缩写汇总：

1. 电动汽车 V2G
2. 注册管理机构 RA
3. 本地聚合器 LAGs
4. 全局分类账 Global Ledge

**基于区块链的车辆到电网的网络隐私保护支付机制**

**摘要**

作为V2G网络的一个组成部分，EVs不仅从电网接收电力，还从其他EVs接收电力，并且可能经常将电力馈送回电网。V2G网络中的支付记录对于提取用户行为，促进优化电源、调度、定价和消费的决策。然而，除了面临现有的安全可靠这个挑战，共享支付和用户信息引起了严重的隐私问题。在本文中，我们提出了一种基于区块链的V2G网络隐私保护支付机制，可以在保护敏感用户信息的同时实现数据共享。该机制引入了基于区块链技术的注册和数据维护过程，该技术确保用户支付数据的匿名性，同时允许特权用户进行支付审计。 我们的设计基于Hyperledger实施，仔细评估其可行性和有效性。

**引言**

V2G网络中EVs作为能源供应商和消费者，正在迅速成为未来智能电网的一个重要增强。在V2G网络中，所有参与者（如EVs和电网）之间的双向输电产生大量的用电支付记录，这些记录可以共享，以提供有价值的服务，如负荷预测、价格预测、最佳能耗调度和电动汽车辅助服务行为建模[1]- 3。但是，共享支付记录可能会引起敏感信息泄漏的隐私问题，如身份、地点以及电动汽车的充电或放电量。因此，在V2G网络中，应仔细分析和平衡隐私保护和信息披露之间的关系。

传统的支付方式，如信用卡和Paypal转账，需要与众多的第三方关联。该关联与多个组织生成分布式支付记录信息，无需用户同意或自愿即可共享。各种匿名支付机制[4–6]支持EVs的隐私保护，其中大多数是集中的，并使用受信任的第三方来处理支付。虽然它们满足保护参与者身份的隐私要求，但在对多个实体之间共享支付记录进行分析时，它们不能隐藏身份。此外，集中设计可能会遇到单点故障的风险。

区块链作为数字货币系统中一种新兴的、有前途的技术[7]，具有交易匿名性、可信度和高分布性等优点，促使我们在满足数据共享要求的同时探索其在建立匿名支付机制中的应用。

为了实现这一目标，我们解决了两个主要挑战。第一个挑战是同时保证交易的可靠性和效率。例如，作为最广泛使用的基于区块链的应用程序之一，比特币每秒仅支持7个交易，并且具有有限的可扩展性。许可（私有）区块链技术（如Hyperledger[8]）实现了更好的可扩展性，但无法保证交易的可靠性，因为它在不验证交易是否有效的情况下将商定的交易记录到分类账中。第二个挑战是基于区块链的系统的可审计性。鼓励这些系统的用户为每个事务生成一个新的假名，以保护其身份不受潜在攻击者的攻击。这种增强隐私的机制为识别恶意交易建立了障碍。这一限制在勒索软件攻击（Wannacry，2017年5月）中表现非常显著，勒索交易被发送到比特币账户，而比特币账户不容易追溯到恶意用户。

在本文中，我们介绍了V2G网络中的各种支付场景，并找出存在的问题，以强调隐私保护和数据共享之间的冲突。在此基础上，提出了一种基于区块链的V2G网络隐私保护支付机制。我们利用基于数字签名的注册过程来保护交易者的隐私，同时允许特权用户进行付款审核。基于Hyperledger，我们提出了一种针对V2G网络中的支付定制的新型交易结构和相应的交易验证算法，通过增强可扩展性以保证交易的可靠性。给出了所提出机制的概念验证原型，并通过实验验证了其可行性和有效性。我们详细阐述了基于区块链支付机制未来研究的挑战和机遇。

**参考模型支付方案**

在V2G网络中，电动汽车和智能电网之间频繁的双向交互，包括电力传输和支付账单。这些账单被发送到一个支付平台，该平台负责完成支付并与所有利益相关者共享记录。基于这些支付记录，V2G网络中的一些用户可以向其他参与者提供增值服务，例如电价、最佳充电和放电策略。例如，电动汽车车主可以获得有关选择划算的时间（如非高峰时间）充电的建议。V2G电网的整个电力支付过程可分为三个阶段，如图1所。

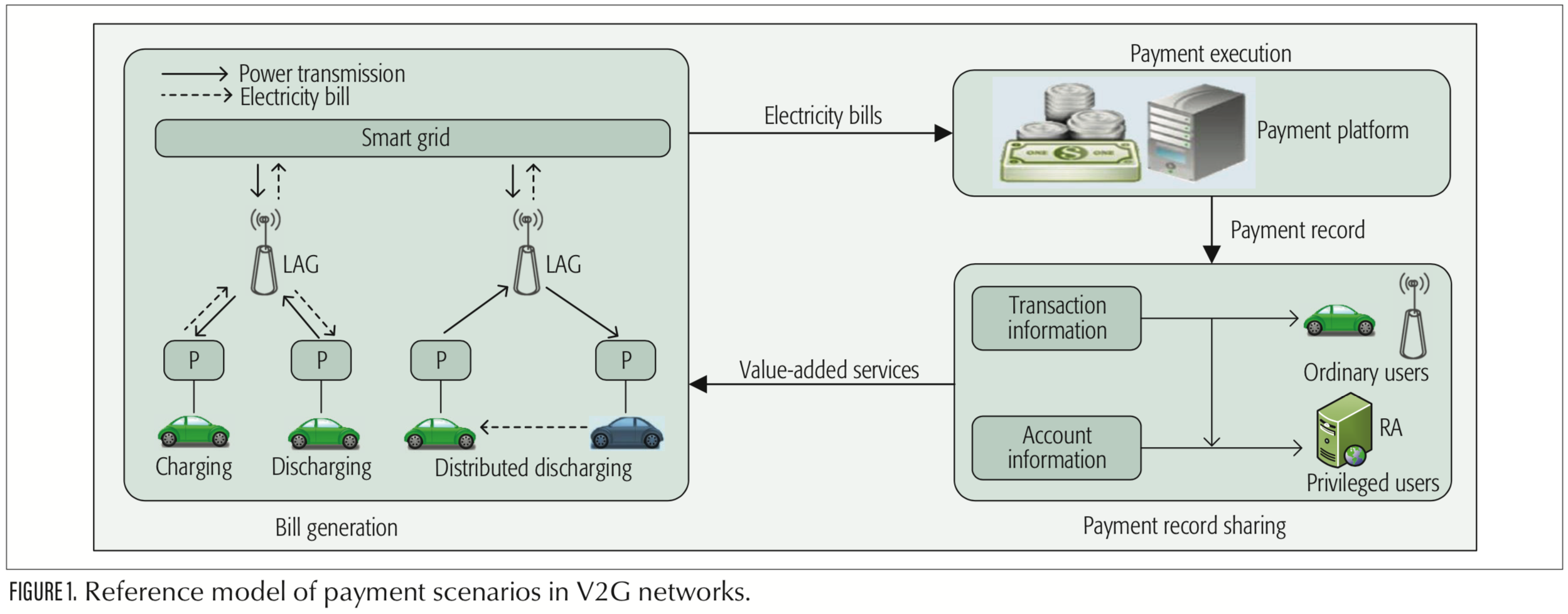


图1. V2G网络中支付方案的参考模型。

**计费：**电动汽车通过停车场专用设施接入V2G网络，并在本地聚合器（LAGs）的控制下向智能电网提供辅助服务[5]。如图1左侧所示，EVs有三种状态：充电、放电和分布式放电。EV充电时，电力从智能电网传输到EV，EV需要向智能电网支付电费。当电网在用户需求高峰时段过载时，智能电网启动放电。EVs可以通过向电网放电来缓解电力短缺，并从智能电网获得经济回报。当一个或多个EVs的电池容量低于某一阈值时，就会启动分布式放电。与充电状态不同，电力充足的EV将暂时充当电力短缺的EV的能源供应商，后者应向供应商EV支付电费。在这些情况下，EV既可以是付款人，也可以是收款人，这需要一个支付机制来支持双向支付。

**付款执行：**图1的右上角显示了付款执行的过程。支付平台负责在收到电费后进行支付，并向V2G网络用户提供详细的支付记录。支付机制应提供可靠的交易，以确保交易的真实性和不可否认性。此外，支付机制应支持审计以解决支付纠纷。

**付款记录共享：**付款记录共享过程如图1右下角所示。付款记录包含两种类型的数据：交易信息和账户信息。交易信息包括总价和单价，可以用来计算电力需求。账户信息包含交易者的身份。普通用户（如EVs和LAGs）可以获取交易信息，提供增值服务，如预测用电趋势。但是，为了保护用户隐私，帐户信息是匿名的。由于注册机构（RAs）等特权用户负责审核交易和识别恶意用户，因此他们需要了解交易的详细信息和帐户信息。因此，支付机制应在数据共享的情况下保护用户隐私，并允许特权用户进行审计。注册过程的主要任务是将用户生成的帐户提交给RA进行身份验证和注册。只有RA签署的账户才是合法的，并且在支付机制中是可接受的。

**威胁模型**

电子交易系统中出现了许多安全挑战。在本文中，我们主要关注两种类型的威胁：隐私披露和不可靠的支付。

**隐私披露：**在V2G网络中，EVs通常通过不安全的无线链接连接到LAGs。因此，攻击者可能会窃听支付信息。由于付款记录将在所有参与者之间公开共享，潜在的攻击者可能推测电动汽车的敏感信息，例如充电地点和时段。此外，攻击者还可以与恶意用户串通，从支付记录中获取隐私信息。例如，恶意的EV所有者可以将其位置信息和付款记录发送给攻击者，从中可以推断其他EV所有者的位置。

**不可靠的支付：**攻击者试图通过创建不可靠的支付来欺骗诚实的用户（或LAG），例如伪造支付和双倍支出（即数字货币至少花费两次的数字现金方案错误）。在没有可信第三方的完全分布式系统中，检测和拒绝不可靠的付款是困难的。

**设计目标**

我们的目标是为V2G网络设计一个匿名支付机制，同时满足数据共享和隐私保护的要求。设计目标总结如下：

**数据共享的隐私保护：**完整的支付记录，而不是统计数据，应该以安全有效的方式在所有参与者之间共享。对手无法从支付记录中推断出交易员的真实身份。

**匿名交易的有效审计：**虽然EVs和LAG的付款记录是匿名的，但授权的审计员应该能够在匿名交易中获得交易者的真实身份，从而能够追踪到参与恶意交易EVs的身份。审计员不应该能够改变交易。

**可靠高效的支付：**应选择并改进高效的区块链技术，以实现支持可靠高效支付的新支付机制。这些技术应该能够发现和拒绝不可靠的付款，如双倍付款、伪造付款和撤销付款。此外，支付机制应具有比当前解决方案更好的可扩展性，以满足V2G网络的实际交易需求。

**V2G网络的现有支付机制**

在过去十年中，许多研究工作都集中在v2g网络上[46]。我们简要总结了匿名支付机制在保护电动汽车隐私方面的最新成就。

Yang等人[4]提出了利用盲签名实现匿名奖励支付的机制p2。Wang等人[5]提出了一个可追踪和隐私保护方案，该方案具有基于许可的策略，类似于具有更强安全保障的P2。这些匿名支付机制通常依赖于受信任的第三方，第三方会遇到各种威胁，例如单点故障和内部和外部入侵。Man等人[6]和Zhao等人[9]提供了分散的匿名支付机制，而不依赖可信的第三方。这些机制要求在每个EV上部署受信任的平台模块，该模块分发存储在不同EV上的支付数据。因此，中间节点和计费服务器不能学习特定的支付信息。虽然用户隐私得到了有效的保护，但支付信息等数据共享却很困难，而且分散在不同的电动汽车中。

**区块链概述**

区块链是一个分布式数据库，它维护着不断增长的数字交易列表[7]，并为匿名参与者之间的在线交易提供了一种安全方法。因此，该数据库本质上与在缺乏可靠的中央服务器的情况下完成可靠的匿名支付机制的需求一致。一些开创性项目已将区块链应用于能源相关交易[10]。典型的区块链系统通常由三个主要组成部分组成，如下所述：

**区块链网络：**由多个节点（运行区块链客户端的独立主机）组成的点对点网络。所有参与节点都具有相同的状态，以避免单点故障的风险。

**区块链交易：**交易记录用户之间的数据交换过程，包括发送方和接收方的地址和交易内容。地址是用于区块链交易的假名，类似于银行卡号。交易内容根据具体应用场景定义。在数字货币应用程序中，交易内容表示事务量，并且可以表示其他应用程序中的字符串或证书ID。在本文中，交易内容应与电力传输相关。

每个交易都是广播的，而不是直接发送到区块链网络中的目标节点（即接收器）。目标节点最终可以从网络接收交易，而无需直接联系发送节点。因此，通过窃听来跟踪交易源很困难，这有助于实现匿名性。

**全局分类账：**全局分类账用于存储区块链系统中的所有交易，该系统通常包含一个区块链。每个块记录一定数量的事务。通过记录前一个块的哈希值，新块将附加到全局分类账。因此，分类账形成了从初始块到最新块的数据链。

区块链网络中的每个节点都维护一个唯一的全局分类账，并通过共识算法与其他节点同步。当交易执行时，支付方节点在区块链网络中广播交易信息，区块链网络根据共识算法选择一个特殊节点对交易进行认证，并将交易写入全局分类账。其余节点通过区块链网络同步其全局分类账。共识算法确保所有合法节点存储相同的全局分类账。

**基于区块链的隐私保护支付机制**

我们提出了一种分散的匿名支付机制，使V2G网络中的EVs能够进行隐私保护数据共享，并结合注册过程来实现设计目标。

**（1）系统实体说明**

**用户：**用户包括EVs和参与交易过程的实体，如充电设施。它们可以作为付款中的两个角色之一，即付款人和收款人。每个用户安装一个区块链客户端来处理支付交易并维护一个全局分类账。大多数现代电动汽车都配备了计算和通信功能，可用于运行区块链客户机模块。

**注册管理机构（RA）**：RA是一个被授权的审计机构，例如仲裁机构，负责账户注册和付款记录审计。RA安装一个区块链客户机来维护一个包含所有付款记录的全局分类账，并维护一个存储所有注册帐户和相应身份的证书存储库。因此，RA被认为是一个安全的实体，它不仅可以查看所有付款记录，还可以查看匿名付款记录中任何人的真实身份。

**区块链网络：**区块链网络是指区块链基础设施和沟通协商机制。在提议的支付机制中，区块链网络的工作方式与下文所述相同，但交易结构和交易验证方法除外。

**（2）体系结构和功能**

基于区块链的支付机制由几个部分组成，如图2所示。

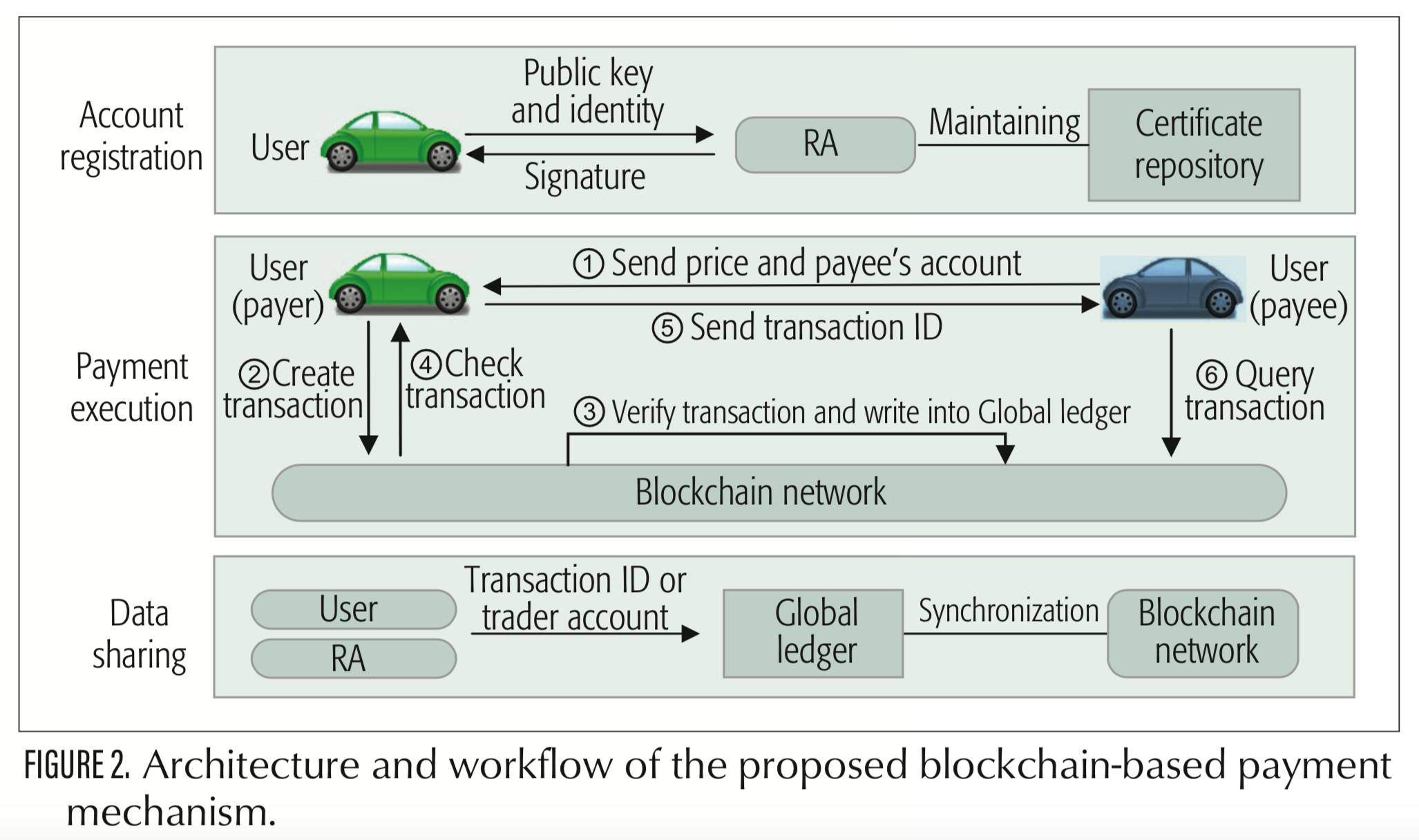
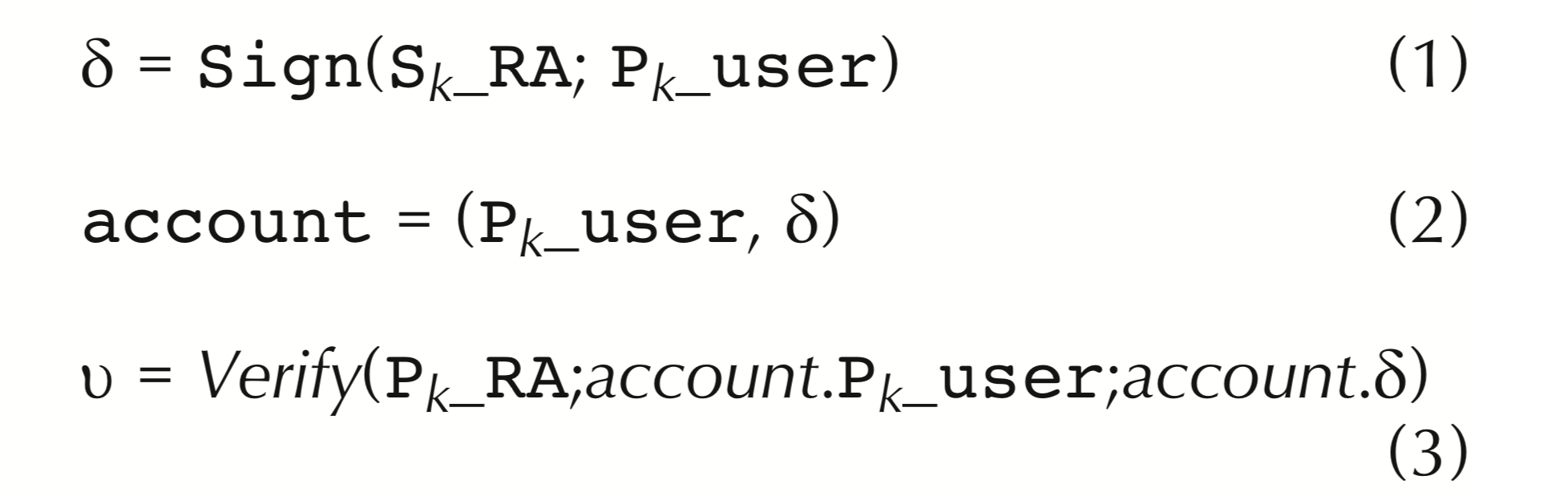


图2.所提议机制的体系结构和工作流

**帐户注册：**注册过程的主要任务是将用户生成的帐户提交给RA进行身份验证和注册。只有RA签署的账户才是合法的，并且在支付机制中是可接受的。

注册过程包括以下步骤。用户使用非对称加密算法（如RSA或ECC）创建一对密钥(Pk\_user; Sk\_user) ，然后将Pk\_user及其身份信息（如个人ID或驾驶证）发送给RA。在检查身份之后，RA用签名δ回复用户，签名δ是使用私钥Sk\_RA 生成的，如等式1所示。RA将Pk\_user和相应的标识存储在证书存储库中。用户与Pk\_user和δ一起生成一个合法帐户。合法帐户格式如等式2所示。我们假设RA的公钥Pk\_RA可以从公共渠道获得。因此，每个用户都可以利用Pk\_RA验证一个帐户，如等式（3）所示，其中v=1表示一个有效的签名和一个合法的帐户，否则v=0。

注册过程包括以下步骤。用户使用非对称加密算法（如RSA或ECC）创建一对密钥(Pk\_user; Sk\_user)，然后将Pk\_user及其身份信息（如个人ID或驱动程序许可证）发送给RA。在检查身份之后，RA用签名δ回复用户，签名δ是使用私钥Sk\_RA生成的，如等式1所示。RA将Pk\_user和相应的标识存储在证书存储库中。用户与Pk\_user和δ一起生成一个合法帐户。合法帐户格式如等式2所示。我们假设RA的公钥Pk\_RA可以从公共渠道获得。因此，每个用户都可以利用Pk\_RA验证一个帐户，如等式(3)所示，其中v=1表示有效的签名和合法帐户，否则v=0。



用户可以一次向RA申请多个公钥的签名，在区块链中周期性更新账户地址(公钥)来抵抗背景攻击，保护身份隐私，所以之前准备的一批公钥签名用光了就要新准备一批再去申请。

**付款执行：**此阶段确保付款方成功支付电费，并使收款方能够验证收据。在提议的支付机制中，支付作为区块链交易实现。因此，付款执行实际上是被验证并写入全局分类账的交易的过程。

收款人将其账户和单价发送给付款人。该账户是在注册过程中生成的，其中包含RA提供的签名信息。收款人可以为每个交易使用不同的帐户来保护隐私。然后，付款人计算电费账单，通过其区块链客户机创建交易，并最终将交易发送到区块链网络。区块链网络收到交易后，对交易进行验证，并将合法交易写入全球账本。一旦在全局分类账中记录相应的交易后，付款即完成。

付款人检查全局分类账，直到付款完成。然后，付款人将交易ID发送给收款人。如果一笔交易的账户和金额准确，收款人开始提供服务，如电力传输。

支付过程的执行频率高于登记过程，电动汽车通常具有有限的计算和通信能力，这导致支付信息保护不足。我们设计了一种适当的机制，以确保在不可靠的通信通道中为EVs提供事务可靠性和隐私，这将在下一节中介绍。

**数据共享：**数据共享过程的重点是支付记录的共享策略。在提议的支付机制中，所有合法的支付记录都会写入全局分类账。由于所有参与者都可以访问全局分类账，因此想要查看或查询付款记录的成员可以简单地在其区块链客户机中同步全局分类账。

由于支付记录中的帐户是假名，因此EVs和恶意用户无法将支付记录链接到特定用户，这会阻止隐私泄漏。RA可以从证书存储库中获取每个帐户的身份信息，从而有效地审计付款记录。

绿格子中的字

由于支付记录中的帐户是假名，因此电子邮件和恶意用户无法将支付记录链接到特定用户，这会阻止隐私泄露。 RA可以从证书库获取每个帐户的身份信息，以有效地审计付款记录。

确保不可靠通信信道中EV的交易可靠性和隐私，这将在下一节中介绍。

# 交易和验证

支付流程涉及多种区块链技术，例如信息传递，交易和共识机制，这些技术等同于现有区块链系统中容易获得的区块链技术。我们专注于交易结构和交易验证方法的设计，这些是实现与现有区块链系统不同的设计目标的关键组成部分。

为了获得更好的可扩展性，我们选择Hyper-ledger [8]而不是Bitcoin [7]来实现建议的支付机制。但是，Hyper-ledger并非专为数字现金而设计，其中每个Hyperledger交易都记录在全球分类账中，而不验证其合法性。因此，我们设计了一种新型的交易结构和基于Hyperledger的相应验证方法，以保证支付交易的可靠性。

交易结构：受比特币的启发，我们设计一个在V2G网络中可靠支付的交易结构，如图3a所示。每个事务都有一个唯一的ID txid和一个唯一的哈希值txhash作为事务的索引。交易内容由三部分组成：源字段，价格字段和目标字段。

源字段列出此事务中的一个输入或多个输入。输入是对先前事务的输出的引用，并且是

表示为<sn\_sf，pre\_txhash，pre\_sn\_df，signa-TURE>。这里，sn\_sf是该事务的源字段中输入的序列号; pre\_txhash是引用事务的txhash值; pre\_sn\_df和signature分别是引用事务中特定输出的序列号和所有者的签名。任何人都可以使用签名来验证付款人对此输入的所有权。

价格字段表示单价（即支付时的电价）和该支付的总金额。执行验证过程以确保所有输入值的总和不小于总量。

目标字段列出一个输出或多个输出。输出是对付款人帐户的引用，用<sn\_df，account，amount>，其中sn\_df是序列号此交易的目标字段中的输出，帐户是收款人的帐户，金额是此输出的值。所有输出共享此交易中输入的组合值。当组合输入值超过此支付的总金额时，还可以将付款人的帐户列为输出以接收更改。

如图3b所示，事务10002中的sn\_sf = 0和pre\_txhash = 3306ff5a-64d900937ad1429466fd2c8f的输入使用sn\_df从输出中导入值在交易10001中= 1。任何人都可以获得来自收款人10001中收款人帐户的公钥并验证签名2。

交易验证方法**：**验证是用于保证支付可靠性。 我们提出了一种验证方法来拒绝伪造的交易，而无需输入账户和非法账户的非法交易。 验证方法的工作流程描述如下：

•验证交易信息是否满足格式要求。

•验证所有帐户是否合法，包括输入和输出帐户。 验证者可以使用RA的公钥来验证帐户的签名，以检查帐户是否合法。

•验证源字段中的所有签名是否正确。 验证签名所需的公钥是从pre\_txhash和pre\_sn\_df表示的事务中的相应输出帐户获得的。

•验证输入量是否大于或等于总产出量。

# 系统设计分析

数据共享**：**在比特币和Hyperledger中，交易数据由所有参与者存储。主要区别在于比特币是一种无权限的区块链，任何人都可以加入比特币网络并自由获取所有支付记录，而Hyperledger是一个经过许可的区块链，其中只涉及授权用户。建议的机制建立在Hyper-ledger上，支付记录只能在注册成员之间轻松共享，例如EV，LAG和RA。例如，成员可以通过运行区块链客户端获取包含所有支付记录的唯一全局分类帐。

隐私保护**：**比特币主要依靠假名来实现匿名交易。但是，流量分析攻击可以轻松识别创建事务的源节点[11]并通过全局分类账中的交易记录推断出假名的交易规则[12]。因此，这些攻击会降低假名的匿名性，攻击者可能会推断出假名的身份。在Hyperledger中，外部攻击者很难窃取私人数据，因为只有授权用户才能访问区块链网络。内部攻击者（如恶意授权用户）可以通过分析全局分类帐中的事务数据来推断假名的身份。拟议的机制引入了一个实施RA以存储相应的假名身份信息以满足审计要求。RA仅在交易争议的情况下提供身份信息，因此不经常参与支付执行过程。因此，与传统的集中支付机制相比，RA能够处理内部攻击。与比特币相比，只有授权用户才能获得交易信息，这可以防止外部攻击者。我们机制中的用户可以在单个注册过程中注册多个帐户，并为每个交易使用不同的帐户。这种一次性帐户策略可以在不同帐户之间传播用户的交易规则，从而抑制基于交易数据分析的攻击。

审计**：**在比特币和Hyperledger中，审计很难，因为审计员无法轻易获得交易背后的身份信息。

我们的机制通过引入注册流程和有效的验证方法来支持有效的审核。通过注册过程，RA维护一个包含所有合法帐户及其身份信息的证书存储库。使用交易验证方法，只有合法帐户创建的交易才能记录在全局分类帐中。因此，RA能够获得任何事务背后的身份信息，这使得能够进行审计。

建议的机制建立在Hyperledger上，支付记录只能在注册成员之间轻松共享，例如EV，LAG和RA。 例如，成员可以通过运行区块链客户端获取包含所有支付记录的唯一全局分类帐。

可靠的支付**：**比特币系统专为数字货币交易而设计，并支持可靠的支付。最初的Hyperledger并非专为数字现金而设计，每笔交易都直接记录在全球分类账中，而无需验证其合法性。

在我们的机制中，我们提出了一种新型的交易结构和相应的验证算法，该算法基于原始的超级分类帐系统，以实现可靠的支付。一旦交易记录在全局分类账中，它就不会被篡改，这可确保先前记录的交易是可靠的。通过清楚地识别输入的来源和其所有者的签名，交易中的每个输入都是可靠的并且是合法授权的。由于全局分类帐是公开的，因此区块链网络中的所有节点都可以使用历史事务来检测先前是否已使用事务中的输出，这有助于防止双重支出攻击。

# 概念验证和评估

我们基于Hyperledger（Fabric V0.6）[8]实现了建议的支付机制的原型。我们采用操作系统级虚拟化技术Linux容器（LXC）来模拟具有中等计算和存储容量的四个V2G用户，其中每个用户都配备了Inter（R）Core（TM）2.5 GHz 64位CPU，8 G DDR3L RAM和1T 5400转硬盘。该

四个用户包括付款人，收款人，RA和普通用户以进行交易验证。注册过程的时间消耗主要由用户侧的公钥 - 私钥对生成过程和RA侧的签名过程决定。因此，我们使用256位曲线secp256k1上的椭圆曲线数字信号算法（ECDSA）模拟密码方案的时间开销。生成新的公钥 - 私钥对和签署公钥的平均执行时间分别约为3.16毫秒和3.45毫秒。图4a显示了注册过程中加密方案的性能。两种方案的处理时间随着帐户数量的增加而线性增加。我们假设每个用户每天采用10个新公钥，并按月执行注册过程，这近似于V2G网络中单个EV的交易频率。因此，每个注册过程包含大约300个公钥 - 私钥对生成和300个签名，这需要大约1.935秒。在支付过程中，我们专注于交易处理速度和交易确认时间。前者指的是支付机制每秒进行的交易数量，而后者指的是从付款人提交交易到全局分类账中此交易记录的时间间隔。

1.0

0.0

0

100

200

300

400

100

200

300

400

450

350

250

150

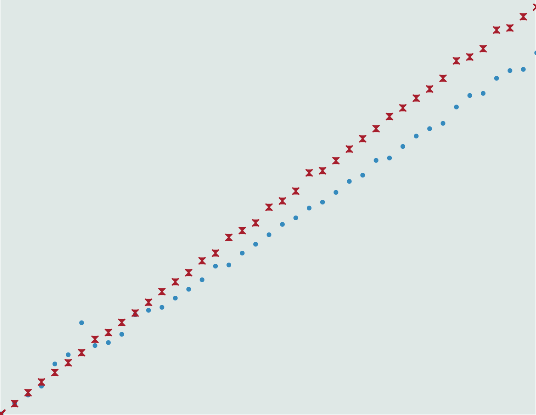
50

350

250

150

50



Key generation ECDSA signing

Number of accounts

(a)

Number of concurrent transactions per second (b)

0.5

1.0

Processing time (s)

Transaction confirmation time (s)

图4.性能评估：a）加密方案的计算时间; b）拟议机制的交易确认时间

典型区块链系统中的事务处理速度和确认时间明显低于传统集中式架构中的事务处理速度和确认时间。例如，比特币系统每秒仅支持七次交易，确认时间大约需要一小时。

为了大幅提高交易速度，我们采用Hyperledger实现支付机制并采用Byzantine算法来达成共识[13]。我们的实施能够实现每秒300次交易。我们发现，当Hyperledger中的配置参数被微调时，事务确认时间可以减少到不到一秒，如图4b所示。图4b中的x轴表示每秒的并发事务数，y轴表示平均事务确认时间。曲线由三个阶段组成。在第一阶段（即，50-250），时间随着事务吞吐量的增加而降低。这种趋势是由区块链系统的批处理机制引起的，也就是说，当并发事务量相对较小时，系统必须等待预定数量的事务记录在单个块中。在第二阶段（即250-350），系统实现最短的确认时间。在最后阶段，交易确认时间开始增加，因为当交易量超过处理能力时，无法及时确认大量交易。从图4b中我们可以得出结论，在并发事务的数量小于最大容量的条件下，交易确认时间可以在两秒内保持，这满足了一般要求。我们的系统在交易吞吐量和交易确认时间方面优于比特币[7]和以太网[14]。如表1所示，比特币每秒支持七次交易，每个交易需要600秒才能记录在全局分类账中。以太坊每秒可完成25笔交易，确认时间为10秒。

|  |  |  |
| --- | --- | --- |
| Systems | Throughput (T/s) | Confirmation time (s) |
| Bitcoin | 7 | 600 |
| Ethereum | 25 | 10 |
| Proposed scheme | 300 | 2 |

表 1. 不同区块链系统的性能比较。

在数据共享过程中，我们关注的是存储需求而不是时间消耗，因为用户可以在同步最新的支付记录后直接查看本地全局分类帐。在区块链网络中，每个节点都保留全局分类帐的副本，该副本包含所有事务记录和一些其他参数。由于主存储消耗包含交易数据，因此我们根据单个交易的大小和每天的交易数估算每个节点的存储消耗。我们假设常规事务包含两个输入和两个输出。

根据图3中的事务结构，我们可以计算事务的大小，如表2所示。事务的大小是536字节。假设V2G网络包含10,000个EV，每个EV每天创建10个事务，每天创建大约100,000个支付记录，交易数据大小约为每天54 MB或每年19 GB。

# 研究方向和机会

将区块链技术纳入V2G网络是一个很有前途的研究课题。 然而，仍然存在这方面的若干挑战，这为未来的研究创造了更多的机会。 基于本文中介绍的工作，我们描述了需要研究团体立即响应的三个主要途径。

多样化的隐私需求：在本文中，我们实现了基本的匿名交易，而没有考虑更复杂的计费方案，例如会员福利政策和现金反馈策略，这需要更复杂和有针对性的隐私政策。随着区块链的快速发展，将设计许多不同的机制来满足不同的隐私要求。例如，以太坊提供图灵完整的脚本语言，可用于在分散的环境中实现传统的隐私保护算法。需要分析更复杂的脚本技术和相关的体系结构更改[15]。

适当的定价政策：这个因素对于吸引电动汽车采用基于区块链的支付机制非常重要。区块链支持高频率，低价值和可靠的交易，有助于实现更灵活，更有效的定价政策。例如，适当的定价政策使得能够准确计费以审核电力传输量，其可用于支持EV的定制电力购买和销售价格。

效率和实用性：区块链可用于简化支付流程;然而，由于特殊的共识机制，它面临着性能瓶颈。以节省时间的方式验证V2G网络中的大量事务是一项挑战。为提高区块链的效率，已经提出了越来越多的新提案，例如Lightning网络，它每秒支持超过47,000次交易。随着新区块链技术的发展，我们可以预见到交易效率将不断提高，以满足V2G网络的要求。

# 结论

本文介绍了一种基于区块链的私有保留支付机制，该机制可以满足V2G网络中数据共享和隐私保护的要求。通过设计注册流程，新的支付机制启用了支付审计，同时保留了数据隐私。增值服务提供商可以轻松获取支付记录以进行分析，而无需推断电动汽车的身份或私人信息。支付机制中使用的区块链技术保证了支付流程的可靠性。签署的交易一旦写入全球分类账，相应的支付记录就是防篡改和不可赎回的。我们实施了拟议支付机制的原型，并使用模拟证明了其可行性和有效性。我们还讨论了未来的挑战和研究机会。

# 致谢

这项工作得到了中国国家重点研究与发展计划的部分支持，授权范围为2016YFB0800301; 部分由中国国家自然科学基金委员会批准。NO.61772236，NO. 61602039，NO.61370027; 部分由CCF-Venustech开放研究基金提供。 孟申博士是相应的作者。

绿字部分：通过设计注册流程，新的支付机制启用了支付审计，同时保留了数据隐私。 增值服务提供商可以轻松获取支付记录以进行分析，而无需推断EV的身份或私人信息。

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Size (bytes) | Number | Total size (bytes) |
| Txid | 2 | 1 | 2 |
| Txhash | 32 | 1 | 32 |
| Sn\_sf | 2 | 2 | 4 |
| Pre\_txhash | 32 | 2 | 64 |
| Pre\_sn\_df | 2 | 2 | 4 |
| Signature | 71 | 2 | 142 |
| Unit price | 2 | 1 | 2 |
| Total amount | 2 | 1 | 2 |
| Sn\_df | 2 | 2 | 4 |
| Account | 138 | 2 | 276 |
| Amount | 2 | 2 | 4 |

表2. Transaction size.

**Biographies**

冯高收到了B.Eng。 2010年获北京理工大学软件工程学院学位。现任博士学位。北京理工大学计算机科学与技术学院候选人，北京，中国。他的研究兴趣包括数据隐私，区块链和智能电网。

朱烈煌是北京理工大学计算机科学与技术学院的教授。他被中国人民解放军教育部选入大学新世纪优秀人才计划。他的研究兴趣包括物联网，云计算安全，互联网和移动安全。

孟申收到了B.Eng。 2009年获得山东大学济南分校博士学位。 2014年毕业于中国北京清华大学，均为计算机科学专业。他目前是北京理工大学计算机科学与技术学院的助理教授。他的研究兴趣包括隐私保护和云计算。他是IEEE的成员。

KaShiF ShariF获得了他的硕士学位。 2004年获得信息技术学位，并获得博士学位。 2012年获得美国北卡罗来纳大学夏洛特分校的计算机和信息学学士学位。他目前是中国北京理工大学的副教授。他的研究兴趣包括无线和传感器网络，网络仿真系统，软件定义和数据中心网络，ICN和物联网。他是IEEE和ACM的成员。

Zhiguo Wan是山东大学计算机科学与技术学院副教授，济南。他的主要研究兴趣包括大数据的安全性和隐私，加密货币，智能电网等。他获得了B.S. 2002年获得清华大学计算机科学学士学位和博士学位。他于2007年获得新加坡国立大学计算机学院的学位。他于2006年至2008年在比利时鲁汶的Katholieke大学担任博士后。他是IEEE的成员。

奎仁现任浙江大学网络安全研究所和计算机科学与技术学院。他的研究兴趣包括云和数据安全，物联网和移动安全以及隐私增强技术。他是IEEE的会员和ACM的杰出成员