**MNMP: 基于区块链的车辆数据监管和共享平台**

**项目计划书**

项 目负责人 林怡静

项 目 成 员 王苗苗、李璜琦、柴泽

所 属 高 校 北京邮电大学

所 在 院 系 计算机学院

指 导 教 师 高志鹏

**摘 要**

随着5G等新一代通讯技术的发展，车辆与终端之间的数据传输变得愈发便捷。车辆可以将行驶过程中产生的行驶状态、位置路况等数据传输到云端保存和记录，以进行用户行为分析。

但是，随着车辆安全事故频发以及行驶数据的缺失和滥用问题不断曝光，让公众不禁对自身数据隐私性和记录的准确性产生了疑虑。特斯拉维权事件引发公众对车企公布的行驶数据的不信任，监管部门查验数据真实性的过程也困难重重。

为解决上述问题，基于区块链的车辆数据监管和共享平台（MNMP: Musk Need Mask Platform）项目提出面向车联网的车辆数据共享和监管解决方案，该方案包含如下部分。首先，为解决车企的数据垄断导致的监管困难问题，本项目提出基于主侧链的车辆数据访问架构。其次，为解决主链、侧链、车企数据中心三者的数据访问问题，本项目提出基于链上链下协同的车辆数据跨链方案，让数据资产全流程价值流通。最后，为最大化利用驾驶数据和保护数据隐私，本项目提出基于联邦学习和差分隐私的驾驶行为分析方案，利用联邦学习、区块链和同态加密实现驾驶数据在车辆之间交互的安全性。

本项目从监管层面和企业层面出发，解决监管难和数据共享问题，上述问题是二者亟需解决的问题，因此具有较大的发展空间和盈利空间。

目录

[1.项目介绍 1](#_Toc73089125)

[2.技术路线 6](#_Toc73089126)

[2.1基于主侧链的车辆数据访问架构 6](#_Toc73089127)

[2.2基于链上链下协同的车辆数据跨链方案 8](#_Toc73089128)

[2.3基于联邦学习和差分隐私的驾驶行为分析方案 9](#_Toc73089129)

[3.项目创新点 11](#_Toc73089130)

[3.1打破数据垄断车企数据垄断，解决监管难题 11](#_Toc73089131)

[3.2打破数据孤岛，维护数据私密性 11](#_Toc73089132)

[3.3高效利用数据，实现数据价值最大化 11](#_Toc73089133)

[4.预期成果 11](#_Toc73089134)

[4.1成果产出 11](#_Toc73089135)

[4.2知识产权归属 11](#_Toc73089136)

[5.可行性分析 12](#_Toc73089137)

[5.1技术路线可行性 12](#_Toc73089138)

[5.2项目先进性 12](#_Toc73089139)

[5.3可靠性分析 13](#_Toc73089140)

[6.应用场景 13](#_Toc73089141)

[6.1监管及事故分析 13](#_Toc73089142)

[6.2交通流量分析及预测 13](#_Toc73089143)

[6.3智能驾驶学习 14](#_Toc73089144)

[7.项目规划 14](#_Toc73089145)

[8.创新策略 14](#_Toc73089146)

[8.1政府数据监管 14](#_Toc73089147)

[8.2企业数据分析及广告投放 15](#_Toc73089148)

[8.3企业数据保存 15](#_Toc73089149)

[8.4个人隐私保护 16](#_Toc73089150)

[9.项目预算 17](#_Toc73089151)

# 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，从而方便日后的查找和检验。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。2021年3月9日，一段“女子站特斯拉车顶维权”的视频，引发人们对特斯拉刹车失灵的激烈讨论。而特斯拉目前对外公布的数据并不完整，无法看出事故发生的真正原因，而其公布的行驶速度的真实性也屡屡遭到质疑。尽管特斯拉声称，存储后的数据采用加密技术记录，无法直接读取、修改、删除相关数据，但这并不足以让公众信服。因此，如何将行驶数据进行存储，来确保用户信息不会被滥用和篡改，便成了如今亟待解决的问题。目前特斯拉可以提供EDR套件查询软件来连接车辆，查询行驶数据并生成相应的数据报告，但其需要1200美元且目前仅在北美发售，并不能很好的解决现存的问题。

为了解决上述问题，将区块链技术引入车辆数据的存储和共享中成为了一种可行的办法。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。中汽协就发布了汽车数据可信存证区块链平台，该平台采用的方案是企业每隔一定时间上传数据指纹。数据指纹不包含原始数据的任何有效信息，只是将车企数据中心的原始数据包通过单向加密算法处理，生成一段若干字节的数据指纹，指纹上传后不可篡改。如果车企遇到数据公信问题，可以调出车企本地数据库的数据包，与事故发生时上传到区块链存证平台上的数据指纹做比对，即可得出真实结论。这种方法虽然能够保护企业数据的私密性、安全性和可靠性，但是并不能够保证数据的完整性。一旦企业方面关键数据缺失，依旧会造成事故无法定则。所以，更好地利用现有的存储资源，既保证数据的完整性、又保证数据的真实性、隐私性成为当务之急。

目前的解决方案有很多，在文献[1]中，为了应对大量数据的产生，使用了车辆云进行存储。但是其需要有受信任的中心化机构提供大量的存储空间，且敏感信息也极易从中心化的云泄露。文献[2]中将原本的车联网数字取证（VDF）进行改进，提出了基于区块链的安全车联网数字取证方案（SVDF）。该方案可以实现车联网数据上传者的匿名身份认证和针对数据访问者的访问控制，并借助区块链记录所有数据上传和访问的记录，保证记录的公开可验证性和不可篡改性。同时，SVDF 还可以抵抗恶意数据上传者的篡改攻击和恶意数据访问者的非法请求。但是文献中对数据的在区块链上具体存储和查询方式缺乏设计，可以用于加密数据却无法解决存储的难题。文献[3]中引入分布式哈希表（Distributed Hash Tables, DHT），使用区块链为分布式数据提供便捷的存储和保护。在设备将数据上传到分布式哈希表之前，首先发布“存储交易”到区块链表明某设备的数据将存储在分布式哈希表的地址，区块链验证交易并记录设备的身份和存储地址。而当设备从分布式哈希表请求数据时，发布区块链的“访问交易”，区块链验证请求者。如果交易经过验证并写入一个块，存储数据的分布式哈希表节点将发送数据给请求者。该文献实际是将区块链取代了传统意义下的“受信任的第三方”，进行数据存储和访问，该文献可以对数据进行分布式存储和检索，但是没有能够被信任的机构或个人提供存储空间。文献[4]中，将数据的处理和存储的任务交给了路侧单元（RSU），车辆由传感器数据组成的区块链副本最终被分发并存储在RSU中，这解决了集中式数据存储的潜在安全风险。但是当需要存储大量行驶数据时，路侧单元的存储能力便受到了挑战。此外，一旦有路侧单元遭到物理破坏，便有可能造成关键数据丢失，而进行数据备份又会对路侧单元的存储能力提出更高的要求，因此，该方案并不能够很好的满足对巨大存储能力的需求。

本项目将当前存在的问题归纳如下：首先是车辆数据存储中心化，易篡改、难溯源；其次是监管部门难以获取原始数据；再者是数据存储资源有限；最后是数据隐私保护问题。

为解决上述问题，我们提出面向车联网的车辆数据共享和监管方案，该方案包含如下部分。

首先，为解决车企的数据垄断导致的监管困难问题，本项目提出基于主侧链的车辆数据访问架构，该架构定义车企和监管部门的主侧链交互规则，以车企为主链、监管部门为侧链，构建车联网中的区块链交互架构，以解决数据篡改问题。

其次，为解决主链、侧链、车企数据中心三者的数据访问问题，本项目提出基于链上链下协同的车辆数据跨链方案，该方案基于跨链预言机和阈值签名，保证数据在主侧链、数据中心之间流转时的真实性和一致性，让数据资产全流程价值流通。

最后，为最大化利用驾驶数据和保护数据隐私，本项目提出基于联邦学习和差分隐私的驾驶行为分析方案，利用联邦学习、区块链和同态加密实现驾驶数据在车辆之间交互的安全性，利用差分隐私实现驾驶行为模型参数在车企之间交互的安全性，在保护车企数据资产的同时实现数据最大化利用。

本项目针对上述解决方案进行相关检索，检索内容如下表1、表2、表3所示。项目方案吸收了相关文献中解决方案的优势，基于项目背景，改进了方案中不足的地方，使用区块链结合跨链预言机、阈值签名、联邦学习、同态加密、差分隐私等技术，设计了适用于5G车联网环境下的车辆数据共享和监管方案。

表1基于区块链的车联网存储解决方案

|  |  |  |
| --- | --- | --- |
| 方法 | 优点 | 缺点 |
| 文献[1]使用了车辆云进行存储。 | 简单，方便管理 | 数据过于集中化，容易泄露，对集中化设备带宽需求高，容易受到攻击。 |
| 文献[2]采用SVDF进行数据加密，并存储在区块链。 | 保护数据隐私 | 文中没有提到由何种机构如何提供存储空间，以及区块链相关共识算法和存储后如何搜索数据，并未提供存储在区块链上的可行办法。 |
| 文献[3]引入分布式哈希表，使用区块链存储。 | 方便数据搜索查找，提供可行在区块链上的数据存入、搜索和记录过程的方法 | 需要“受信任的第三方”，本质上与受信任的中心化存储方存在相似性，缺少保证第三方能够去中心化和被信任的机制。 |
| 文献[4]将数据的处理和存储的任务交给了路侧单元。 | 解决了集中式数据存储的潜在安全风险 | 路测单元易受损害且存储能力有限，无法保证大量数据的存储和备份需求。 |

表2跨链解决方案

|  |  |  |
| --- | --- | --- |
| 方法 | 优点 | 缺点 |
| BTC-Relay 中继跨链实现了比特币和以太坊之间的单向跨链通信。 | 允许以太坊用户使用比特币支付 | 只能单向通信，无法互联互通 |
| Wanchain 创世块降临，其在以太坊的所有机制之上引入跨链的交易机制。 | 实现了链上资产的匿名性及隐保护的功能。 | 更多的用于虚拟货币资产而非数据信息。 |
| Polkadot 正式上线，其提供的互操作性和跨链通信实现了用户能够在链之间传递信息。 | 实现了跨链数据和信息的传输，打破了区块链数据孤岛的状态。 | 更多的适用于现有的商业化区块链之间的交互，不适用于政府监管和隐私数据保护。 |

表3联邦学习解决方案

|  |  |  |
| --- | --- | --- |
| 方法 | 优点 | 缺点 |
| FedAvg联邦平均算法[5] | 适合求解非凸问题，可以基于非独立同分布数据进行学习 | 没有收敛性保证、在当数据是异构的情况下可能会发散、不考虑恶意节点 |
| FedProx算法[6] | 在有界设备不相似假设下，提供了异构系统下的收敛性保证 | 中心化的机器学习算法、不考虑恶意节点 |

**参考文献**

[1]Olariu, S.; Khalil, I.; Abuelela, M. Taking vanet to the clouds. Int. J. Pervasive Comput. Commun. 2011, 7, 7–21.

[2]LI Meng, SI Chengxiang,ZHU Liehuang.Secure vehicular digital forensics system based on blockchain [J].Chinese Journal on Internet of Things,2020,4(02):49-57.

[3]KANG J, YU R, HUANG X, et al. Blockchain for Secure andEfficient Data Sharing in Vehicular Edge Computing andNetworks[J]. IEEE Internet of Things Journal, 2019, 6(3):4660-4670.

[4]ZHANG X, CHEN X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Adhoc Network[J]. IEEE Access, 2019, 7(99): 58241-58254.

[5]H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Aguera y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proc. 20th Int. Conf. Artificial Intelligence and Statistics, 2017, pp. 1273–1282.

[6]T. Li, A. K. Sahu, M. Sanjabi, M. Zaheer, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” in Proc. Conf. Machine Learning and Systems, 2020.

# 2.技术路线

由于车企存储的车辆数据量大、安全级别高，无法直接共享给其他公司用以数据分析。不仅如此，当前车辆数据存储于车企管控的数据中心，数据的真实性和有效性难以保证，使得监管部门要求车企提供数据时，无法直接确认数据的真伪，需要执行一系列复杂的行政行为。因此，本项目针对车辆数据的访问困难和不真实的问题，研究基于区块链的车辆访问方案，该方案分为三个部分，分别是基于主侧链的车辆数据访问架构、基于链上链下协同的车辆数据跨链方案和基于联邦学习和差分隐私的驾驶行为分析方案，以提高数据真实性和可用性，改进对车企的监管手段。

2.1基于主侧链的车辆数据访问架构

传统基于云计算的数据存储方式使得车企在监管和数据共享方面拥有极大的议价权利。在面对监管时，监管难以辨别车辆数据的真伪，执法的行政成本提高；在数据共享时，其他公司几乎无法获得车辆数据，形成数据孤岛。为解决车企的数据垄断导致的监管困难问题，本项目提出基于主侧链的车辆数据访问架构，如图1所示，该架构以多个车企构成主链，以监管部门构成侧链，共同维护车辆数据。主侧链之间的交互规则包括，车企所在的主链无法访问监管部门所在的侧链数据，侧链不能随时随地获取主链数据。不仅如此，由于车辆数据的宝贵性，车企的数据不直接上传于区块链网络中。此外，监管部门的资源有限，无法存储所有车企的车辆数据。因此，基于主侧链的车辆数据访问流程如下。

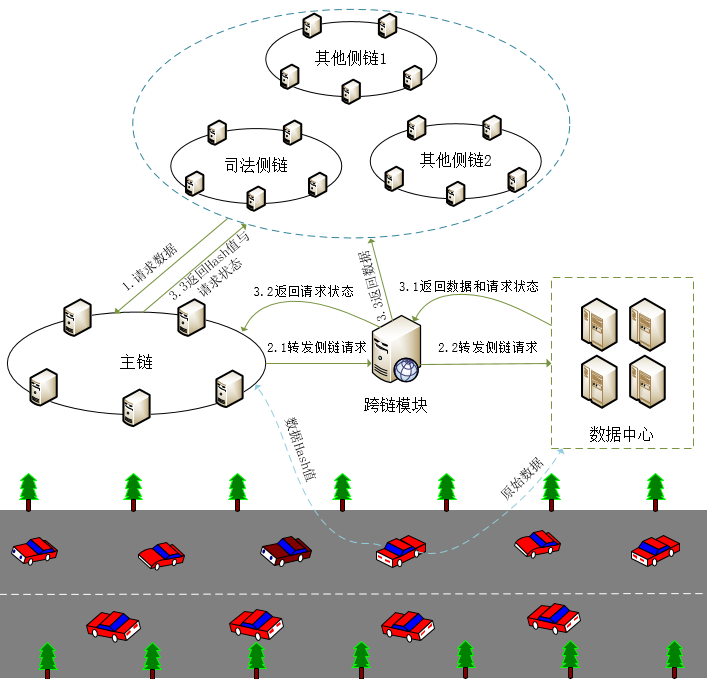


图1基于主侧链的车辆数据访问架构

（1）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哈希值作为交易数据提交到主链共识。由于数据存储于云数据中心，主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。

（2）当侧链中的监管部门需查验车辆数据以判断事故责任时，首先监管部门需在侧链中提交数据访问请求，使得侧链中的其他监管部门本地留有记录以达到从上而下制衡监管部门行政权力的目的。侧链主体的监管特殊性，使得其可采用DPoS共识算法，从当前交易的上级部门中选择节点作为记账节点，以提高区块链网络的吞吐量；其次，由于区块链本身是封闭的网络，主侧链之间无法主动获取数据，本项目利用基于链上链下协同的车辆数据跨链方案帮助侧链与主链交互，使得侧链可访问主链的数据。

（3）监管部门利用链上链下协同方案转发侧链的数据访问请求的同时，需要向主链写入交易数据，包括车辆编号、请求时间等，并将该交易提交主链车企主体的共识，以达到从下而上制衡监管部门行政权力的目的。

（4）主链的车企监听到侧链监管部门的交易请求后，根据交易内容向监管部门返回数据哈希值的同时，到链下的数据中心获取交易映射的数据，并通过链上链下协同方案将数据状态和数据分别回调给主链和侧链，以在主链和侧链上进行双重验证，以保证数据请求的可靠性。

通过主侧链之间的数据请求和访问，在保证车辆数据真实性和一致性的前提下，实现监管部门对车辆数据的监管以及对监管部门行政权力的限制。

2.2基于链上链下协同的车辆数据跨链方案

为保证车企数据的安全性以及限制监管部门的行政权力，本项目采用基于主侧链的车辆数据访问架构，由车企和监管部门各自组成区块链，以起到数据隔离和相互监督的作用。但是，由于区块链是封闭的网络，无法主动与外部世界交互，使得主链和侧链之间、主链和链下数据中心的数据无法互联互通，形成数据孤岛。为解决主链、侧链、车企数据中心三者的数据访问问题，本项目提出基于链上链下协同的车辆数据跨链方案，在满足主侧链交互规则的前提下，打破主侧链、数据中心的数据孤岛，实现车辆数据在主链、侧链以及链下全流程流通。

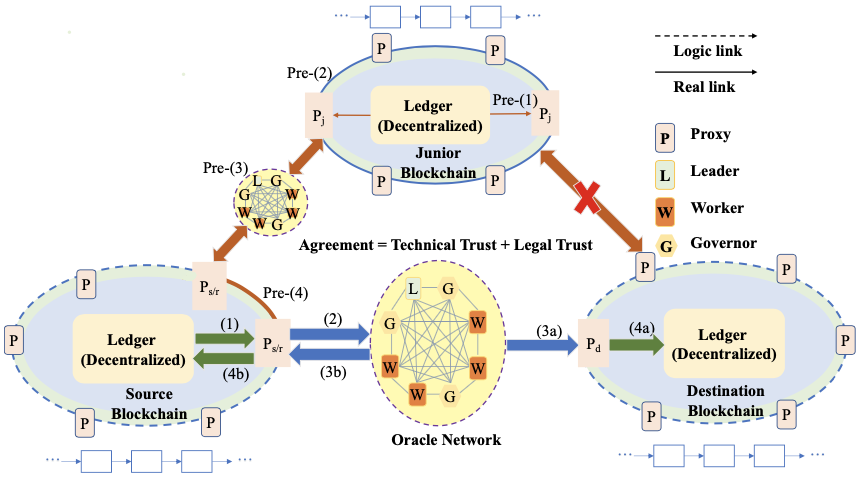


图2基于链上链下协同的车辆数据跨链方案

基于链上链下协同的车辆数据跨链方案采用跨链预言机作为主侧链、主链和链下数据中心交互的桥梁。由于数据存储于车企的云数据库中，主侧链交互的是与属性数据，因此跨链预言机网络可由其他车企组成。基于链上链下协同的车辆数据跨链方案的具体流程如下：（1）跨链预言机首先监听侧链的跨链数据访问请求，该数据请求被写入跨链预言机网络。（2）跨链预言机网络在本地共识后将该请求提交到主链参与共识，并将数据哈希值回调给侧链。（3）跨链预言机监听主链针对该跨链请求的共识后，到链下数据中心获取数据，将回调数据写入跨链预言机网络以及回调给侧链网络，将数据请求状态写入主链网络，进行二次共识。与资产跨链不同，主侧链之间的跨链交互只需要保证数据在不同区块链网络之间流转，因此无需考虑交易原子性等特性。

2.3基于联邦学习和差分隐私的驾驶行为分析方案

当前，自动驾驶赛道聚集大量的车企，车辆驾驶数据成为车企最宝贵的资产之一。随着车辆数据集的增大，针对用户行为的分析模型将更加准确，更能促进自动驾驶技术的落地。但是，一般来说，车企不愿意也不可能将车辆数据共享给他人，一方面是出于商业利益的考量，另一方面是出于保护用户隐私的目的，这导致车企本身形成数据孤岛。不仅如此，当前车辆的数据通过云中心转发共享，将带来巨大的带宽成本，导致车辆响应时延增加。为最大化利用驾驶数据和保护数据隐私，本项目提出基于联邦学习和差分隐私的驾驶行为分析方案。

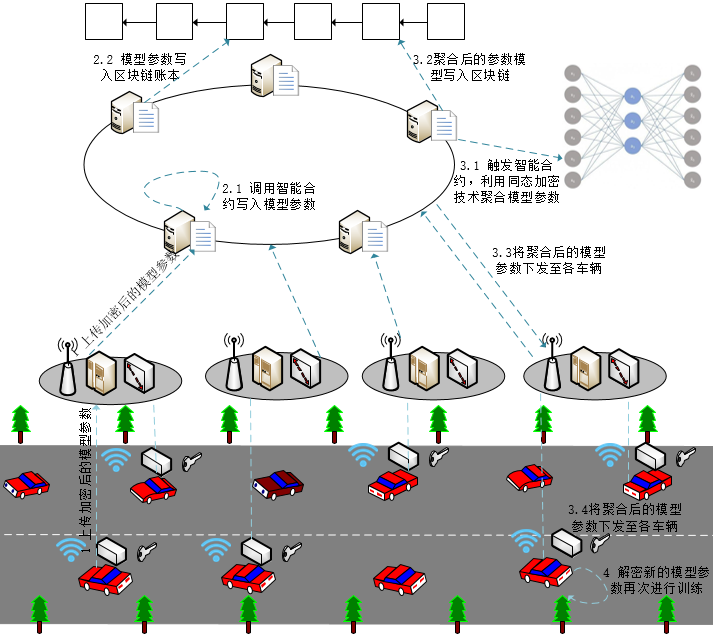


图3基于联邦学习和差分隐私的驾驶行为分析方案

为解决车企内车辆驾驶信息数据孤岛的问题，本项目设计了基于区块链的联邦学习交互方案。区块链的去中心化、不可篡改、安全可验证等特性能够很好的解决联邦学习中中心服务器单节点故障、不可信等问题。联邦学习中中心服务器的职责由联盟链担任，其功能以智能合约的形式部署在区块链节点上，车联网中的汽车作为设备端，在中心服务节点的协调下共同训练模型，模型参数作为区块链交易打包成区块。而区块链中交易的透明性对于各车辆的隐私性很不友好，更新信息向中央服务器报告的时候，虽然梯度是原始信息的映射，但是攻击者可以通过与模型交互，对更新信息中的敏感部分，如梯度信息、参数特征等进行逆向推理，反推出参与方本地数据信息，因此，我们将各车辆训练的模型参数进行加密后上链，中心服务功能的智能合约利用同态加密的特性将各车辆的模型参数进行加权聚合，再分发至各车辆，经过多轮迭代后得到一个趋近于集中式机器学习结果的模型。

# 3.项目创新点

3.1打破数据垄断车企数据垄断，解决监管难题

本项目提出基于主侧链的车辆数据访问架构，定义车企和监管部门的主侧链交互规则，构建数据交互架构，解决数据篡改问题。

3.2打破数据孤岛，维护数据私密性

本项目提出基于链上链下协同的车辆数据跨链方案，该方案基于跨链预言机和阈值签名，保证数据在主侧链、数据中心之间流转时的真实性和一致性，让数据资产全流程价值流通。

3.3高效利用数据，实现数据价值最大化

本项目提出基于联邦学习和差分隐私的驾驶行为分析方案，利用联邦学习、区块链和同态加密实现驾驶数据在车辆之间交互的安全性，利用差分隐私实现驾驶行为模型参数在车企之间交互的安全性，在保护车企数据资产的同时实现数据最大化利用。

# 4.预期成果

4.1成果产出

1）提交《区块链和联邦学习在车联网中的应用》研究报告1份，完成对当前业界相关技术的调研和技术先进性分析。

2）投稿1篇反映研究成果的高水平论文。

3）提交1个专利交底书。

4）提交1个原型系统

4.2知识产权归属

1）研制过程中由项目组独立完成的研究成果(如专利、论文或软件平台的独立 模块等)，其知识产权由项目组独立拥有。

2）共同研究形成的软件平台原型系统的知识产权由参与单位共同拥有。在权益方一致同意的情况下，推荐以开放源代码的形式共享。

3）由本项目共同研究的成果可能产生的经济收益，根据各参与方贡献的大小，经协商后按比例分配。

4）研究过程中，涉及到企业内部数据的，均按照企业内部资产管理方式进行合作。

企业承诺为研究单位提供真实数据，研究单位必须承诺保证企业数据安全。推荐企业和研究单位签订保密协议。

# 5.可行性分析

5.1技术路线可行性

1）项目路线清晰可行

项目遵循“理论研究-技术攻关”的总体思路，对车联网场景下的可信数据共享及分析模式进行研究，依托区块链、物联网、联邦学习等前沿技术，建立了完整的系统架构，系统角色权限及分工明确，数据业务流程闭环，可以为技术研究和技术应用提供充分支持和保障。

2）定位行业前沿研究和实际需求

本项目以车联网可信交互、安全共享、高效融合、场景协同等前沿问题为抓手，提出相应的研究方案和技术方案。理论研究、技术攻关与实际需求紧密结合，推动车联网数据治理和共享技术水平走向业界前列。

3）研究基础和团队实力雄厚

研究团队深耕区块链领域，曾发表或录用多篇论文，申请区块链相关专利若干，拥有丰富的学术经验以及良好的实践能力。

4）研究团队合作紧密

研究团队在大数据、区块链、人工智能等领域有着紧密的合作，团队成员之间有非常密切的联系和交流，团队融合度良好，具体良好的研究基础和丰富的项目经验和合作基础，在人员配置方面是完全有能力达成既定的研究目标

5.2项目先进性

本项目面向车辆数据可信数据监管及隐私数据分析的需求，聚焦车联网中的数据流转生命周期，融合区块链、预言机、联邦学习等领域前沿技术和研究成果，研制面向车联网的车辆数据共享和监管方案。

项目设计基于区块链的数据可信授权、验证、共享网络架构，以预言机、智能合约、联邦学习等技术为基础，将数据收集、数据验证、数据分析过程解藕，研究数据可信交互和授权方案，构建多机构主体业务数据验证、授权共享平台，以解决车联网中跨域异构数据互通和可信问题、跨域数据加密及访问权限控制问题以及跨域数据的的高效交互和链上链下互通问题，同时结合差分隐私和分布式机器学习技术，解决互不信任主体间的多方数据共享分析问题，保障车联网跨域业务中数据的安全高效共享。

5.3可靠性分析

项目采用去中心化的点对点的分布式网络架构，可以有效防止由于中心服务器宕机产生的单点故障，同时数据更新及维护基于区块链的共识算法，保证恶意节点无法对数据进行篡改，有效防止脏数据上传，保障数据真实可信。

项目访问基于主侧链模式的车辆数据访问架构，可以基于智能合约对访问角色权限进行细粒度管理，降低了不同个体之间的勾兑成本；同时项目系统会对接入行为进行追踪记录，既保证数据在不同区块链及企业数据中心之间顺畅流通，又能防止监管部门角色权力滥用。

项目数据分析采用基于联邦学习的分布式机器学习系统，将数据留存在本地，结合差分隐私技术，防止恶意方根据模型反推隐私数据，在不暴露私域流量的前提下打通信息屏障，为隐私保护下的数据分析协作提供了条件。

# 6.应用场景

6.1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。

6.2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。

6.3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。

# 7.项目规划

|  |  |
| --- | --- |
| 时间 | 完成内容 |
| 2021.5.1-2021.5.28 | 完成项目申报表和申报ppt相关内容 |
| 2021.5.29-2021.6.14 | 进行项目调研，调查主侧链、跨链、联邦学习和差分隐私等研究现状和技术实现路线 |
| 2021.6.15-2021.8.14 | 进行相关实验内容和流程设计和实验环境准备，设计主侧链交互实验、跨链预言机的实现和联邦学习的实现思路。 |
| 2021.8.15-2021.11.1 | 基于上述成果，研发原型系统，进行技术仿真和实验验证，分别完成每个模块的实验和仿真内容。 |
| 2021.11.2-2021.12.1 | 整合实验代码，模拟在政府、企业相关平台下的数据存储和访问控制。 |
| 2021.12.2-2022.1.1 | 优化相关模块，形成相应报告。 |

# 8.创新策略

8.1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。

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

8.2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。

本项目可以出售给相关车企，来帮助车企之间更好的共享数据，避免不同企业因为缺乏信任而在智能驾驶的训练中进行重复的测试，从而节约企业的开销，促进企业合作。

8.3企业数据保存

将现有车企的数据存储空间进行联合，根据汽车销量要求存储空间占比，并将数据切割成数据块，进行加密和分布式存储，同时借用Proofs of SpaceTime原理进行数据存储状况检查。从而使得任何企业无法直接知晓自身数据存储位置，无法在本地直接篡改、删除相关行车数据来逃避监管。同时，通过不断扫盘还可以实时确认车企是否良好的保存行驶数据，有没有数据篡改、丢失或损坏。本项目将原有的数据保存方法和分布式存储相结合，联合大多数企业来共同保管、运维数据，改变了原有企业自己负责自己数据的存储方式，极大的避免了数据遭到篡改和丢失的可能性，使得公布出来的数据完整、真实，更易得到公众的信任。

本项目可以出售给政府相关监察部门，从而使得在发生事故时可以公布完整、真实的数据信息，更好的协助法律判决，避免因数据问题在社会舆论上造成不良的影响。

8.4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。

本项目可以出售给政府相关监察部门，以便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。

# 9.项目预算

**项目名称：Musk Need Mask Platform 金额单位：20万元**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **预算科目名称** | **合计** | **主办方资金** | **其他来源资金** |
| **（1）** | **（2）** | **（3）** | **（4）** |
| 1 | 一、资金支出 | **20** | **20** | **0** |
| 2 | （一）直接费用 | **15** | **15** | **0** |
| 3 | 1.设备费 | **5** | **5** | **0** |
| 4 | （1）购置设备费 | **0** | **0** | **0** |
| 5 | （2）试制设备费 | **0** | **0** | **0** |
| 6 | （3）设备改造费 | **0** | **0** | **0** |
| 7 | （4）设备租赁费 | **5.4** | **5.4** | **0** |
| 8 | 2.材料费 | **0** | **0** | **0** |
| 9 | 3.测试化验加工费 | **0** | **0** | **0** |
| 10 | 4.燃料动力费 | **0** | **0** | **0** |
| 11 | 5.出版/文献/信息传播/知识产权事务费 | **5.1** | **5.1** | **0** |
| 12 | 6.会议/差旅/国际合作交流费 | **1.4** | **1.4** | **0** |
| 13 | 7.劳务费 | **0.8** | **0.8** | **0** |
| 14 | 8.专家咨询费 | **2.7** | **2.7** | **0** |
| 15 | 9.其他支出 | **284.6** | **0** | **0** |
| 16 | （二）间接费用 | **5** | **0** | **0** |
| 17 | 二、资金来源 | **20** | **20** | **0** |
| 18 | （一）主办方资金 | **20** | **20** | **/** |
| 19 | （二）其他来源资金 | **0** | **/** | **0** |