发展。

4.3.3 CTN 平台还建立碳积分评价体系，通过制定全面评价标准，对碳积分的质量、价值和实用程度进行评估。该体系采用多元化评价方式，包括专家评估、用户投票、数据分析等，以确保评价结果公正、客观和准确。

4.3.4 CTN 平台通过建立全面评价标准，采用动态价值分配机制和建立碳积分评价体系，实现碳积分公开、透明和可验证交易，促进碳市场的健康发展，助力全球绿色低碳经济发展。

4.4 CTN 用户钱包功能及用途

(1) Store Carbon Reduction Assets：钱包可以安全地存储用户的碳减排资产，包括用户碳减排配额、减排项目的认证和清算信息，管理用户在 CTN 中购买、出售和交易碳排放权

(2) Asset management：钱包可以帮助用户管理其碳减排资产，包括查看资产余额、交易历史记录和资产变动、对碳积分、碳排放权等碳交易相关数字资产等。

(3) Carbon Emission Trading:用户可以通过钱包进行碳减排交易，包括购买和销售碳减排配额、参与碳信用交易等。时追踪自己碳信用余额，了解自己在减少碳排放方面的表现。此外，用户还可以通过钱包查看其他用户碳信用情况，互相学习和激励。

(4) Data authentication and validation:钱包会记录并验证碳减排项目认证信息，确保交易真实性和可信度。用户在区块链碳交易网络中进行身份验证，确保只有合法用户才能参与碳交易。这有助于打击非法碳排放行为，保护环境。

(5) Connect to other service:钱包可以与其他碳交易网络平台或服务进行连接，实现更多的碳减排和可持续发展应用

(6) Wallet security: 安全保障、相关安全功能保证了数字资产的安全性，包括多重签名、身份验证、私钥保护等功能。

4.5 CTN Payment System

(1) 分布式账本节点是指参与分布式账本网络的各个计算机，它们通过共同维护账本安全性和完整性来实现账本分布式存储和处理。每个节点都有一份完整的账本副本，并通过共识机制达成一致，确保账本一致性和可信度。 分布式账本节点可以分为以下几类：

(2) 全节点：全节点是分布式账本中最重要的节点，它存储了完整账本副本，并参与共识机制的决策过程，确保账本一致性和可信度。全节点需要大量的存储和计算资源来维护账本安全性和完整性。

(3) 轻节点：轻节点是一种较为轻量级的节点，它只存储了部分账本数据，可以通过其他节点获取完整账本数据。轻节点不直接参与共识机制决策过程，但可以通过验证其他节点决策结果来确保账本的一致性和可信度。

(4) 验证节点：验证节点是指参与权益证明（PoS）共识机制节点，它们通过持有一定数量碳积分来参与共识机制的决策过程。验证节点需要保证节点安全性和可靠性，同时也需要遵守共识机制的规则

4.6 CTN 平台

(1) CTN（Carbon Trading Network）平台作为绿色环保为主题的交易所，旨在促进碳排放权买卖，降低全球温室气体排放。平台类似于 Ebay、Amazon、Wish 等购物网站，并采用 MVGX 的交易所模式。CTN 的愿景是实现全球范围内碳排放权交易互联互通，形成碳交易市场。

(2) 塔罗可助力您：

(3) 提供透明、安全和可追溯的碳交易系统，用户通过 Wallet 窗口登陆平台页面

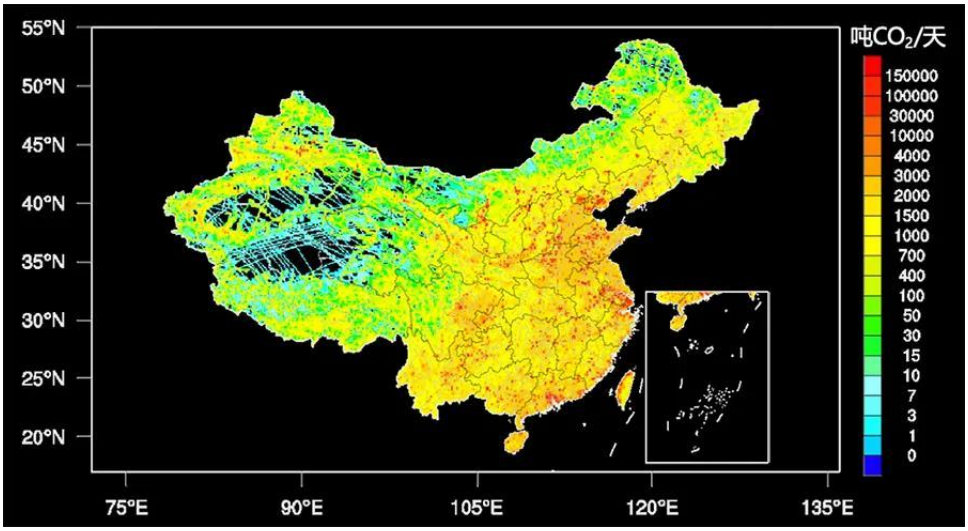
(4) 在 CTN 中购买、出售和交易碳排放权提供交易平台，以碳积分形式达成交易数额

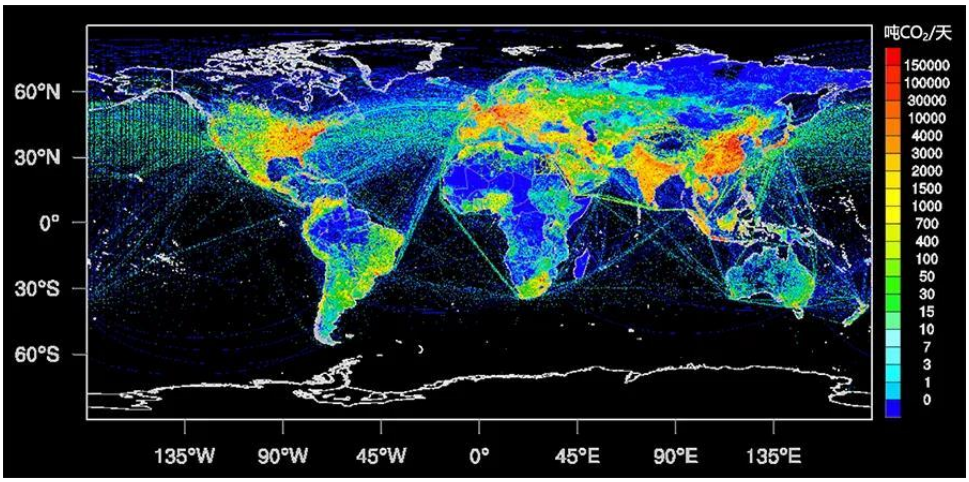
(5) 通过 Scoring system、Recommendation system 以衡量碳积资产来认证用户等级

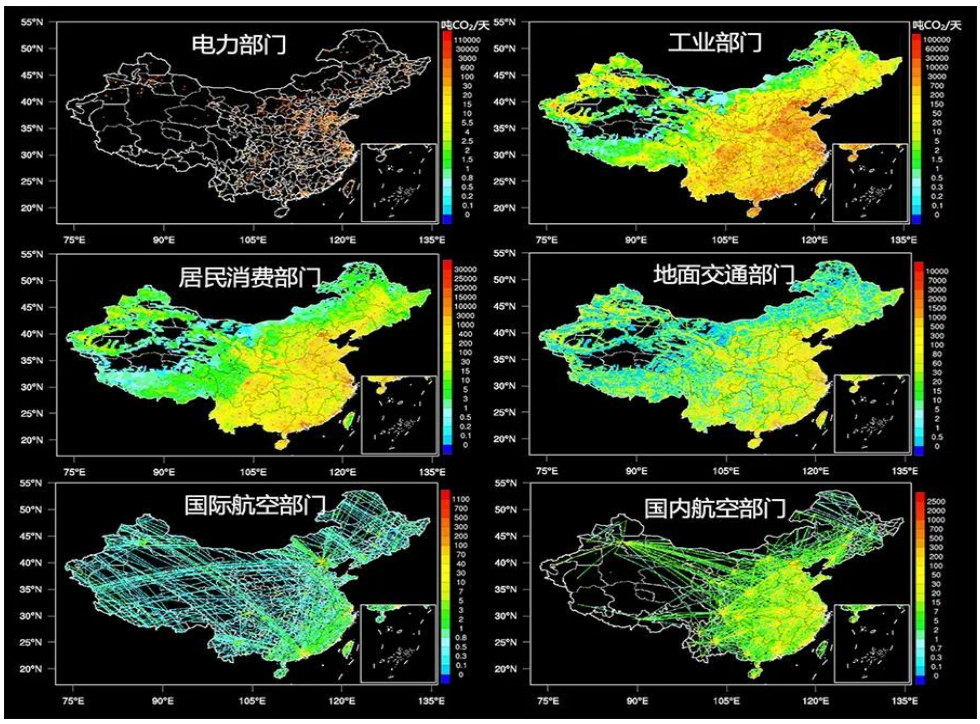
五、结语

碳交易市场是以实现“3060”双碳目标重要保障，而区块链具有去中心化、透明开放、不可篡改、可追溯等特点，可以精准定量、交易溯源。可在碳交易领域广泛应用，实现我们“3060”碳达峰、碳中和的全球愿景，更好地完善碳排放交易机制，从而推动上下游碳产业链深度融合。

附录 1：碳排放量追踪图


55°N
50°N
45°N
40°N
35°N
30°N
25°N
20°N
75°E
90°E
105°E
120°E
135°E
吨CO2/天
150000
100000
30000
10000
4000
3000
2000
1500
1000
700
400
100
50
30
15
10
7
3
1
0


60°N
30°N
0°
30°S
60°S
135°W
90°W
45°W
0°
45°E
90°E
135°E
吨CO2/天
150000
100000
30000
10000
4000
3000
2000
1500
1000
700
400
100
50
30
15
10
7
3
1
0


电力部门
工业部门
居民消费部门
地面交通部门
国际航空部门
国内航空部门


Carbon Trading Network


THALLO