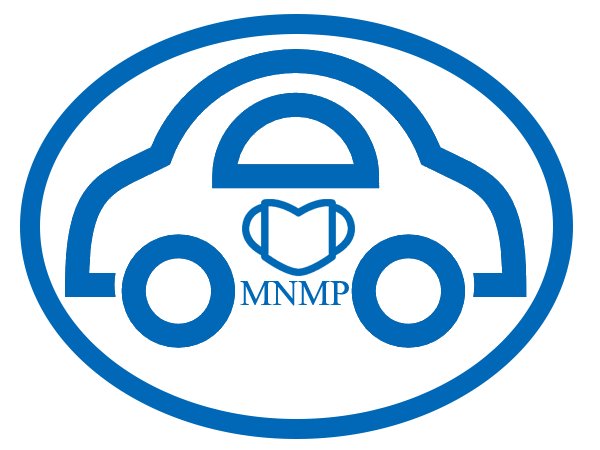
基于区块链的车辆

数据监管和任务协同平台



**Musk Need Mask Platform**

**项目团队：林怡静、王苗苗、吴孟晓、柴泽**

**所属院校：北京邮电大学**

**指导教师：高志鹏、芮兰兰**

项目简介

在高速发展的移动互联网时代，数据成为新一代的“石油”，正成为宝贵的数字资产。然而，移动互联网带来极高互联网普及率的同时，让数据成为宝贵却廉价的资产，在车联网场景中尤为甚是。对于车企来说，车辆数据是其宝贵的数字资产；对于用户来说，车辆数据的收集和使用却非常廉价。同时，因车辆数据安全引发的监管争议，让大众逐渐关注车辆数据的价值。除监管争议以外，车辆数据和资源协同困难的问题也困扰着用户和车企，包括车辆数据域内协同难、车辆数据跨域协同难以及车辆计算资源协同难等。

为解决上述问题，项目结合区块链、联邦学习、阈值签名、可验证随机函数、预言机等多种技术，构建基于区块链的车辆数据监管和任务协同平台。第一，针对车辆数据监管难的问题，提出基于双层多链的车辆数据监管流通框架，使得车辆数据在监管部门的监督下进行全流程流通；第二，针对身份认证难的问题，提出基于区块链的车辆身份认证授权机制，使得车联网场景中的实体需经过认证方可实现协同；第三，针对车辆数据域内协同难的问题，提出基于数据预言机的车辆数据域内协同机制，使得车辆数据在信任域内的实体间高效可信协同；第四，针对车辆数据跨域协同难的问题，提出基于跨域预言机的车辆数据跨域协同机制，使得车辆数据在不同信任域内的实体间高效可信协同；第五，针对车辆计算资源协同难的问题，提出基于计算预言机的车辆计算资源协同机制，使得计算资源有限的实体可充分利用其它实体的计算资源；最后，为验证和集成上述技术路线，项目研发基于区块链的车辆数据监管和任务协同平台，该平台基于Xuperchain构建区块链底层框架，设计车辆数据监管和任务协同应用场景、支撑构件和服务平台，实现车辆数据在区块链生态网络中高效可控全流程流通。

# 目 录

[目 录 3](#_Toc83398358)

[1.项目介绍 5](#_Toc83398359)

[2.技术方案 7](#_Toc83398360)

[2.1基于双层多链的车辆数据监管流通架构 7](#_Toc83398361)

[2.2基于区块链的车辆身份授权认证机制 9](#_Toc83398362)

[2.3基于数据预言机的车辆数据域内协同机制 9](#_Toc83398363)

[2.4基于跨域预言机的车辆数据跨域协同机制 10](#_Toc83398364)

[2.5基于计算预言机的车辆计算资源协同机制 10](#_Toc83398365)

[2.6基于区块链的车辆数据监管和任务协同平台 11](#_Toc83398366)

[2.7创新点 11](#_Toc83398367)

[3.系统研发 13](#_Toc83398368)

[3.1智能合约设计 13](#_Toc83398369)

[3.1.2数据结构 13](#_Toc83398370)

[3.1.2功能模块 14](#_Toc83398371)

[3.1.3工具模块 16](#_Toc83398372)

[3.2预言机设计 16](#_Toc83398373)

[3.2.1数据结构 16](#_Toc83398374)

[3.2.2功能模块 16](#_Toc83398375)

[3.2.3工具模块 17](#_Toc83398376)

[4.应用场景 18](#_Toc83398377)

[4.1监管及事故分析 18](#_Toc83398378)

[4.2交通流量分析及预测 18](#_Toc83398379)

[4.3智能驾驶学习 18](#_Toc83398380)

[4.4广告转化归因 18](#_Toc83398381)

[4.5金融数据共享 19](#_Toc83398382)

[4.6政务数据共享 19](#_Toc83398383)

[5.项目团队 19](#_Toc83398384)

[5.1核心团队 19](#_Toc83398385)

[5.2顾问团队 21](#_Toc83398386)

[5.3合规团队 22](#_Toc83398387)

[6.创新策略 22](#_Toc83398388)

[6.1政府数据监管 22](#_Toc83398389)

[6.2企业数据分析及广告投放 23](#_Toc83398390)

[6.3政务数据共享 23](#_Toc83398391)

[6.4个人隐私保护 24](#_Toc83398392)

[结束语 25](#_Toc83398393)

# 1.项目介绍

随着5G等新一代通讯技术的发展，车辆与终端设备之间的数据传输变得愈发便捷。在行驶过程中，车辆可以将其产生的大量与行驶状态、位置路况等相关数据传输到云端进行保存和记录，以进行用户行为分析。但是，随着行驶数据的缺失和滥用问题不断曝光，让人们不禁对自身数据隐私性和记录的准确性产生了疑虑。特斯拉维权事件的爆发就引发公众对车企存储的行驶数据的准确性与真实性的质疑；而滴滴赴美上市时传言其将个人信息，道路信息，交通数据等等外泄，更是引发人们对于数据隐私性和安全性的担忧。除此之外，公安部等七大部门入驻滴滴，全方位调查滴滴侵犯用户隐私问题，直接在大数据时代下，把用户个人隐私信息保护问题推到了前台。因此，如何规范企业对数据信息的存储和使用，来确保用户信息既不会被篡改，也不会被泄露和滥用，成了亟待解决的问题。

为此，国家先后出台《汽车数据安全管理若干规定》、《个人信息保护法》、《数据安全法》等等，体现了国家规范数据处理活动，整治违法收集数据、维护数据主动权的决心。为了更好的解决上述问题，协助国家相关法律的实施，我们提出了基于区块链的车辆数据监管和任务协同平台，将区块链技术和联邦学习引入车辆数据的存储和共享当中。区块链因其去中心化、开放性、防篡改性、匿名性及可追溯性等特点，可以很好的保存车辆行驶中的数据信息，一方面保证其数据真实有效，不会被恶意篡改和丢失；另一方面也能对数据进行加密，从而保护用户的隐私。联邦学习则能够在保障数据隐私的情况下，帮助企业或政府进行数据的分析，从而训练相应的智能模型，更好的发挥出数据的价值和效用。

本项目将当前存在的问题归纳如下：首先是车企数据垄断，监管部门需要采取复杂的行政手段才可获得原始数据，导致监管困难以及难以保证真实性；其次是数据的安全性存在问题，数据收集、处理的合规性难以保证，数据全生命周期难以追踪；接着是车企不可能与其他企业共享原始数据，导致数据孤岛；再者就是车企难以与其他企业协同完成域内共享、跨域共享和计算共享，导致数据资产价值降低。

针对上述问题，我们提出的基于区块链的车辆数据监管和任务协同平台包含如下部分，此平台除解决上述问题外，也可应用于如广告归因、金融、政务数据共享等类似领域。

首先，为解决车企的数据垄断导致的监管困难问题，本项目提出基于双层多链的车辆数据流通架构，该架构按照监管层和执行层分为联邦链和本地链。联邦链由监管部门、车企等节点组成，对车辆数据进行全局性治理，包括车辆数据域内协同、车辆数据跨域协同、车辆计算资源协同等。以解决数据篡改问题。

其次，为解决跨域身份认证难的问题，提出基于区块链的车辆身份授权认证机制，该机制由多个车辆网域、域内的授权认证中心组建的联盟链网络和区块链账本构成。车辆在接入时首先进行认证，通过后将证书的元数据保存在本地数据中心，唯一映射证书的元数据索引上传到区块链，使得证书可追溯。在车辆数据跨域交互的过程中，通过将车辆提供的信息与区块链上保存的信息进行对比来判定是否同意请求，以此保护车辆数据跨域协同的安全性。

接着，针对车辆数据域内难以获得实时链下数据、难以存储多源异构数据的问题，提出基于数据预言机的车辆数据域内协同机制，该机制在联邦链的监管下，帮助区块链高效获取链下的数据接口、数据库表以及数据文件等多源异构数据，打破区块链生态与链下真实世界的数据交互壁垒，实现车辆数据域内多源流通。

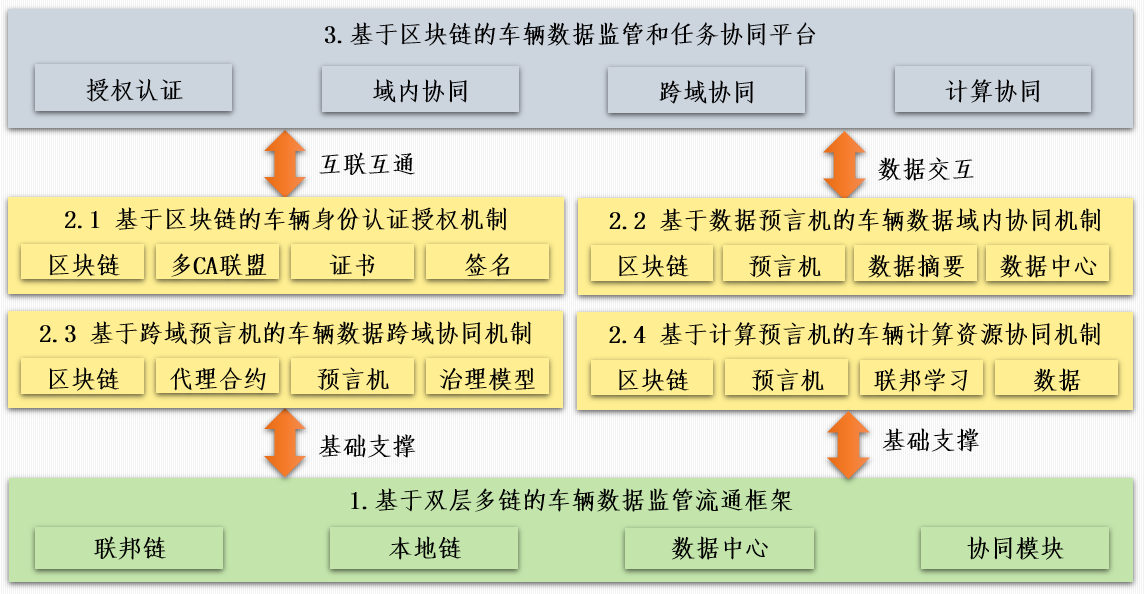
随后，针对不同信任域内车辆数据协同难的问题，提出基于跨域预言机的车辆数据跨域协同机制，在基于双层多链的车辆数据监管流通架构的基础上建立区块链车辆数据跨域协同。通过多链车辆数据跨域协同，打破区块链的数据孤岛，实现车辆数据的全域流通。

此外，针对车辆节点资源有限、难以执行复杂计算任务的问题，提出基于计算预言机的车辆计算资源协同机制，该机制结合区块链、计算预言机、联邦学习等技术，将原本在链上执行的复杂计算任务转移到链下执行，并在链上进行聚合和验证，以排除错误结果，从而提高车联网的计算能力。

最后，本项目综合上述内容，开发基于区块链的车辆数据监管和任务协同平台，面向车辆数据授权认证、域内协同、跨域协同、计算协同要求，构建车辆数据监管和任务协同应用场景、支撑构件和服务平台，实现车辆数据在区块链生态网络中高效可控全流程流通。

# 2.技术方案

项目采用的技术路线包括以下四个部分，分别是基于双层多链的车辆数据监管流通架构、基于区块链的车辆身份授权认证机制、基于数据预言机的车辆数据域内协同机制、基于跨域预言机的车辆数据跨域协同机制、基于计算预言机的车辆计算资源协同机制以及基于区块链的车辆数据监管和任务协同平台。授权认证确保车联网场景中的节点是经过认证的节点，可减少恶意节点出现的概率以及被恶意攻击的概率；域内协同是实现车联网中的车辆、基站等节点在可信域内实现域内数据高效安全协同；跨域协同指分布于不同信任域的车辆、基站、边缘服务器等节点实现跨域数据高效安全协同；计算共享指车联网中计算资源有限的边缘节点将计算任务外包给其他边缘节点，如边缘服务器等，实现计算资源高效安全协同。



基于区块链的车辆数据监管和任务协同平台

## 2.1基于双层多链的车辆数据监管流通架构

针对传统基于云服务的车辆数据存储可能存在的中心化、垄断、监管难的问题，项目提出基于双层多链的车辆数据监管流通架构，该架构按照监管层和执行层分为联邦链和本地链。联邦链由监管部门、车企等节点组成，对车辆数据进行全局性监管，包括车辆数据域内协同、车辆数据跨域协同、车辆计算资源协同等。本地链由车联网场景中的实体组成，对车辆数据进行局部治理，包括车辆数据域内协同、发起车辆数据跨域协同请求、发起车辆计算资源协同请求等。车辆产生数据，将数据上传车企云数据中心的同时取数据哈希值，并将车辆编号、时间戳、数据所在位置和数据元数据等信息作为交易数据提交到区块链共识。由于数据存储于云数据中心，区块链中的其他车企获取到交易数据也无法还原出原始数据，以保护数据隐私。

车联网的开放特性，即允许车辆节点随意加入或者退出网络，导致恶意节点可能加入网络，破坏域内协同、跨域协同、计算协同的过程，最终拖垮车辆数据流通的效率。为解决该问题，基于双层多链的车辆数据流通架构引入身份授权认证机制，利用区块链的不可篡改特性满足车联网环境中高密度链接的可信跨域认证需求。区块链的封闭特性，即需要确保去中心化网络中的不同节点针对相同的输入可以产生相同的输出，使得其无法主动与外部数据交互。因此，车辆数据难以在区块链生态网络中高效快速流通。为解决该问题，基于双层多链的车辆数据监管流通架构分别引入数据预言机、跨域预言机以及计算预言机，实现车辆数据的域内协同、跨域协同以及计算资源的协同。

车辆数据在区块链和数据预言机、跨域预言机和计算预言机之间流转时，可能出现数据节点被篡改的风险。因此，在基于双层多链的车辆数据监管流通架构中，采用基于阈值签名和可验证随机函数的共识算法，该算法结合智能合约、阈值签名和可验证随机函数等技术，使得本地链在发起域内共享、跨域共享、计算共享等请求时，需要获得联邦链的同意方可由数据预言机、跨域预言机和计算预言机转发相应请求。具体的流程为，以区块链高度和监管部门所在联邦链生成的随机数作为种子，利用可验证随机函数选出一个可验证的预言机节点作为广播消息的广播节点；随后广播节点接收来自区块链的车辆数据身份授权认证请求、车辆数据域内协同请求、车辆数据跨域协同请求以及车辆计算资源协同请求；广播节点先验证上述请求是否经过监管部门所在的联邦链的批准，即是否具有有效的联邦链默克尔根，若验证通过则将上述请求广播给预言机网络中的其他节点，否则不广播上述请求；其他节点根据车辆请求内容执行操作，获得相应结果，并对该结果进行签名，最后将该签名和结果返回给广播节点；广播节点首先聚合节点签名和结果，实现车辆数据链下聚合，并将聚合签名和结果上传到智能合约，实现链上验证；智能合约首先基于可验证随机函数验证广播节点的身份，防止恶意节点冒充广播节点；其次基于阈值签名验证结果的有效性，防止广播节点恶意篡改数据；最后，修改相应的车辆数据状态，完成本次的数据请求。

## 2.2基于区块链的车辆身份授权认证机制

在车联网中，各车辆厂商拥有一套独立的车辆身份认证流程。该过程依赖证书授权中心，并采用数字证书和公钥基础设施技术保障认证、交易流程的主体可信，进而保证车辆数据交互的安全性。但是，上述跨域认证方案涉及复杂的证书管理，计算开销大，导致跨域身份认证难。

为解决上述问题，项目提出基于区块链的车辆身份授权认证机制，该机制由多个车联网域、域内的授权认证中心组建的本地链共同构成。链下的授权认证中心需向联邦链发起授权请求方可在链上获得合法的授权身份，即获得批准该请求的交易默克尔根；车辆在接入车联网时首先进行注册和身份认证，认证流程与域内证书认证流程相同；认证通过后，域内的授权认证中心将证书的元数据保存在本地数据中心，唯一映射证书的元数据索引上传到区块链，使得证书可追溯。

在车辆数据跨域交互的过程中，车辆实体需要进行跨域认证，方可执行他域的状态转移操作。他域的授权认证中心向车辆实体发送随机数，车辆需要利用私钥对该随机数签名，并将随机数签名、数字证书的元数据索引和证书源数据返回给授权认证中心；授权认证中心接收到车辆实体的身份认证数据后，验证车辆的信息，并将车辆提供的证书源数据、元数据索引与区块链上保存的信息进行对比，若一致则跨域认证成功，否则拒绝跨域请求，以此保护车辆数据跨域协同的安全性。

## 2.3基于数据预言机的车辆数据域内协同机制

针对基于区块链的车辆信任域难以获得实时链下数据、难以存储多源异构数据的问题，在基于双层多链的车辆数据监管流通架构的基础上，项目提出基于数据预言机的车辆数据域内协同机制。该机制在联邦链的监管下，帮助区块链高效获取链下的数据接口、数据库表以及数据文件等多源异构数据，打破区块链生态与链下真实世界的数据交互壁垒，实现车辆数据域内多源流通。

项目提出的基于数据预言机的车辆数据域内协同机制分为链上部分和链下部分，链上部分包含接收用户指定数据接口、数据库表以及数据文件的应用合约以及提供域内协同接口的代理合约，链下部分为去中心化的数据预言机网络。源区块链的车辆节点首先调用应用合约指定相应的数据对象，应用合约随后调用代理合约提供的接口，触发域内协同事件；同时，该请求将由联邦链在该链指定的监管节点转发到联邦链，获取联邦链的共识许可；数据预言机监听到请求之后，根据指定的数据存储地址获取数据，并返回给链上的节点。

## 2.4基于跨域预言机的车辆数据跨域协同机制

针对不同信任域内车辆数据协同难的问题，立足基于双层多链的车辆数据监管流通架构，结合车联网的多链互联生态考量，项目提出基于跨域预言机的车辆数据跨域协同机制。该机制在车辆数据监管流通架构上建立区块链车辆数据跨域协同。通过多链车辆数据跨域协同，打破区块链的数据孤岛，实现车辆数据的全域流通。

项目提出基于跨域预言机的车辆数据跨域协同机制设计通用的数据交互架构，提供逻辑统一的数据交互机制。该机制主要包含三个部分，源区块链、目的区块链和跨域预言机。在源区块链和目的区块链上分别部署两个智能合约，一个是实现用户逻辑的应用合约，另一个是提供跨域协同接口的代理合约。源区块链的车辆节点首先调用应用合约发起跨域协同请求；随后该请求由应用合约转发至代理合约，触发跨域协同事件，同时该请求将由联邦链在该区块链上指定的监管节点转发到联邦链，获取联邦链的共识许可；跨域预言机的广播节点通过监听跨域协同事件获取请求，并验证该请求是否包含联邦链的交易默克尔根，验证通过后将该请求转发给网络中的其他节点；跨域预言机中的节点执行共识算法后转发到目的区块链的代理合约；目的区块链的代理合约调用应用合约修改跨域协同请求状态，完成车辆数据的跨域协同。

## 2.5基于计算预言机的车辆计算资源协同机制

针对车辆节点资源有限、难以执行复杂计算任务的问题，立足基于双层多链的车辆数据监管流通架构，项目提出基于计算预言机的车辆计算资源协同机制。该机制结合区块链、计算预言机、联邦学习等技术，将原本在链上执行的复杂计算任务转移到链下执行，提高车联网的计算能力。

该机制分为链上和链下两个部分，具有计算资源协同需求的车辆节点需要将请求写入智能合约，请求的内容需要包含数据集地址、模型、随机种子、训练轮次、通信轮次等必要信息，经由区块链和智能合约广播给计算预言机网络，同时该请求将由联邦链在该区块链上指定的监管节点转发到联邦链，获取联邦链的共识许可。计算预言机网络接收到请求后，并验证该请求是否包含联邦链的交易默克尔根，验证通过后根据请求执行相应的计算任务。为高效利用计算资源，计算预言机网络中的节点协同执行计算任务，每个节点训练数据集的一部分，将模型参数发送给广播节点聚合，得到最终的模型结果。

在协同训练的过程中，首先，计算预言机网络中的普通节点可能故意上传错误的参数结果，为解决该问题，项目的广播节点将采用部分测试集对参数进行验证，并对效果进行排序，选取部分节点作为本轮的计算结果；其次，广播节点故意下放错误的聚合参数，为解决该问题，项目基于阈值签名使得节点对车辆请求结果进行签名，使得恶意的广播节点提供的车辆模型参数无法通过验证。

## 2.6基于区块链的车辆数据监管和任务协同平台

面向车辆数据授权认证、域内协同、跨域协同、计算协同要求，项目立足基于双层多链的车辆数据监管流通架构，研发基于区块链的车辆数据监管和任务协同平台，构建车辆数据监管和任务协同应用场景、支撑构件和服务平台，实现车辆数据在区块链生态网络中高效可控全流程流通。该平台包括基于Xuperchain的车辆数据监管和任务协同服务平台、全链条协同一体的车辆数据资源流转构件。基于Xuperchain的车辆数据监管和任务协同服务平台将在百度超级链Xuperchain中验证和集成上述技术方案，实现车联网场景下的车辆数据授权认证、域内协同、跨域协同以及计算协同。全链条协同一体的车辆数据资源流转构件将提供基于区块链的身份认证构件、基于数据预言机的域内协同构件、基于跨域预言机的跨域协同构件、基于计算预言机的计算协同构件等。

## 2.7创新点

1. 数据私密性及可追溯性

项目立足车辆数据监管需求和用户驾驶数据隐私性需求，提出基于双层多链的车辆数据监管流通架构。区块链账本的公开透明性和数据不可篡改性保证了上链的车辆数据具有可追溯性。链上存储数据摘要、数据协同任务、协同计算任务，链下预言机分发任务请求、数据中心存储元数据，保证了车辆数据的私密性。

1. 数据全生命周期的安全管理

项目立足车辆数据监管需求，结合多链互联的区块链产业生态，提出基于双层多链的车辆数据监管流通架构，实现数据流通全生命周期的安全管理。车辆数据进行摘要后发布到区块链账本，避免数据隐私泄露；域内和跨域的数据请求由联邦链共识后，基于预言机转发请求，实现数据协同，保证请求和数据的可靠性；车辆对计算协同任务的计算结果进行阈值签名，防止恶意节点对计算任务的攻击。

1. 高效的授权认证

在基于双层多链的车辆数据监管流通架构上，项目基于区块链构建身份授权认证机制，该机制允许授权认证中心通过区块链获取他域证书关键信息，避免了传统跨域认证中的授权认证中心之间的信任交互和复杂的计算，实现了车辆的快速跨域身份认证，保证车辆在后续的交互过程中身份可信可追溯。

1. 全域数据协同共享

在基于双层多链的车辆数据监管流通架构上，为解决区块链封闭性带来的车辆数据域内协同难的问题、多链区块链生态带来的区块链车辆数据孤岛问题，项目提出基于预言机的车辆数据域内协同机制和跨域协同机制， 该机制在联邦链共识许可下允许车辆节点获取域内外数据，打破区块链的封闭性，实现车辆数据的域内互联互通和跨域互联互通。

1. 可靠的计算协同

为解决车辆计算资源有限导致无法执行复杂计算任务的问题，项目在双层多链的车辆数据监管流通架构之上构建基于计算预言机的车辆计算资源协同机制，该机制允许资源有限的车辆在联邦链共识许可下将复杂的计算任务转移给链下的计算预言机执行，打破车辆资源的限制，在保证安全性的前提下实现车辆计算资源协同。

# 3.系统研发

## 3.1智能合约设计

智能合约的设计中，在区块链公链上共存储五种数据，名称与结构如下：

{

CAR\_FILE\_ASSET\_COUNT []byte

TASK\_QUEUE []byte(Queue{})

META []byte(map[string][]byte{})

RESULT []byte(map[string][]byte{})

}

其中CAR\_FILE\_ASSET\_COUNT存储二进制的字符串，含义为元数据的计数器，每当有新元数据上传时，该变量自动增加一；TASK\_QUEUE为简化后的任务队列，存储二进制的队列结构体，队列结构体能实现入队出队等操作；META为元数据哈系字典，通过Id查找对应的元数据；RESULT为结果字典，通过Id查找查询或计算共享结果。

### 3.1.2数据结构

本节主要介绍智能合约中的结构体。

|  |  |  |
| --- | --- | --- |
| Struct | Param | Description |
| MetaData | Uploader 数据上传者  Name 数据名称  Type 数据类型  Ip 数据存放服务器IP  Route 数据存放路径  Abstract 数据摘要 | 区块链存储的元数据 |
| QueryTask | Id 任务Id  MetaData 待查询元数据 | 查询任务队列结构体 |
| FaderatedAI-  Demand | Model 模型  Dataset 数据机  Round 通讯轮数  Epoch 本地迭代次数 | 联邦学习需求结构体 |
| FaderatedAIData | Id  MetaDataByte 二进制元数据  FaderatedAIDemandByte 二进制需求结构体 | 联邦学习任务结构体 |
| FaderatedAI-  Result | ParamAddr 参数所在地址  ParamAbstract 参数摘要  CorrectRate 正确率 | 联邦学习返回结构体 |

### 3.1.2功能模块

合约从逻辑上区分为应用合约、代理合约与回调合约。其中应用合约为被客户端调用的合约，是一次事件的发起者；代理合约被应用合约调用，实现具体的业务逻辑并提交事件；回调合约只有当预言机完成任务后才可调用，主要功能是上传结果、任务队列出队等。下面分别从这三个方面介绍智能合约。

1. 应用合约

|  |  |  |
| --- | --- | --- |
| Method | Param | Description |
| Initialize | Nil | 初始化函数，对元数据计数器、任务队列、元数据字典以及返回结果字典进行初始化 |
| Query | Id 需查询的元数据Id  Inquirer 查询者  Expiration 截止时间 | 域内共享与跨域共享应用合约，负责验证传入参数，查询Id对应元数据，将其结构化为查询任务后调用代理合约 |
| ComputingShare | Id 元数据Id  FaderatedAIDemand 联邦学习需求 | 计算共享应用合约，负责验证传入参数，查询Id对应元数据，结构化为FaderatedAIData后调用计算共享代理合约 |
| CreateCfa | MetaData 待上传的元数据 | 上传元数据应用合约，验证传入参数后生成Id，更新计数器并上传 |
| UpdateCfa | Id 元数据Id  Operator 操作者  MetaData 新元数据 | 更新元数据应用合约，验证传入参数、操作者是否为上传者，通过后更新链上元数据 |

1. 代理合约

|  |  |  |
| --- | --- | --- |
| Method | Param | Description |
| QueryAgentAccept | queryTask 查询任务 | 域内共享与跨域共享代理合约，接收由应用合约格式化后的查询任务，负责将查询任务加入任务队列，并发出查询事件 |
| ComputingShareAgent | FaderatedAIData 联邦学习任务结构体 | 计算共享代理合约，接收由应用合约格式化后的联邦学习任务结构体，负责任务队列入队、出发计算共享事件 |

1. 回调合约

|  |  |  |
| --- | --- | --- |
| Method | Param | Description |
| QueryCallback | Id 任务Id  Data 查询的数据  Asig 各链下节点签名  Pks 各链下节点公钥 | 域内共享与跨域共享回调合约，负责验证回调数据、回调结果上链、任务队列出队 |
| ComputingCallBack | Id 任务Id  FaderatedAIResult 联邦学习任务结构体  Asig 各链下节点签名  Pks 各链下节点公钥 | 计算共享回调合约，负责验证身份、结果上链、任务队列出队 |

### 3.1.3工具模块

|  |  |  |
| --- | --- | --- |
| Method | Param | Description |
| CheckExpiration | Expiration 截止时间 | 检查是否超过截止时间 |
| CheckIfCrossChain | Metadata 元数据 | 判断为跨链查询或链下查询 |
| Sign | Data 跨链数据  Generator 随机数 | 在链上聚合时对数据签名 |
| Verify | GroupPubkey 阈值签名组公钥  Signature 阈值签名 | 验证阈值签名的有效性 |

## 3.2预言机设计

预言机分为数据预言机、跨域预言机和计算预言机三种类型。数据预言机即根据区块链提供的接口获取数据，跨域预言机即转发区块链的请求给另一条区块链，计算预言机即根据区块链的计算任务要求在链下执行计算任务。

### 3.2.1数据结构

本节展示预言机中用到的数据结构。

|  |  |  |
| --- | --- | --- |
| Struct | Param | Description |
| Client | NodeID 节点标识  Url 地址  Keypair 公私钥对  KnownNodes 相连节点  Request 请求  ReplyLog 返回日志  Mutex 互斥锁  StartTime 开始时间  EndTime 截止时间 | 监听链上事件，向预言机发起请求 |
| Node | NodeID 节点标识  KnowNodes 相连节点  SequenceID 请求序号  MsgQueue 请求队列  Keypair 公私钥对  MsgLog 消息日志  RequestPool 请求池  Mutex 互斥锁  BlsSK 阈值签名私钥  BlsPK 阈值签名公钥  BLSLog 阈值签名日志 | 节点处理预言机请求 |
| NetMsg | Header 消息标识  Signature 节点签名  ClientNodePubkey 客户端公钥  CLientUrl 客户端链接  RequestMsg 请求消息  TrainMsg 计算协同消息  AggMsg 聚合计算协同消息  DataMsg 数据协同消息  AggDataMsg 聚合数据协同消息  CrossMsg 跨域协同消息  AggCrossMsg 聚合跨域数据协同消息  ReplyMsg 回调消息 | 网络中传输的消息结构 |

### 3.2.2功能模块

本节展示预言机用到的功能模块。

|  |  |  |
| --- | --- | --- |
| Method | Param | Description |
| SendRequest | 接收事件内的消息 | 向预言机网络发送请求 |
| HandleReply | Payload 消息内容 | 接收回调请求 |
| HandleMsg | Msg 消息 | 根据消息的类型分流 |
| HandleRequest | Msg 消息  Signature 签名  ClientNodePubKey 客户端公钥  ClientUrl 客户端地址 | 预言机广播节点接收消息，并验证该消息是否有效 |
| HandleTrain | TrainMsg 消息  Signature 签名 | 执行计算协同任务 |
| HandleAgg | AggMsg 消息  Signature 签名 | 聚合计算协同任务结果 |
| HandleData | DataMsg 消息  Signature 签名 | 执行域内数据协同任务 |
| HandleAggData | AggDataMsg 消息  Signature 签名 | 聚合域内数据协同任务结果 |
| HandleCross | CrossMsg 消息  Signature 签名 | 执行跨域数据协同任务 |
| HandleAggCross | AggCrossMsg 消息  Signature 签名 | 聚合跨域数据协同任务结果 |

### 3.2.3工具模块

本节展示预言机用到的消息模块。

|  |  |  |
| --- | --- | --- |
| Method | Param | Description |
| HandleConnection | Conn 网络请求 | 与其他节点建立网络连接 |
| SignMessage | Msg 消息  Privkey 私钥 | 消息签名 |
| VerifySignature | Msg 消息  Sig 签名  Pubkey 公钥 | 验证签名 |
| VerifyDigest | Msg 消息  Digest 摘要 | 验证摘要 |
| GenRandom | Start 开始  End 结束  Count 个数 | 生成随机数 |
| GenDigest | Msg 消息 | 生成摘要 |

# 4.应用场景

## 4.1监管及事故分析

交通事故现场还原是交通事故调查的重点，由于项目系统会不断收集车辆行车数据，同时将数据的验证信息存储在主链，当出现交通事故时，监管部门可以通过主链请求事故方的行驶数据，如时间、车速、制动踏板物理移动信号和制动主缸压力等，同时通过主链返回哈希值对企业方提供数据进行验证，校验通过的数据可以为事故判定提供依据。

在该场景下，本项目系统可以为司法部门提供可信、有效的数据，协助司法部门进行数据分析，同时系统会对车辆的行驶数据进行记录和验证，为政府对车辆和车辆制造商的监管提供了有力帮助。

## 4.2交通流量分析及预测

本项目系统以联邦学习为核心，提供了隐私保障下的数据分析功能，政府或企业可以通过系统，基于各个车企本地数据训练数据分析模型。例如在交通治理方面，模型可以根据企业本地的汽车行驶数据，分析不同时间段的各个路段的交通压力和汽车行驶数据，交通管理部门可以使用模型进行交通流量预测，更好的进行交通信号灯控制、交通管制和通行策略的制定。

## 4.3智能驾驶学习

智能驾驶学习需要大量数据进行训练，单个企业掌握的驾驶数据往往有限，但是由于数据泄露风险，大部分企业无意共享其核心驾驶数据。通过项目系统的数据加密和联邦学习方案，不同车企之间可以在保护隐私和核心机密的情况下共同训练智能驾驶模型，帮助各个车企完善自动驾驶或者辅助驾驶的学习和测试。

## 4.4广告转化归因

将流量方的曝光和点击数据与广告主的转化数据从用户维度进行求交，但是双方存在信任和隐私问题。多流量平台归因通常需要借助第三方DMP平台来完成。原因是多渠道间的数据孤岛需要通过第三方DMP平台来建立关联关系。本项目通过跨域交互和联邦学习，可以通过用户识别的方式来将多渠道间的用户关联起来，在保证用户个人隐私的前提下，统一按照归因模型来分析转化数据，从而帮助广告投放平台进行归因。

## 4.5金融数据共享

将不同银行的核心用户数据、风控数据进行共享存在信任和隐私问题，如何在打破“数据孤岛”和保护“个人隐私”的之间实现平衡，是一个全球性难题。本项目力图在个人金融信息保护、共享和发挥效用三者之间维持平衡，不泄露原始数据和个人信息，通过联邦学习和隐私计算等方式进行可寻踪的数据共享和使用，以发挥数据在金融行业中的经济效益。

## 4.6政务数据共享

政务数据打通是政务信息化发展的必由之路，政府部门已经成为最大的信息数据生产、收集、使用和发布单位。但因跨部门共享机制不健全、政策制度滞后等原因，“不愿共享”、“不敢共享”、“不会共享”等问题突出，影响了数据资源共享应用的整体效能。本项目针对共享中的信任和途径问题，建立跨地区、跨部门的数据共享方法，串联起各个数据孤岛，进而深入发掘政务信息资源潜力，全面释放数据红利。

# 5.项目团队

## 5.1核心团队

|  |  |
| --- | --- |
|  | 林怡静，北京邮电大学网络与交换技术国家重点实验室博士研究生   * 研究方向为区块链与边缘计算 * 获得北京邮电大学博士生创新基金、优秀博士生后备计划奖学金 * 参与多项国家级科研项目，包括国家自然科学基金、国家重点研发计划等 * Tron Accelerator三等奖 * 通过国家法律职业资格考试 * 获得大学生创新创业训练计划国家级优秀 * 三创赛北京赛区三等奖 * HuobiLabs举办的HotChainer区块链应用设计大赛第一名 |
|  | 王苗苗，北京邮电大学网络与交换技术国家重点实验室博士研究生   * 研究方向为区块链与边缘计算 * 参与多项国家级科研项目，包括国家自然科学基金、国家重点研发计划等 * 参与区块链版权保护等多项标准的研究 * 阿里巴巴高校联盟Java网站大赛二等奖 * 用友第一届全国移动创新大赛三等奖 * HuobiLabs举办的HotChainer区块链应用设计大赛第一名 |
|  | 柴泽，北京邮电大学网络与交换技术国家重点实验室硕博连读研究生   * 研究方向为区块链与联邦学习 * 参与多项国家级科研项目，包括国家自然科学基金、国家重点研发计划等 * 多次获得蓝桥杯、中国/美国大学生数学建模竞赛二等奖、三等奖 * 曾在某大型外企参与物联网相关项目的开发 * HuobiLabs举办的HotChainer区块链应用设计大赛第一名 |
|  | 吴孟晓，北京邮电大学网络与交换技术国家重点实验室硕士研究生   * 研究方向为区块链与边缘计算 * 参与多项国家级科研项目，包括国家自然科学基金、国家重点研发计划等 * 曾在多所知名互联网企业参与系统后端开发 * 曾获得大学生创新创业比赛一等奖 |

## 5.2顾问团队

|  |  |
| --- | --- |
|  | 高志鹏，博士，北京邮电大学网络与交换技术国家重点实验室教授，博士生导师   * CCF高级会员、区块链专委会委员，YOCSEF副主席 * 大数据智能管理与分析技术国家地方联合工程研究中心副主任、北邮“边缘计算与网络系统”联合实验室学术委员会主任，长期担任国家发改委、科技部、工信部、国家自然科学基金委项目评审专家 * 中国信通院云边协同创新应用创新实验室专家委员会委员、技术推进组组长 * 主持和参与多项国家自然科学基金项目、国家科技重点研发计划、国家973项目、国家863项目、国家科技支撑项目和十二五/十三五预研项目等重点科研项目 * 研究成果获北京市科技一等奖1次，通信学会科技一等奖1次，中国通信标准化协会科技一等奖1次，其他省部级二等奖6次。形成了30多个国家发明专利、4项国际标准和多项行业/企业标准。 |
|  | 芮兰兰，博士，北京邮电大学网络与交换技术国家重点实验室副教授，博士生导师   * 主持10余项工业与信息化部标准研究项目、2项国家重点实验室自主研究课题和1项北京邮电大学青年科研创新计划专项项目 * 参与完成10余项包括国家863、国家攻关、国家自然科学基金、国家重大专项、国际合作在内的重大项目 * 研究成果获国家科技进步二等奖1次，省部级科技进步奖10次 * 多次参加国际标准化组织（3GPP和3GPP2）的标准制定工作，研究成果已形成4项3GPP国际标准，被3GPP SA5授予突出贡献奖荣誉称号 * 主持编制了18项中国通信行业标准和4项3GPP国际标准，参与完成了3项ITU-T国际标准和10项中国通信行业标准 |

## 5.3合规团队

|  |  |
| --- | --- |
|  | 戴雨勤，中国政法大学民商经济法学院商法专业学术性硕士研究生   * 研究方向为公司法方向，关注实务、注重案例研习 * 本科就读于西南政法大学，曾获得全国大学生模拟法庭竞赛亚军 * 曾在知名电商平台实习，针对业务合规、广告合规、数据保护等方面提供法律意见 * 曾在多家知名律所实习，针对数据跨境、信托计划纠纷、债券纠纷、证券纠纷等方面提供法律意见 |
|  | 黎想，美国范德堡大学法学院国际商法方向硕士毕业   * 研究方向为跨境贸易与公司并购 * 曾在外资律所知识产权组实习，参与跨境专利的申请与维护，并为境外客户提供高相关数据合规、企业合规等方面的法律服务 * 曾在某四大国有股份制商业银行分行法律合规部实习，针对企业合规与风险防范方面提供法律意见 |

# 6.创新策略

## 6.1政府数据监管

将区块链技术引入车辆数据存储中，利用区块链的不可篡改来确保数据的真实性、有效性和完整性，免去事后监察时对数据真伪的求证。同时采用主从链和跨链技术，免去政府在调用数据时与车企交互时的一系列手续，可以更加及时、便捷的查找数据，简化行政流程。同时，由政府出面负责、可以增加发生事故时披露的行驶数据的公信力，更好的进行事故的分析和定责。

本项目改变了原有的企业全权管理自身行车数据的方式，将政府存储、监管和企业自身存储数据相结合，极大的简化了原有的数据求证流程，提高了行政与司法监察的效率。政府和企业共同维护数据，增加了行车数据的公信力，更容易的使用数据进行责任判定。

本项目可以简化政府与企业之间为了获取数据而进行的行政流程，协助政府下辖的相关交通管理部门的监察工作，节约人力成本和时间开销，帮助政府节约时间和资金。

## 6.2企业数据分析及广告投放

采用联邦学习、同态加密、差分隐私的保护策略，在保证用户隐私和车企核心数据不会泄露的情况下，进行数据的共享，来方便不同车企之间进行数据交流共和分析。同时采用区块链技术，确保分享数据的真实性，方便车企进行智能驾驶等相关领域的训练和检验。本项目打破了原本企业和企业之间沟通的壁垒，减弱了企业之间对于数据分享的担忧与不信任，给予了不同企业之间合作的可能性。使得企业在竞争之外，可以进行更多的合作，来共同促进自身科技的发展与技术的进步。

本项目可以帮助企业之间更好的共享数据，打破企业之间的数据孤岛，避免不同企业因为缺乏信任而不敢共享数据造成信息壁垒，从而节约企业使用数据的开销，促进企业合作，还可以帮助广告公司更好的进行广告归因，节约采集和分析数据的成本。

## 6.3政务数据共享

采用预言机和主从链进行数据跨域协同和共享，针对各个地区或部门尚不相同平台和标准体系，建立数据共享的桥梁，对不同对数据格式、数据可读性、质量标准建立协同机制，同时进行身份认证和隐私保护，避免数据泄露，进而加快推动政府数据共享，深入发掘政务信息资源潜力，有利于全面释放数据红利，引领激发技术红利、制度红利和创新红利。

本项目顺应《政务信息资源共享管理暂行办法》，可以用于辅助政府共享平台建设，协助各部门业务信息系统向政务内网或政务外网迁移，并接入共享平台。有效打破“信息孤岛”，大大提升政务信息共享管理和约束效力，帮助政府构建全国信息资源共享体系。

## 6.4个人隐私保护

通过主从链技术对数据的访问方进行限制、记录和公开，可以更好的方便群众进行监督，避免用户数据被不相关方进行买卖和滥用。本项目旨在创建一个人人皆可查看自身数据是否被访问，被何机构访问的公开系统，让公众拥有更多的对自身数据被使用状况的知情权，从而让公众自发的监督、限制不良机构对公民隐私的泄露。

本项目旨在响应国家政策和法规，可以用来帮助政府更好的对公众隐私进行保护，减轻大数据时代公众对自身隐私泄露问题的担忧与不安，提升公众生活的幸福感。

## 结束语

从特斯拉车主维权到滴滴上市争议，再到出台监管车辆数据的法规，车辆数据正在成为新一代的数字石油，成为现代型企业必不可少的数字资产。但是，目前车辆数据的管理存在监管难的问题，体现在监管部门难以监管数据、用户难以维护数据的所有权。同时，车辆所在的边缘网络的开放性可能导致相关的安全认证问题。此外，车辆数据的管理还存在协同难的问题，体现在数据所有方难以与数据使用方协作完成任务，导致域内协同难、跨域协同难以及计算协同难的问题。

为解决上述问题，项目提出基于区块链的车辆数据监管和任务协同平台。针对车辆数据监管难的问题，项目提出基于双层多链的车辆数据监管流通架构；针对车辆身份认证难的问题，项目提出基于区块链的车辆身份授权认证机制；针对车辆数据协同难、计算资源协同难的问题，项目在基于双层多链的车辆数据监管流通架构的基础上，分别提出基于数据预言机的车辆数据域内协同机制、基于跨域预言机的车辆数据跨域协同机制、基于计算预言机的车辆计算协同机制；为验证和集成上述关键架构和技术，项目研发基于区块链的车辆数据监管和任务协同平台，实现车辆数据在区块链生态网络中高效可控全流程流通。