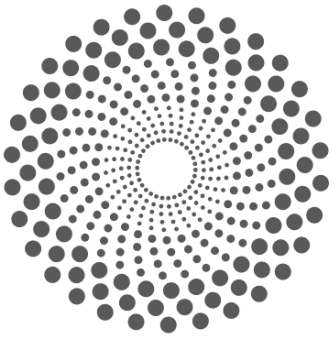


EVA.IO

A decentralized Platform for Electric Vehicle Application

电动汽车分布式数据库及应用平台

The evaio team

www.evaio.info

1. 背景

随着特斯拉为首的新一代汽车企业崛起，汽车行业正在经历一场智能革命。越来越多的汽车开始搭载 4G 模块，车载操作系统也变的更友好和开放，开发者们也将可以在车内平台上开发第三方应用为生活创造价值。目前区块链的进化引发了资产流通模式革命及利益再分配革命，可预见车辆资产数字化及车载去中心化应用也将成为现实；

2017 年 Elon Mask 在特斯拉的下个 10 年主计划内描绘这样的场景，你的爱车清晨送你去上班，你下楼时它已停在那里，你靠近门自动打开；你不需要自己驾驶，车辆已通过深度学习掌握了熟练的驾驶技巧，你可以解放双手来做更多的事；送完你，爱车会跑出去提供无人打车共享服务，为你赚钱。

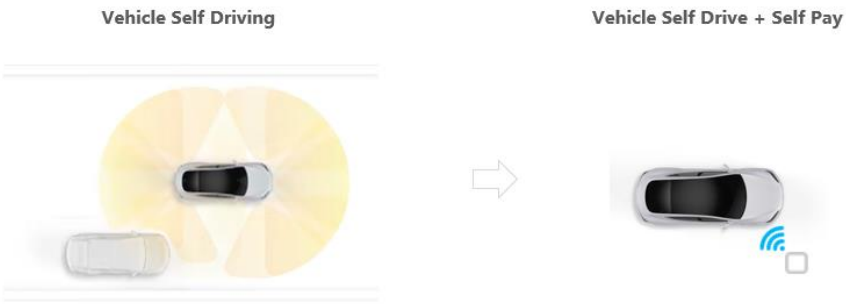
在多年第四级的自动驾驶数据积累和系统持续改进后，实现第五级的全自动无人驾驶也被特斯拉定为短期目标；那时汽车将解放人类，人们从而有更多的时间在车内工作或娱乐，车内环境将变成高频娱乐和商务类应用场景，更多的车载 APP 和 DAPP 需要被开发出来，以让我们在车内的时间被充分利用。

2. 机遇

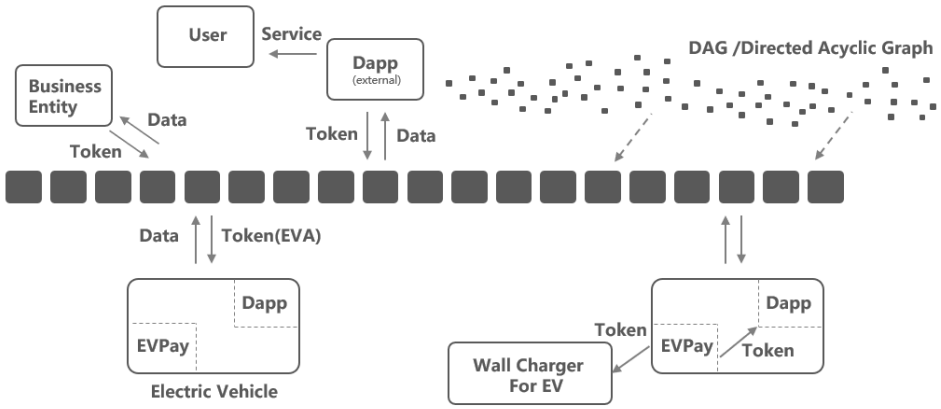
目前众多电动车企并没有很好的解决一些问题，例如：很多的特斯拉购买者都会在车位安装家用充电桩来为自己的车辆充电，但车主并不能方便的在其他私人充电桩充电，大量私人充电桩并不能很好的共享出去，充电桩和车之间缺少一个可信任的支付系统，在无人值守的情况下，这非常重要。如果这么多私人充电桩能够有效利用，不仅可以加速从化石能源向可持续能源过度，又能为车主和电桩所有者创造一定的财富。

其实充电桩和车辆链接起来就已经构成了一个 P2P 网络，区块链技术的崛起让这个 P2P 网络实现价值创造和利益再分配成为可能。

EVA.IO 用区块链技术创造车辆的可信任支付系统可以解决上述充电桩支付问题，当然我们也会对电桩和车辆增加极少量硬件改造，便可在无人驾驶情况下，让车辆有能力和充电桩自主交易；因贡献数据车内账户将收到代币奖励，代币可以用来支付停车费、洗车费等；当然在无人驾驶状态下车辆可以自己去买麦当劳，可以自己去做维修保养并用代币支付，让车辆真正成为一个独立个体变为人的朋友； EVA.IO 的愿景是为电动汽车提供区块链底层技术构架，当自主驾驶成为现实时推动车辆进化到拥有自主支付能力，如下图。同时 EVA.IO 是一条高速公链，可搭载丰富的车载去中心化娱乐应用，通讯应用，共享出行应用，为生活带来更多价值。



3. EVA.IO 特点

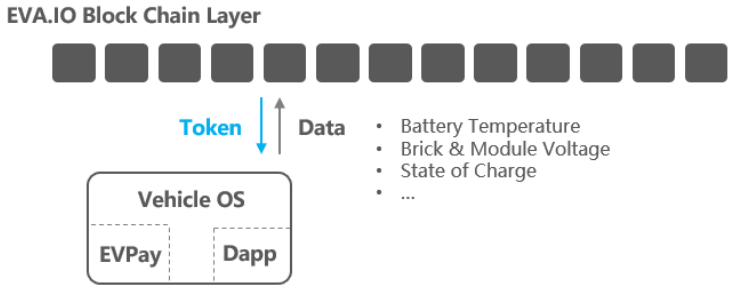


1. DAG 和区块链双构架
2. 电动车预装
3. 里程挖矿
4. 无人驾驶时的全自动代币支付系统
5. 跨币种后台自动兑换能力
6. 影子币和恒定价格支付能力
7. DPOS 机制来选区块生产者和 DAG 节点及 DAG 见证人
8. 免费的电动汽车去中心化 APP 应用平台

4. 基于数据价值创造代币

司机开车的过程中产生了大量数据，数据可以是跟车辆相关的，也可以是跟车主习惯相关的，也可以是APP和DAPP的使用数据；数据可以用来做分析以提供更多精准服务，也可以被反馈以促进产品迭代，毫无疑问这些数据蕴含着巨大价值，但司机们从未真正从这些数据中获利，尽管这些数据是他们跑出来的。

在过去没有汽车可以通过OTA升级，也让数据锁在了车里，特斯拉汽车首创了汽车联网，我们也因此看到了数据快速变现的希望；因为有了区块链技术，数据交易的变现模式变得更简单，每个车主可以立即将数据安全地保密地传输给分布式数据库，同时立即获得代币奖励，代币可以在生态中来用作支付来形成价值转移闭环。



如上图所示EVA.IO被设计成在用户可选的情况下自动将有价值的数据上传至区块链中，作为奖励车辆账户获得代币，它将和交易数据一起被打包进区块，但这些数据并不像交易数据一样被公开，而是进行了加密存储，EVA.IO允许任何第三方在支付一定金额EVA代币从区块链中获取一定的数据，从而实现了价值的变现；第三方可以是整车厂、咨询机构、售后服务商、APP或DAPP开发者，车辆相关的其他服务商。

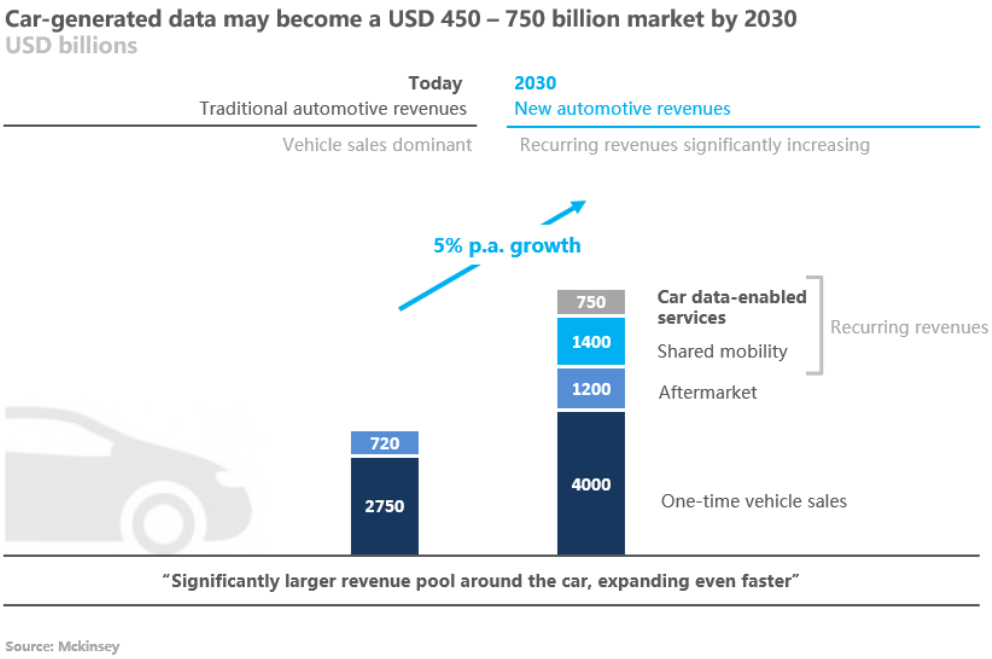
因行车而不断获得代币奖励，这样一个稳定的代币持有群体将吸引更多第三方应用来思考如何提供更个性化的、更未来的应用来鼓励用户把代币消费出去，从而激活了EVA.IO的生态，并形成基于新服务而创造出来的新价值，特别是在无人驾驶后，我们可以预见车内已经变成了一个高频工作或娱乐场景，新服务的形态种类也会超出我们现在的想象。代币将更加活跃且流动起来，更好的服务生态。

5. 丰富的数据

在特斯拉model s中我们看到了很多有意思的数据；例如battery module的温度和电压，传感器读取电压及温度后传输至BMS进行状态监控，实际上BMS只会发出一个动作指令，就是在触发闭合或断开contactor以最终供应或断开电源；battery module的温度在至关重要，不同的温度导致了battery 在充电和放电时表现不一致，长期的结果就是，有些

电芯的寿命衰减的快有些慢；而这种结果会加速电池整体的性能衰减，最终影响电动汽车的质量。这种数据的公开让公众更客观的了解一款产品，也有助于促进产品的性能，在我们看来只有预装型区块链系统才是真正的未来。

特斯拉已收集20亿公里Autopilot数据，将录入其内部程序，用于训练自动驾驶系统”。无独有偶，截止2016年10月底，谷歌累计收集到近350万英里数据，其中包含220万英里的自动驾驶数据和130万英里手动驾驶数据，汽车所产生的数据及价值远超我们想像。在一篇题为“汽车数据货代币化：创造消费者利益的服务业新商机”的报道中，麦肯锡研究员总结道：“全球范围内，汽车数据货代币化的整体利润到 2030 年将达到 4500 亿到 7500 亿美元。”



6. 谁拥有车辆大数据?

Facebook 数据泄漏事件让我们看到了，提供服务的公司把用户产生的数据变相售卖，而用户却没有因此收益，上市公司却因售卖数据而获得收益。

目前已经有车企周期性地传回用户车辆数据，也已有政府机构要求车企将用户车辆运行的数据上传至政府数据库，数据就是价值，如果是用户拥有这些数据的所有权，那么相关机构是否被用户授权免费使用?

虽然目前用户并没有把行车数据把控在自己手中，但这依然改变不了数据的所有权，车主在购买车辆后对车辆及通过车主驾驶而产生的一切数据拥有不可争辩的所有权，在车联网后，数据的传输成为现实，在车区块链化后，数据变现也将成为现实。

7. 数据分级机制

EVA.IO 让用户对开放什么样的数据拥有绝对的控制权，以电池为例我们列举一些数据如下，

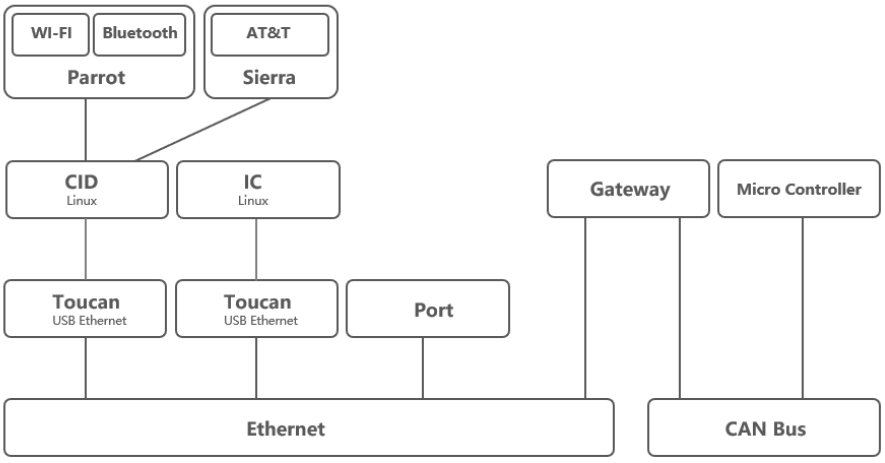
这样的数据上链会非常有意义，除了车辆系统本身的数据外，DAPP 和 APP 的使用衍生数据也将被包含；最终的数据清单和价值将被梳理，并通过社区投票以确定哪些数据应该被上链。

a) 电池电量
b) 电池容量
c) 行驶里程
d) 电池及模组一致性
e) 电池寿命

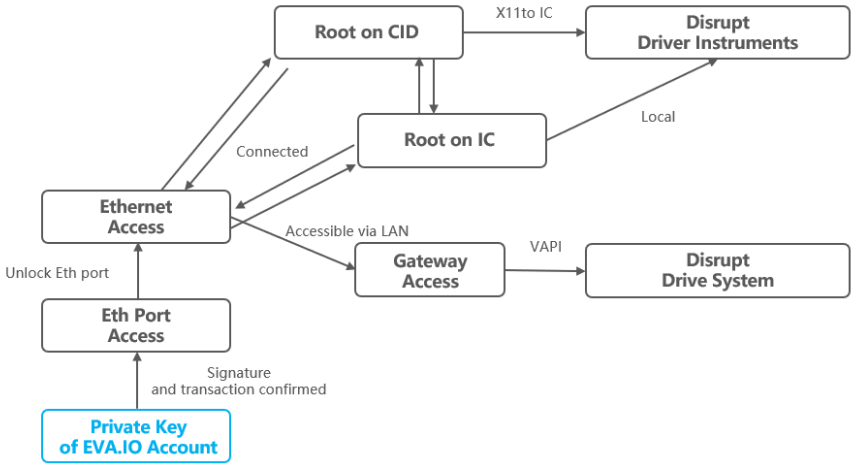
同时，数据将被划分成至少 3 个等级，敏感数据，非敏感数据和隐私数据；让用户根据自己的需要公开全部或部分数据，而获得的代币数量也会根据数据的价值做更精确的模型设计。

8. 车辆安全

无人驾驶情景下，汽车操控安全是最重要的问题，EVA.IO 通过私钥读取数据让车辆更安全，这相当于在车辆联网的情况下，增加一层区块链数据保护层；电动无人驾驶汽车数据可分为车载娱乐、商城等应用层系统数据和 CAN 总线底层数据两大部分，EVA.IO 从安全、性能等角度考虑，对两部分数据采用不同管理方式。以特斯拉 Model S 为例，车载娱乐系统所有组件的信息沟通均透过车载局域网完成，但为了能和车内 CAN 总线实现信息互换，所有指令必须经由车载局域网和 CAN 总线之间的网关传递如下图。



在无人驾驶功能的推动下，车联网功能、近场通讯手段的愈加增多，汽车对外交换数据越来越频繁，导致上可被攻击的地方也越来越多。在上述架构的基础上，EVA.IO 将汽车创造的数据打包进区块链并形成加密代币,最终以交易的形式被区块链节点验证，区块链特有的账户和私钥系统有天然的保密优势，在数据传输时没有通过验证的交易将被排除在外，也因此不能够进一步向车辆系统传输数据，这样的机制大大增强了车载局域网环境的安全性。



9. 对行业的正面推动作用

从大众排放门事件到近期的斯巴鲁篡改数据事件中，可以看到我们无法 100%信任整车制造商给我们看到的数据，无法相信由利益相关方或某一方给出的对比数据，而这些数据严重影响着消费者；通过区块链得到的数据将在真实性上克服这个障碍，EVA.IO 为生态中各个服务方定义了一个面向终端客户的无边界数据共享市场。通过对 DBC 数据交换格式的统一存取，将各 ECU 代表的产品测试运行数据在业界跨厂家共享，从而在 EVA.IO 上生成出汽车产业链信用。同样基于汽车区块链的 DAPP 数据和 CAN BUS 数据一起，在车主受控的前提下，打破企业边界让数据在汽车生态中按用户所需创造满足用户需求的价值。

同时可以想像如果大众或宝马单独做了类似 EVA.IO 的系统，它同样不会被大家相信，因为那将是中心化的产物，我们不能排除他们再次欺骗我们，这也是联盟链不能够和公有链相提并论的原因；EVA.IO 作为一个由社区共同维护的汽车信任生产者，将正面促进汽车行业。

10. EVPAY 跨代币种高速支付工具

每辆电动汽车在向链上传递数据都将获得代币奖励，这些代币将存储在车辆的 EVA.IO 客户端中，在此基础上我们构架了 EVPAY，你可以理解它为一个车辆的支付宝；在此 EVPAY 需要解决交易速度、跨代币种支付、代币价剧烈波动三个障碍才能更好发挥作用；我们用以下三个方案来解决这些问题：

1. 使用“DAG+区块链”的双构架来达到支付级交易速度和系统智能合约的同时调用。
2. “跨币种汇兑和交易所联动模块”来完成系统内的不同币种抵押及汇兑。
3. “影子币 EVAX 结合做空期货模式”来实现交易接收方可以直接收到稳定价值的影子币。

上述解决方案将在本文后部详细描述，除了数字资产本身的问题，阻碍数字资产支付的

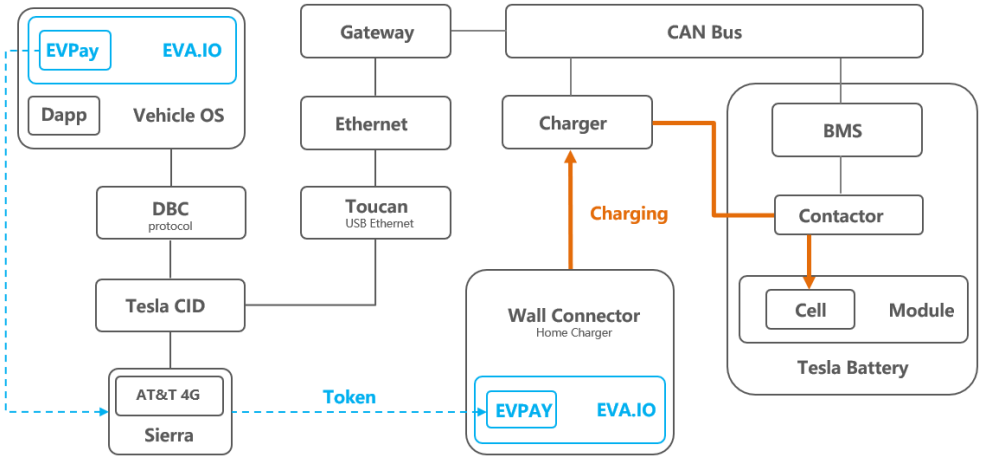
更最重要的原因是：当前实际缺乏将零散、独立的商家和消费者聚合起来的商业场景和驱动力，也就没有了随之而产生的商业应用，从以下观点来看 EVA.IO 的路线图将有效积累用户，留住用户，催生第三方服务，并最后形成真正的车辆支付宝，并最终推动车辆自主驾驶变为车辆自主驾驶+车辆自主支付。

1. EVA.IO 创造了基于数据价值的代币，使其生来就有了基础价值；
2. 在共享电桩支付场景中用法代币价值锚定物支付充电服务来跑通交易闭环，使 EVA.IO 可以顺利用于支付。
3. 推动车企合作，扩大 EVPAY 部署范围。
4. 更多车辆挖矿累积的庞大的拥有代币的客户群。
5. 随着智能汽车的到来，车内服务 DAPP 和 APP 增多，促使客户群在车内产生更多消费。
6. 无人驾驶电动汽车实现 “驾驶时间”向“消费时间”迁移，车内封闭、无聊的场景，加上大把的“消费时间”，会衍生更高频车内消费应用和消费场景。
7. 无人驾驶到来后的“无人共享汽车模式”，将从“共享”、“智能驾驶”、“自带加密账户”、“自带数字资产”四个维度重新定义车辆，以车为中心的车外消费场景将存在更大的市场空间，这时当你在上班时，车辆自己去给你买个麦当劳似乎会很容易。

接下来我们先介绍 EVA.IO 如何实现去中心化共享充电桩的应用场景，再来讲述 EVA.IO 的系统构架。

11. 共享无人充电桩 - EVA.IO 的一个应用

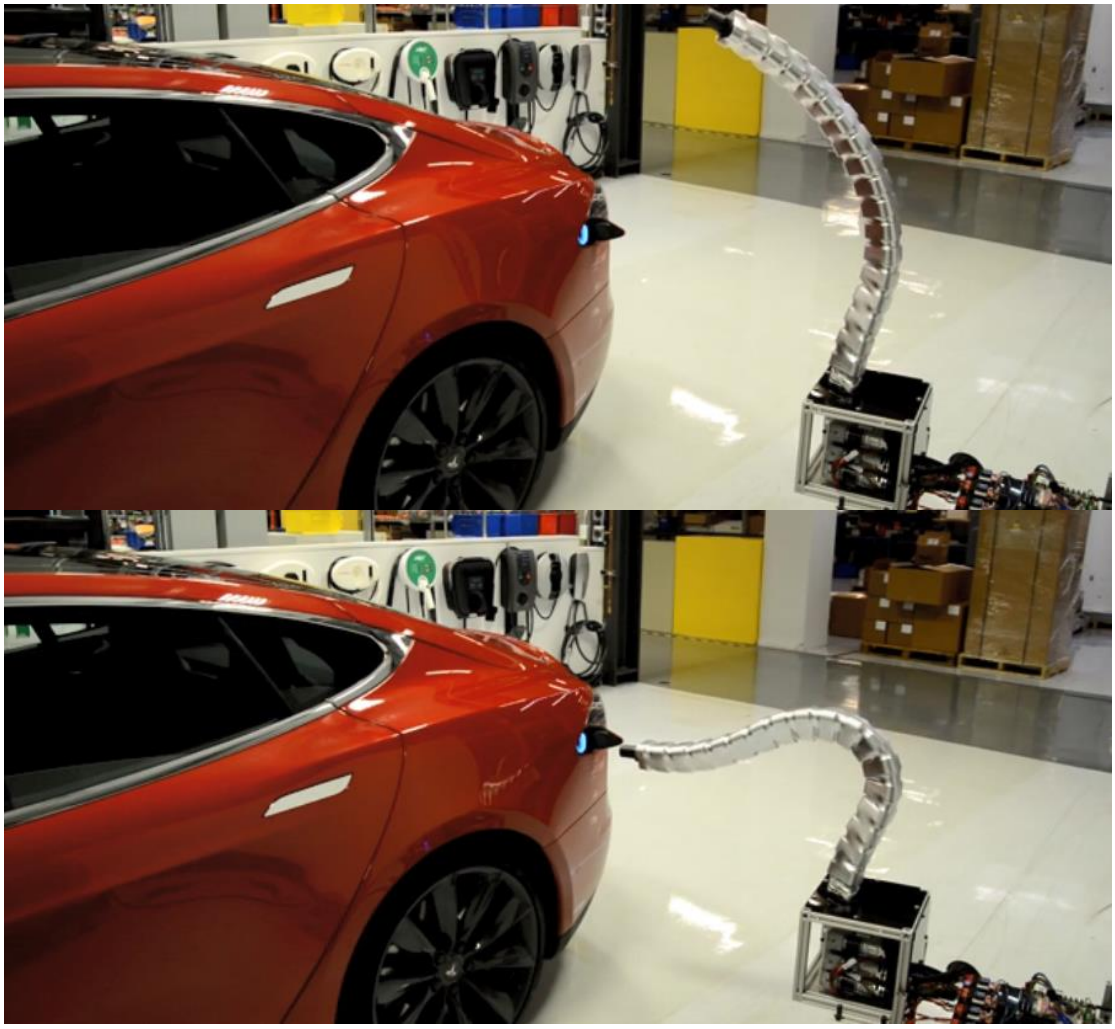
汽车数据资产交易支付系统后，EVA.IO 可以立即支撑第一个应用场景，共享无人充电桩，这部分工作将由 EVA.IO 基金会资助一个第三方技术运营公司共同实现；在此场景下充电桩会被区块链化和网络化升级，让充电桩拥有去中心化客户端 EVPAY 并允许用户用数据资产交易得到的代币用于支付充电费用；同时，电桩变成一个可出售充电服务的“共享加油站”，实现了电桩主人的稳定盈利模型，甚至很多人可以构架小批量的电桩群来形成商业模式，从而加速充电桩在全球布置的物理密集度，推动电动汽车产业发展。我们用以下图片来细节描述如何实现。



1. 家用充电桩做智能化改造，部署轻客户端，用以接收任意数字资产支付购电(可以是

比特代币或者以太坊)，并向车辆展示期望接收的数字资产。改造充电桩的费用我们已评估会非常低。

2. 车辆和电桩通信后确定充电是否可行。
3. 车内电池管理系统 BMS 向 CAN 总线传递所需要的电量数据。
4. 数据经过网关向 CID 中的 EVPAY 确定需要支付的金额。
5. EVPAY 经过 4G 模块向电桩支付电桩期望接收的数字资产。
6. 充电桩 EVPAY 收到代币经过 EVA.IO 区块链得到交易确认后，开放充电。
7. 在无人驾驶状态下，不需人的参与，蛇形充电桩自动伸出并充电，如下图。



上面的蛇形充电桩的思想来源于特斯拉 CEO ELON Musk 的一个梦。

在完成去中心化共享充电应用的同时，也验证了 EVA.IO 赋予汽车的自主支付能力；进一步 EVA.IO 将向第三方开放 API，让更多基于汽车的快捷服务存在于 EVPAY 中，可以是支付洗车费，停车费等等，就像我们习惯用支付宝来交水电费一样。

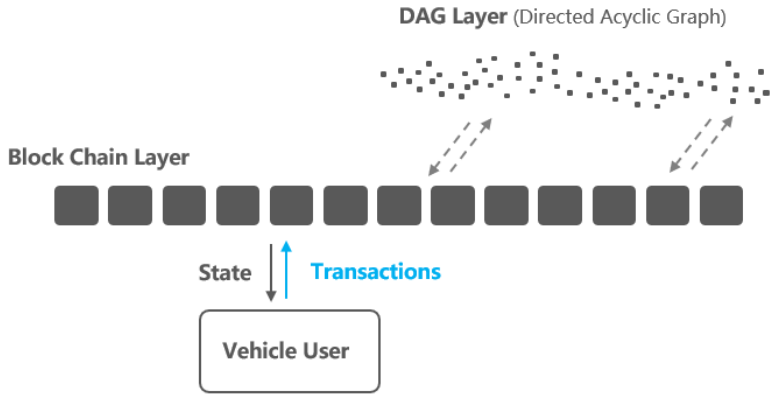
同时作为一个公链，EVA.IO 可以支持很多未来的车载去中心化应用，例如去中心化的车载电台将带来更丰富的内容，因为电台的内容创造者可以是任何人，去中心化带来的代币系统更好的实现了内容的价值变现，从而形成更有激励性的商业模式，会大大激发内容创造者为车辆提供服务，同时它让内容变现的流程缩短，这样的应用在效率上也更高。

另外一个有意思的应用可能是车和车之间基于距离和习惯而产生的开车社交工具，当你在开车的同时，其实眼睛和手需要完全专注，但你的嘴巴完全可以和说话而不影响开车，开车时和其他开车的朋友组成群组来聊天认识新朋友，因为活跃度而被奖励代币，用户的活跃度带来了广告价值，这样的商业模式相比传统会更有生命力，因为去掉运营公司，将代币和 DAPP 的分红权相关联，把商业收入回馈给价值创造者也就时用户。

在无人驾驶实现后，车内的去中心化应用将会更丰富，各种去中心化游戏，资讯，社交应用都将面临重大机会，去中心化应用在商业模式上有着天然的优势，他们的生命力将更顽强，这让为去中心化应用服务的 EVA.IO 变得更重要。

12. DAG 和区块链双构架

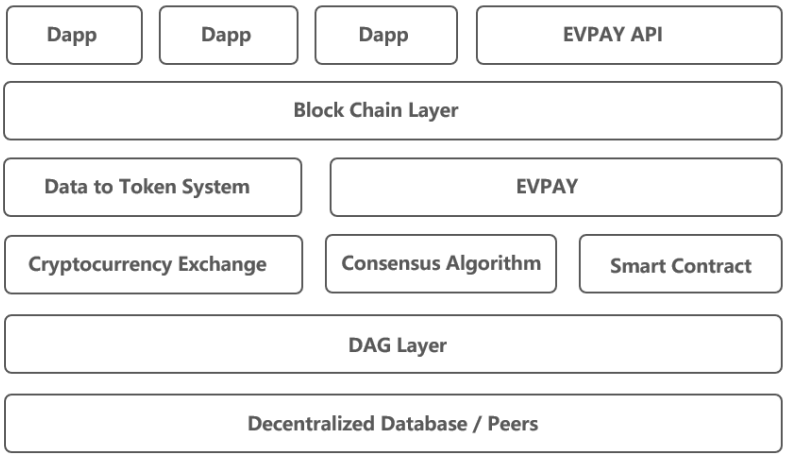
比特代币向世界展示区块链构架和加密货代币，在开始相当大比例的相关项目都是在区块链模式下进行的，后来 DAG Coin 和 IOTA 把 DAG 构架推到了我们面前，不可否认的是区块链构架和 DAG 构架都有自己独有的优势，大家的讨论重点都围绕着交易免费，交易速度，和更去中心化这三个关键点上。在解决交易速度问题上，EOS，Ethereum 都在围绕分片在实现，IOTA, Byte ball 在 DAG 方向进步，其实这些都是并行思路的表现形式，但是不经过理念到实践的检验，我们并不知道解决交易速度问题上哪种方案会成为最终的优胜者，特别是解决了交易速度的同时不影响去中心化的特性；而且不同的行业，最终的优选方案是不同的。



EVA.IO 向大家带来一种新思路，整合式 DAG 和区块链双构架。 在这样的构架中如上图，对车辆物联网支付部分 EVA.IO 会使用 DAG 层进行高速交易，而 Blockchain Layer 被用来处理智能合约类交易，DAG 层交易形成的汇总，跨链资产兑换等任务。当一笔交易提交到 EVA.IO 客户端，区块链不验证交易的有效性，也不对结果形成共识，而是先判断交易类的类型，把高频类交易提交到 DAG 层，智能合约类的交易被保留在区块链层，并转交给运行环境，被区块链节点来运算，运行结果作为一个交易，送到 DAG 层形成共识来保证状态不被修改；

这样的整合式结构充分发挥了 DAG 的高并行能力，能更好地去解决 EVPAY 中的高速支

付部分，另外区块链层和智能合约保证了 EVA.IO 可以作为一个 DAPP 开发的分布式平台，以便搭载更丰富的为车辆服务的应用，来提高 EVPAY 的使用率。



我们看到 EOS 的 DPOS 共识算法让社区更好的参与区块链的治理，虽然这样减少节点数量，来提高交易速度，但这并不能真正的去中心化；就像西方国家选举中可能会出现很多内幕一样，EOS 的做法依然让权力过于集中。

所以我们用 DAG 和区块链双结构的另一个重要原因是让系统更去中心化，为此区块生产者和 DAG 节点需要物理上不为同一个节点。我们用以下不精确的比喻来描述 EVA.IO 在让权力更分散方向上做的设计。

区块生产者像是财务总监，DAG 节点更像是记账会计，DAG 见证人像会计师事务所；三个角色都有各自的职能，也同时分散了权力。当然在 EVA.IO 中这些角色的选择都会通过 DPOS 共识算法来确定。关于这三个角色我们会在下文进一步描述。

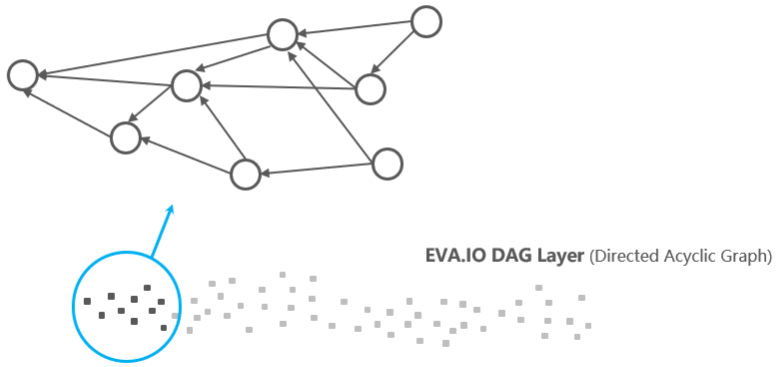
所有发生的交易，也就是被EVA.IO DAG层验证过的交易，其汇总信息将被最终送到区块链层，并被区块生产者验证打包进当前区块，从而形成EVA.IO区块链。

EVA.IO区块链层允许任何人来创建智能合约和去中心化车载应用，可以针对所有权来创造特有的规则，也可以创建不同的交易形式和状态交易函数。我们的跨币种汇兑模块和影子币同样也通过系统内的智能合约来实现。EVA.IO智能合约是图灵完备的，可以去编码任何逻辑和算法并最终被顺利执行。对于车辆形成的数据，区块链层同样有访问控制协议，除非这些数据被付费，否则这些数据无法被访问或获取。

区块生产者不需要使用基于挖矿的算力来形成共识，15 个区块生产者被投票选出，并且由超过三分之二的生产者一致投票最终形成一个生产序列来顺利产生区块。

13. EVA.IO DAG 层

在标准的 DAG 构架中是没有区块或链的概念，取而代之的是如果我们想广播出一个交易，我们需要先验证并批准之前的其他人的一个或多个交易。这样每个交易发出者同时也是交易验证者，大家共同维护一个去中心网络的安全，默认前提是节点确认是否之前的交易有问题，如果节点发现之前的某个交易和总体的交易历史有冲突，那么节点不会去批准这个交易。所以 DAG 结构不像区块链一样把确认过的交易打包进一个个区块，并按顺序排列，而是以散开的单独的交易由后向前确认而形成单向不循环的单独交易网，如下图所示。



DAG 构架让交易的可扩展性变的更强，交易越多时 DAG 网络所具备的并发处理能力越强，交易的确认速度越快。这也是为什么 EVA.IO 在系统构架中增加了 DAG 层来解决交易速度的主要原因。在 EVA.IO 中 DAG 层只参与单纯的交易，最初的 TPS 目标被设定为 5000 笔交易每秒并根据实际交易数据实时无上限扩展。

在我们的设计中，同样引入了DAG见证人角色，见证人是网络的参与者，他们通常可以是不匿名的有声誉的人和机构，通过社区投票选出。9个见证人会最终参与到系统中，并验证DAG层的交易并公布到主链中。同时我们有理由相信他们能诚实的履行他们的指责，当然我们也不能单纯相信某一个见证人。

选取DAG主链的方法是通过选择一个最佳的子母交易链，选择的方法需要基于现有网络中的交易，包含交易数据本身和他们所有之前的母交易。从任何一个交易分支起，向前寻找交易历史中的最佳父辈链，并最终达到交易的源头创始交易。

当DAG层收到一个交易时，系统使用MCMC蒙特卡洛算法来随机为用户选择DAG节点。这是为了确保DAG节点不会提前知道他们要去验证什么交易，并最终降低DAG节点攻击系统的可能性。

在EVA.IO DAG层中，节点的数量会随着交易的增多而增加，确认时间是一笔交易进入分布数据库达到稳定的时间，它取决于多长时间DAG见证人来提出更新最新的主链。为了达到交易的稳定，需要更多的被见证人批准的交易被不断的增加到主链中。为了减少确

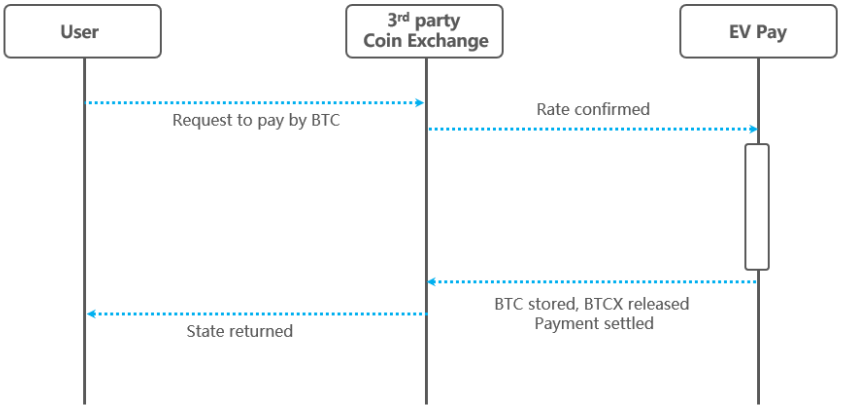
认时间，主链的更新时间需要足够快，频率足够大。同样见证人也由社区投票选出，来保证他们能顺利的达到预期能力。

14. 跨链通兑支付

数字资产的种类不断增加，如果我们设计的系统不能为接受其他数字资产，那将是非常差的体验，如果作为买家的你有 10 个以太坊，而服务或商品销售者希望收入比特代币，我们需要让 EVPAY 在用户无感知的情况下在后台完成快速兑换，并顺利完成支付；而 BTC 和 ETH 的区块链构架决定了他们的速度很慢，想通过比特代币的区块链或以太坊的区块链完成交易会非常困难；我们用下面的方案来解决跨代币种快速支付问题。

1. EVPAY 客户端为每一种数字货代币设置一种影子币，例如 BTCX，ETHX。
2. EVPAY 和交易所合作设定一个汇率询价及交割协议。
3. EVPAY 会根据此汇率在买卖系统中计算期望报价，如果你希望用 BTC 支付，你将看到 BTC 报价。
4. 以 BTC 支付为例，买家支付后触发智能合约在多重签名机制下锁定 BTC 资产，同时系统 1：1 兑换出影子币 BTCX。
5. BTCX 根据交易所的汇率兑换成 ETHX 并支付给卖家完成支付。这一切都被 DAG 高速记账网络记录，并最终经过哈希函数总结到区块链层。
6. 协议交易所将同时 BTC 对以 ETH 的各自链上交易完成汇兑。
7. 汇兑完成后，ETHX 被换成 ETH。

为了保证影子币和数字资产之间 1：1 对应的关系，不产生某个群体可以解锁或乱放影子币的现象，锁定资产和影子币间的兑换和释放权限交给了矿工节点，用多重签名方式保证智能合约的执行如下图。



15. 影子币 EVAX 及价值锁定做空合约

数字资产的高度不稳定性，是阻碍数字资产在实际交易支付中被广泛使用的重要原因。我们认识到要将数字资产应用于日常交易支付场景，就需要数字资产的价格稳定；而目

前大多数数字资产实际是公链的股权、分红权以及使用权的整合体，这使得目前的数字资产价值每时每刻都在波动，而交易收款方或许并不关注分红权，而更关注他今天具体收入了多少钱，这样的状态限制了收款方大规模接受加密支付；为此我们设置了影子币EVAX来使支付到卖家的资产恒定，它具有以下特点：

1. EVAX被设计与美元价格在任何时间都相等，1EVAX=1USD
2. EVAX不会单独交易，也不单独出现，只充当代币的影子价值。
3. EVAX的产生由智能合约根据抵押的EVA代币价值触发。
4. EVAX的产生数量=被抵押EVA数量*EVA代币当时价格/1
5. 与第三方运营公司合作，在抵押EVA代币的同时在二级市场上做空EVA代币，以保证在交割期内EVA价格始终等于兑换时所代表的美元价格。

下面我们以无人共享充电桩为例来描述EVAX的产生和交易过程，以及如何使用期货做空工具来恒定卖方代币价值；

Alice驾驶一辆特斯拉Model S在寻找一个共享充电桩；这时她发现Bob的电桩装在附近，于是她到达了Bob的充电桩旁，车辆识别了Bob的充电桩并向BMS征求需要充的电量并通过EVA.IO中的EVPAY通过4G网络向Bob的充电桩付EVA代币；此时EVA代币价值为10美元，Alice为此充电支付了1个EVA代币，这笔EVA代币的支付触发了EVA.IO链上的智能合约，并把这笔EVA划转到一个锁定的公共地址，这一过程被多重签名以确保抵押的EVA的安全；

而影子币EVAX的价格始终是恒定的1美元的价格；系统在抵押了EVA的同时，通过智能合约从系统向Bob的充电桩支付了10个EVAX代币；区块链记录了这笔交易并触发事件告知Bob的充电桩，充电桩开始充电直至结束。如果仅仅如此，EVA代币的价值波动实质上会给汇兑带来严重影响：

如果EVA在1分钟后价格跌至9美元，那么系统中依然抵押了一个EVA，目前价值9美元；而Bob收到了代币价值恒定的EVAX价值为10美元，当Bob在EVPAY中提出将10个EVAX兑换成EVA代币时，系统只能兑换出1个EVA代币共价值9美元，而没有谁可以承担另外1美元的损失。

这时我们引入了做空期货智能合约，当系统在将EVA抵押且兑换成EVAX时，同时触发EVA代币的做空期货，以保证在期限内由期货合约来担保EVA抵押品+期货合约总价值始终恒定在10美元。这样的做法保证了任何时间Bob拿着10个EVAX都能被兑换成为价值10美金的EVA。

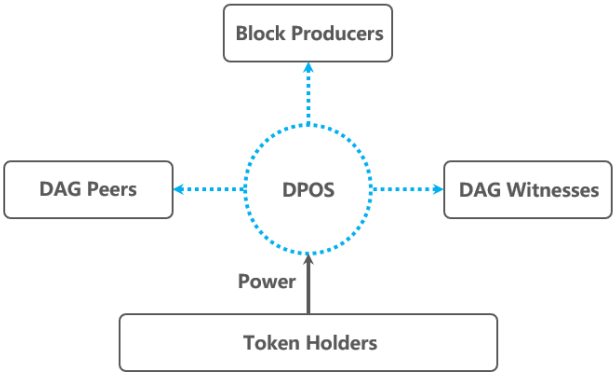
16. 共识算法（DPOS + MCMC + PBFT）

EVA.IO 使用 DPOS 机制来选择系统中 3 个重要角色，MCMC 算法来随机发送交易到 DAG 节点，PBFT 算法用来解决区块链层中的状态通讯问题。在 DPOS 机制下，社区会根据代币的多少来投票选出区块生产者、DAG 节点以及 DAG 见证人。

任何人都被给与机会参选区块生产者，DAG 节点以及 DAG 见证人，他们需要做的就是说服 EVA 持币人来给他们投票。

总的来说，DAG 节点为终端用户发出交易并验证交易，DAG 见证人需要定期找出最佳的子母交易链作为 DAG 的主链，DAG 见证人就像 DAG 层的监管机构或媒体一样向公众曝光最新的主链以确保双花不会发生。区块生产者最终将 DAG 层的交易汇总信息打包进区块。

在此模型中这三个角色分别负责不同的工作内容，却为了共同的目标，确保账本数据的安全，我们不严谨的称之为“三权分立”，而这些权力都来源于持币人，相比于 EOS，这样做的会让系统更去中心化，更符合社区自治的原则。



EVA.IO 中的共识算法按如下方式运作。

1. 使用 DPOS 共识算法来选择区块生产者、DAG 节点和 DAG 见证人。
2. 使用 MCMC 算法来随机选择将交易发给哪个 DAG 节点。
3. DAG 节点收到交易后做轻型 POW 算法来寻找常数并最终将交易发布到 DAG 交易网中。
4. DAG 见证人频繁发布最佳子母链为 DAG 主链。
5. 区块生产者间使用 PBFT 算法来解决拜占庭将军问题。
6. 区块生产者将把 DAG 交易总结打包进最新区块。

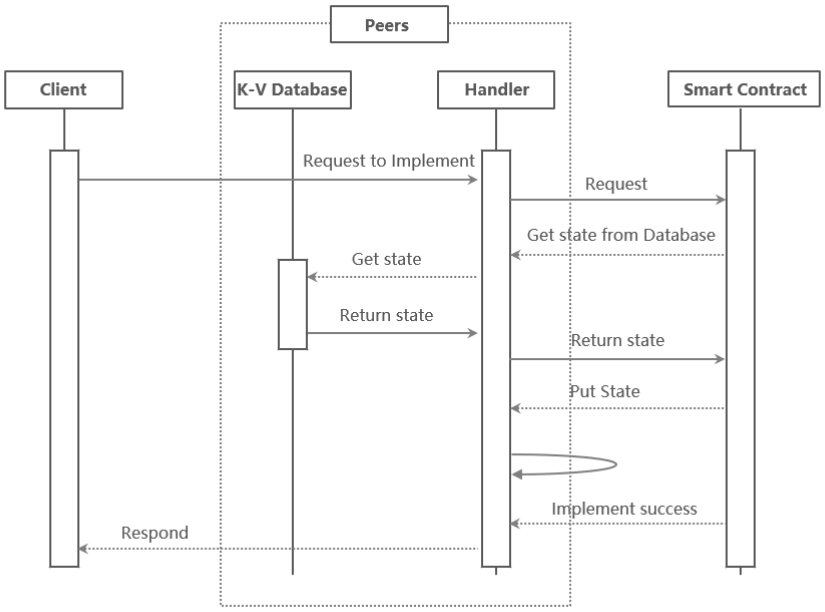
与传统单一区块链结构相比，这样的 DAG 和区块链双结构可以更好的促进去中心化，并有效提升了系统可扩展性。同时对比传统的 DAG 单结构，可以更有效的搭载智能合约，更好的布置和创造去中心化应用。而我们的支付跨链汇兑等模块不得不使用智能合约，这让 DAG 和区块链双结构变成了必然。

17. 智能合约

EVA.IO的智能合约分为系统合约和用户合约。系统合约用来实现系统层面的功能，用户合约实现用户的应用功能。合约被编译成一个独立的应用程序，运行于隔离的Docker中。和以太坊相比，EVA.IO智能合约和底层账本是分开的，升级智能合约时并不需要迁移账本数据到新合约当中，实现了逻辑与数据的分离，从而可以实现将账本数据委托给DAG的高速网络执行并存储，合约采用Go、Java、Nodejs语言编写。

以下介绍如何如何在区块链层和DAG层中处理一个智能合约类交易。

1. 节点收到客户端请求的输入(propsal)后，会通过发送一个合约消息对象（带输入信息，调用者信息）给对应的合约。
2. 合约调用ContractBase里面的invoke方法，通过发送获取数据（getState）和写入数据（putState）消息，向DAG peer节点获取账本状态信息和发送预提交状态。
3. 合约发送最终输出结果给DAG peer节点，节点对输入(propsal)和 输出(propsalreponse)进行签名，完成第一段签名提交。
4. 之后客户端收集所有DAG peer节点的第一段提交信息，形成交易（transaction）并签名，发送交易到Blockchain节点排队，最终block producer产生区块，并发送到各个DAG peer节点，把输入和输出落到账本上，完成第二段提交过程。



智能合约支持下，可完成数字资产管理交易，基本业务流程如下：

1. 用户发起资产寄存请求，向EVA.IO打入数字资产
2. EVA.IO返回代币到用户客户端，并触发EVPAY和数字资产发行网络中的联合记账请求。
3. 卖家以期望接收的数字资产定价商品。
4. 买家以自身持有的数字资产的代币完成即时支付。
5. 更新数字客户端中数字资产与代币的映射关系。
6. 发起代币与数字资产赎回承兑请求，触发跨链交易。

18. TPS 水平扩展

用户思考时间为T_think
并发用户数为$U_concurrent$

交易响应时间为$T_response$
则系统吞吐量$TPS=U_concurrent / (T_response+T_think)$
EVPAY保证确保每笔交易的时间为$C_time = Confirmation\ time$
假设$T_response = a*C_time$
则$TPS=U_concurrent ／ (a*C_time +T_think)$
结论 $C\_time ＝ (U\_concurrent／TPS - T\_think)/a$

19. EVA 代币奖励机制

我们相信为终端用户提供免费的服务对应用开发者来说相当重要。用户不应该在使用去中心化应用前还要支付交易手续费。这意味着 EVA.IO 是一个无手续费的分布式应用数据库平台。那么为了保证区块生产者、DAG 节点和 DAG 见证人的利益，至少能保证他们购买硬件及维护网络，EVA.IO 设计每年为他们增发低于 0.5%的代币平均分配给所有物理节点以保证系统健康运转，社区将参与并最终投票决定年度增发比例，但比例被系统锁定为小于 0.5%。

在 EVA.IO 系统设计中，将有总量为 200 亿的代币，其中的只有 120 亿 EVA 代币在项目初期使用 ERC233 协议产生。在 EVA.IO 系统开发完成后，120 亿 ERC233 代币将需要被映射到 EVA.IO 系统中，以形成真正的 EVA 代币；另外的 80 亿 EVA 代币只有主网上线后才有可能被车辆挖出，车厂在车主挖出 EVA 代币的同时也将收到奖励，每当一个车主挖矿获得 10 个 EVA 代币奖励，车厂将同步收到 1 个 EVA 代币奖励。

另外我们设置了类似比特代币挖矿一样的分级递减代币奖励机制：

1. 当车主+车厂已被奖励的 EV 总数<=5 亿时，车主每日可被奖励 EVA 为 100 个；
2. 当车主+车厂已被奖励的 EVA 总数>5 亿且<=10 亿时，车主每日可被奖励 EVA 为 50 个；
3. 当车主+车厂已被奖励的 EVA 总数>10 亿且<=15 亿时，车主每日可被奖励 EVA 为 25 个；
4. 当车主+车厂已被奖励的 EVA 总数>15 亿且<=20 亿时，车主每日可被奖励 EVA 为 15 个；
5. 当车主+车厂已被奖励的 EVA 总数>20 亿时，车主每日可被奖励 EVA 为 10 个，这个过程一直持续直至 80 亿 EVA 被挖完。

车主可能不能收到上述所描述的 100%的挖矿 EVA 奖励上限，因为挖矿跟当日行驶里程和数据等级相关，我们可以形容 EVA.IO 的挖矿模式为里程挖矿。

EVA.IO 允许应用开发者消耗相应比例的带宽、存储等系统资源，前提是他们持有相应比例的 EVA 代币。如果一个账户持有了 1%的代币，那么这个账户可以使用系统存储的比例为 1%。

20. 结论

我们提议了一个全新的“区块链+DAG”的双结构，可以达成高可扩展性而不需要牺牲系统的更去中心化特性。代币在车辆大数据的基础上被创造，终端用户不需要付手续费就能使用车

辆去中心化应用，收款方将收到期望的加密货币种类而不需要自己去交易所兑换，一个恒定价值的影子币将帮助收款方更容易接受加密货币，最终这将允许车辆在自动驾驶时拥有自主支付能力。

参考引用

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.
2. EOS.IO https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper
3. Anton Churyumov, Byteball, https://byteball.org/Byteball.pdf
4. Sergio Demian Lerner. Dag Coin, https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf, 2015.
5. Serguei Popov. The Tangle, http://iotaEVA.com/IOTA_Whitepaper.pdf, 2016.
6. Tom Holden. Transaction-Directed Acyclic Graphs, https://bitcointalk.org/index.php?topic=1504649.0, 2016.
7. https://github.com/bitcoin/bitcoin