各位评委老师，各位参赛选手，你们好！

我是来自泉州海洋学院的王中第

【Page1】下面由我来向大家阐述Carbon Trading Network底层碳交易网络和 Thallo 碳交易市场。

评委们请看PPT

【Page2】Thallo是基于区块链和隐私计算的碳交易市场，利用区块链技术构建去中心化的碳交易平台，为我国 “3060” 碳达峰、碳中和 提供碳配额/初始化、碳定价、碳交易等行业级/一站式解决方案。在2023年11月中旬的中美气候联合声明中，也强调了双碳对全球气候的重要性。所以我们将持续建设全球领先的碳交易市场thallo，以响应国家号召。

【Page3】Thallo的系统架构共计四层，其中核心技术由Carbon Trading Network提供（以下简称为CTN），并构建在海峡链上。CTN由分布式账本技术、隐私AI框架Athena和基于MPC的私钥分片、TSS门限签名和零知识证明共同构成。通过暴露的合约接口与海峡链进行网络对接，记录和验证碳排放权的交易信息，保障数据的透明和可追溯性，从而增强碳交易市场的平台可信度。在Thallo，我们通过去中心化身份和KYC/KYB认证系统，为每一位用户构建唯一的数字形象，提供个性化交易偏好，满足用户的客制化交易需求。为确保碳交易平台的市场流动性，Thallo平衡去中心化与中心化的交易机制，打造大深度、宽碳池的动态供需模型。

【Page3】在基础数据层，Thallo将企业数据、碳资产数据、能源数据、用户信息等多源异构化数据和验签数据通过隐私保护存储在海峡链上，防止潜在的敏感信息泄露和数据丢失风险。并且Thallo还采用MPC私钥分片技术打造TSS门限签名，使得用户隐私和用户资产得到妥善保障，而基于零知识证明的交易算法可确保买卖双方的隐私安全。

【Page4】在Thallo系统架构的支持下，利用分布式网络向多元化用户提供网络服务，实现完整的四方清结算体系。其中个人用户向企业用户出售低碳收集量，以获取对应的收益；同时企业用户可以与政府单位进行政企交易，增加市场流动性，活跃碳交易数据；而政府用户和其他机构单位使用我们平台服务，在交易的同时，也为Thallo提供数据反馈；并且机构用户和个人用户共同提供数据，可以有效撮合碳排放，强化我们的数据监听,建立碳清算网络，从而促进碳交易的正向循环。

【Page4】Thallo的交易流程如下，首先初始化碳配额会导入碳交易市场，以碳积分的形式进行价值锚定，进而引导碳交易的自然发生，交易双方将会在链上储存碳排放数据，通过安全多方计算，以及零知识证明，在实现数据安全的同时，确保数据流动的平稳进行。另外，Thallo的碳积分绑定碳价值，增强碳交易的流动性，从而推动碳排放权的稳定落地。

【Page5、6】Thallo构建在海峡链上，支持国密算法；将数据交互的全过程，进行全密态上链，并支持根链、侧链跨链协议。而且还提供多种基于密码学的场景化和隐私保护解决方案。同时，我们的核心链层提供完整的链上监管和治理功能，包含准入机制、敏感过滤、信息风控，以及链上数据审查等解决方案。由于海峡链是多链结构，采用单核心、多链合作的架构体系，作为可扩展性最强的底层联盟链，能够较好地平衡链间安全和计算互操作性。

【Page7】同时Thallo采用MPC私钥分片，保障TSS门限签名的可信验证，并通过零知识证明与隐私AI框架为碳积分钱包提供多种功能。并且采用RSA，ECC等非对称加密技术，实现合约审查、代码审计等方面的数据安全。全平台采用自动做市商算法，优化碳排放权资源配置方式，通过市场机制对交易进行动态调节，利用CTN核心技术和海峡链底层服务对接Thallo碳交易市场，从而确保交易的安全高效。

【Page8】在Thallo平台，我们采用碳积分作为支付和结算手段，将碳数据锁定在内核层，以支付逻辑的输入和身份验证，共同调动碳排放交易和碳资产管理。

【Page9】Carbon Trading Network & Thallo从2023年11月9日开始立项，与泉州海洋学院和泉州海洋计算机学会联合开发，截至2023年11月27日我们完成了官网开发的第一阶段。由于我们现在还是大一新生，而我们的网络及系统服务十分庞大，业务逻辑十分复杂，我们需要更多的时间去完善和雕琢我们的系统服务。

【Page10】感谢评委们的倾听。

核心技术CTN:

1.分布式账本技术：

2.隐私AI框架Athena:

3.基于MPC的私钥分片:

4.TSS门限签名:

5.零知识证明:

KYC/KYB认证系统：是线上的实名认证过程，银行等金融类App会在你进行业务操作时，通过手机自带的 NFC 功能识别身份证里的芯片信息，然后传输到公安系统内进行确认，再将认证结果反馈给银行或者其他金融应用，这个过程中你的身份证信息将只被公安系统知晓，而公安系统只输出“是本人”或“不是本人”的信息给相关应用，所以信息的安全也能得到有效保护。

四方清结算体系；清算机构作为连接持卡人（Account holders）、发卡方（Issuers）、收单方（Acquirers）和商户（Merchants）四者的中间清算环节。

自动做市商算法：

卖点：

1.区块链（信息安全公开透明

2.隐私计算：[隐私计算概念、技术及应用介绍 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/383607686)

3.数字形象

4.个人与企业，政企交易

5.支持根链、侧链跨链协议

6.链上监管和治理功能

7.采用RSA，ECC实现合约审查、代码审计

8.碳积分

* 市场问题：

当前在数据要素价值盘活过程的**数据生产加工、数据资源汇聚、数据流通交易、数据模型训练与部署**过程中仍然面临**数据确权难、投入成本高、数据集质量低、数据资源有限**等问题。各数据主体之间、甚至数据主体内部之间都因为数据安全问题而存在着数据孤岛现象，在数据流通、数据应用等方面都存在诸多问题。