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。

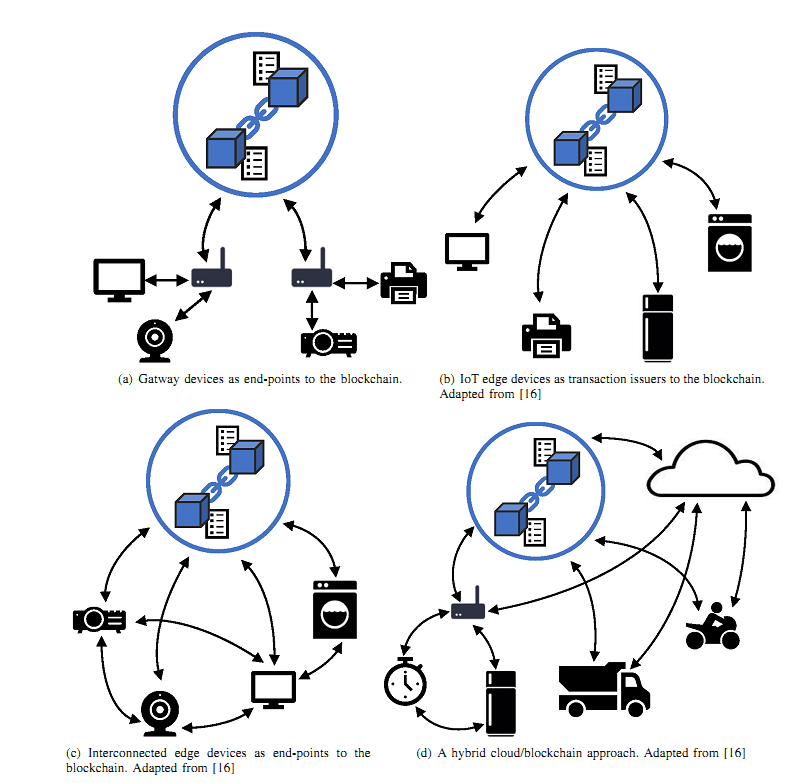
这一部分我们将分析车联网+区块链的基础构架，保障系统隐私安全、数据可信和提高效率的一些方案。

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、高性能数据库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。Securing Cognitive Radio Vehicular Ad Hoc Network with Fog Node based Distributed Blockchain Cloud Architecture[]在roadside unit’scloud and blockchain based distributed cloud中间使用雾计算节点。每个基于雾的small cloud都覆盖了小的关联网络，负责以最小的延迟进行安全的数据分析和服务交付。

4.2 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forged messages 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[]中由于采用了k-anonymity作为防止泄密的工具，需要K个互相信任的车辆相互合作，把他们的消息相互混杂。如果有恶意参与者参与到混杂过程中，很容易造成信息泄露，所有车辆必须选择信誉度较高的车辆来进行合作。为了防止恶意车辆在破坏性行为之前通过recent honest behaviors快速伪装为可信车辆，或者通过在网络中保持较高的信誉度来进行on-off攻击，此方案将historical trust information and the current behaviors evaluation赋予相同的权重。

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，供车辆通过轻量级的区块链快速获取信誉值信息。

Trust bit: Reward-based intelligent vehicle commination using blockchain paper[]中不再采用投票评价的方式来生成信誉值，而是采用了一种类似于比特币的加密凭证——trust bit来建立系统中的信任。Trust bit拥有唯一的ID，由车辆的销售商或authorized dealers发布，并由车辆完成group communication中一定的计算任务之后赚取。Bit trust会随着车辆完成的计算量增多而增多，也说明车辆拥有更高的respect and honor。本方案的假设是，当车辆为系统做出更多贡献之后，也会获取更高的收益，因此采取恶意行为的成本更高，理智的参与者会更倾向于诚实地参与车辆间的通信。这与现实的情况是相符的。CreditCoin A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles[]也采用了类似的数字货币CreditCoin，车辆在发起上传一项正确的信息时，会邀请其他见证者一起对信息进行签名，正确的上传会使发起者和参与签名者得到奖励，否则将得到惩罚。

Bars: a blockchain-based anonymous reputation system for trust management in vanets[]中使用Law Enforcement Authority (LEA)来监视汽车行为，并对每个车辆的信誉值进行评估，除了奖罚善恶行为，还鼓励对恶意行为进行检举。在此方案里，车辆的信息根据重要程度分为三个等级（）：lv.1 紧急情况（车辆失控等）广播。 Lv.2 车辆行驶状态（制动，刹车，拐弯）。 Lv.3 对poor road conditions进行广播。信息在网络内的影响力也被纳入考虑：作为The relative density of vehicles，, 其中 is set to 20 vehicles per Km。从信息的重要程度和影响范围来选择车辆善意或恶意行为的奖罚力度，相对于简单的相互投票，有一定的优越性。但使用中心化的节点LEA作为监督者和评价者，可能会导致潜在的被针对攻击的危险。

4.2.2 RSU的可信度

在RSU作为矿工节点的区块链网络中，RSU不仅负责满足车辆的信息服务需求，还需要完成区块链共识算法等繁杂的事务。作为数据的处理者，RSU存在有恶意行为或者被恶意攻击的可能，需要信誉度等作为一个评价指标来保证车辆可以获取更可信的数据。此外，如果区块链中采用PoW这样消耗大量计算力的共识算法，会造成网络中信息交流的延迟大大增加，还有潜在的通信质量不佳导致的区块链分歧问题。因此，一种基于DPoS的以RSU的信誉度为矿工选举资格度量的算法被人提出：Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory[]由车辆根据RSU的表现来评价其信誉水平，拥有较高信誉的RSU会在缴纳一定保证金后作为候选矿工。候选矿工会分为两部分：候选矿工中信誉值更高的一部分作为活跃矿工，每个活跃矿工会在一段时间充当区块管理员的角色，完成区块生成、广播、验证和区块管理的工作；而信誉值较低的则作为备用矿工，会配合活跃矿工一起完成区块链验证的工作，保证区块管理者没有被贿赂。每当所有活跃矿工完成一次挖矿后，系统会重新评估RSU的信誉，重新选举候选矿工。

4.3数据安全和隐私保护

4.3.1 基于区块链的车联网的防篡改性

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。当某一区块被篡改，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，所有的交易会通过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树的哈希结果截然不同，导致区块整体的哈希发生改变。这是区块链技术相比于其他数据存储技术的优势之一。

4.3.2 数据的防泄露

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）。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。

在这样的情况下，保证信息能够在车联网中隐秘安全地传输就成为了方案里最重要的关注点。事实上，在几乎所有的车联网方案中，都或多或少的考虑到了信息的安全或者隐私保护的问题，也有一部分研究者将较为成熟的安全传输方案应用到基于区块链的车联网中，下面，我们来总结一下各种方案的实现方式。

1. 非对称密钥加密
2. 进阶，环签名和多签名
3. DataTagging

4.4车联网系统的优化

为了在现有的硬件发展水平下，使“车联网+区块链”的体系能够实现更强大的功能，更加满足我们对便捷性和舒适性等方面的需求，优化系统性能也是我们不可忽视的研究领域。通过借助一些针对性的系统设计理念，可以在一定的硬件配置下提高车联网方案各方面的效率指标，如通信效率、存储效率、计算效率等等。研究者在这方面做了大量的努力，一些方案中都提出了较为有效的方法，来降低系统中的延迟、提升系统的事务吞吐率等等。还有一部分研究致力于提高系统的可用性，提高鼓励用户提交真实有用的数据来加强系统内数据的真实性和丰富性，使用户能够从中获取有用的信息。

4.4.1 效率优化

车联网的构建往往基于较大的地理范围，为不断运动的会有数以千万计的车辆提供信息交互服务。大量的用户会带来大规模的数据流量，对计算力、通信带宽和存储空间都是极大的考验。接下来，我们将逐一分析各种方案中对这些问题的解决办法。

分层，分区

将车联网分而治之，形成分层次的系统结构，是有效降低整个网络上通信量、提高区块链效率的经典办法之一。对于大多数应用场景，车辆只关心其附近范围内的事件（如智能交通系统、电动车充电系统、事故记录系统等），而不必把信息传播到整个系统中，也不需要时常获取整个系统中的信息，因此我们可以像行政区域划分一样，将车联网根据地理位置划分为较为独立的cluster，实现cluster内部的事务自治和cluster之间的交互。

Blockchain: A distributed solution to automotive security and privacy[]的做法是不依靠RSU等基础设施通信，直接由相近车辆组成集群，以实现集群内高效的数据交互，在集群之间没有消息交流。Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication[]采用联盟链方式，将一定区域内的车辆和RSU划分为cluster，在其内部完成共识算法后，再由每个集群的集群头一起完成整个网络的共识。

MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X[]提出了一种微区块链架构来为GDID范式构建可靠的入侵策略。该架构包含一个宏观区块链和几个微观区块链。本地入侵样本和入侵检测策略可以通过部署和运行在特定区域的微区块链架构快速存储、预付和传播。多个微区块链可以构建更大的微区块链，为在大区域内移动的车辆提供时空动态入侵检测策略。微区块链收集的所有数据都将存储在宏观区块链中，以验证所收集数据的合法性，并为数据提供者生成加密货币。

快速的交易确认

SpeedyChain: A framework for decoupling data from blockchain for smart cities[]采用了一种customized blockchain，它依赖于每个车辆产生的由其公钥标识的块，来存储已签名的事务，以解决通过共识算法来验证交易造成的高延迟与计算力消耗。这种区块链允许通过前面信息的散列将数据直接追加到现有块，并对新创建的信息进行签名。车辆会从传感器收集数据、签名并生成一个新事务，并发送到最近的RSI以求验证。RSI可以访问存储在区块链块标头中的车辆公钥。当事务被认证为有效时，它会立即被附加到该车辆的当前块中，（如果这是一个新加入网络的车辆，则创建一个Genesis Block）。为了确保车辆的私密性，通信使用的非对称密钥对会在特定的时间段之后(称为KUI)进行更改。由于车辆的资源有限，它们只需要维护一个块的Merkle树，而不是保持整个区块链。

高效的共识算法

4.4.2 鼓励数据交流