



AMO 白皮书

车辆数据市场的区块链

© 2018 AMO Foundation. All Rights Reserved.

目录

第 1 章 概述	6
1.1 车辆数据管理问题	6
1.1.1 非系统性的数据收集	6
1.1.2 低效且无补偿的数据供应	7
1.1.3 缺乏数据安全和隐私保护	7
1.2 AMO解决方案和目标	7
1.2.1 标准化数据收集和车辆数据作为交易单位	8
1.2.2 数据供应的补偿体系	8
1.2.3 将数据安全和隐私保护应用在区块链中	8
1.3 AMO如何不同：创建未来车辆生态系统	9
第 2 章 AMO 市场	10
2.1 AMO市场如何运作	10
2.2 AMO 市场参与者	11
2.3 AMO 区块链	13
2.4 AMO 平台	14
第 3 章 技术细节	16
3.1 车辆数据收集	16
3.1.1 车辆数据收集的局限性	17
3.1.2 车辆数据收集	18
3.1.3 车辆数据的储存/传输	19
3.2 AMO区块链结构	20
3.2.1 要求	20
3.2.2 共识算法	21
3.2.3 时间序列数据	22
3.2.4 智能数据合约	23
3.3 数据隐私和安全	24
3.3.1 遵守安全准则	24
3.3.2 个人信息加密	24
3.3.3 加密后的通信和加密后的数据存储	25
3.4 车辆数据交易	25
3.4.1 数据所有权和访问数据	25
3.4.2 数据所有权	26
3.4.3 通过端到端加密的权力分散	26
3.4.4 加密后或未识别数据的交易	26
3.4.5 AMO 度量管理系统	26
3.5 报酬系统	27
3.5.1 生产数据报酬	27
3.5.2 参与作节点报酬	27
3.5.3 区块生成报酬	27
第 4 章 服务例子	28
4.1 车辆维护服务	29
4.2 车辆事故分析服务	29
4.3 准确的保险费率计算服务	30
4.4 车辆充电和停车服务	30
4.5 音乐和视频流服务	31
4.6 本地动态地图服务	31
4.7 个人信息的安全监督	32

4.8 数据移动服务	32
4.9 开放参与赏金	33
第 5 章 逆向车辆数据应用通证分配	34
5.1 AutoCrypt®	35
5.2 AuthentiCA®	36
5.3 Penta CryptoWallet™	37
第 6 章 路线图	38
第 7 章 团队成员与顾问	39
第 8 章 法律问题	42
参考文件	43

内容概要

AMO是旨在创建并运营可共享和交易车辆数据的AMO市场的区块链项目。

AMO 市场 = 车辆数据市场

随着互联车辆、电动车辆、自动驾驶车辆和智能车辆的迅速发展，车辆行业的交易需要分散开放的市场。AMO市场将支持所有利益相关者之间的数据交易。

AMO市场的参与者，无论是车辆用户、车辆制造商还是车辆服务提供者，均为车辆行业内的利益相关者。这些人同时作为价值共享和创造循环中的数据生产者和数据消费者参与AMO市场。这是一种技术辅助式经济系统，AMO市场建立在AMO区块链上，且支持数据的公平估值和报酬分配。数据的价值按照供求来调整，AMO通证就是其支付手段。¹

车辆数据不再局限于少数特定的狭隘用途，而是经过数据所有者的明确同意，成为一种有益于AMO市场其他参与者的共享资产。当服务提供者或车辆制造商希望访问车辆用户数据时，与数据所有者协商适当的授权，得到数据所有者的许可以后便可经由良好的授权系统使用。以确保信息安全，所有信息和敏感数据均使用加密技术予以保护。

AMO市场的目标是创造一个环境，使车辆数据和信息不再由少数挑选的公司使用和持有，而是通过合法安全的过程和交易来使用和共享。因此，车辆数据将成为公共资产，回归相关方所享受的更有价值和更优化的服务。

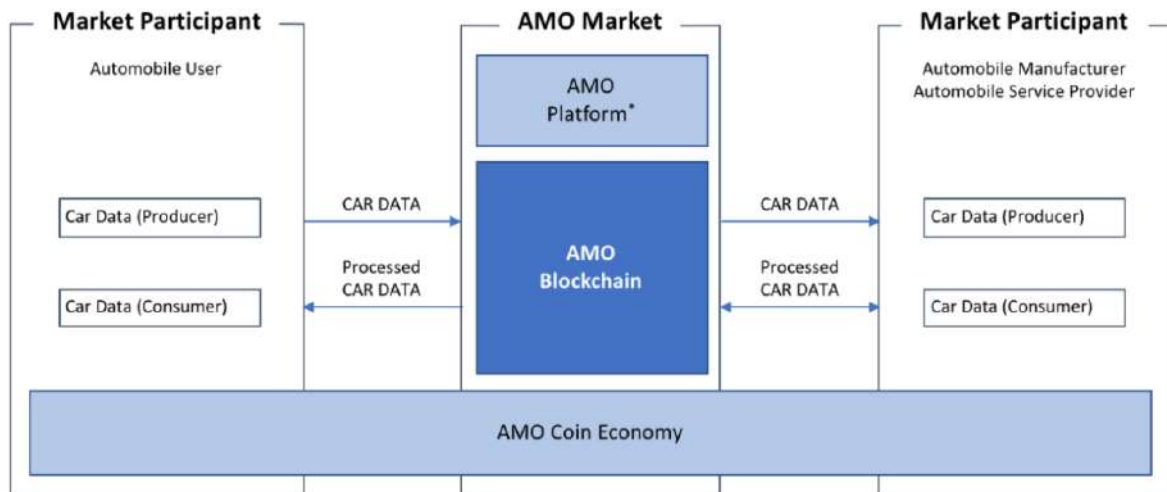


图 1. AMO 结构概述

¹ AMO通证是指AMO代币和AMO货币。AMO代币随后将转换为AMO通证。

* AMO平台：AMO平台使用AMO区块链提供AMO市场运营。该平台支持参与者之间的通信，并管理运营政策和IT系统，包括软件。

第 1 章 概述

在快速发展的车辆行业中分散后的车辆数据市场的需要

今天的车辆正在生成和处理无法预料的数据量。车辆行业的进步带来了互联车辆、电动车辆和自动驾驶车辆等的发展。车辆现在正成为信息的移动中心，而不仅仅是一种将某人从A点带至B点的交通工具。这种车辆新概念正在改变我们对时间、金钱管理、娱乐和整体生活的思考方式。

推动智能车辆革命五个关键元素是安全性、平台、自动化、互联、电气化-缩写为SPACE。

每个元素均促成用于提高车辆服务质量的车辆数据。在车辆行业中，车辆数据在支持服务发展方面发挥核心作用；因此业务成果的成功趋向于由车辆数据的可用性决定。这就是迫切需要既能顺利促进车辆数据共享，又能保证车辆数据和市场本身的安全性和可靠性的车辆数据市场的原因。

AMO市场是一个以AMO区块链和AMO平台为中心的车辆数据市场。AMO区块链和AMO平台将由安全专家通过将区块链技术应用于Penta Security Systems 已有的技术（即AutoCrypt®、AuthentiCA®和Penta CryptoWallet™）进行开发。

AMO市场将通过从车辆数据中获得附加价值并激励AMO市场的参与和互动，为重振车辆行业做出重大贡献。

1.1 车辆数据管理问题

由于收集、存储和共享的困难性，因此车辆数据的价值虽然非常宝贵和昂贵，但是有限。

车辆从开始至结束 — 从车辆制造商开始至报废设施结束的整个路程中产生了各种各样的数据。这些数据反映了车辆的寿命周期，并能够用于改善车辆制造、车辆租赁、车辆共享、保险和度假行业的状态。但是，目前仍不存在共同商定的标准或系统以系统性地收集、存储和使用这些数据。有时，独立服务提供者可能会利用车辆数据，但他们往往忽视了从车辆数据中获得更多价值的可能性，且无法充分利用车辆数据。

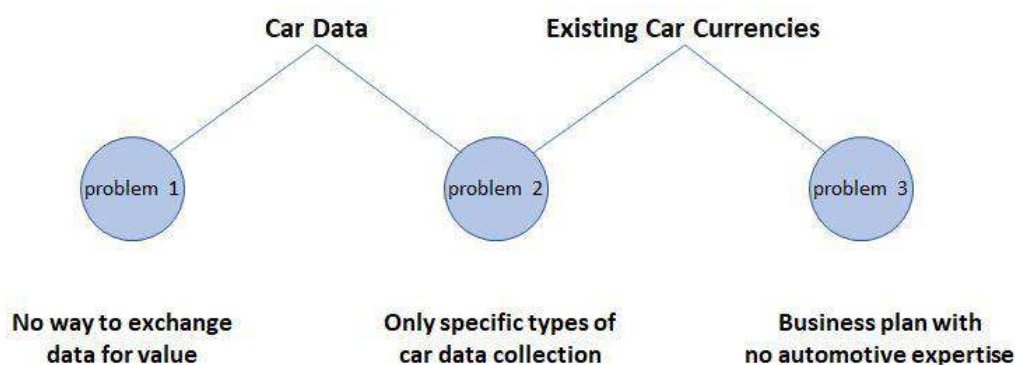


图 2. 车辆数据和现有车辆首次通证分配存在的问题

1.1.1 非系统性的数据收集

虽然有关车辆使用、设备和构件的外部 and 车内来源的数据早已可用，但数据的系统收集和管理极为有限。大多数车辆制造商和服务提供者均依靠个性化系统进行数据存储和管理。只有采用最近引进的互联车辆，才使得电动车辆和自动驾驶

车辆能够使用通过与道路、车辆、行人以及整体交通基础设施互动而产生的V2X数据。随着电动车辆行业的进步，不仅车内数据，而且有关充电和电池相关的见解均视为有价值的信息。智能车辆的进步也增加了对各种应用程序产生的用户数据的需求。

问题是所收集的车辆数据的格式因车辆制造商和服务提供者而异。在大多数情况下，数据在技术上与其他系统不兼容，且无法共享。虽然法律限制可能导致了缺乏数据共享，但共享车辆数据的主要障碍是缺乏通用技术框架。由于缺乏收集数据的公共协议，参与者无法正确了解其个人信息的使用方式以及和保护的全知权。此外，即使个人同意根据合同协议与服务提供者共享其数据，但其贡献也并未得到公平补偿。

目前，没有任何机构或公司能够全面收集每个部分中生成的有价值的车辆数据，从车辆操作过程包括通信系统，内部和外部系统以及应用层

1.1.2 低效且无补偿的数据供应

因为车辆数据的获取，服务提供者开辟了新的商机，可为车辆用户提供个性服务。但是，由于车辆用户和服务提供者（例如，车辆制造商、车辆服务开发商、车辆保险提供者等）之间的数据交易关系不平等，因此也无法奖励车辆用户所作的贡献。一般，个人数据仅作为识别各人的证据，而非相当于任何生成的附加值。特别是，无法提供高级数据保护的服务提供者很容易以超出协议范围滥用客户数据，甚至泄露数据。

因此，有必要建立一个值得信赖的平台，以量化车辆数据的价值并为数据贡献提供公平的补偿体系。通过这种方式，数据提供者和数据消费者均将从交易中保持获益。

1.1.3 缺乏数据安全和隐私保护

车辆数据能够基于是否包含个人信息进行分类。包含个人信息的车辆数据必须按照数据主体的权利以提供充分隐私保护的方式收集和存储。特别是，此类数据的任何分配均须遵循保护协议和过程。例如，在无适当安全措施的情况下收集和存储诸如日常驾驶模式等敏感数据可能会引发有关隐私的社会问题。解决目前依靠便携式设备（数码安全卡等）存储车内生成的重要数据、通过车内网络传输的数据以及其他车辆相关数据的方法至关重要。

任何包含私人信息的信息都必须在完成数据的非识别化²以获得充分隐私保护后才能共享和使用。

不共享或使用的车辆数据仅具有潜在价值，无任何实际价值。由于目前缺乏有关车辆数据的规则和安全指南，因此车辆数据的共享和使用只能视为风险，而非创造价值的机会。

1.2 AMO解决方案和目标

AMO为车辆数据提供安全可靠的市场。

AMO的愿景是建立一个安全可靠的环境，以共享建立于我们有关车辆行业的专业知识的车辆数据。实现这一愿景的第一步是解决如下详细解释的车辆数据行业的当前问题。

² 非识别化是指从数据集中删除可用于识别某人的所有个人可识别信息的过程。这通常通过假名化来执行，其中实名全部或部分由符号、通证或临时身份证明取代。这两种方法均依赖于加密技术。

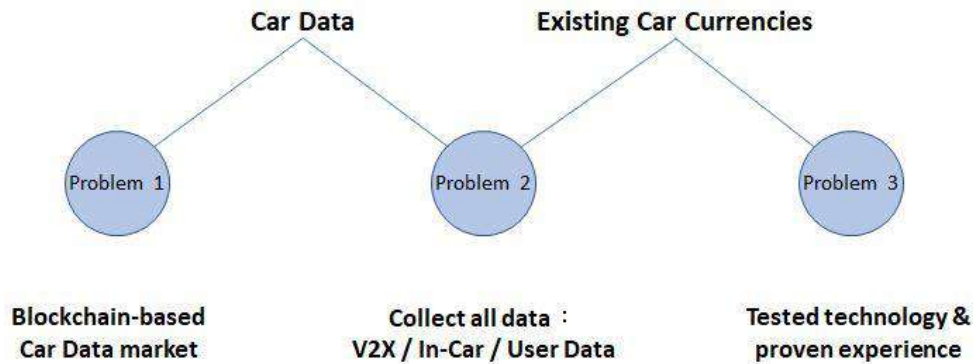


图 3. 现有问题的解决方案

1.2.1 标准化数据收集和车辆数据作为交易单位

为解决非标准化数据收集系统的问题，开发了一系列硬件和软件数据收集器用于部署AMO。其中包括硬件数据收集器（AMO Data Collector™）、移动应用程序（AMO 移动钱包™）、车辆娱乐信息（IVI）应用程序、嵌入车辆远程信息处理系统的软件以及用于V2X设备的软件数据收集器（AMO车辆钱包™）。这些工具将针对涉及车辆的所有三个级别的数据：V2X数据、车内数据和用户数据执行数据收集。

从车辆的首次注册至车辆所有事故记录或已参与服务的记录至车辆的最终报废的车辆整个寿命周期，均可系统性地收集车辆数据以用作各种广泛用途，而不论车辆的国界或类型。此外，将发布车辆数据的公开规范，以便任何人均能够参与并为车辆数据市场做出贡献。这将防止任何一家公司或组织垄断车辆数据以用作商业工具。为此，类似AMO区块链的公共区块链是允许该类型开放式数据共享所必需的。

数据不仅包括由驾驶员和其他车辆用户生成的数据（车辆数据），还包括来自在车辆行业内提供任何类型服务的商家的二次生成数据（处理后的车辆数据）。车辆数据和处理后的车辆数据的规范也将得到定义并通过区块链共享，以鼓励使用。

1.2.2 数据供应的补偿体系

AMO为用户提供了一个AMO市场，这是一个基于区块链的车辆数据市场，也是一个促进数据生产者和消费者之间进行交易的环境。AMO市场仅提供交易环境，无数据所有权。车辆数据成为一种商品，数据生产者和消费者致力于确定车辆数据的价值。任何涉及提供车辆数据的基于市场的价值交易均将获得AMO通证的合理补偿。

该补偿模式激励市场参与者提供车辆数据。未来，预计通过补偿模式激励的主动市场参与和数据生成将鼓励甚至无活跃车辆制造业的国家建立和发展他们的车辆相关业务。

1.2.3 将数据安全和隐私保护应用在区块链中

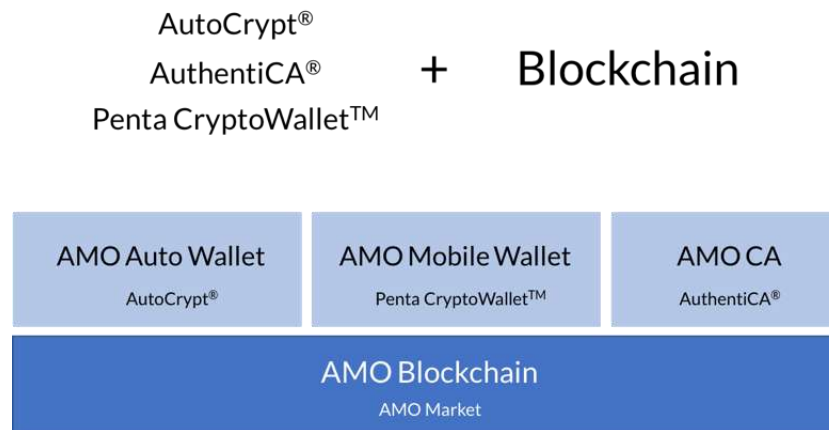
用户同意共享的车辆数据将存储于在AMO区块链中，并附上有关交易、数据所有权和数据使用权的其他相关信息。与数据通常存储在区块链中的方式类似，所有这些数据均将存储在区块中。包含敏感个人信息的原始数据将予以加密、去识别化并碎片化，以保证最高安全性。这种分散式存储方法将通过AMO区块链的对等存储功能实现。通过对等存储，构成区块链节点的计算机和物联网设备将提供数据存储资源，以换取适当的补偿。因此，通过该有机系统创建的存储空间可能是无限的。

只有通过合法数据所有者的授权，才能根据数据购买者的要求解密分散式存储的数据。AMO平台有助于验证凭证和权限的过程。但是，AMO平台仅涉及对等网络的连接，且仍无法完全访问数据。

1.3 AMO如何不同：创建未来车辆生态系统

对车辆和IT行业的深入了解和技术理解以及实践经验对建立车辆数据市场至关重要

由于车辆是由几万多个物理部件和数以亿计行代码组成的复杂机器，因此掌握大量内部和外部数据极其困难。而且，创建一个安全可靠且基于区块链的生态系统并不简单。为了克服这两个挑战，开发商的核心团队必须具备车辆和运输技术、车辆相关敏感信息的管理以及具有集成安全性的一般系统开发方面的综合知识和技能。在无成熟结果和能力的情况下建立和维持基于区块链技术的生态系统几乎不可能。AMO拥有建立AMO市场所需的最佳技能和经验。



- Penta Security Systems Inc 了解车辆和交通基础设施：作为智能交通系统（ITS）开发工作的一部分，Penta Security 2007 年以来一直与韩国政府和主要车辆制造商合作运行 AutoCrypt®项目。继韩国世宗、骊州和华城市中的自动车辆复合体的成功建设和运营后，该项目将扩展至在首尔、济州和大邱建设类似的智能道路。
- 在车辆和智能对象之间建立和运行稳定的基础设施需要物联网环境中的成功经验。Penta Security 在物联网环境优化的解决方案方面的专业知识体现在其开发的 AuthentiCA®，这是一款面向智能车辆、智能工厂、智能能源和智能家居环境的基于云的认证授权服务。
- 通过使用区块链技术，开发了 Penta CryptoWallet™和 AMO Data Collector™。

具有成熟结果和技术的路线图不仅只是工程中的一项计划或空洞愿景，现在正在进行之中。

第 2 章 AMO 市场

所有参与者均受益的车辆数据交易的良性循环

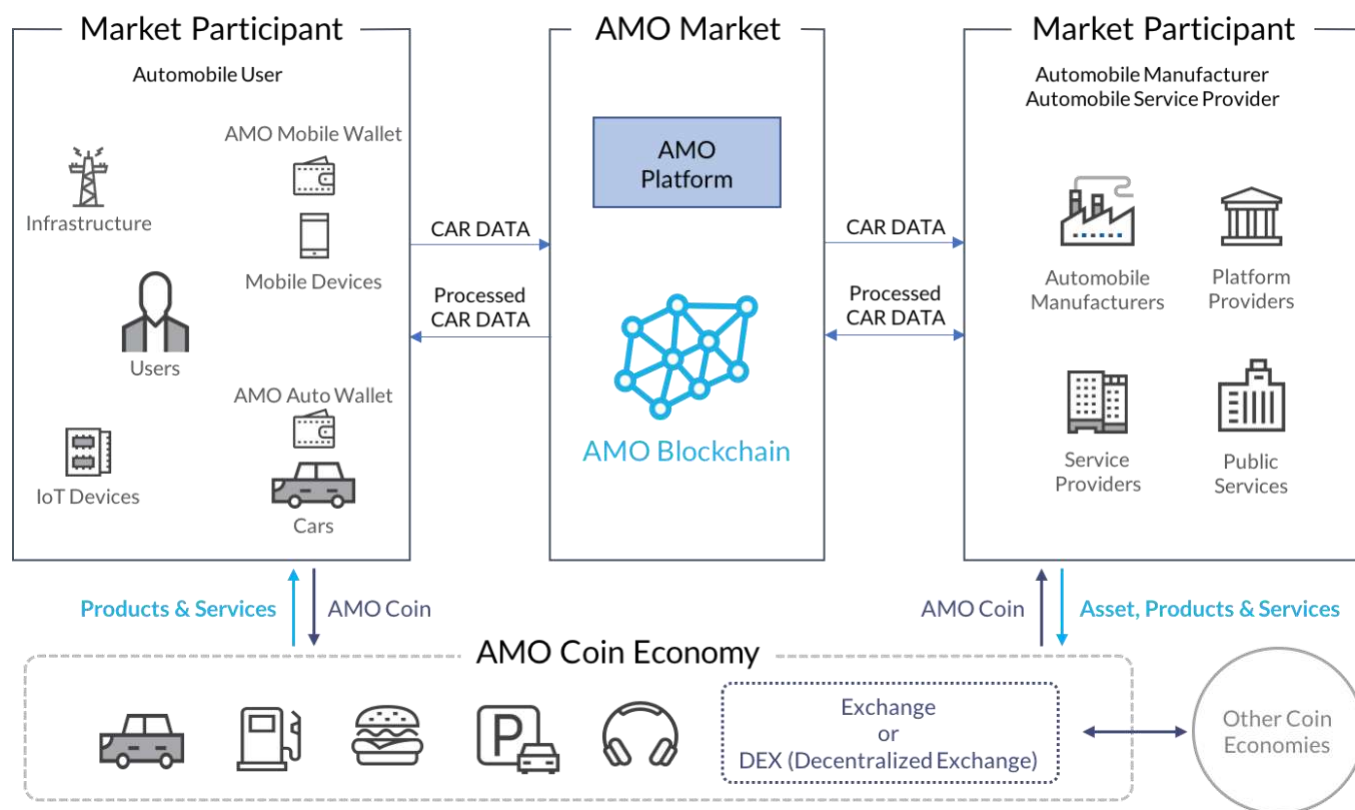


图 4. 市场与AMO通证经济

AMO市场提供了一个开放平台，其中任何人都可以参与共享车辆数据或将其处理为更有价值的输出。AMO市场基于区块链技术构建并在设计时考虑到端到端安全原则，在稳定运营的同时保证数据安全，并保护市场参与者的权利和个人数据。作为车辆数据经济生态系统的一部分，AMO市场参与者在为车辆行业的进步做出贡献的同时获得经济报酬。

2.1 AMO市场如何运作

所提供数据的市场价格根据供求规律确定

AMO市场利用区块链技术改善当前由众多利益相关者组成的车辆生态系统。AMO市场的核心特征是车辆数据的自动供应和适当补偿。车辆用户、制造商、服务提供者 and 车辆行业的所有其他参与者均将能够提供车辆数据并根据市场价值获得其贡献的适当补偿。

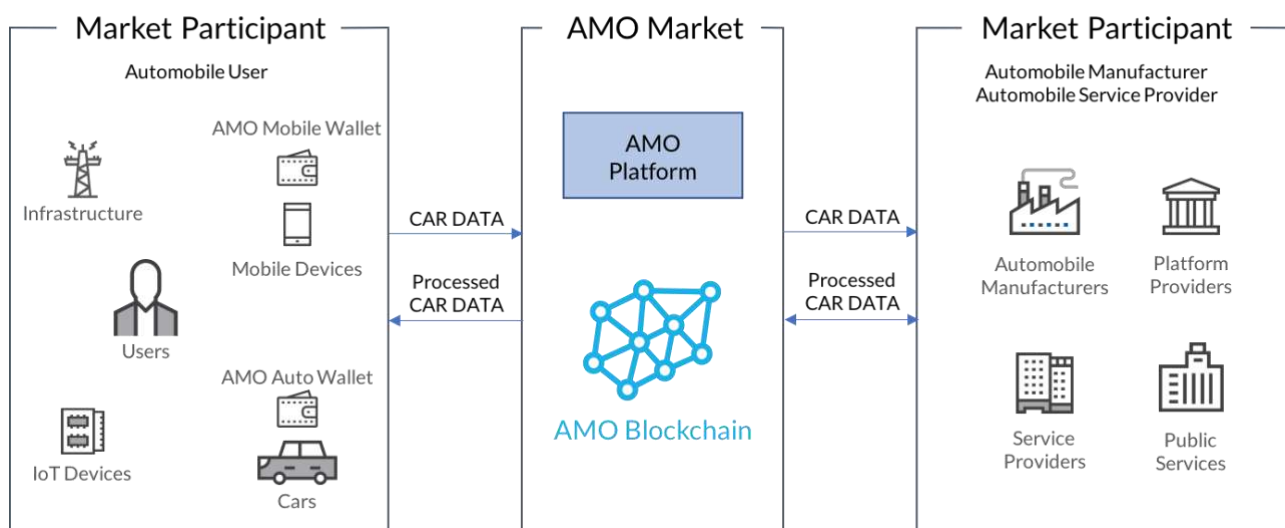


图 5. AMO 市场

AMO市场由AMO区块链及其支持功能、AMO平台组成。市场参与者承担数据生产商和消费者的角色。将在市场中交易通过初始车辆使用以及二次输出生成的车辆数据（处理后的车辆数据），数据的市场价值将根据供求规律以及通过各种由AMO平台提供的支持系统收集的信息确定。

2.2 AMO 市场参与者

每个参与者均同时以数据生产商和消费者的身份（“产消者”）为市场活动做出贡献。

通过可以轻松连接至车辆OBD-II端口的AMO数据收集器™设备，结合安装在车内的AMO移动钱包™智能手机应用程序和AMO车辆钱包™软件，车辆用户能够收集车辆数据以供在AMO市场上共享。车辆用户已同意共享的车辆数据随后将存储在AMO区块链中，以根据所提供数据的价值换取AMO通证。通过使用这些AMO通证，车辆用户能够购买由参与AMO市场的制造商和服务提供者提供的各种产品和服务。

数据生产商能够共享数据并根据评价后的数据价值获得AMO通证形式的补偿。数据消费者能够通过以AMO通证支付评价后的价值获得提取和使用数据的权利。

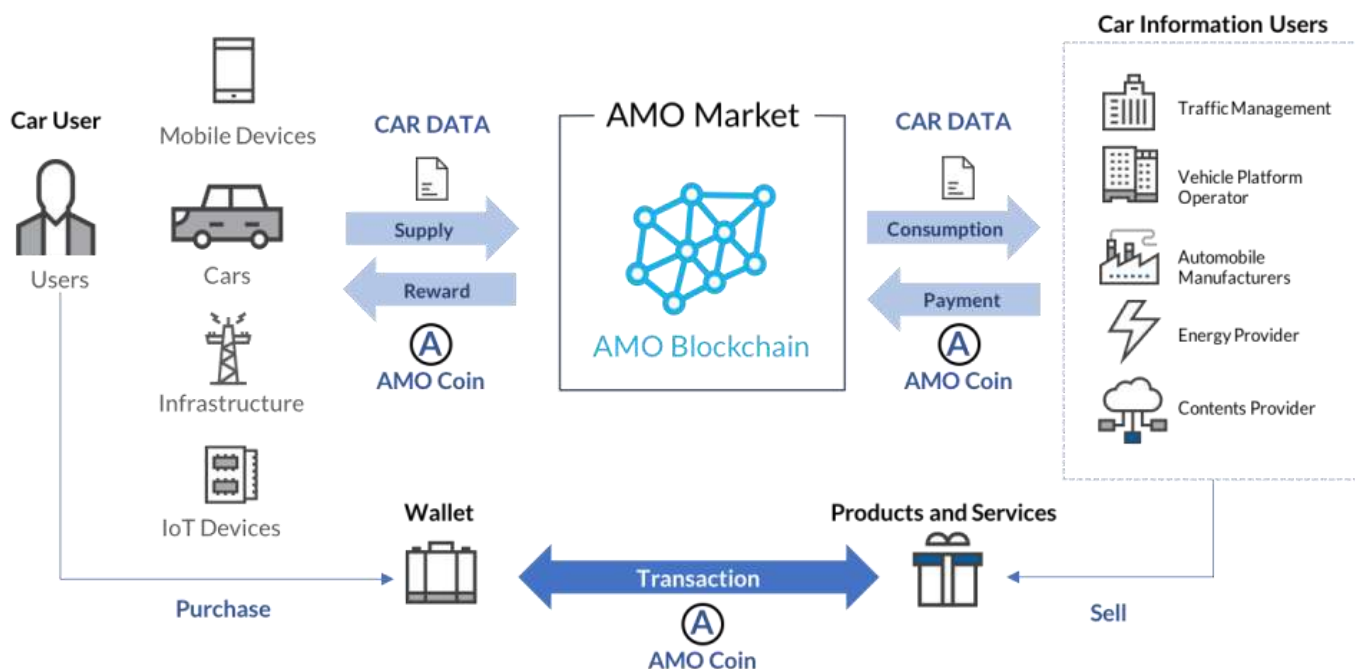


图 6. 车辆用户/数据生产商的车辆数据寿命周期

车辆制造商和服务提供者能够购买记录在AMO区块链中的车辆数据，以便为车辆用户提供最新服务。服务提供者、制造商和维护公司也可以反过来在AMO区块链中提交二次处理后的数据并根据该数据价值接收AMO通证。

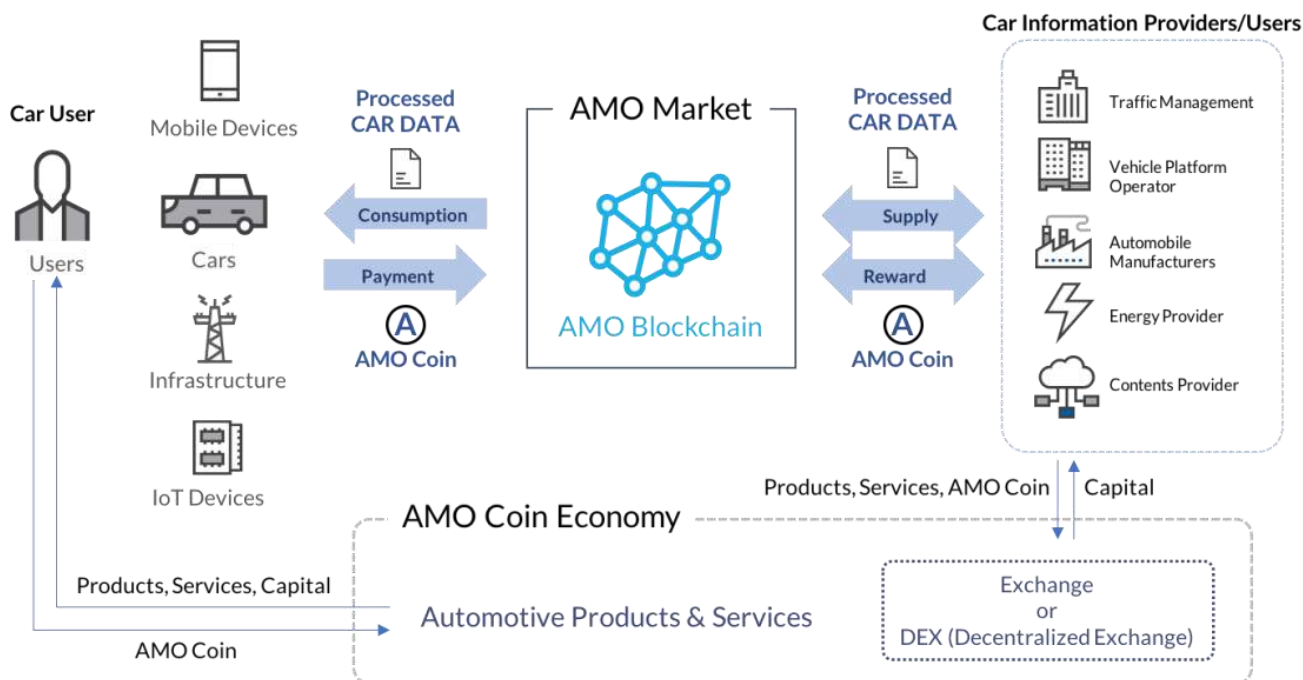


图 7. 制造商、服务提供者和数据生产商处理后的车辆数据的寿命周期

因此，车辆用户、车辆制造商和相关服务提供者成为AMO市场的供应商和消费者。通过这种提供和接收数据和补偿的结构，创建了一个车辆数据更加丰富和和市场得到激活的循环。进行中的循环反过来有助于AMO市场的增长。

2.3 AMO 区块链

AMO 区块链是专为存储和交易车辆数据而优化的区块链。

AMO区块链是AMO市场所有参与者参与的网络。如下所示，无论是车辆用户、制造商还是服务提供者，所有参与者均共享AMO区块链上的车辆数据。

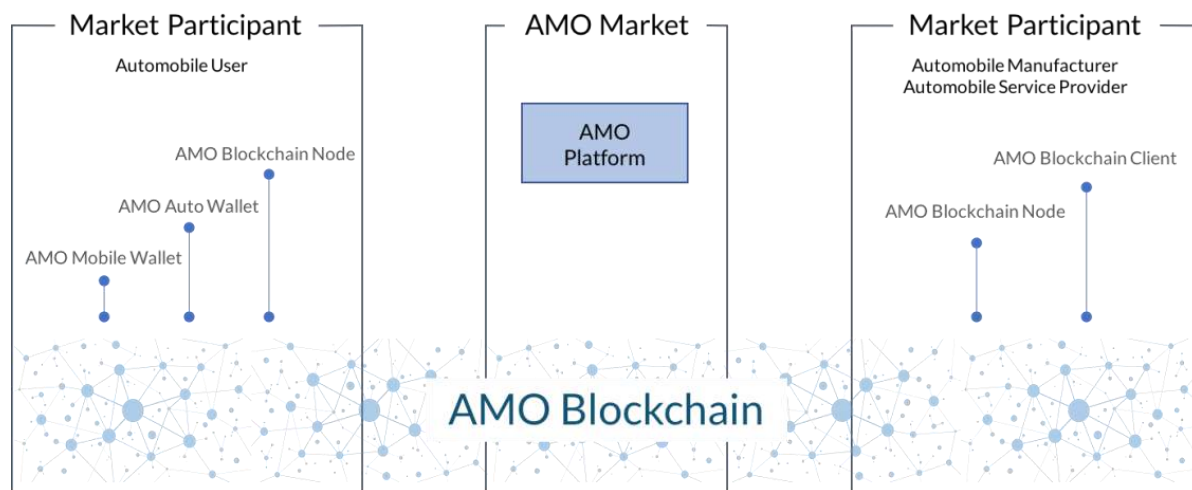


图 8. AMO 区块链连接至每个市场参与者

为了进行交易，AMO市场参与者通过AMO区块链客户端和AMO钱包连接至区块链。作为市场参与者，数据生产商获得AMO通证以作为其共享和交易的数据的报酬。另一方面，参与区块链作为AMO区块链节点的市场参与者能够按其在维持区块链的贡献比例获得报酬。这些报酬用于区块生成或为AMO区块链的对等存储提供资源。

车辆用户生成的车辆数据和来自服务提供者处理后的车辆数据将上传至网络上并存储在AMO区块链中。此时，所有通信均予以加密，且任何交易细节、数据所有权和使用权均以与在典型区块链上完成存储的相似方式作为区块一并存储和管理。另一方面，包含个人信息的原始数据在存储在对等存储之前将予以加密和去识别化。存储在对等存储中的此类数据已碎片化并以分散式方式存储在多个区块链节点中。通过这种方式，即使向对等存储的物理访问已妥协，所获得的数据也不存在任何价值，因为这些数据不完整，因此无法解密。

车辆数据和处理后的车辆数据均直接与AMO区块链接触，且在任何情况下均不会通过AMO平台。AMO平台负责策略和软件的管理以及参与者身份验证所需的密钥管理和证书颁发，而不涉及任何车辆数据管理。

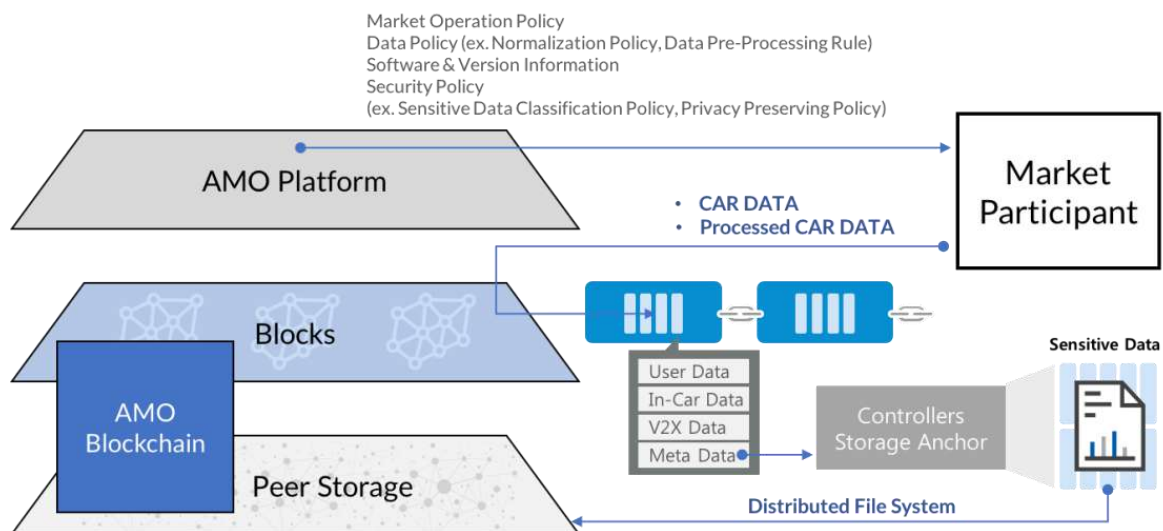


图 9. AMO 区块链的数据存储结构

连接至AMO区块链的AMO钱包³包含AMO区块链节点功能。这些功能将允许未来具有网络和计算能力的其他物联网设备连接节点，提高AMO区块链的可伸缩性。

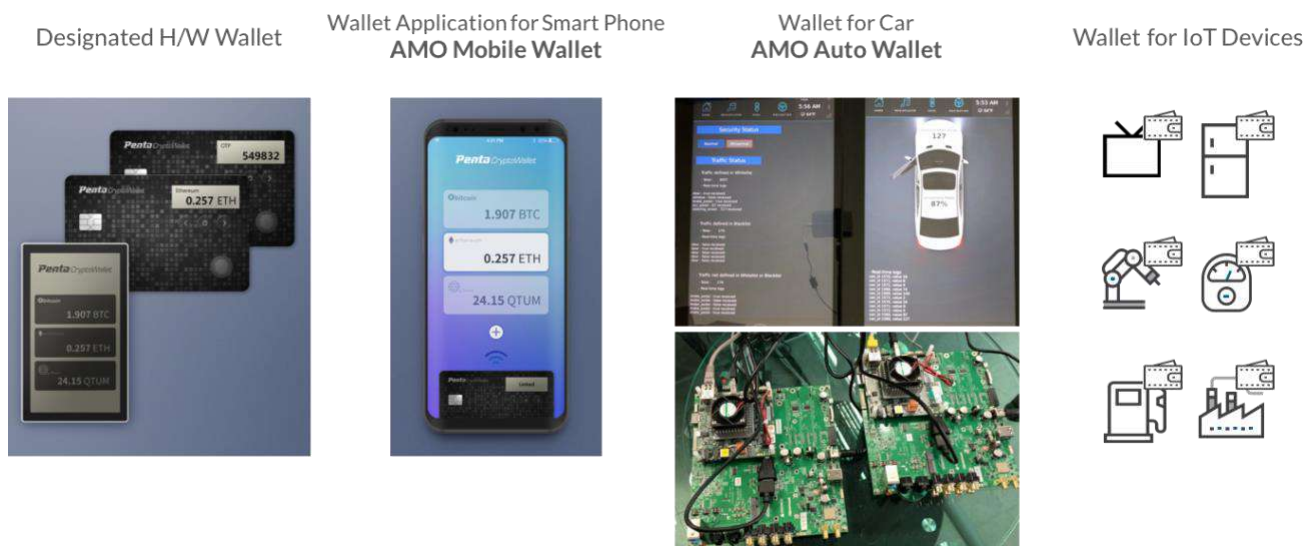


图 10. AMO 钱包

2.4 AMO 平台

AMO 平台负责车辆数据市场的运营和管理功能

AMO平台本质上是由AMO市场运营策略、数据策略、安全策略和软件组成的IT系统。它还负责参与者之间的社区运营以及AMO区块链运营的系统支持。主要构件包括AMO CA、AMO通证管理系统、AMO度量管理系统、AMO节点管理系统等。

³ AMO钱包同时用作AMO区块链的客户端和节点。AMO钱包可以是AMO移动钱包™或车辆钱包™。

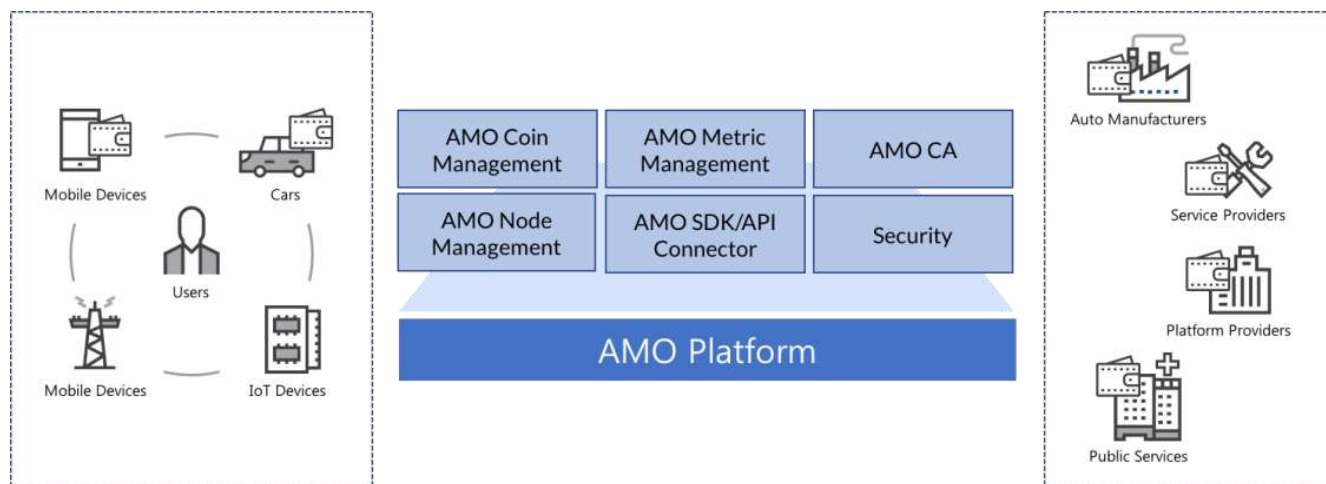


图 11. AMO平台的概念图

尽管车辆数据需求上升，但仍未收集和共享数据的主要原因之一是车辆数据标准因车辆制造商而异。为解决这个问题，每个制造商的车辆数据标准均将转换为符合国际标准。虽然这可能会重新排列数据值的顺序，但不会更改数据本身的价值。此外，还将为车辆数据用户提供丰富的应用程序编程接口（API），这意味着数据购买者将能够方便地从AMO区块链访问车辆数据。

车辆数据的价值取决于市场数据的供应和需求。AMO平台使用机器学习和合作协议来计算最优估价，以在进行补偿时避免市场平台数据的数量与质量问题。

AMO平台不干预市场参与者与AMO区块链之间的车辆数据流和处理后的数据流。该平台支持通信，以实现AMO市场的平稳运营，其中包括策略和软件分配、密钥分配和参与者身份验证证书。

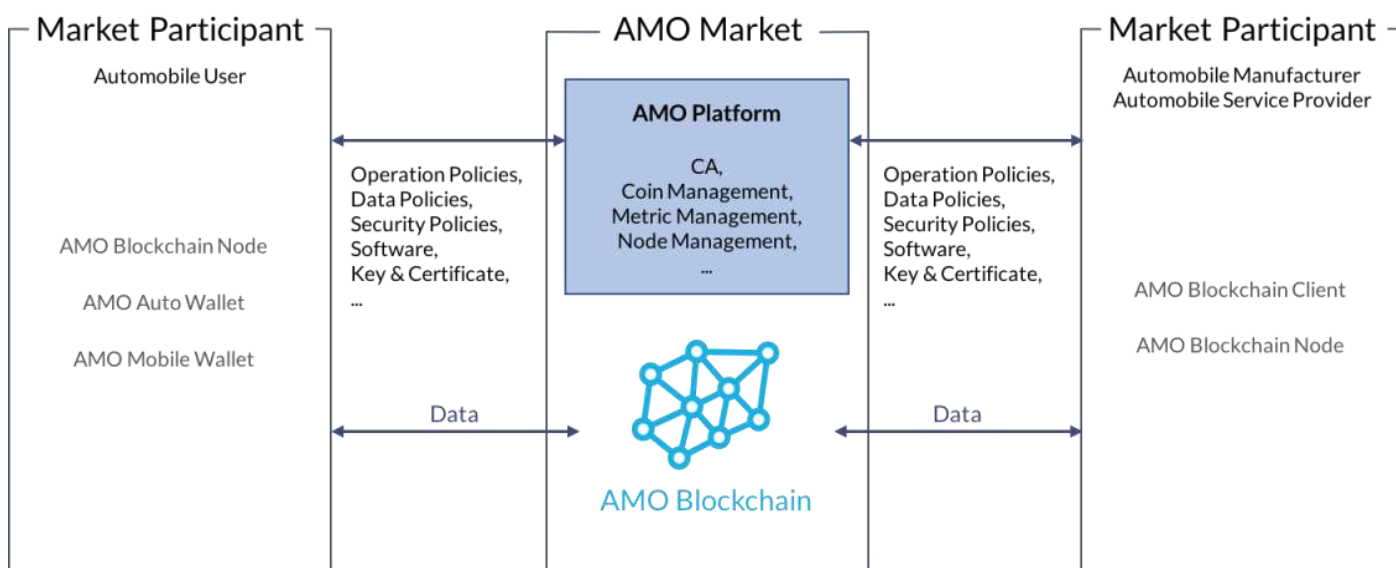


图 12. AMO 平台与数据流

作为运营支持的一个例子，AMO平台调解数据所有权和使用权。加密后的车辆数据只能由已购买数据的人员解密。AMO平台促进数据生产商和数据消费者之间的互动，以管理拥有数据所有权的人员。

第 3 章 技术细节

3.1 车辆数据收集

收集自动驾驶车辆系统、网络和应用程序的车内数据/V2X数据/用户数据

互联车辆、电动车辆和车内信息娱乐系统的发展已使得自动驾驶车辆成为现实。AMO市场中交易的车辆数据将包括生成与车辆相关的所有数据，其中包括从与下一代车辆互动的环境中收集的信息。

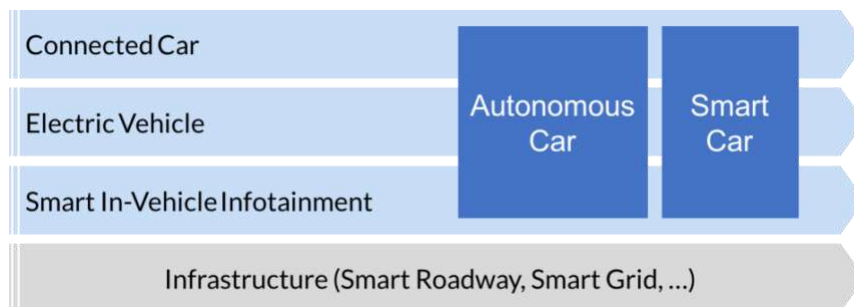


图 13. 车辆数据中技术的范围

车辆数据包括来自车辆三个层面的所有数据。

	Layer	Data	Example
Connected Car	Network	V2X Data	Traffic information Communication information Location information
Electric Vehicle	System	In-Car Data	Vehicle maintenance information Charging information Battery information Sensor detection information
Smart In-Vehicle Infotainment	Application	User Data	Data usage Location information regarding applications Billing information

图 14. 车辆数据的技术范围和类别

存在三类数据：内部数据或来自车辆本身的数据（车内数据）、通信数据（V2X数据）以及来自使用应用程序的数据（用户数据）。

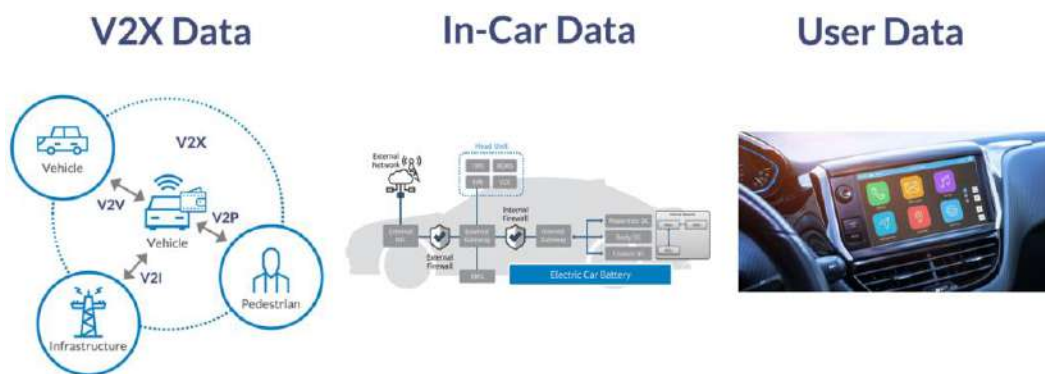


图 15. 车辆数据

V2X数据是指通过有线和无线网络基础设施在车辆、道路和其他关联节点之间传达的交通数据。根据数据交易中涉及的相关方，可将V2X数据分类如下。

- V2V（车辆对车辆）：车辆之间的通信，例如，联系紧急车辆
- V2I（车辆对基础设施）：车辆和道路基础设施之间的通信，例如，即将转红灯的交通灯
- V2D（车辆对设备）：车辆和移动设备之间的通信，例如，车辆网络共享
- V2P（车辆对行人）：车辆和行人之间的通信，例如，正在过马路的行人

V2X数据包括通过外部设备和交通基础设施之间的车辆通信收集的信息。实时交通信息、离前方车辆的距离以及天气信息均难以通过车辆内部运营获得。V2X数据允许车辆用户即使在面对能见度低或恶劣天气条件的道路时也能够获得充分的信息。

V2X数据是指有关车辆周围环境的数据，而车内数据涵盖任何内部车辆数据，其中包括车速、状态或车型。其他示例包括车辆识别码（VIN）、车辆所有者、车辆保险、运营数据和车辆服务的细节。

用户数据指从车辆和车辆用户之间的通信中收集的信息。该类信息包括常去的地点、喜欢的音乐、加油时间和驾驶习惯。

3.1.1 车辆数据收集的局限性

目前，车辆数据仅在特殊情况下使用并用于非常有限的目的，例如，服务提供者需要执行维修或故障或事故原因排除的情况。在这些情况下，作为车辆数据实际拥有者的车辆用户无法从其生成的数据中获得任何通证报酬，甚至可能不知道所获数据具有的任何通证价值。

其结果导致车辆用户不作任何努力去保存或者收集数据，进一步而言，车辆制造商、保险机构或者车辆行业的其他服务提供商将无法获得可靠的车辆数据。因此，他们可能会自行尝试生成车辆数据或者进行调查来获取缺乏客观性的不完整数据。

此外，并无任何动机鼓励去进一步提取车辆数据或者车辆数据处理中的价值，因为他们并未将数据作为服务提供商资产进行共享，其中这些服务提供商花费了大量时间和资源在数据处理上。

随着AMO市场的蓬勃发展，车辆用户和服务提供商之间的数据交易将会提高现有服务质量并加速开发新服务。

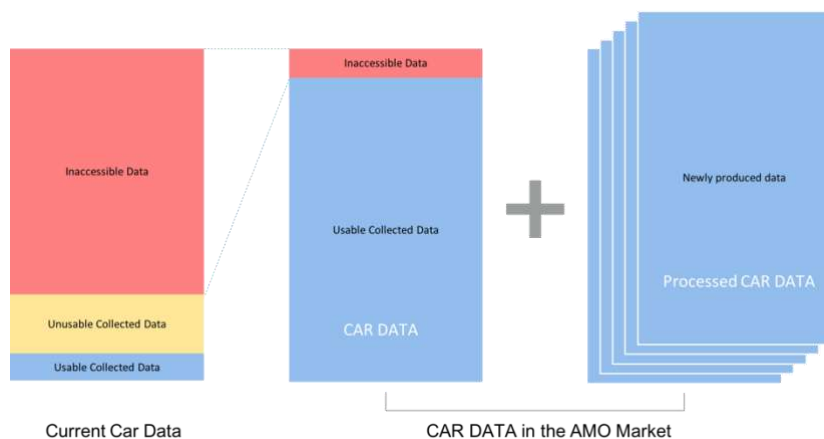


图 16. AMO市场的数据使用量和数量

3.1.2 车辆数据收集

利用软件和硬件来收集车辆数据。可使用以下两种方法收集内外部生成的车辆数据：

- 使用AMO移动钱包™的数据收集

将AMO数据收集器™插入车辆的OBD-II端口进行数据收集。首先将收集到的数据发送至安装在用户智能手机上的AMO移动钱包™，然后将传输的车辆数据传送至AMO区块链。首先对任何包含个人或者机密信息的车辆数据进行加密，然后传输至AMO区块链。

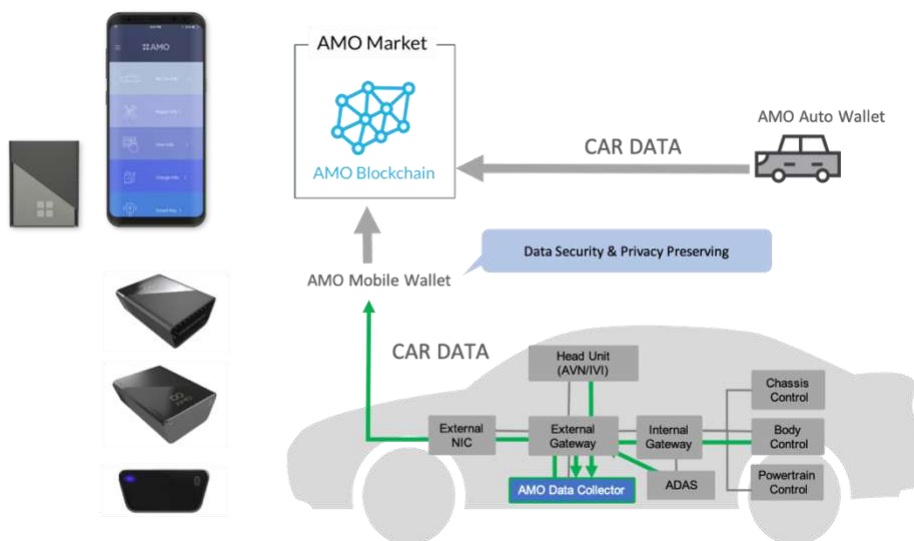


图 17. 使用AMO数据收集器™和AMO移动钱包™的数据收集过程

- 使用AMO车辆钱包™的数据收集

安装在车辆上的AMO车辆钱包™收集内部和外部生成的车辆数据，并将其存储在AMO区块链中。首先对任何包含个人或者机密信息的车辆数据进行加密，然后传输至AMO区块链。

3.1.3 车辆数据的储存/传输

将由AMO数据收集器™收集的车内数据和V2X数据，通过蓝牙传输至智能手机上的AMO移动钱包™。对于由AMO车辆钱包™收集的车辆数据，首先对包含在数据中的高度敏感个人信息进行加密，再将其上传至AMO区块链。

车辆数据仅包含部分事件数据以及任何原始数据的元数据。因此，由于其体积小，车辆数据可实时通过LTE/3G移动通信网络进行上传。但是，如果收集到的数据更加多样化，且包含像视频或者语音等尺寸更大的数据时，则可通过Wi-Fi进行上传或者先输入至额外存储位置，然后再进行批量上传。

产品	收集的数据类型
AMO数据收集器™ (H/W)	车内数据 - 运行数据（距离、速度、燃油效率等） - 各种故障排除信息（超过 400 个故障代码） - 车辆状况（发动机油位、轮胎压力等）
AMO移动钱包™ (S/W)	用户数据 - 车辆识别号码（用户输入） - 个人信息（用户输入） - 用户位置 (GPS) 车内数据 - 来自AMO数据收集器™的信息
AMO车辆钱包™ (S/W)	V2X 数据 - 包括交通信号信息在内的交通数据 - 实时交通信息 - 车内通信数据 - 地理信息和本地动态地图（LDM） 用户数据 - 车辆识别号码（用户输入） - 个人信息（用户输入） - 用户位置（GPS）信息 - 数据使用信息 - 车内数据运行数据（距离、速度、燃油效率等） - 各种故障排除信息（超过 400 个故障代码） - 车辆状况（发动机油位、轮胎压力等） - GPS 信息 - 电动车辆计费信息 - EV 电池信息 - 视频/传感器检测信息 .

表1 可收集数据示例

3.2 AMO区块链结构

AMO区块链可提供比现有区块链更高的性能和更强的安全性

AMO区块链结合了现有的区块链技术和AMO对等存储。AMO对等存储支持基于对等网络的分布式存储，以实现高效存储、使用和车辆数据共享。AMO对等存储功能与AMO存储锚连接，并连接至AMO区块链的节点，如下图所示。

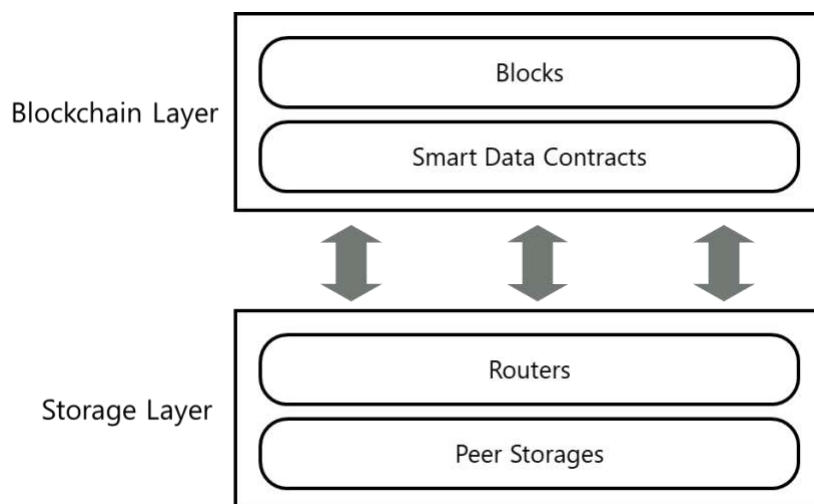


图 18. AMO 区块链节点概念架构

通常，区块链的设计是为了扩展，且随着参与节点数量的增加，数据的完整性变得更强，从而几乎不可能篡改或伪造数据。但是，当存储大量数据时，这并非一个适当方法，因为当每个数据块上的数据过多时，整个网络的效率会变差。

此外，在存储和利用以毫秒（1/100sec）的时间帧生成的时间序列数据方面存在限制。因此，为有效管理大量车辆数据和时间序列数据，启动AMO区块链试验网和主网后，将激活AMO区块链中的对等存储。

AMO虚拟机通过索引市场中AMO通证交易、市场参与者的通证余额和其他信息，同时像含大量时间序列数据的智能数据协定一样智能运行，来处理节点内存中的流程。AMO区块存在于节点内存以及文件系统（硬盘等）中，以保存和存储区块链中生成的区块数据。每个区块包含来自AMO通证交易、车辆数据交易以及敏感加密数据的锚定数据的关键信息。

将开发并发布AMO对等存储至区块链社区以作为一个分散式分布的存储空间，以便安全高效地存储敏感的加密数据，否则这些数据会因为太大而难以存储在现有的区块链中。通过这种开发，检查数据时可以最大限度地减少区块数据量较大时可能出现的问题，例如同步错误或效率低下。通常，对于区块链而言，尝试解决容量挑战问题会使用分布式存储作为集中式文件系统。不过，这并不符合AMO区块链的性质，即车辆数据标准可以共享，还允许提供和购买数据使用。

3.2.1 要求

AMO 区块链必须满足多种要求才能开发数据交易平台，从而安全高效地处理车辆数据交易以及其他类型的数据（物联网、医疗保健等）。对等存储必须能够从数以万计的车辆中收集数据，并且应在消费者请求时实时向其提供数据。为此，AMO 区块链必须保证每秒 1000 次交易的初始容量，随后还能根据需要扩大处理能力。由于车辆数据的非结构化特性，对等存储需要存储从几个字节到甚至几千兆字节的更大数据。数据消费者必须能够快速有效地搜索所需数据，因此应提供时间戳索引，以便根据数据生成的时间和地点来检索数据。另外，应提供连续的查询功能以为用户提供便利。车辆和其他物联网设备会生成大量的个人信息。因此，必须有一个保护、去识别化且只有在数据拥有者的同意下才能解密个人信息的平台。

- 能够处理每秒 1000 次交易及以上的容量
- 能够划分和保存大量的非结构化时间序列数据
- 快速搜索和连续查询功能
- 去识别和解密功能

3.2.2 共识算法

AMO区块链设计用于快速高效地处理大量时间序列数据，结合了实用拜占庭容错算法（PBFT）和股份授权证明机制（DPoS）概念，与Tendermint的算法类似。对于第一类别，这种方法每秒可处理超过1,000次交易，消除了在使用工作量证明（PoW）或权益证明（PoS）一致性算法时可能发生的带宽浪费问题。车辆和物联网设备将生成大量的数据，并将这些数据记录在区块链中，AMO将为具有最多计算资源和共享节点（AMO通证）赋予区块创建权限，而非让节点竞争区块。因此，AMO区块链具有以下优点：

- 1) 保持每秒超过 1,000 笔交易（保证 1,000 TPS）
- 2) 由验证者保存区块创建权限。区块创建只能由验证者以 2/3 的多数协议进行，因此没有分支问题
- 3) 通过通证所有权补偿具有有限计算资源的节点参与者（如物联网设备或车辆）

在现有的股份授权证明机制共识算法中，候选人通过网络参与者投票过程被选为验证者，通知其社区他们的承诺和计算规范。但是，依赖投票过程时存在验证者选择问题。

首先，候选人可注册关于他们节点的错误信息（计算规范等），并且在候选人经选中之后很难评估他们的承诺。其次，投票选举候选人可能会出现错位，他们认为这些候选人肯定会赢以得到补偿。最后，也许最重要的是，为选择验证者，网络参与者必须重复进行投票过程。

为解决这些问题，只有满足特定资格标准的节点才能选作验证者。最初，将选择22名验证者候选人，但为适应变化可能会增加数量。对于每个需要的验证者，将首先确定10名候选人，使总候选人达到220人。

22名选定的验证者将保持不变，直至创建500个区块。在创建500个区块后，他们将从候选组中随机选择一名新的验证者。将在当前组中排除具有验证历史的节点，从而确保每个节点在验证者角色中具有相同的转向。

对于区块生成的共识机制遵循在Tendermint协议所概述的“提议→预投票→预提交→提交”过程。根据该协议，恶意活动的风险极低，因为平均阻断时间预计仅为1~2秒，并且参与共识流程的验证者持有保证金，如果发现任何违规行为，可能会没收该保证金。

通过采用DPoS共识算法随机选择验证者的系统，网络参与者可保持高效快速的网络，而不会有重复投票过程带来的不便。

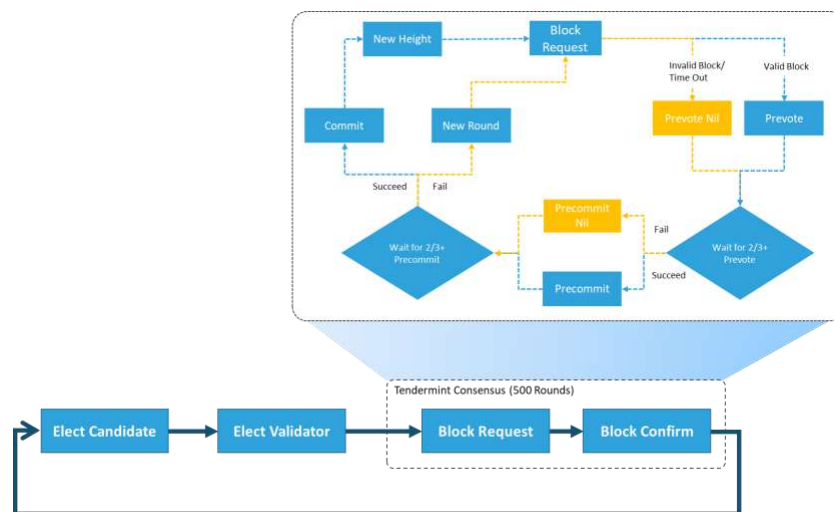


图 19. AMO 区块链共识算法

上图简要概述了 AMO 区块链的一致性算法。

- 1) 所有符合最低资格条件的节点将有平等机会成为验证者。资格要求包括对 AMO 生态系统具有一定贡献和最低水平的计算能力。拥有这种计算能力的证明可能由 PoW 测试确定。
- 2) 将随机选出符合 1) 要求的人为验证者候选人的一部分（验证者×10）。验证者的初始数量为 22，但数量可能会有所变化。
- 3) 将从 220 名候选人中按顺序挑选 22 名验证者。
- 4) 选定的验证者将使用 Tendermint 共识算法生成 1,000 个区块。
- 5) 生成一个区块的过程称为一轮。经过 1,000 轮后，该过程将从 3) 再次开始，直至该循环运行 10 次。该过程将从 1) 开始。

3.2.3 时间序列数据

在分散环境中存储和处理大量时间序列数据的能力是AMO区块链的独特优势。为有效存储和搜索AMO区块链上时间序列数据，类似于集中式环境中典型时间序列数据库（TSDB）的东西将在区块链上构建。

1) 数据模型

AMO 区块链可存储来自各种类型设备的时间序列数据。但是，由于有数百种不同类型的设备均拥有各种类型数据。当使用单个设备收集不同类型的数据时，不同类型的数据称为“度量”。

每个度量均具有在特定时间点创建的数据块。该数据块是在区块链中存储和交易的最小数据单位。数据块可分为头和主体。数据块头存储一般信息，并且数据购买者可识别和检索存储在数据块头中的信息。

数据块头的重要部分包括块的唯一标识值、创建块的装置唯一标识值、数据块度量（例如燃料平衡、当前速度等）、数据块的开始和结束时间、用于搜索的用户输入元数据等等。

数据块体将包含以相应度量标准生成的数据。存储的内容将包含数据的确切时间，并将在指定的时间段内按顺序存储。将块内的每个事件称为“记录”。

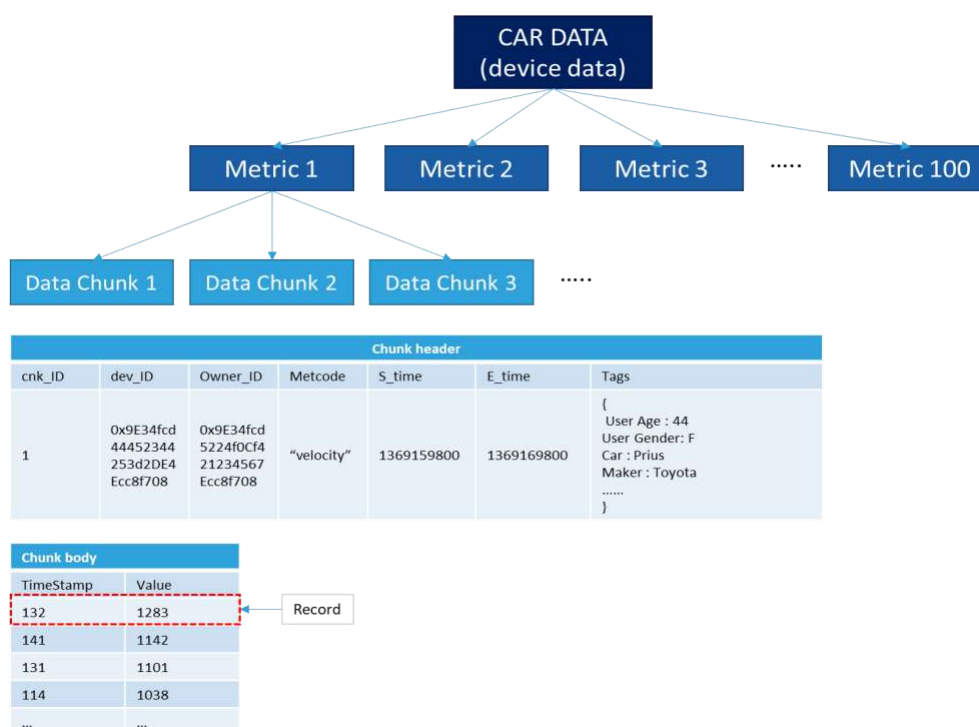


图 20. AMO 区块链对等存储数据结构

AMO区块链的数据结构可与像MySQL这样的关系数据库的现有组件进行比较，如下所示：

AMO Blockchain	Relational Database
Metric	Database (Scheme)
Chunk	Table
Record	Row

2) 数据压缩

车辆和其他物联网设备可产生大量的数据，这意味着高效的网络使用可能具有挑战性。这就是数据在上传到 AMO 区块链之前必须进行优化和压缩以便消耗最少的网络资源的原因。在传统的压缩算法不适合压缩时间序列数据的情况下，使用快速无损压缩来大量减少所需的网络带宽和存储空间。

AMO 团队开发了两种压缩数据的方法，其中第一种方法是处理时间戳数据。当收集时间戳数据而非记录整个时间戳时，计算前一记录与新记录之间的时间间隔，以得出第一个增量值。接下来，计算前一次记录与早期记录之间的时间间隔，以得出第二个增量值。增量的增量是第一个和第二个增量值之间的差值，其将代替整个时间戳值存储在区块链中，从而最大限度地减少消耗的压缩数据存储。

$$\text{增量的增量: } D = (t_n - t_{n-1}) - (t_{n-1} - t_{n-2})$$

第二种数据压缩方法涉及一个简单的异或 (XORing) 过程，即异或新记录的值与前一次记录的值以求最大化的压缩。Gorilla 项目提出的方法证明了前文提及的两种时间序列数据压缩方法。

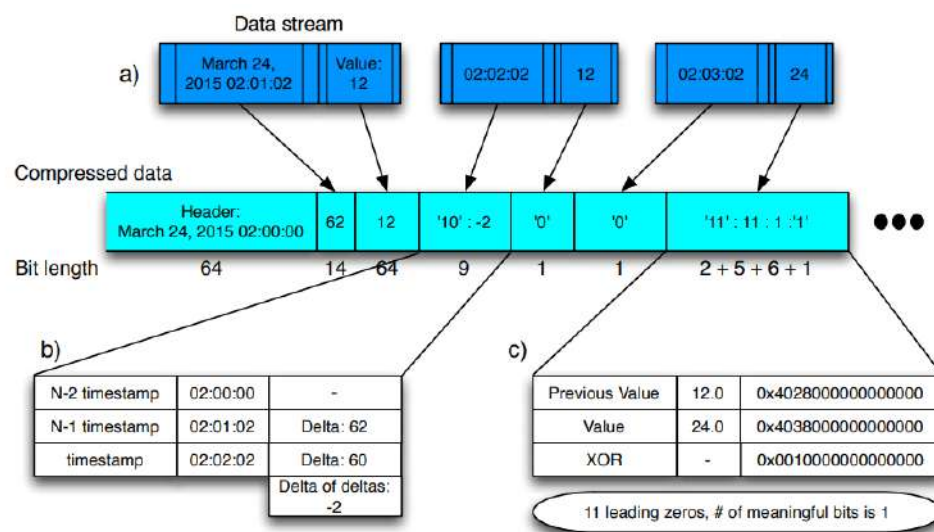


图 21. AMO 区块链对等存储数据协议

3) 存储协议

AMO 链的存储层包含存储对等体的内容寻址网络。来自特定设备的数据块通过受 IPFS 数据结构启发的 Merkle 有向无环图 (DAG) 结构连接。数据块的哈希摘要作为元数据的一部分保存在 AMO 区块链层中。这不仅用于寻址目的，还用于检查区块内容的完整性。我们使用多哈希格式以存储哈希摘要。这为数据收集器指定哈希算法的使用提供了灵活性，具体取决于应用需求。

AMO 链通过用于不可变数据单元的可恢复方案优化的高效基于 merkle 证明，提供对等存储审计性。这允许网络执行常规的加密审计，以确保存储的数据块仍可使用，并准备好检索。这也是奖励对等存储节点的指标之一。AMO 存储对等体使用类似于 IPFS 实现的分布式哈希表 (DHT) 进行按路线发送。AMO 数据块内容对应 IPFSObject 的数据字段。

3.2.4 智能数据合约

向前迈进时，AMO 区块链力求成为一个不仅支持车辆数据，而且支持各种时间序列数据的数据平台。为此，区块链将采用智能数据合约，这是一种针对数据处理进行优化的智能合约。这将允许任何实体或个人希望通过分散平台使用 AMO 或其他货币，以获取时间序列数据。

为让参与者轻松创建自己的智能数据合约，AMO 团队将公开提供软件开发工具包。软件开发工具包具备以下特点：

1. 数据所有权应用程序编程接口 (API)

数据所有权的准确管理在分散的环境中至关重要，这种数据所有权的概念是数据销售的核心。除数据的原始生产者之外，所有其他市场参与者只能购买数据使用权，而数据所有权本身不可转让。

通过使用智能数据合约的数据所有权 API 集，市场参与者将能够执行一系列授权管理功能，例如存储和验证数据所有权，以及验证用户在访问数据时是否拥有使用权。

2. 数据搜索 API

为准确、有选择地购买在 AMO 区块链上存储的大量时间序列数据中的数据，需要采用先进的搜索机制。通过适当的索引，可对由数据生产者直接输入的元数据以及每当将一段数据上传至 AMO 区块链时自动生成的元数据执行直观搜索。特别是，AMO 区块链可针对处理时间序列数据进行优化，并使用基于时间的索引使其能够支持快速准确的数据搜索。

3. 数据交换 API

当用户搜索并选择一段数据用于购买时，将会发生一个复杂的过程，用于检索数据并获取数据的访问。首先，验证数据所有权和使用权，然后在最后用数据拥有者的加密密钥解密数据（如有必要）之前，检索分散和存储在点对点存储网络中的所有数据。AMO 团队将提供一个 API 集，以便轻松管理整个流程。

4. 数据存储 API

为在 AMO 区块链的点对点存储上存储大量时间序列数据，数据在分布和存储在点对点存储网络之前，必须按照智能数据合约指示的方式进行处理。根据数据的重要程度，可能需要多次复制并进行分散式分布，以防止数据丢失。该 API 集将启用各种存储属性的规范，例如要存储在 AMO 区块链上的数据结构、内容和位置。

5. 服务发现 API

以 AMO 区块链为平台，可开发各种 dapp（分布式应用程序）。AMO 区块链可为 dapp 开发人员提供一个 API，使其能够提供对 dapp 的简要描述，并且还可为用户提供一个搜索和检索 dapp 信息的 API。如此可轻松识别 AMO 区块链上的有用 dapp。

3.3 数据隐私和安全

隐私设计（隐私意识架构）在车辆环境中至关重要。

随着车辆成为用户生活方式中更加不可或缺的一部分，车辆数据无意中包含了可能认为是敏感的个人数据。为保护 AMO 市场参与者免受敏感数据的曝光，特别是针对日益严重的网络犯罪，需要采取多重保护措施。

3.3.1 遵守安全准则

按照严格的法律法规收集、传输、存储和使用车辆数据。整个开发过程中均考虑了国际车辆安全和隐私准则。AMO 市场的开发符合以下法规和准则：

- 1) 《关于车联网和自动驾驶车辆网络安全的关键原则》（英国，2017年）
- 2) 2017年《车辆安全与隐私法案》（美国，2017年）
- 3) 2015年《驾驶员隐私保护法》（美国，2015年）
- 4) 《联邦自动驾驶车辆政策》（美国，2016年）

3.3.2 个人信息加密

必须特别注意任何内部或外部生成的车辆数据，因为其包含高度敏感的个人数据。在收集车辆数据期间，AMO 钱包会识别并加密这些敏感的个人数据。AMO 钱包使用的加密密钥由 AuthentiCA® 发布。只有在获得数据生产者的许可后，数据消费者才能解密数据。AMO 市场平台支持请求许可和执行密钥交换解密的过程。通过端到端的加密可保护数据生产者和消费者之间的授权过程，这意味着 AMO 平台无法解密或访问任何通信。

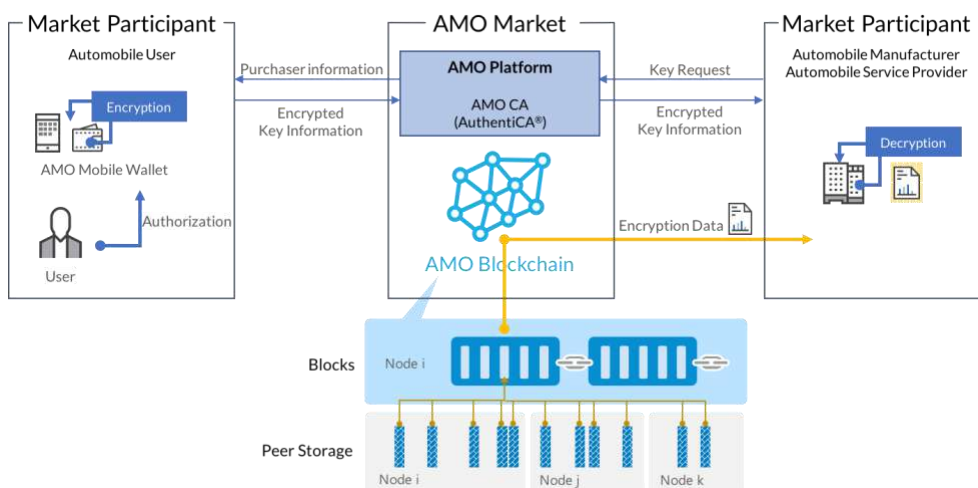


图22. 通过AMO平台可获取使用加密数据的权利

3.3.3 加密后的通信和加密后的数据存储

除个人信息的加密之外，AMO市场还通过支持SSL/TLS的安全通信以加密通信通道本身。采用多层安全性可防止车辆和AMO钱包之间的数据传输过程中的数据泄漏，其中车辆数据尚未加密，还可防止在AMO钱包和任何AMO节点之间的传输过程中的车辆数据和不敏感、未加密的个人信息泄漏。将加密密钥和证书管理服务AuthentiCA®部署至加密通信通道。

3.4 车辆数据交易

购买车辆数据的所有权和权利可保证公平交易

在AMO市场上，车辆数据生产者可向市场提供数据且车辆数据消费者可获得使用数据的许可。车辆数据消费者使用AMO通证支付数据的使用，然后将其用作车辆数据生产的补偿。市场上交易的数据包含车辆数据和处理后的车辆数据。

3.4.1 数据所有权和访问数据

车辆数据生产者保留数据的所有权，但车辆数据消费者能够在购买时获得对特定车辆数据集的单独访问权。因此，禁止转售这些数据。数据使用的时间或范围限制可应用于不同的情况基。

处理后车辆数据的所有权属于参与车辆数据二次处理的人。然而，重要的是注意数据所有权并不涉及用作处理车辆数据源的初始车辆数据。有关车辆数据和处理后的车辆数据的所有权的任何潜在争议将根据相关法规得到解决。

3.4.2 数据所有权

通常情况下，在每种使用数据的情况下，数据拥有者的许可都是必需的。然而，为方便数据拥有者，将采用自动给予许可以使用不包含高度敏感个人信息的车辆数据的方案。此授权过程由AMO平台支持并由AMO移动钱包™实施。

数据类别	数据类型	说明
高度敏感的个人信息 (Lv1)	- 车辆用户的真实姓名 - 车辆识别号码 (VIN) - V2X通信数据	可用于识别车辆及其用户的信息
常规个人信息 (Lv2)	- 车辆用户的年龄和性别 - 车辆品牌和型号、位置	可用于对车辆及其用户进行细分的信息
常规车辆数据 (Lv3)	- 速度、运行状态 (发动机温度等) - 故障数据等。	具有通过OBD收集的普遍性且不可用于识别车辆及其用户的信息
大容量车辆数据 (Lv4)	通过传感器、CAN数据等检测的事件信息	收集方法变为可用后的实施

表2个人信息的等级

3.4.3 通过端到端加密的权力分散

AMO市场交易的加密车辆数据只能由其购买者解密。加密也是AMO平台中的一项中心技术，其使用端到端的加密防止控制服务器到中央服务器和高级节点的集中。

3.4.4 加密后或未识别数据的交易

加密数据的交易和使用需要访问数据生产者拥有的加密密钥。如果使用加密数据创建二次输出，则处理后的车辆数据不得包含部分或完全解密的源数据。同样，对处理后的车辆数据中包含的任何加密数据的访问都需要原始密钥拥有者的许可。由AMO市场平台支持该交易。如果使用或交易，则去识别化的数据必须保持去识别化。

3.4.5 AMO 度量管理系统

AMO平台的指标管理系统为车辆数据和处理后的车辆数据设定标准市场价格。AMO指标管理系统考虑数据的供求情况、数据量、流通中AMO通证的总量、稀缺价值和数据的及时性，以确定市场价格。AMO指标管理系统使用机器学习技术，以预测和分析未来的价格变动。

3.5 报酬系统

AMO 市场可让所有参与者对其所做的贡献获得适当的奖励。

3.5.1 生产数据报酬

数据生产通过消费者在AMO市场上购买数据的方式获得补偿。然而，奖励并不仅仅取决于供求。相反，数据的价值是基于购买过程中的各种元素。基于数据价值和交易的确定奖励是AMO市场健康运营的核心原则。这是市场进行自我调控以确保只有高质量数据流通并调整和稳定AMO通证价值的基础。

3.5.2 参与作节点报酬

AMO节点的参与提高了AMO区块链的可靠性，并有助于AMO市场的发展。因此，AMO通证作为奖励给予。通过对AMO对等存储的贡献，向节点提供额外补偿，并通过评估对AMO区块链和市场的贡献来确定补偿金额。

3.5.3 区块生成报酬

AMO 区块链使用 DPoS（股份授权证明机制）算法作为快速高效的区块生成的共识模型。使用超过一定数量的 AMO 通证获取股权的节点将能够选择代表性节点。AMO 区块链中代表性节点的数量并非固定不变，相反，代表性的数量将根据节点的需求而改变，以便在保持稳定性的同时优化区块生成的速度。

AMO 平台衡量和披露贡献给 AMO 区块链的信息，以支持公平和公开的代表性选择过程。贡献信息包含数据交易的容量和数量、AMO 通证余额、设定时间段内的平均存储量以及交易的贡献。这些信息为投票人的选择提供透明度，减少了选择恶意节点的风险。新 AMO 区块生成将由平台内的 AMO 通证管理系统运营，且 AMO 平台的运营政策由市场参与者共同决定。新区块生成后，AMO 通证将支付给代表性节点和生成区块的投票人节点，且通证的一部分将用于区块链运营的节点。有代表性节点的 AMO 通证管理系统将促进选举人节点补偿。

第 4 章 服务例子

以下列出的是具有蓬勃发展AMO市场的车辆数据的各种用例。但是，请注意，AMO项目的目标不是自己启动服务。相反，AMO的目标是提供一个可以实施和不断更新此类服务的环境。

- 寿命周期管理（包括车辆零部件更换）
- 车辆故障预测及安全改善
- 车辆及其零部件的正品认证和防盗
- 车辆事故分析
- 个性化车辆保险计划
- 二手车的可信赖P2P售卖
- 适于车辆充电的P2P电力售卖
- 提供车辆充电和停车场的位置信息服务
- 音乐和视频流和计费
- 在多辆车辆内同时体验内容流
- 本地动态地图（LDM）服务
- 车辆数据用户的开放参与赏金
- 车辆相关个人信息的安全监督
- 车内或联网车辆商业/支付

以下章节将介绍AMO市场如何支持上述服务，从而支持车辆行业中的各种活动。

4.1 车辆维护服务

通过由AMO Data Collector™收集的车内数据以及由加油站、车辆维修店和其他服务提供者提供处理后的车辆数据，AMO市场促进车辆在整个生命周期内的维护。

例如，购买二手车时，涉及大量的资产移动，使得追踪和管理变得困难。事实上，车辆所有权的转移涉及与多方利益相关者共享信息，其中包括车辆制造商、保险公司、二手车经销商、车辆注册办事处和车辆维修店。当来自车辆制造商、车辆维修店和其他服务提供者的处理后车辆数据（车辆损坏、检修或检查记录等）存储在AMO区块链中，且因此具有可靠性和防篡改性，可节省购买过程中的大量时间和精力。通过这种方式，车辆用户能够在购买二手车时享有安全性，且在维修其车辆时享有数据支持指导。与此同时，通过向用户提供数据，保险公司、车辆维修店和其他服务能够利用新的商业机会提供增值服务，例如，及时维修或更换零部件。

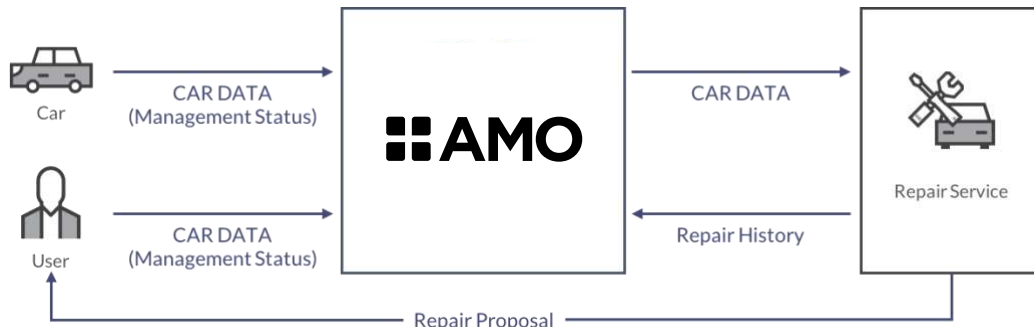


图 202. 车辆维护服务

4.2 车辆事故分析服务

AMO市场收集车辆内部和外部生成的数据。在发生事故的情况下，从车辆传感器生成的数据将存储在AMO区块链对等存储中。通过有保证的数据完整性，该信息可作为合法证据与黑匣子（事件数据记录器，EDR）数据结合使用。事故期间获得的数据可用于创建模拟以及调查事故原因。

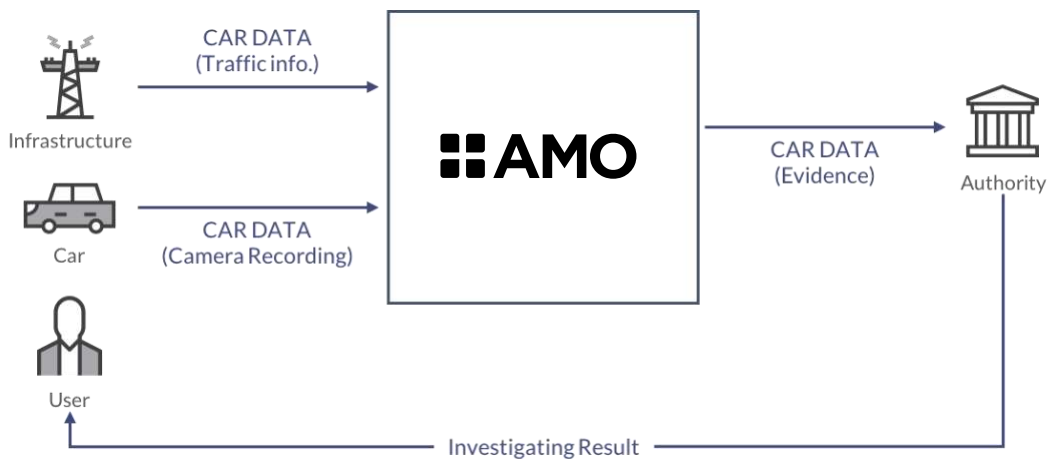


图 23. 车辆事故分析服务

4.3 准确的保险费率计算服务

保险服务提供者根据驾驶员的驾驶历史确定车辆保险费率，并根据评级因素和事故数量调整折扣。目前，车辆保险提供者要求客户提供关于其里程数、车型、黑匣子使用等信息，将其纳入保险费率中。与现有模型不同，AMO市场无需人工输入信息。相反，有关车型、注册年份、里程等所有信息均收集并存储在AMO区块链中。使用该车辆数据作为参考，保险公司可以提供更准确和个性化的保险计划，且该计划反映驾驶员的驾驶模式。



图 214. 准确保险费率计算服务

4.4 车辆充电和停车服务

很多人都会有过几次驾车在街区寻找停车场或充电站的经历。可以使用AMO市场中有关这些充电站和停车场的信息来创建和实施与充电站和停车场可用性相关的服务。如果在路上电量不足或需要停车，与充电站或停车场状态相关的服务提供者可以帮助他们的客户找到最近的位置。

这可以通过建立对等（P2P）电力交易进一步进行。与必须从中央机构获取电力的现有方法不同，用户可以利用买卖双方的配对直接交易服务，这将使用AMO市场使买方与卖方进行配对，并管理收费状态以及与位置相关的信息。

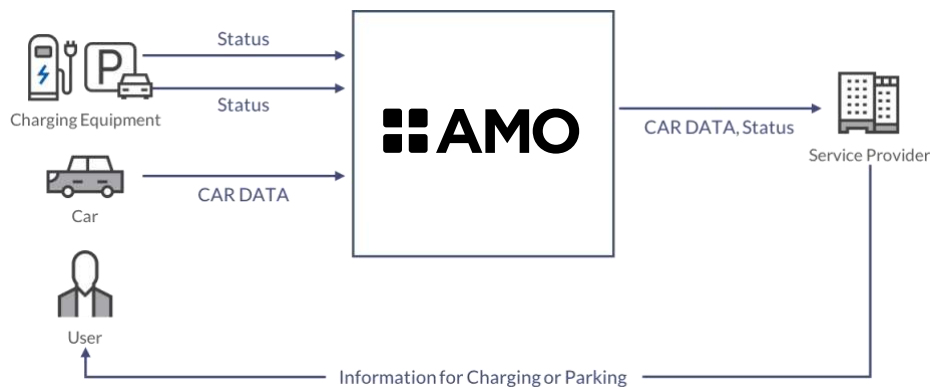


图 25. 车辆充电和停车服务

4.5 音乐和视频流服务

自动驾驶车辆技术的进步激起了人们对车内娱乐潜力的兴趣，许多人预测未来车辆将主要用作娱乐平台。AMO市场可以让车辆用户实时访问各种媒体内容，其中包括电影和音乐。



图 22. 音乐和视频流服务

4.6 本地动态地图服务

AMO市场可以让驾驶员访问本地动态地图（LDM），LDM具有比典型交通地图更详细和最新的交通状况信息。从主动车辆传感器和V2X通信收集的所有数据将存储在AMO区块链中，以收集有关车辆外部环境的信息。服务提供者可以使用该信息生成更准确的驾驶环境描述，并将该信息提供给车辆、车辆用户、服务提供者和所有其他市场参与者。

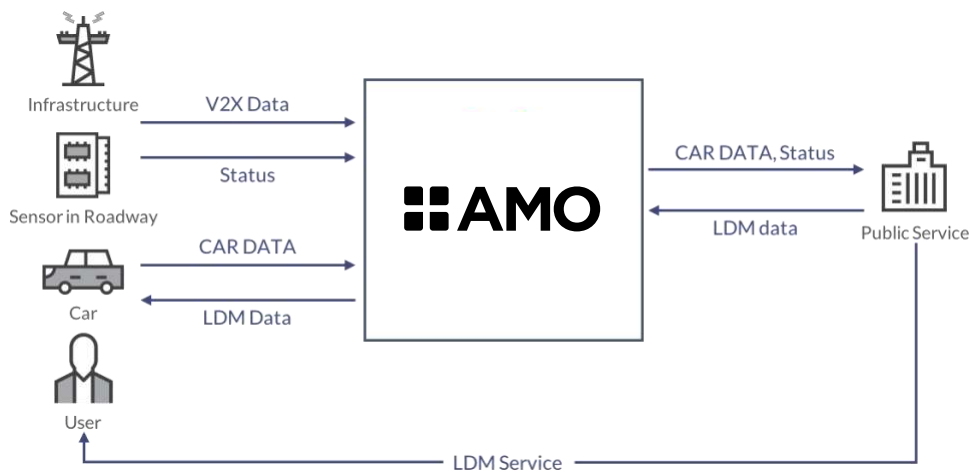


图 236. 本地动态地图服务

4.7 个人信息的安全监督

智能手机用户现在习惯在他们的设备上收到关于个人信息使用和数据访问的大量通知。与外部环境进行通信的车辆也应如此，特别是由于某些车辆数据可能包含个人信息。AMO市场加密所有存储的个人数据，且不允许在未经驾驶员许可的情况下使用任何数据。由于禁止未经车辆用户同意使用数据，且已记录所有权利和权限的历史，因此参与者可以亲自监督和控制其数据的使用。

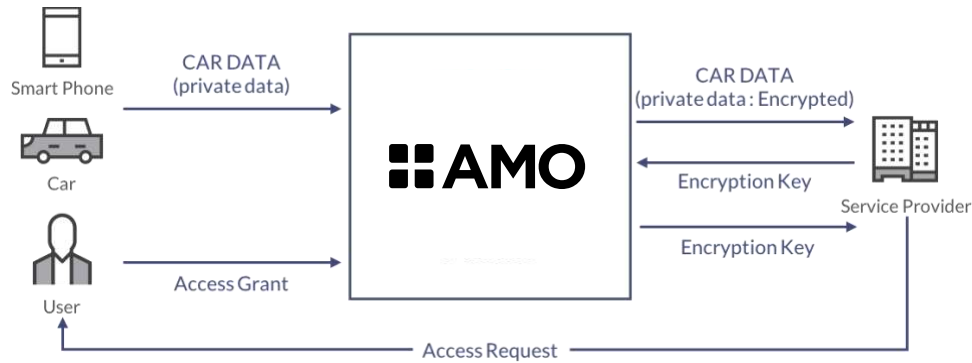


图 247. 个人信息的安全监督

4.8 数据移动服务

AMO市场记录的其中一种数据类型是用户数据，其中包括对内容订阅。如果车辆用户使用车辆/共乘服务、购买新车或使用属于他人的车辆，则该用户可以通过简单的认证过程轻易地将这些数据从一辆车中转移到另一车辆中。

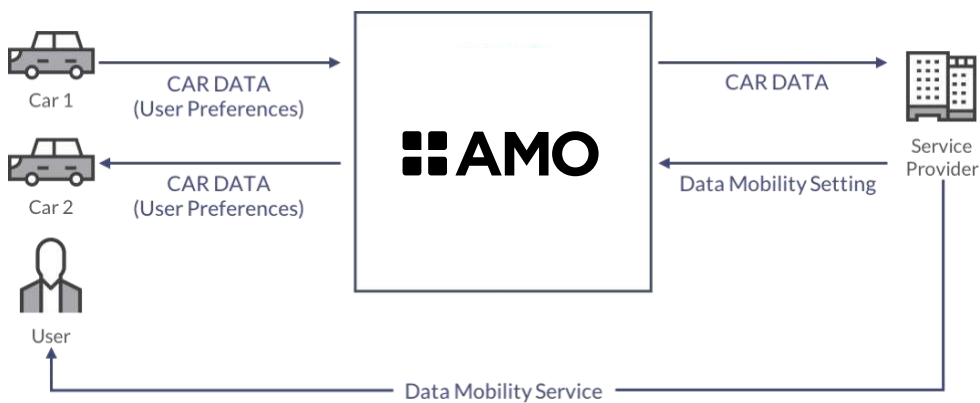


图 28. 数据移动服务

4.9 开放参与赏金

随着AMO市场的增长和参与者数量的增加，购买者想要购买的数据类型也可能多样化。这可能导致消费者可能无法找到他们想要的数据类型的情况。如果出现这种情况，消费者可以为他们所需的数据类型提供赏金，并吸引其他数据生产商生成数据。在这种情况下，数据所有权将取决于双方之间的双边协议。

记录赏金金额、所需数据类型以及数据所有权后签署智能合同，从而允许买方能够快速有效地获取高质量的数据。这种情况下，数据生产商能够获得额外的补偿，且现已创建先前不可用的数据，从而允许AMO市场的进一步增长。

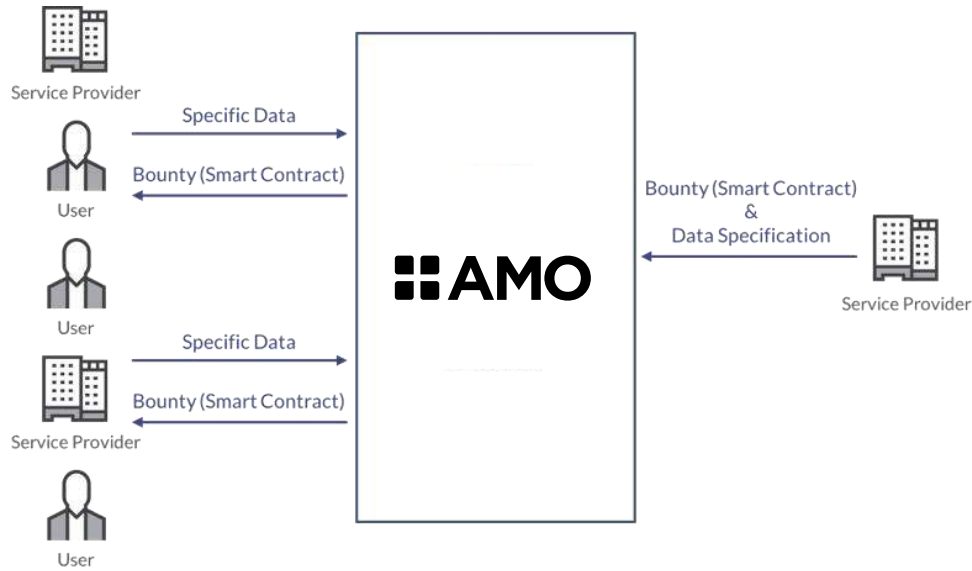


图 259. 开放参与赏金

第 5 章 逆向车辆数据应用通证分配

车辆数据的收集需要嵌入式技术、移动技术、服务器技术和安全等多个领域的专业知识和经验。特别是在处理个人信息等容易受到违反尝试的敏感数据时，因此需深入了解加密和去识别化技术。

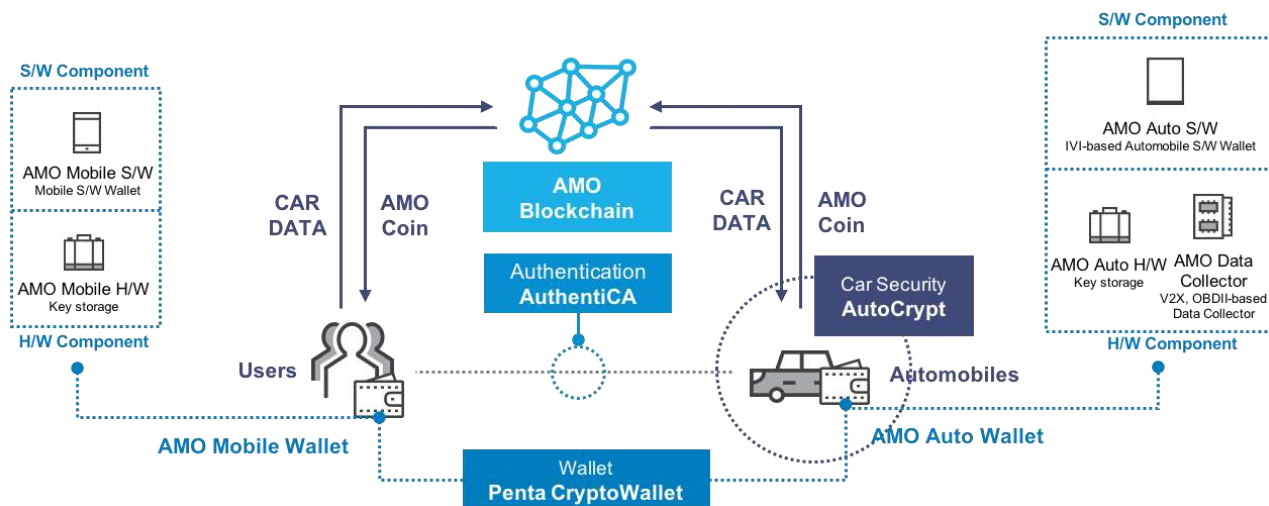


图 30. 车辆数据收集方面的专业知识和安全

即使在收集车辆数据之后，为数据交易和通证经济系统设计、实施和运营安全系统也非常重要。

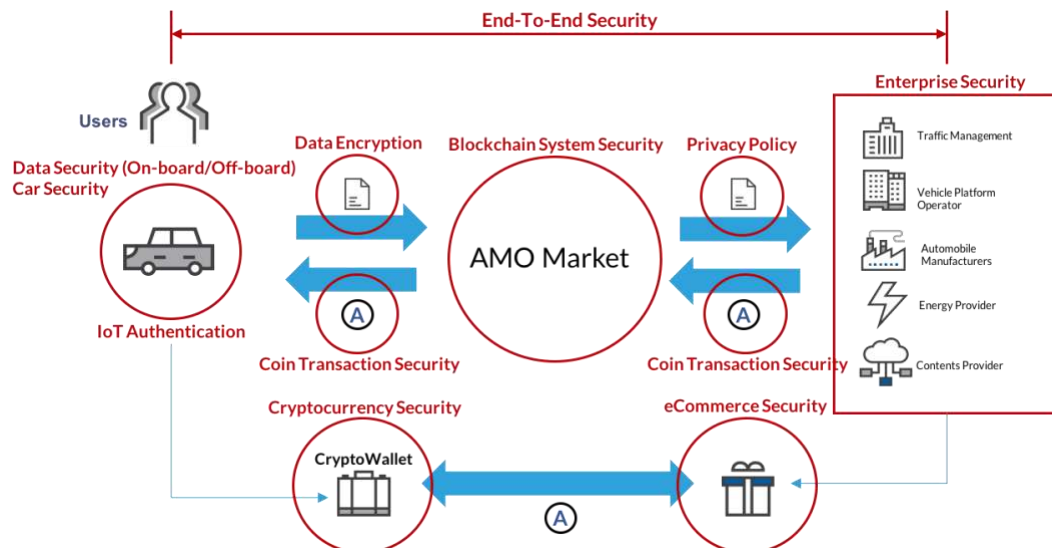


图 261. 在市场中交易数据的安全元素

Penta Security的AutoCrypt®、AuthentiCA®和Penta AuthentiCA™现可以解决有关车辆数据和现有车辆首次通证分配的问题。

AutoCrypt® AuthentiCA® + Blockchain Penta CryptoWallet™

AutoCrypt®	- 能够收集所有数据：V2X、车内数据和用户数据 - 与Penta CryptoWallet™结合，AMO车辆钱包™可用作车内区块链客户端以及钱包
AuthentiCA®	- AMO CA 作为不同市场参与者使用的 IT 系统相互认证的 PKI - 提供加密功能，以使得市场参与者能够授予数据权限 - 提供加密密钥，以允许数据加密和去身份识别
Penta CryptoWallet™	- 发布的 AMO 移动钱包™具有数据收集、社区参与、交易和区块链客户端等功能 - 未来AMO货币经济扩张的各种附加功能

表3. Penta Security Systems technologies 技术的利用

5.1 AutoCrypt®

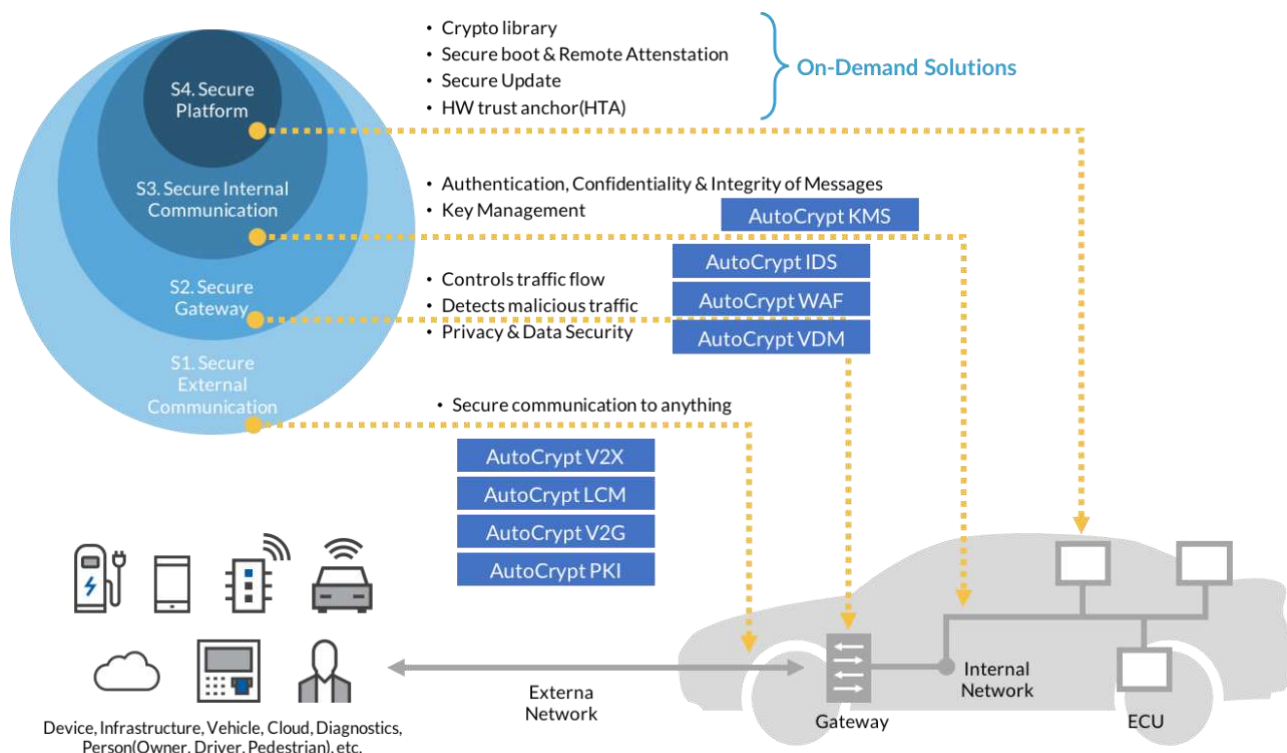


图 32. AutoCrypt® 组成结构

AutoCrypt®是互联车辆、自动驾驶车辆和智能车辆的安全解决方案。AutoCrypt®作为韩国首个专用车辆安全解决方案于2015年启动，而实际开发始于2007年，是车辆零部件和车辆制造商的按需应变安全解决方案。全面车辆安全所需的技术可以分为四大类，且AutoCrypt®提供以下功能：

1. 保护车辆和外部设备之间的通信：通过公钥加密为外部通信提供加密和认证。

物联网或IoT是类似于智能车辆、智能工厂、智能电网、智能家居以及手持设备（可穿戴设备和传感器）等大型设备的技术网络。但是，无论物联网设备的规模如何，均需优先确保设备与服务伺服器之间的通信安全。安全通信可以通过对两个实体之间的保密数据进行认证和加密来实现。但即使加密仅在认证后进行，使得认证成为物联网中的关键和基础技术。

AuthentiCA®是一种基于云的认证授权服务，允许用户轻松创建、签署和管理密钥和证书，以创建安全的物联网环境。由于其与微软的Azure IoT套件兼容，因此微软云平台Azure的用户可以方便地使用由AuthentiCA®提供的物联网安全技术。

AMO市场参与者使用AMO CA（优化AuthentiCA®技术用于AMO市场）发行的密钥和证书进行身份验证，以支持车辆数据的安全交易。

5.3 Penta CryptoWallet™

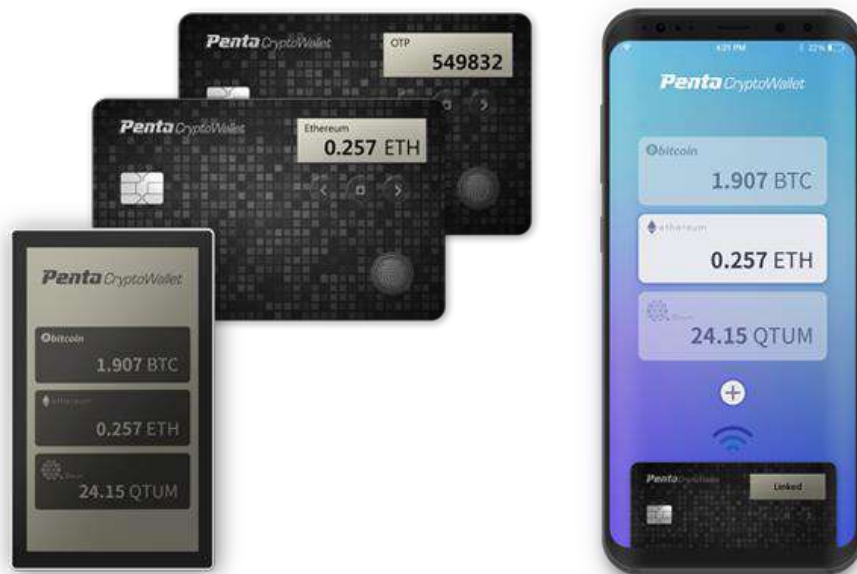


图 285. 三种形状参数中的Penta CryptoWallet™

加密数字通证（Cryptocurrency）已激起人们极大的兴趣，因为其有潜力改变现有在线商业模式，并有助于发展新的线上到线下（O2O）商业机会。事实上，涉及加密数字通证交易的高水平安全事故以及针对钱包提供商的黑客攻击之后，该行业一直在挫折中挣扎。

许多现有数字钱包要么仅为加密数字通证提供所需的密钥存储，要么缺少用于网络连接的安全选项，这使得许多钱包易受攻击。Penta CryptoWallet™可安全地管理用于加密数字通证交易的加密密钥的整个寿命周期。其还兼容各种电子通证转账服务，并提供电子通证的安全存储和交易服务。

将优化Penta CryptoWallet™背后的技术用于AMO市场，以开发AMO移动钱包™和AMO 车辆钱包™。除用作促进AMO通证交易的加密数字通证外，其还将用作参与AMO区块链的AMO节点。

第 6 章 路线图

为在首次通证发行之后建立AMO市场，将按照路线图分阶段启动开发和服务。发展蓝图旨在促进市场参与者的职能参与和顺畅互动。随着参与的益处扩大和AMO市场增长，路线图可能会发生变化。



第 7 章 团队成员与顾问

AMO团队由各自领域的专家组成，且有实力将AMO的愿景变为现实。

 SangGyoo Sim CEO • Creator of AutoCrypt • Ph.D & M.S., POSTECH • R&D Engineer, Samsung Electronics • Adjunct Prof. in Dongduk Women's University • Adjunct Prof. in Soonchunhyang University • Head of Penta IoT Convergence Lab • 15+ years experience in IT & Security	 Daniel ES Kim CSO • Creator of D'Amo • B.S., POSTECH • Chief Technology Officer, Penta Security Systems • 20+ years experience in IT & Security	 DS Kim CTO • M.S., POSTECH • Cloudbric Co-Founder • XBrain Founding Member & Advisor • 20+ years experience in IT & Security
 KyungMoon Nam Head of Strategy • WebCash • 15+ years of experience in IT	 Erik Tan Head of Operations • B.A., University of Wales • Senior Manager, Certis CISCO • Senior Manager, LHN Group • 10+ years experience in IT	 Jaeson Yoo Chief Evangelist • B.A., Occidental College • Principal Consultant, Cooper21 Consulting LLC. • 15+ years experience in business development
 SungKyoong Chung Head of R&D • Creator of Penta CryptoWallet • M.S., POSTECH • Founder of GRock Information • 15+ years experience in IT & Security		

顾问



Gilles Delfassy [in](#)

Board of Directors at ON Semiconductor

Gilles Delfassy is a member of the Board of Directors of ON Semiconductor, Cavendish Kinetics Inc., and e-Lichens S.A. and Chairman of the Board of Kalray S.A.. He started his career with Texas Instruments and created and led the Smartphone Semiconductor business of TI, growing it to a five-billion-dollar operation. He was Senior VP and Executive Officer of TI until 2007. From 2009 to 2012 he was President and CEO of ST-Ericsson.



Chance Du [in](#)

General Partner at Coefficient Ventures

Chance Du is Founding Partner at Coefficient Ventures, a multi-strategy crypto fund with presence in North America, Asia, and Europe. Her passion and knowledge for decentralized governance protocol has led her to speak about blockchain technology at leading industry conferences including the Stanford Cryptocurrency Exchange conference, De/Centralize 2018 Singapore, Ether Denver, Google Female Founders Summit, and Fintech Silicon Valley among many others.



Seokwoo Lee [in](#)

Founder and CEO of Penta Security Systems

Lee founded Penta Security Systems, a Korean IT-security firm, in 1997. The company quickly globalized its operations, entering Japan, the United States, and Singapore. Lee transformed the company by diversifying its technologies and advancements from WAF to IoT security technologies. In 2010 He was awarded by (ISC)²® with the Information Security Leadership Achievements award. In addition to co-founding xBrain, he is also adjunct professor at POSTECH as well as the founding chairman of POSTECH's Association of POSTECH Grown Companies.



Kazunari Miyazaki [in](#)

Head of NEC Venture Fund, Director of BIGLOBE

Kazunari Miyazaki is the former head of the NEC Venture Fund and Director of BIGLOBE, the Yahoo of Japan. Since its beginning in July 1996, BIGLOBE has expanded the services offered beyond ISP connection services to extend to portal sites, broadband content and numerous other Internet services. Miyazaki has 10+years of experience in M&A, accounting and finance, supporting portfolio companies, conceptualizing and identifying market needs, and implementing result-oriented strategies.



Carol Streitberger Brighton [in](#)

President and Owner, CSBrighton Consulting

Carol Brighton is President of CSBrighton Consulting, specializing in advising high-tech companies in Europe and the US and helping to pave the way for successful and profitable acquisitions. Formerly the Group VP of Corporate Internal Communication for STMicroelectronics in Switzerland, Brighton's expertise in communications and investor relations also comes from a career as Vice-President of Global Communication for ST-Ericsson and previous work in Texas Instruments.



YoungHa Kim [in](#)

Former CEO, Samsung Electronics China

YoungHa Kim spent over three decades at Samsung Electronics, focusing on the Chinese market. His previous appointments as the head of the Beijing, Hong Kong, and Shanghai branches before being elected the CEO of Samsung Electronics China in 2011 were due to his business acumen and his ability to achieve financial results for the company. He has been credited with developing strong retail sales networks in China, bringing Samsung mobile phones to hold the top market share position in the country from 2013 onward. Retired in 2015, Kim is currently Professor at Dankook University.



Bonghan Brian Cho [in](#)

Founder and CEO of Equalkey Corp., Korea

Dr. Cho is the founder and CEO of Equalkey Corp., an AI firm focusing on transforming education using an innovative and systematic approach. He is also a member of the Board of Directors of DBS Group Holdings Ltd and DBS Bank Ltd. Previous appointments included Executive VP and CIO for Samsung Fire & Marine Insurance, Deputy CEO and CIO for Hana Financial Holdings, and CTO of the Next Banking Generation System at KB Kookmin Bank. Cho holds a Ph.D and M.S. in Computer Science, specializing in AI. Cho has also received recognition for his contributions to the software industry with the Republic of Korea President Award.



Teddy Hyunwoong Kim [in](#)

Co-Founder of Gridwiz, Chief of R&D Center & EV Dept.

Teddy Kim co-founded Gridwiz, a company specializing in solutions that economically manage customers' energy consumptions. Gridwiz's Distributed Resource (DR) solution is considered the number one solution in the industry, and Gridwiz provides solution packages for DR, Distributed Energy Resource (DER), Smart Factory, and Electric Vehicle (EV) charging infrastructure. He also currently heads the R&D center the Electric Vehicle department as the resident expert in ISO/IEC 15118 standardization (wired and wireless V2G communication). He is a specialist on Distributed Energy Resource (DER) including EV application.



Gu-Min Jeong [in](#)

Professor, Kookmin University

Jeong is a Professor at the School of Electrical Engineering, and also a chair of mirror committee for ISO TC22 SC31/32 in KATS, and of the IT convergence committee of KAMA. He is also a chair of the Infineon Center (funded by Infineon, Germany) and the Hyundai Odin Center, both at Kookmin University. His previous appointments include his positions as Advisory Professor for Samsung Electronics regarding IoT and In 2016, Advisory Professor for NAVER regarding smart cars and autonomous driving, and Visiting Associate Professor of ICS, UC Irvine, CA, USA. Before joining Kookmin University, he co-founded NeoMtel and was a manager at SK Telecom.



Huy Kang Kim [in](#)

Associate Professor, Department of Cyber Defense, Korea University

Professor Kim is currently an Associate Professor in the Department of Cyber Defense and Graduate School of Information Security at Korea University. His main research areas include data-driven security (e.g., fraud detection system, intrusion detection system in vehicles, and user behavior analytic system). His previous appointments include leading the KAIST UNIX Society (KUS), Technical Director and Head of Information Security of NCSOFT, and founder of A3 Security Consulting, the first ever information security consulting firm in Korea.

第 8 章 法律问题

AMO团队撰写了本白皮书，以提供更多有关AMO区块链的信息。该白皮书仅供参考。白皮书的撰写并非旨在为AMO团队或区块链投资提供建议。白皮书是根据“现状”撰写而成，换言之说，本白皮书基于当前状态撰写而成，意味着在未来可能会发生变化。

此外，AMO团队不就本白皮书提供任何担保声明或任何形式的保证，也不承担法律责任。例如，AMO团队不保证（i）白皮书基于合法权利且不侵犯第三方权利；（ii）白皮书具有商业价值或益处；（iii）白皮书适合实现具体议程和（iv）白皮书的内容无错误。责任和职责的范围不限于上述例子。

如果以任何方式提及白皮书以做出决定或采取行动，其后果将由读者负责，AMO团队概不负责。例如，如果发生任何损害、金钱损失、伤害或债务，AMO团队将不以任何方式补偿或赔偿。

参考文件

- Cyber Security and Resilience of smart cars:
<https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/>
- Federal Automated Vehicles Policy - September 2016:
<https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016/>
- Testing automated vehicle technologies in public:
<https://www.gov.uk/government/publications/automated-vehicle-technologies-testing-code-of-practice>
- Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System:
<http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system>
- Million lines of code:
<http://www.informationisbeautiful.net/visualizations/million-lines-of-code/>
- Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles:
<https://www.strategyand.pwc.com/reports/connected-car-2016-study> (2016.09)
- Service Fabric Customer Profile: BMW Technology Corporation:
<https://blogs.msdn.microsoft.com/azureservicefabric/2016/08/24/service-fabric-customer-profile-bmw-technology-corporation/>
- Monetizing car data - New service business opportunities to create new customer benefits:
<https://www.mckinsey.com/~media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx>
- Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061 :
<https://www.sae.org/standards/content/j3061/>
- U.S. DoT chooses SAE J3016 for vehicle-autonomy policy guidance :
<http://articles.sae.org/15021/>
- ISO 15118-1: General information and use-case definition[4] :
<https://www.iso.org/standard/55365.html>
- ISO 15118-2: Network and application protocol requirements[5]:
<https://www.iso.org/standard/55366.html>
- ISO 15118-3: Physical and data link layer requirements[6]:
<https://www.iso.org/standard/59675.html>
- ISO 15118-4: Network and application protocol conformance test[7]:
<https://www.iso.org/standard/55366.html>
- ISO/FDIS 15118-5: Physical and data link layer conformance test[8] :
<https://www.iso.org/standard/61725.html>

- ISO/DIS 15118-6: General information and use-case definition for wireless communication[9] :
<https://www.iso.org/search/x/query/15118-6>
- ISO/CD 15118-7: Network and application protocol requirements for wireless communication[10] :
<https://joinup.ec.europa.eu/solution/isoiec-15118-7-road-vehicles-vehicle-grid-communication-interface-part-7-network-and/about>
- ISO/FDIS 15118-8: Physical layer and data link layer requirements for wireless communication[11]:
<https://www.iso.org/standard/62984.html>
- IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013) - IEEE Standard for Wireless Access in Vehicular Environments-- Security Services for Applications and Management Messages:
<https://standards.ieee.org/findstds/standard/1609.2-2016.html>
- Design and Implementation of IEEE Std 1609.2 Message Encoder/Decoder for Vehicular Communication Security:
http://www.cseric.or.kr/literature/ser_view.php?searchCate=literature&SnxGubun=INEN&mode=total&gu=INKO051A0&cmd=qryview&SnxIdxNum=195047&rownum=2&f1=KW&q1=WAVE
- Road vehicles — Functional safety — Part 1: Vocabulary :
<https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en>
- The Automotive Standard ISO 26262, the innovative driver for enhanced safety assessment & technology for motor cars :
https://ac.els-cdn.com/S1877705812031244/1-s2.0-S1877705812031244-main.pdf?_tid=9b6b6ae1-1b1f-4060-86cc-35f582c1bef5&acdnat=1523670019_5a6e2ef4e9fa6acf1756ee22a018914c
- Cyber security Guide book for Cyber-physical Vehicle System :
[https://webstore.ansi.org/RecordDetail.aspx?sku=SAE+J+3061-2016+\(SAE+J3061-2016\)](https://webstore.ansi.org/RecordDetail.aspx?sku=SAE+J+3061-2016+(SAE+J3061-2016))
- Connected Car: Vehicle Platforms Increasingly Use Smartphone Connectivity:
<https://www.gartner.com/doc/3838867/connected-car-vehicle-platforms-increasingly>

© 2018 AMO Foundation. All Rights Reserved.