目录

1. 引言
2. 技术介绍
3. 应用情景和挑战
4. 区块链+车联网数据交互  
   4.1 各种基础的方案，多领域的应用情况  
    4.1.1 区块链的构架  
    4.1.1 平台  
   4.2 构建一个可信数据交换平台  
   4.3 隐私保护方案（匿名性）  
   4.4 提高交互的效率（数据存储，网络规模）
5. 区块链+电动汽车的充电方案  
   5.1 各种基础的方案  
   5.2 效率和节能  
   5.3 对隐私保护的改进
6. 区块链+智能交通

引言

随着半导体技术水平的提高，我们拥有了计算能力更高的芯片，读写速度更快且容量更大的存储器，而以5G为代表的通信技术的成熟和应用，使信息传播的速度达到了质的飞跃，信息时代的大门正在徐徐向人类展开。而这个时代，也是汽车的时代，性能优良的交通工具和发达的道路系统让我们在现实生活中的物质交流也越加频繁。当信息时代遇上汽车时代，车联网就应运而生，我们在汽车上安装微型的专用计算机，为他们建立专用网络，记录并交流这些丰富的数据。而这些数据带来了现代社会的一场全新变革：驾驶汽车而产生的操作信息、车载传感器产生的路况信息以及为汽车提供的各种服务信息，都让我们向一个更智能、更便捷、更人性化的时代前进。

据一项调查显示，在如今这个信息爆炸的年代，每天都有2.5 quintillion bytes的新数据产生，我们已然身处一个信息极度充盈的年代。

但是，在这个过程中，我们应该意识到，车联网系统中存在许多急需解决的问题。例如，如何解决信息分享中涉及隐私数据的问题；在较大地理范围内，如何解决车辆之间的信息同步问题；如何解决数据的安全问题和真实性问题。如果这些问题不能解决，那么我们的车联网系统永远只能停留在设想中。幸运的是，区块链技术的提出在很大程度上解决了这些问题。（介绍区块链）。

在这篇文章中，我们主要对区块链在车联网中的应用方案进行了调查和对比。由于车联网和区块链技术都属于新兴的计算机技术，所以目前在车联网+区块链的方案中，绝大多数都处于初级的理论分析和探索性的实现阶段。在以理论分析为主的论文中，许多文章都提出了新颖且合理的车联网+区块链的架构，同并将一些更高效合理的区块链共识算法思想（例如POS，DPOS等）引入架构中，解决了车联网系统内的信任问题、数据隐私性问题和效率问题。在面向具体应用场景的方案中，以电动汽车充电系统和智能交通系统的方案最多，并且已经经过了若干次的改进，具有较高的可用性，而其他的应用方案例如保险行业、交通事故检测、汽车的销售和维修还处于较为初级的阶段，在未来具有很大的发展空间。接下来，我们将逐个分析区块链在车联网各个领域内的发展现状。

4. 车联网+基于区块链的方案

车联网作为物联网的一个重要分支，沿用了许多在物联网中提出的技术与方案，汽车作为交通工具，有许多传统物联网系统不具备的特性和需求：首先，车辆作为人员与货物流动的载体，其数据交流对隐私安全有较高的要求，同时也提高了整个系统利用数据作出分析的难度。其次，车联网对数据的真实性有很高的要求，由恶意参与者产生的虚假数据或者是直接攻击轻则可能会导致车辆误判而带来不必要的麻烦，重则带来大范围的交通事故，这对驾驶员与乘客的人身安全都是巨大的挑战。还有，汽车会在较大的地理范围之内活动，涉及到车辆信息的身份认证、交互信息传输和系统信息的更新，这对通信系统的架构是一个考验。

在Towards Blockchain based Intelligent Transportation Systems[0]一文以基于区块链的智能交通系统为例，类比计算机网络的多层结构，提出了普适“车联网+区块链”的各种方案的层次化架构。通过将结构分层为Application Layer, Contract Layer, Incentive Layer, Consensus Layer, Network Layer, Data Layer and Physical Layer，消除了异构网络与硬件组成的差异，同时也使具体方案的提出者可以根据实际情况对效率、隐私、可信度的侧重修改某层的实现过程，并保证系统稳定。

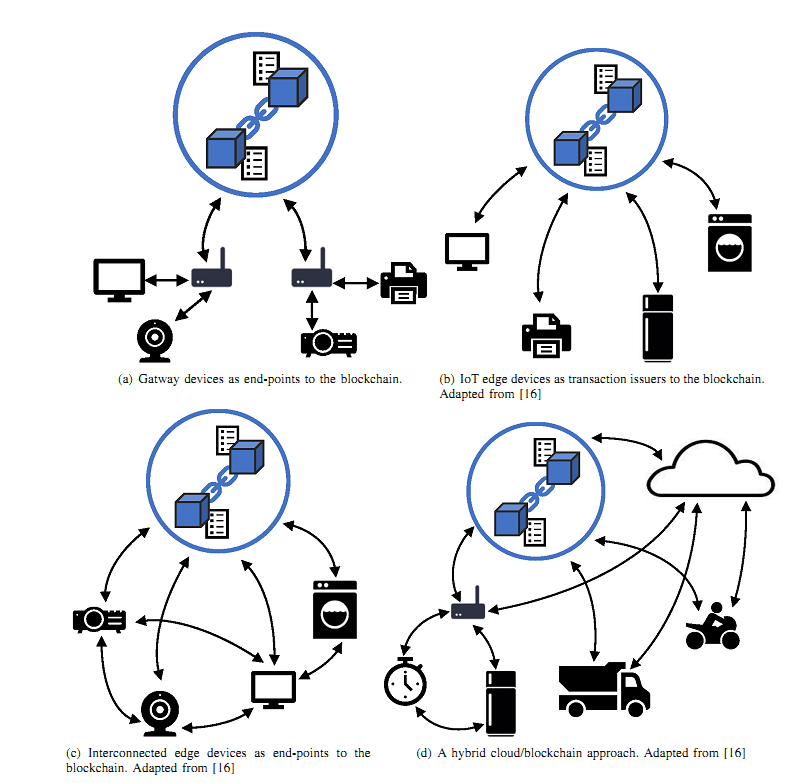
这一部分我们将分析车联网+区块链的基础构架，保障系统隐私安全、数据可信和提高效率的一些方案。

4.1 各种基础的方案，多领域的应用情况

4.1.1 几种区块链的物理层构架

在谈论车联网+区块链之前，我们先看一下普通的物联网是如何构建的。On blockchain and its integration with IoT. Challenges and opportunities[1]经过对物联网的区块链架构方案的调研，总结出3种区块链的大致架构，分别为：a) IoT-IoT, b) IoT-Blockchain, c) Hybrid approach。而Applications of Blockchains in the Internet of Things: A Comprehensive Survey[2]这篇文章在其基础上，总结出4种区块链的大致架构，分别为：

1. Gateway devices as end-points to the blockchain
2. Devices as transaction-issuers to the blockchain
3. Interconnected edge devices as end-points to the blockchain
4. Cloud-blockchain hybrid with the IoT edge



而车联网+区块链的方案大多数也沿用了这些架构。

相对而言，”Devices as transaction-issuers to the blockchain”的架构是在硬件和软件上都最容易实现的，因为它不需要额外的基础服务设施。而受到车载单元计算能力和通信能力的限制，这样的架构更适用于交互数据量低且实时性要求较低的应用场景中。在A blockchain-based reputation system for data credibility assessment in vehicular networks[3]中提出，车辆可以与其通信范围中的行驶路线相近车辆组成集群，集群内的车辆直接进行数据交互。每个集群会独立维护一个区块链网络，集群内车辆会把数据交互信息打包为交易，在集群内部广播和验证，最后通过一种改良过的PoW共识算法生成区块。这个方案虽然考虑到了汽车有限的通信能力，将通信范围控制在较小的集群中，但它仍存在很大的可用性和普适性问题：车载计算机是否能PoW的运算效率需求先不谈，事实上，现实中很难找到一个长久稳定的车辆集群——陌生车辆组成的集群会在几小时内解体，车辆会不断进入不同的集群中；并且，集群的范围边界也是一个难以确定的问题，在这样的方案中，可能仅隔几米之遥的两个车辆会因为不属于同一集群而无法进行数据交互。我认为，这个方案最多只适用于特定道路上的信息记录或者运输车队的消息交流记录，其中，后者可以使用联盟链来省去繁重的共识过程。在BlockChain: A Distributed Solution to Automotive Security and Privacy[4]中，由车联网中的结点（可以是smart vehicles, OEMs (original equipment manufacturers, i.e., car manufacturers), vehicle assembly lines, software providers, cloud storage providers, and mobile devices of users such as smartphones, laptops, and tablets.）作为区块链的节点直接负责交易的传播和验证、区块的产生与验证等区块链功能。但该方案的优点在于，它维护的是Smart vehicles系统中所有车辆与汽车服务相关信息的区块链，车辆不必在不同的区块链网络之间切换。同时，为了降低网络中的通信量以便扩大系统规模，该方案将节点划分为较小的集群，每个集群选择cluster head作为overlay block managers (OBMs)来处理该集群内的事务，并打包为交易广播到区块链中，还要负责产生或检验区块。考虑到车辆时常会发生位置变动，该方案还提出了soft handover method来动态划分集群来降低网络时延。在Blockchain Based Transparent Vehicle Insurance Management[7]中也采用了相同的架构，使individual drivers, business organizations such as insurance companies, and governments agencies等参与者直接组成用于储存和管理车辆保险信息的区块链网络。考虑到参与者较高的可信度和较低的计算能力，本方案采用permissioned blockchain以避免在达成共识上浪费时间。为了避免遭受恶意行为导致的信息泄露危险（诸如车辆行程和车主身份的隐私信息等），车辆每次会从若干个不同的非对称密钥对中选出一对，来加密上传的信息。这些信息会在需要向特定参与者公布的时候（例如事故发生后的保险理赔）用对应的私钥开启。该方案利用了区块链上记录的信息不会被篡改的特性，保证了数据的完整性（integrity），还提出了今后的方案中可以将zero knowledge proofs and bilinear pairings等advanced cryptographic techniques加入到隐私保护中。

更多的方案都采用了较为合理的” Gateway devices as end-points to the blockchain”架构，基本方式是采用地理位置固定的计算设施（例如RSU, Road Side Unit）作为Gateway来进行区块链的数据传输和达成共识，车载单元只负责数据的收集和传输，这在很大程度上减轻了车载单元的计算和通信负担。例如：Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework[8]中，common vehicles 和 sensor-rich vehicles只通过MECN（Mobile Edge Computing Node）来传输信息。MECN会存储landmark的位置信息、收集sensor-rich vehicles发送的车辆对应于Landmark的位置信息并把修正过的GPS数据发送给所有车辆，同时，会把所有的这些操作写入区块并在MECN之间完成共识算法。

而” Interconnected edge devices as end-points to the blockchain”与” Gateway devices as end-points to the blockchain”构架的不同点在于，车辆之间允许进行直接的通信，而不必将全部信息经过区块链来传递。这种架构在降低车辆之间的通信延迟和减少区块链通信量上非常有效，数据的产生者也可以（某种程度上）自由地选择被广播的数据。因此，它适用于那些信息交流频繁、通信延迟的容忍度较低的应用场景，例如智能交通系统、事故检查系统等。”Blockchain-based message dissemination in VANET”[6]基本采用了这样的构架，它还提出，可以借助RSU来实现Proof of Locaiton (PoL)，为其附件的车辆提供地理位置的认证，以提高系统中数据的可信度（防止恶意的参与者在根本没有到达某地的情况下捏造该地的数据）。该方案仍处于探索的早期阶段，没有太高的可行性：方案没有考虑到RSU或车辆可能遭受的攻击，以及攻击导致的虚假信息的散布和信息泄露等问题，并且对分享数据的车辆没有任何激励机制，这些可能会导致车主不愿意向网络中广播真实有效的数据。然而，隐私保护和数据分享的激励措施已经有许多研究者提出了进一步的解决方案，我们会在后面进行阐述。在” Self-managed and blockchain-based vehicular ad-hoc networks”[5]中也采用这样的架构，在此基础上使用以太坊构建区块链网络，使之能够适用于Trafﬁc Regulation Application (TRA)和Vehicle Tax等多种应用场景。

”Cloud-blockchain hybrid with the IoT edge”构架结合了之前几种架构的优点，以一种更加灵活的方式去构建区块链。车辆have a choice to use the blockchain for certain interaction events, and the remaining events occur directly between vehicle，同时，车载单元性能较高的车辆可以作为区块链网络中的节点，直接参与区块链的各种事务，而那些性能有限的车辆可以通过gatway devices进行各种事务。此外，网络中的车辆还可以使用雾计算等来克服一些车载计算单元的性能瓶颈。在Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach[12]中使用一种有望取代HTTP的分布式的数据存储、数据sharing方式——Interplanetary File System (IPFS)，RSU负责维护区块链的基础功能，处理车辆上传的各种信息（路况，信誉度评价）。而数据存储的工作由IPFS完成，当车辆向RSU发送查询信息的请求时，RSU会向IPFS系统请求对应的数据。

* 1. 可信的车联网平台

基于区块链的车辆网中，数据会在不同的参与者之间流通，帮助车辆或者系统的管理者做出决策。在区块链生成的过程中，矿工会验证网络中被广播的交易的合法性，并在共识算法生成区块之后对区块进行验证，这保证了区块链上的数据是合乎规范的。但是，这还不能满足我们的需要。区块链作为一个去中心化的、分布式的系统，数据由多方生成并上传。在基于公有链的大多数区块链+车联网方案里，是没有办法保证所有参与者都是诚实且不出错的，换句话说，恶意的参与者可能会上传格式合乎规范但内容虚假的数据（例如：某一车辆为了便于自己的出行，向区块链网络中广播自己所在路线上并不存在的拥堵信息，使收到该信息的其他车辆选择其他路线）来造成区块链中的信息可信度降低。为了解决平台上数据的可信度问题，一些方案提出了信誉度评价方案，对数据的产生者（车辆）或数据的处理者（例如RSU等）的可信度做出评判，使车辆或系统的决策者能够根据这些信息做出最正确的决定。鉴于车联网中基础架构的差异、应用场景的不同，信任问题非常复杂，解决方案也五花八门。根据信任值产生的层次, trust management models can be divided into three categories：entity-oriented trust model, data-oriented trust model, and combined trust model。

entity-oriented trust model.

entity-oriented trust model的关注重点在于根据车辆的历史经历来预测其行为是honestly的可能性，而不关注车辆进行的交易或者提交的信息的可信度。A privacy-preserving trust model based on blockchain for VANETS[], A blockchain-based reputation system for data credibility assessment in vehicular networks[]中的区块链上存储的信誉值只针对车辆，由汽车的历史来确认和更新信誉值。以A privacy-preserving trust model based on blockchain for VANETS[]为例，系统中存在一个可信且安全性很高的law enforcement authority（LEA）来收集区块链网络中的可信度相关信息。车辆会在发送authentic messages时提高自己的信誉值，在发送错误的forgedmessages to deceive other vehicles时降低信誉值，此外，为网络中正确的信息作证或检举错误的信息都会提高自身的信誉值。当车辆的信誉值将为0时，负责区块链维护的RSU节点将不再广播该车辆发出的信息。

data-oriented trust model

data-oriented trust model关注事件或信息的可信度，对事件的参与者或信息的发送者不感兴趣。该模型在一定程度上提高了信誉值评价系统的工作量和复杂度：网络中data的数量远远多于车辆的数量，并且data也没有历史信息可供借鉴。但它可以提高信息的利用率，使不诚实车辆提交的信息也可以被利用。同时，也降低了系统被攻击的风险：原本诚实的车辆可能因为偶然的失误或攻击而提交错误的数据，系统评价这些信息时不会受到历史记录的干扰。由于种种原因，目前暂无基于区块链的车联网方案采用该模型。

combined trust model

combined trust model将前面所述的两种方式结合起来，借助对应的entity的可信度来作为对data可信度评价的参考，或者根据entity产生的data可信度来评价entity的可信度。Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET[]

而根据被评价的单位，trust management models can be divided into two categories：车辆信息的可信度，RSU的可信度，以及可能会出现的二者结合的情况。

4.2.1车辆信息的可信度

A blockchain-based reputation system for data credibility assessment in vehicular networks[3]中，车辆会根据自己掌握的信息对其他车辆上的车载传感器产生的信息进行投票，若正确则对该信息投票1，否则投票-1。此外，还有trusted authority (TA)会为车辆上装载的传感器单元的性能（精度、范围）打分，并在车辆集群选择矿工节点时，为那些传感器性能较高的车辆赋予更高的几率：该方案在车辆集群中选择符合Hash(ID; time;PreHash) < C的车辆节点来产生区块，而C就是TA对车载传感器的评分。当车辆节点被选为矿工时，它会把自己对集群内其他车辆的信息投票结果包装在区块中，并发送给集群中所有其他车辆。其他车辆会检验矿工的资格、区块的签名，并在ratings recorded in the block do not conﬂict with their local ratings的情况下接受rating更新的结果。该可信度方案比较依靠TA做出的车载传感器性能评分，恶意节点可能会攻击TA或者伪造传感器性能指标，从而影响到整个系统的信息可信度。

Blockchain-based decentralized trust management in vehicular networks[10]中在[3]的基础上进行了一些修改：车辆只作为数据（来自车载传感器）和rating的产生者，而增设RSU来负责收集车辆投票情况并以此评估车辆信誉值，并响应车辆发出的对其他车辆信誉值的查询。RSU负责收集和广播车辆上传的传感器信息与rating结果，并通过共识算法生成区块。考虑到如果让拥有较多信息量的RSU生成区块的话，会使更多的信息尽早被确认，从而对整个系统的效率带来提升，文章提出了PoW+PoS的共识算法，takes the sum of absolute values of offsets in the candidate block as the stake，使拥有更多stake的节点拥有更低的PoW难度。文章还分析了车联网信誉管理系统面临的几种风险：A）恶意车辆的两种行为：1) Message spoofing attack, 2) Bad mouthing and ballot stuffing attack. B) Compromised RSU，可以在之后的方案中将解决这两个问题的能力作为一个指标。

Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles[11]沿用了[10]中的基本思路，为基于区块链的车联网中车辆之间的计算资源sharing提供了解决方案：作为Task Owners (TOs)的车辆 intend to offload their computation tasks to an adjacent Resource Providers (RPs)车辆 to implement cooperative computation，在此过程中，TOs会使用称为Resource Coins (RCs)的数字加密货币向RP支付其提供的资源。Each vehicle determines its role（Tos or RPs）according to its service requirement and resource availability，并将这些信息以交易的形式发送到区块链网络中触发智能合约以寻求匹配。当交易结束后，TOs会检查RPs运行结果的integrity and correctness，并以交易的形式生成对RPs的reputation评价。每当RSU收集到一定数量的交易时就会自动产生一个区块，并记录区块中所有交易的reputation的总和。PoR共识算法要求节点将当前slot内reputation总和最高的区块加入区块链中，以保证可信度较高的交易被优先确认。Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach[12]也采用了[10]中车辆之间互相评价的方式，并把信誉值信息存放在Interplanetary file system (IPFS)中。

4.2.2 RSU的可信度

4.3 保护隐私的方案

4.3.1存储数据的防篡改和防泄露

区块链特殊的机制使基于区块链的车联网中存储数据具有防篡改功能：矿工们每生成一个区块的时候，都会将该区块的前一区块的hash值写入到生成的区块中。但某一区块被篡改，其hash值会因此发生改变，从而我们可以从链接该区块的后一区块中发现。在每一区块中，所有的交易通过Merkle树产生一个哈希值，当任意一笔交易信息被篡改，就会导致merkle树的结果截然不同。

区块链中存储的数据虽然具有较强的防篡改能力，却在防泄露方面很薄弱。原因在于，区块链作为一种分布式记账本，设计的初衷就是为了公开和透明信息的：交易会被广播到整个区块链网络中，并由网络中的节点进行验证。在大多数方案中，所有的节点都会保存一份的完整的区块链信息（不一定从创世区块开始记录，但会从某一时间开始或固定数量区块前开始）。相对而言，这些节点在面对恶意节点时是非常薄弱的，恶意节点可以伪装为网络中的正常节点来申请共享区块链信息，或者直接攻击正常节点以获取区块链信息。在车联网中，区块链中的信息常常具有较高的隐私性，例如在Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework[8]中，提出使用车辆的传感器协助提升GPS（Global Positioning System）的准确度，车辆的位置信息会被传输到MECN组成的区块链网络。在Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles[9], A tiered blockchain framework for vehicular forensics[10]等文章将基于区块链的车联网应用在刑事侦查、事故定责中，车辆的拥有者信息（包括姓名，年龄甚至是居住地和工作单位）、行驶路线、保险信息等都会被记录。即使方案提出者使用了安全性较高的permission BlockChain，仍然不能避免信息泄露的风险。  
  
4.3.2 车联网中的隐私保护方案