CarBlock

全球交通数据协议及应用标杆

A GLOBAL TRANSPORTATION DATA PROTOCOL WITH DECENTRALIZED APPLICATIONS

WHITEPAPER

Version 4.0
Last Update: August 13 2018

目录 2

综述

CarBlock服务于整个汽车及出行行业，打造一个基于区块链的交通数据协议及基于此的垂直应用，并以此建立一个全新的交通行业生态。互联网的本质是让信息流动起来，而CarBlock将使交通数据在生态中充分流动，以交通数据作为入口来驱动汽车及出行行业基于数据来进行决策，将所有业务高效的运转在CarBlock平台上，并吸引有创新能力的个人、团队、高校、研究所进入生态，最终进一步改变并提升整个汽车及出行行业。

CarBlock的发起有一个非常重要的时代背景：21世纪以来，“联网化”、“数据化”、“电子化”正在对汽车工业及周边行业带来颠覆性的变化[1]。CarBlock由知名的车联网智能硬件公司 nonda (NO NDA inc) 孵化并最终独立运作，核心团队经历了 nonda 从初创到北美车联网智能硬件市场占有率第一的整个历程，亲身感受到变革大潮的来势汹涌，汽车及出行行业的所有传统观念都将被颠覆，无可避免。我们将在下一个章节详细分享我们在这方面的认知。

对于CarBlock生态，团队有一些基础性的重要共识，必须告知每一位阅读者：

汽车及出行数据的所有权和利益必须归属于数据提供者，绝大多数场景下即车主。一方面这在法律（特别是欧美法律）上是大势所趋，另一方面车主必须是CarBlock生态的基础，这是后续商业和数据的结合点。我们高兴地看到，去中心化的区块链技术已经为这个理念提供了完美的解决方案。我们将在后续“核心问题”章节详细探讨这一点；

CarBlock不是从汽车数据牟利的中间商，相反，CarBlock将尽量确保数据在生态中的自由流动并努力降低摩擦系数，流转消耗的目的只是覆盖流转系统成本，甚至CarBlock可以为有创新能力的个人、团队、高校、研究所提供补贴。我们将在后续“创新者的困境”章节详细探讨这一点；

数据流动将实现CarBlock生态所有参与者的多赢。

车主将会从提供数据获得奖励，并在CarBlock生态中获得基于个人的，更精准、更经济、更优质、更创新的服务及产品。

汽车和出行行业将可以获得海量的数据，而数据将驱动竞争，使从业者要基于数据来提供更精准、更经济、更优质的服务和产品。由于数据本身必须是脱敏的（即不包含车主联系方式等关键信息），一切交易和服务的履约必须通过CarBlock的去中心化平台来完成，CarBlock平台将成为一个高效的桥梁，连接车主和服务者，完成报价、合同、支付、履约等一系列业务流程；
创新者将会被从缺乏数据的困境中解放出来，获得精准的车主数据，并在CarBlock生态中为车主提供更多样的创新服务和应用。实际上，CarBlock团队已经在欧美尝试过一些基于数据的创新服务，并获得了很好的回应，比如我们将胎压和油耗进行了大数据分析，为数十万车主节约了数百万美金的油耗成本；再比如我们为数万车主提供了基于里程的退税服务，每位车主可以每年平均获得上千美金的退税。这些尝试让我们深知创新者+数据将能迸发出怎样的火花。

作为多年的行业从业者，我们认为车联网数据应用是一个颠覆性的新兴行业，但发展远远没有达到预期。究其原因，我们认为一个最基础的痛点是数据拥有者、采集方与需求方之间缺乏共识，利益关系无法得到平衡。数据拥有者没有得到很好的隐私保护，或没能直接得到收益，最终导致数据拥有者根本没有动力参与生态建设，在这样的生产关系下所有的上层建筑都如同沙滩上的城堡，注定无法成功-这是我们提出基于区块链技术的CarBlock来解决车联网数据流通问题的出发点，也是我们认为的CarBlock最终将推动人类交通出行完成革命性进步的信心来源。在后续章节我们将从前景、问题、方案、团队等各方面对CarBlock提供详细介绍。

车联网及其数据生态将颠覆整个汽车行业

几乎所有关注车联网的汽车行业专家都会持有类似的观点：“车联网将颠覆汽车及周边行业”。这是专家的“耸人听闻”吗？本章节将试图以最简单的语言来阐述这个巨大的行业变迁趋势。

智能设备和移动互联网的发展

一个重要的时代背景是智能设备和移动互联网的发展，已经在不知不觉中对汽车这个“百年产业”产生了巨大的影响。一方面使得汽车行驶数据的收集和分析成为可能，另一方面各种智能电子系统、驾驶辅助系统也使汽车的驾驶行为产生了重大的变化。

精确数据建模将取代传统统计分析

“ 汽车联网对于汽车行业的作用，将比过去一个世纪所有汽车技术所提供的都要大。汽车是一个巨大的数据中心，能够采集和分享大量的多维度数据。它会知道你去哪里购物、哪里工作、你什么时候开了车，甚至你周末干了什么。汽车会变成一个更加智能的终端，来理解你的行为并作出反馈。”

– Tom Rivers, Automotive connectivity specialist Harman 营销副总裁”

不仅仅是车辆本身的升级，掌握车联网数据建模的公司将在业务运营中占据极大的优势，从竞争中脱颖而出，并重新定义汽车行业的格局。比如，掌握汽车行驶数据的保险公司可能比竞争对手提供更低的报价，但获得更高的利润，最终淘汰掉传统的车险公司。我们注意到，在北美已经有一些类似的尝试了: 比如初创公司Metromile[2]允许用户根据行驶里程来选购车险，虽然方式稍嫌初级和粗糙，但保险报价已经颇具竞争力。

最终，数据将会成为整个交通出行领域的核心。

车联网生态

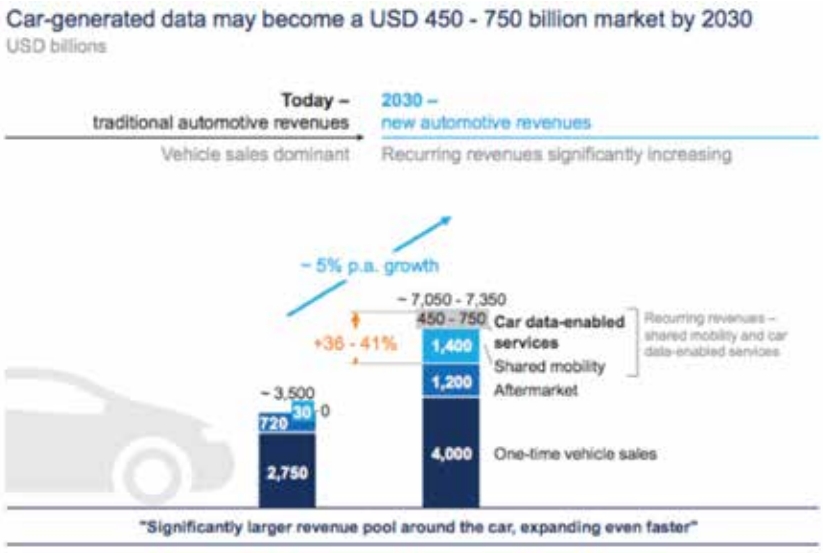
车联网是以数据为核心，形成的多方合作生态。生态中的各个角色或是数据的贡献者，或是数据的消费者。由于汽车行业是一个成熟产业，整个消费生态已经就绪。围绕着数据，生态伙伴可以彼此协作，形成生态互补，促进行业进步，让人类的出行更加方便与安全。

车联网生态

根据埃森哲的分析报告[3]，全球车联网市场规模在2025年将达到8400亿美元（未包含汽车制造厂商），中国会在其中占据约26%[4]，发展趋势乐观。

埃森哲对车联网市场的预期

另一份来自麦肯锡的研究报告指出，2030年，车数据将创造出一个7500亿美金的大市场。



麦肯锡对车数据市场的预期

车联网数据生态的核心问题

在上一章节我们探讨了车联网、及汽车行业的未来，但目前车联网仍是星星之火，深受以下问题困扰，它们就是我们CarBlock要优先解决的对象：

问题1: 数据所有权－商业公司与隐私数据的矛盾

汽车拓展了人类出行的边界，给予了人们巨大的自由空间。据统计，北美驾驶者平均1/5的生命是在车上度过的。出行的数据代表着人们每天的居住、工作、购物、甚至健康与生命安全。数据是属于车主个人的，数据如果不能在完善的加密与严格的授权中得到保护，出行者的个人隐私与安全都会遭遇巨大的威胁。

而汽车行业是一个充分市场化的行业，如何确保商业公司能严格尊重并保护用户的隐私数据？如何能在严格保护下发挥数据的价值？这是车联网领域一直探索却从未解决的问题，并对车联网数据的采集和存储带来了实质的影响。

现在车数据的所有权一直存在很大争议，几乎所有车厂都开始在车内预装T-BOX收集车辆数据；而个人用户则认为车辆数据属于个人隐私，拥有权属于个人，车厂等商业公司的个人隐私承诺没法让用户信服，必须要从机制上来保证个人的车联网数据属于个人。

（在CarBlock上下文里，联网汽车少不是好事情，无需提及）

问题2: 数据的回报与激励－数据贡献者得不到回报

毋庸置疑，数据的权益属于贡献数据的人。而当我们驾驶车辆出行，在整个过程中产生的数据，却不”归属”与我们自己。导航软件知道我们去了哪里，给我们推送对应的广告，广告商把钱给了导航软件，而数据的贡献者却没有因此得到任何回报。这恰恰也是导致目前车联网进展缓慢的原因——用户得不到激励，个人没有动力来提供相关数据。

虽然既得利益的厂商不会愿意共享收益，但全球用户对“个人数据”的权益意识已经逐渐觉醒：

在北美，“厂商从个人数据获得盈利是否正当”已经是媒体上时常出现的话题讨论[5]；

在中国，“支付宝的年度账单是否侵犯个人隐私”话题已经成为一个全民热点[6]；

我们相信，厂商对数据的无偿占用会在2、3年内出现重大的改变，而且CarBlock将极大地推进这一历史进程。

问题3: 数据本身的价值－脱敏数据 Vs 用户精准数据

尽管交通数据的价值巨大，然而由于隐私保护及法律问题，行业中普遍还是基于脱敏数据在进行应用和开发，由于脱敏数据本身无法对应到车主个人行为，只能基于大数据的分析来做出一定的行业判断和同质化产品和服务的开发，并不能真正促进行业的快速发展。另一方面，相比于脱敏数据仅占2.5%的数据总量，那些价值更高的，大量的用户实时精准数据（97.5%）无法得到有效利用而处于闲置，也是对于行业本身发展最大的浪费。

问题4: 创新者的困境－数据应用方很难得到数据

举一个例子：据 Waymo（前Google自动驾驶汽车项目）公司报告，他们每天有数以百辆的车辆在收集数据。Waymo在2016年12月将其车队扩建至100辆车，并于2017年5月报告称已收集了三百万英里的数据[7]。组织这样规模的车队与真实世界的路测，需要耗费巨大的成本，数据变成巨头才有资格玩的游戏。除此之外，就是极其散落的个人车辆数据，这样的小数据量数据又达不到应用意义。

因为缺乏有效获得车数据的通道，真正有想法、有创新能力的个人、团队、高校、研究所，都很难参与到人工智能时代对人类出行的贡献中。

还记得移动互联网时代，大量普通开发者与初创公司可以加入APP开发并为全球用户服务，最终创造了移动互联网这个巨大的生态吗？同样，只有构建一个开放的平台，能便捷、低成本、安全的交流真实世界的交通及出行数据，让整个生态都有机会参与开发，才能实现车联网领域未来的突破。车联网应用的最终繁荣，必定需要一个车数据基础架构让数据需求方可以简单的获得大量有效的车数据。

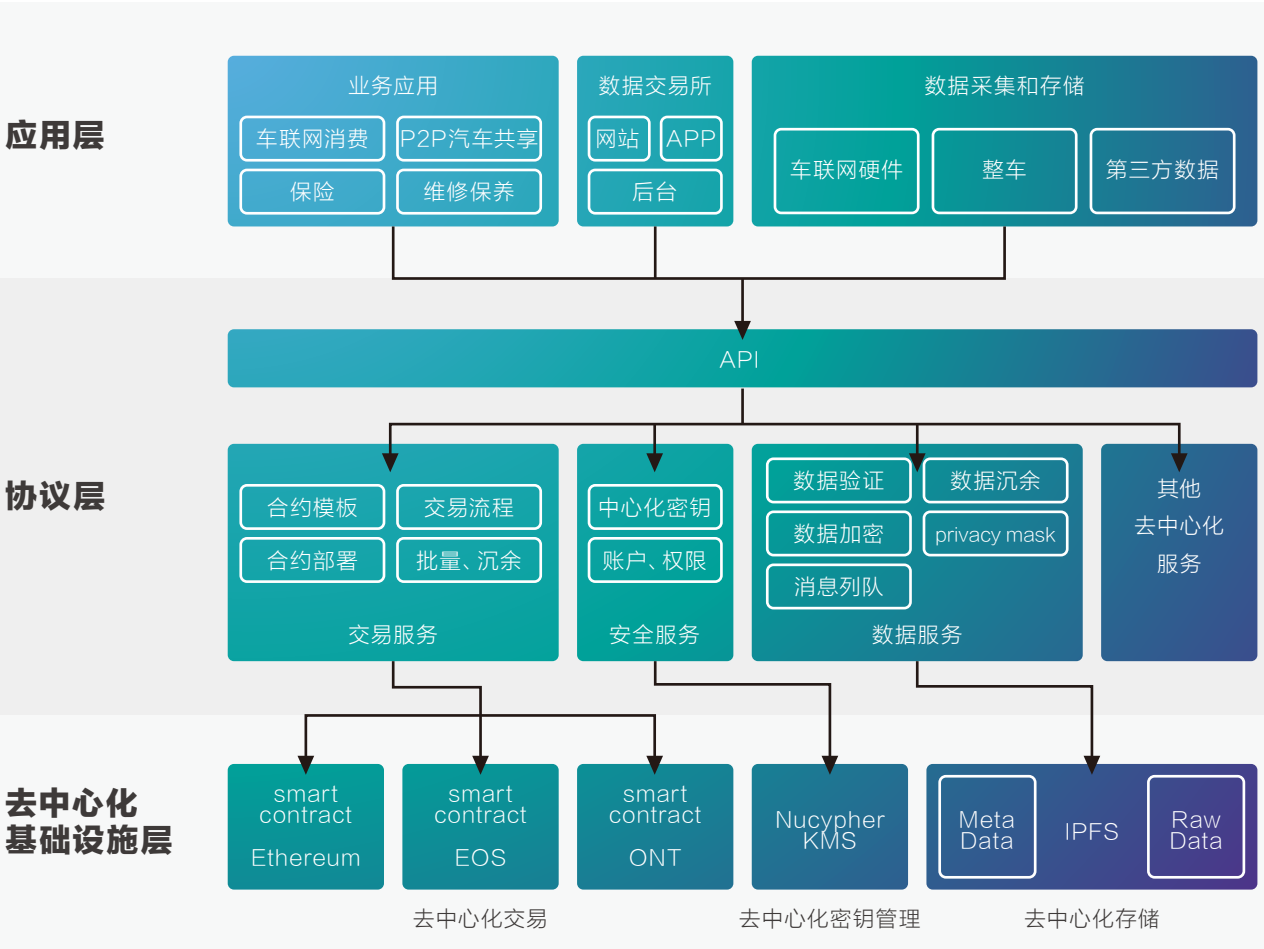
核心系统设计

系统架构

CarBlock的理念是利用区块链技术提供平台，通过完成这几个目标：

1. 制定交通数据上链协议标准
2. 推出交通数据上链交易平台
3. 实现交通数据去中心化应用快速获取数据和快速无缝整合

以方便交通数据和业务上链，打造去中心化交通数据生态。据此我们将整体架构分为3层，如下图所示：



核心系统架构

去中心化基础设施层：当前流行的各个公链本质上提供了去中心化生态中的基础设施，如Ethereum的去中心化交易、Nucypher的去中心化密钥管理、IPFS的去中心化存储。其特点是功能接口较底层和较原始，某些方面有一定局限性（如并发性能），车联网终端用户（B端、C端）直接去使用和整合，存在较大的技术门槛和风险。

协议层: CarBlock最重要的责任是建设各公链之上的统一平台和标准协议，一方面对原始的接口进行封装和各功能的进行整合，制定上链标准并提供开放API，另一方面由于当前的区块链技术并不成熟，在性能、可用性等方面不一定满足需求，因此现阶段我们采用了部分中心化的技术来作为补充，比如操作的批量化、数据的冗余和缓存等。整个协议层通过当前互联网业界流行的无状态微服务架构打造，可用性、可扩展性、并发能力都很强。

应用层: 数据是整个系统的基石，因此最核心的应用就是数据的采集、存储和交易，应用开发者不需要直接和底层区块链交互，而是通过CarBlock系统协议层提供的更为友好和统一的接口，大幅度降低了应用开发门槛，简化了开发者工作。同时当整个CarBlock生态拥有大规模的车联网相关数据之后，在这之上即可构建各种去中心化的垂直业务应用，如P2P汽车共享、保险、维修保养等。

我们的理念是: 在当前原生公链技术存在相当局限性的前提下，使用中心化的CarBlock协议层辅助，更好更快的将去中心化交通数据业务推动起来:

1. 本质上所有的数据最终都会落实到去中心化的公链设施上，并可不通过CarBlock协议层而直接访问，比如通过区块链浏览器直接去查询交易，通过IPFS客户端查看数据。数据和交易依然以公链上的为权威，CarBlock协议层只作缓存和冗余。
2. CarBlock协议层的重点工作是制定交通数据与业务协议标准和接口规范，并基于当前公链技术实现接口，这些标准和规范不因底层技术的演进而产生较大变化，从而使得上层应用也不会因之产生过多的迭代。
3. 未来当各种去中心化技术成熟时，CarBlock协议层可能会以多种形态存在，比如轻量级的库，各应用集成后即可更便捷的使用底层公链。
4. CarBlock协议层代码开源，保证技术实现的完全透明，同时也是汇集社区力量一起完善整个系统。

为了便于理解，我们可以将车联网的数据业务归纳为两个主要场景: 数据采集与存储、数据交易，以下我们就两个具体的业务场景，和贯彻于两个场景始终的数据安全来详细介绍CarBlock系统的每个核心模块。

数据采集与存储

数据采集和存储是CarBlock系统的基石应用程序，通过收集车辆终端各种使用数据，经过CarBlock平台中转，汇总存储到IPFS上。CarBlock生态中的业务应用都将基于这些数据展开。

数据采集方式与内容

数据采集首先支持的是使用nonda智能硬件进行采集，最底层是IoT硬件与传感器层，例如：nonda的ZUS Smart Car Charger可以提供车辆点火/熄火数据，电瓶电压数据，OBD可以将发动机相关的数据收集起来，TMPS监控轮胎气压与温度。传感器采集的原始信号会经过硬件加密，变成原始数据。加密后的数据通过蓝牙连接智能手机完成传送，或直接通过设备上的联网模块传送，协议层的数据验证器(Validator)首先会校验来自硬件通讯数据的真实性。数据分两部分存储：

元数据(Metadata)，仅包含所有用于查询的维度信息，以及指向它们对应的原始数据的索引，例如在IPFS上的哈希(Merkel Hash)[8]。Metadata还将包含一些有效性验证数据，例如基于IPFS储存的数据将采用与Filecoin[9]同样的“复制证明”技术[10]，实现车联网原始数据存储及验证(存储有效性)。

原始数据(Raw Data)，经过验证、加密和压缩的原始数据存储在IPFS上

类似nonda产品和CarBlock的整合，CarBlock后期会推出硬件认证服务，只要符合CarBlock的数据标准的认证硬件即可通过CarBlock平台接口进行车联网数据的存储。更进一步，CarBlock也在和车厂合作，让正在开发的新车可以方便地接入CarBlock，

数据存储方式与优化

目前考虑到目前IPFS公网的性能、可用性可能达不到生产标准，CarBlock团队对其作出以下优化：

只要数据提供者愿意转让部分数据收益，他们可以采用第三方提供的存储服务点。在初期，CarBlock基金会可以作为一个第三方存储提供者存在，在IPFS网络中提供高质量的存储服务节点

CarBlock平台通过诸如Kafka这种持久化消息队列，对IPFS写入操作频度进行削峰填谷，提高性能和吞吐量

CarBlock平台建设IPFS私有网络作为只读的数据冗余，提高数据的查询性能和可用性

由于IPFS只是原始的对象文件存储，而车联网数据具有时序性和多维度特征，CarBlock团队正在研究IPFS之上的扩展，以更友好的支持车联网数据存取。

数据有效性保证

车联网数据有巨大的应用价值，因此提供数据的人会直接获得CAR（Token）的奖励（具体算法详见下节），不排除有人存在经济利益诱惑下攻击社区的动机。对区块链去中心化账本与智能合约的攻击已经有比较成熟的解决方案。而通过产生大量无效数据，骗取社区激励的攻击，是CarBlock重点解决的问题。为此，我们主要将采用以下这两个方案来验证数据有效性：

数据采集有效性： 在数据传输的阶段，CarBlock系统有数据验证器(Validator)来保证数据均由真实的传感器采集获得。而在数据交易阶段，数据采购者也有权在智能合约中要求提供样本，作为真实性检验的参考，如果发现有奇异数据的存在，会终止合约的执行，伪造数据的数据提供者将得不到任何回报。CarBlock基金会也会为数据提供者与对应的车辆(VIN)做KYC验证，任何伪造传感器数据的数据出售方都会得到基金会的惩罚，永久锁定交易市场帐号。此外，CarBlock协议的一个重要的应用场景是二手车交易，伪造的虚假行驶数据会增加车辆的使用度评估，降低车辆估值，从而动机上对试图作弊者进行惩罚。

数据存储有效性： CarBlock基金会部署去中心化的数据储存验证节点来完成日常储存校验任务。验证节点可以用比下载数据还高效的方式来验证数据存储的完整性。通过对一组随机数据块进行采样和提交小量数据来生成拥有的概率证明作为给验证节点的响应协议。其原理与同样基于IPFS的Filecoin类似。

“挖矿”与贡献证明

可以认为，CarBlock的数据提供者（车主们）在生态中扮演“矿工”。和比特币一样，CarBlock的“矿工”们为了巨大的奖励而竞争式挖区块，但CarBlock的“挖矿”采用车联网数据贡献模式，“挖矿”效率是与贡献数据的价值成比例的，这直接为数据需求方提供了有价值的出行数据（不像比特币的“挖矿”仅是为了维护区块链的共识），推动人类更快、更好、更安全的出行。这种方式给“矿工”们创造了强大的激励，激励他们尽可能多的采集出行的数据，并且把它们存储下来，共享给数据需求方。

在CarBlock生态中，每天“矿工”社区将获得固定数量的Token，决定“矿工”收益的因素主要有：

数据维度(v)，即不同类型Sensor所提供数据的多样性；
时间跨度(t)，持续提供长时间跨度的数据将获得奖励；
数据量(x)，“矿工”之间就提供的数据量进行compete；

在构建“挖矿”模型时，数据维度(v)和时间跨度(t)这两个参数有一个非常实用的模型可以使用，即人工智能计算中常用的指数方法（Exponential Function）[11]的累积分布算法（Cumulative distribution function）[12]。具体来说，计算公式存在一个基本形态，和一个变种形态，如下所示：

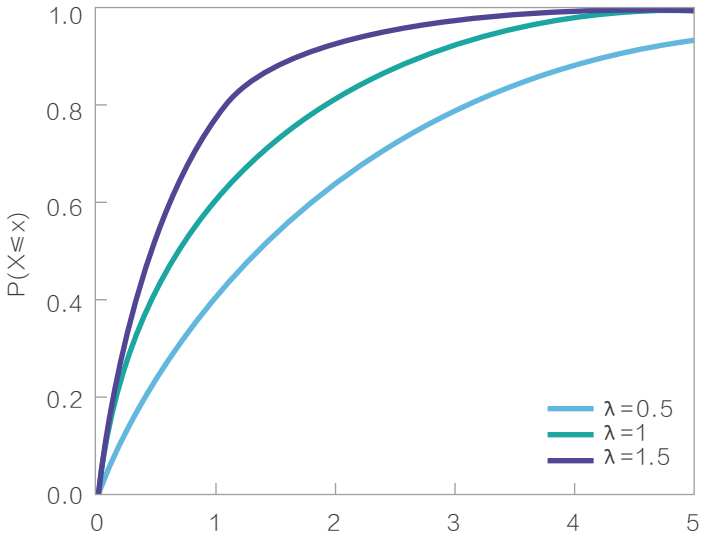
The cumulative distribution function is given by

$$F(x;\lambda) = \begin{cases} 1 - e^{-\lambda x} & x \geq 0, \\ 0 & x < 0 \end{cases}$$

Alternatively, this can be defined using the Heaviside step function, H(x)

$$F(x;\lambda) = (1 - e^{-\lambda x})H(x)$$

我们采用以上计算方式的目的是：一方面鼓励用户增加投入（采购更多Sensor设备、持续多年提供数据等），另一方面增益指数在达到一定程度后即衰减，控制产出增加速度，避免出现比特币等“挖矿”产出垄断的情况，欢迎更多新“矿工”加入。



Cumulative Distribution Function示例

如果把数据维度(v)和时间跨度(t)视为加权值的话，数据量(x)就是“挖矿”受益的基础值，受“有效性证明”的检验（见上文）。对于整个CarBlock生态来说，假设每日产出Token数量为L，则总收益公式 f(x) = F(x, v, t) 在数学上的极限为：

$$\lim_{x \to \infty} f(x) = L$$

在实际应用中，系统分配将确保Σf(x) = L，Σ为当日参与“挖矿”的“矿工”总和。

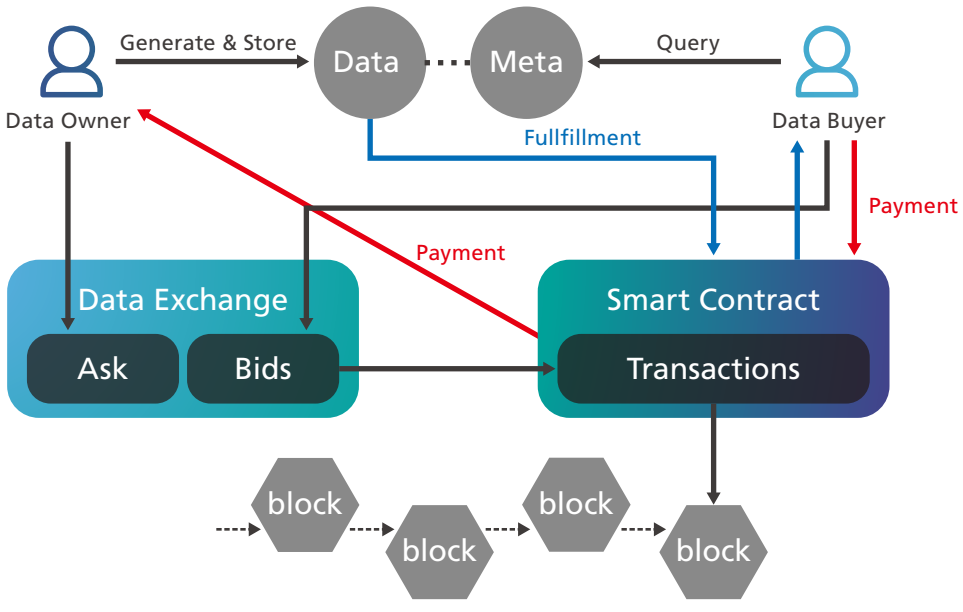
数据交易

同数据采集和存储一样，数据交易所也是CarBlock系统的基石应用程序，只有数据在系统中得到充分流转和利用，整个CarBlock生态才能健康快速向前发展。

数据交易流程

数据交易所中的数据交易将由智能合约来驱动，大致流程是：

1. 选择一个合适的智能合约设置模版（configuration template）；
2. 设置参数，如：购买哪些维度（sensor）的数据、scope（如所在地区、车型等）、数据量上/下限、报价、合约开始/结束时间、数据接收网关等；
3. 提交到数据交易所后会先进行一轮预处理，拒绝不合理的交易请求（如违反当地隐私保护相关法律的请求）；
4. 自动生成智能合约并开始运行；
5. 智能合约将根据维度和scope等参数来寻找合适的数据：
   a. 如数据提供者已预定义授权规则（Authorization Rules），则根据规则自动决定是否参与；
   b. 否则将发送请求到数据提供者，采用Request & Approval来进行决策；
6. 智能合约通过滤镜获得最终数据，将数据发送到指定的接收网关，并同时将Token（扣除一定手续Cost）发送到数据提供者的Wallet。



数据交易过程

以Ethereum公链为例，数据将会以一枚ERC 721独立代币的形式被买方用CarBlock Token购买，该代币则指向IPFS上的某个数据链接，在一定时效期限内买方随时可以访问，而其上存储的数据已通过买方的公钥加密，只能由买方的私钥解密，保障数据安全。我们将在后面详细介绍交易中的数据安全问题。

因为当前跨链技术如Cosmos、Polkadot等都不成熟，目前CarBlock暂不考虑跨链交易，数据的买卖都会发生在同一公链上。我们也将持续关注跨链技术进展，以期未来能用统一的CarBlock Token在多链上自由交易。

智能合约模板和审核

智能合约设置模版（configuration template）是数据交易所（Data Exchange）的核心，系统将由CarBlock团队及生态伙伴共同开发和维护。由于要保护车主隐私，车主个人信息（姓名、联系方式等）将不会发给数据使用者，因此涉及车主和数据使用者之间的商业逻辑必须在CarBlock链上发生。更复杂的使用场景可能会包括“报价”、“数字合同”等多种后续环节，例如：保险公司要为加州车主提供精确车险报价，则智能合约发送数据到接收网关后，还将等待并接受到保险公司计算出精确报价，然后发送到车主端。如果车主同意，则自动划拨保险金额的Token到保险公司，并证明双方完成数字合同。

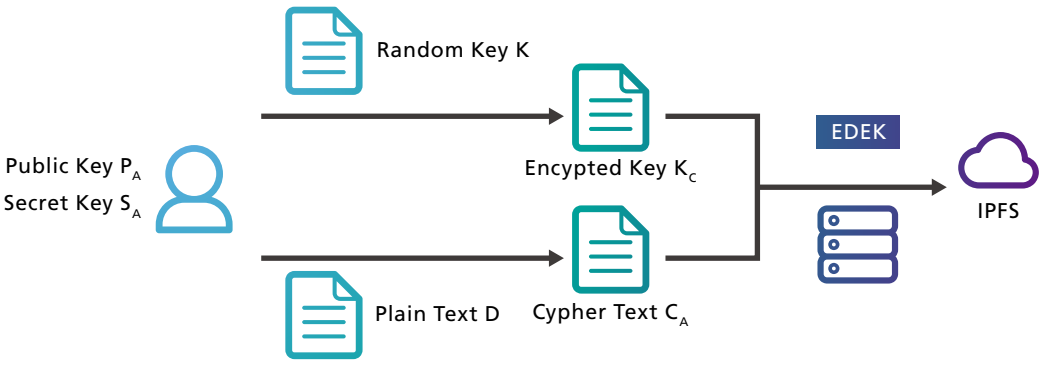
由于智能合约是跑在CarBlock平台上的开源（Open Source）代码，可以从机制上（如“代码审核”等）确保商业逻辑安全、不会对双方的隐私或机密造成风险，因此我们认为未来必然将越来越受到公众的信任，从数据服务延伸到后续商业服务，随着更多生态伙伴的加入，让使用场景越来越复杂和多样化。

数据安全

数据安全的重要性毋庸赘述，而CarBlock系统针对车联网数据流转的每一环节，都做了充分的考虑：

数据存储安全

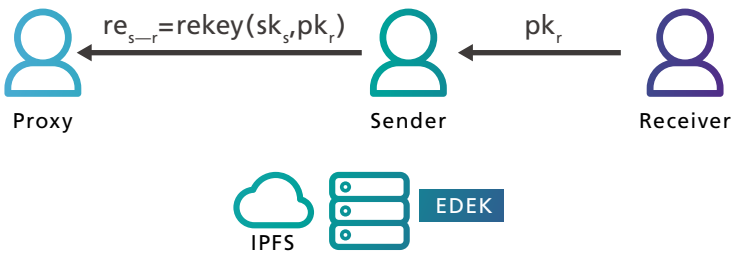
在IPFS协议之上，CarBock将采用Proxy Re-encryption[13]来实现数据的加密和访问控制。在原始数据存储到IPFS的时候，将进一步分为2部分：对随机秘钥K的加密串（EDEK）与加密数据文件，如下图所示：



数据加密并添加到IPFS

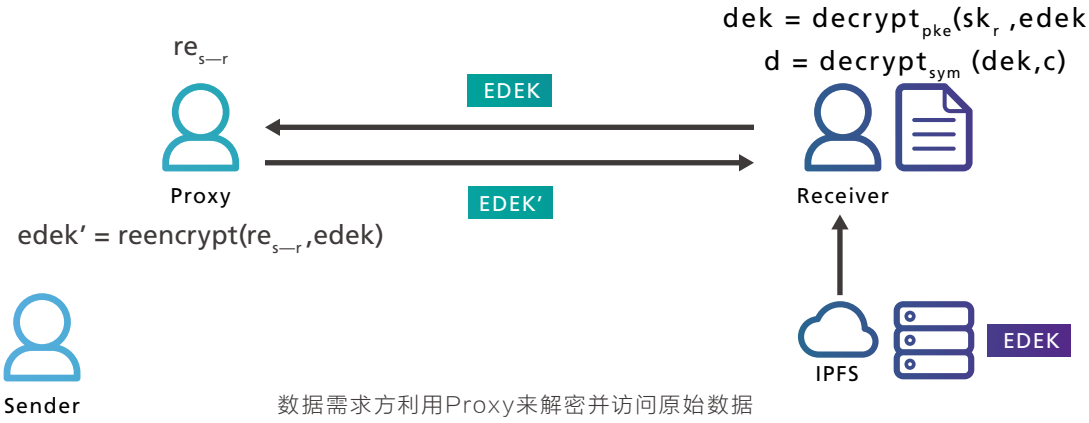
数据交易安全

当数据需求方希望访问并解密数据时，它需要先向数据提供者发起请求，数据提供者同意后向Proxy发送一个rekey。在这个场景下，还可以有一些第三方服务存在，比如验证数据需求方的身份、提供访问日志服务等，在这里就不进一步展开了：



数据需求方发起请求

接下来数据需求方将向Proxy发起请求，并获得一个rekey后的EDEK，再加上数据需求方的私钥，数据需求方就可以解密并访问原始数据。



数据需求方利用Proxy来解密并访问原始数据

利用Proxy Re-encryption，我们可以实现数据的一次加密+多次授权，并且确保了：

一方面，只有指定被授权方使用自己的秘钥才能解密并访问原始数据；

另一方面，被授权方只能访问数据提供者的指定数据而并非全部数据；而且幸运的是，在去中心化的世界中已经存在对Proxy Re-encryption的实现，即Nucypher KMS[14]。CarBlock团队可以直接利用这样现有的服务，进一步节约开发资源和项目时间。

隐私保护

Privacy Mask，是CarBlock专为车联网数据设计的隐私保护模块，提供数据解密与保护用户隐私数据不被泄露的功能。这也是来自于我们的理念：数据的所有权属于提供者，对数据的访问必须得到提供者用户的授权，包括单次授权模式（Request & Approval）和授权规则模式（Authorization Rules）。

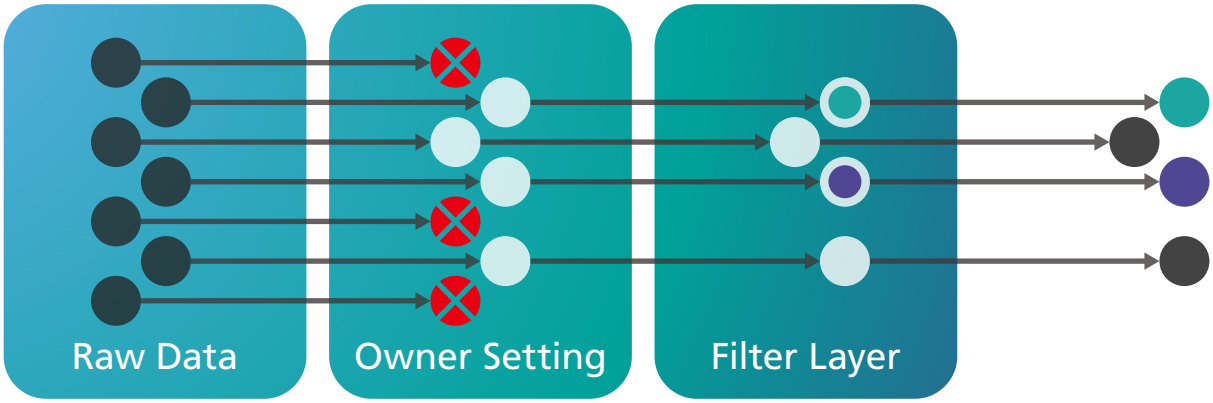
模块的最底层是数据所有者（Data Owner）的自定义设置，它负责数据访问的最底层权限控制，任何用户未授权的数据请求都将在最底层被拦下。它的默认设置是“匿名数据”，即用户真实身份相关的信息都不会以任何形式被访问到。“滤镜层”（Filter Layer）会将数据请求方要求的非核心数据做混淆与染色，在保证数据可用的前提下，最大限度的保护用户隐私。

滤镜层的策略有3种（未来根据业务需求而增加）：

混淆策略：比如把多段不同的行程混淆拼接。

模糊策略：比如在位置精度范围内，对地理位置做偏移处理，模糊精确位置。

乱序策略：比如在时间精度范围内，对时间先后顺序打乱。



Privacy Mask（隐私保护模块）工作原理

通过多样的用户设置和滤镜策略，一方面可以确保普通用户隐私的最大保护，另一方面也可以允许部分用户为了利益对外开放更多细节数据，实现数据市场的丰富性和自由性。

基于数据水印技术的版权保护

在数据交易完成后，可能会产生数据泄露、非正常途径转卖的等情况，我们使用了数据水印技术，将一些标识信息直接嵌入数据当中，对数据的使用价值无影响，也不容易被探知和再次修改，但可以被生产方识别和辨认。通过这些隐藏信息，实现防伪溯源、版权保护的目的。

目前比较常见的针对关系型数据库或大数据的水印算法有：

利用数值型数据的误差容忍度，在数值型数据中随机选取不重要位置，嵌入少量水印信息

基于数据集合统计特征，对某元祖数据进行排序后构建子集，取连续序列数据作为嵌入水印的基本单位

我们的水印算法会基于这些常见算法，并作出自身的优化：

结合车联网数据特点，对不同类别数据采取相应的算法，比如以地理位置为核心的行车轨迹数据，和设备元器件参数为核心的车况数据，其水印信息生成和嵌入方法会不同，提高水印信息的隐蔽性

多个维度上加入水印信息，提高水印的鲁棒性（即难以去除或者难以完全去除）

部分水印数据本身有加密和混淆，保障水印信息本身的安全性

当前各种水印去除和破坏的攻击手段层出不穷，攻击者和水印算法设计者也是魔高一尺道高一丈的不断攻防，CarBlock安全团队会持续研发出更高质量的水印算法以保障数据版权安全。

CarBlock经济模型

“挖矿”成本分析

如前文所述，CarBlock的数据提供者（车主们）提供大量有价值的出行数据，并获得CAR Token奖励，所以可以认为车主们在生态中扮演“矿工”，他/她们提供数据并获得Token的过程可以形象的称为“挖矿”。

“挖矿”的成本（价值）问题一直是一个有意思的话题，有些理论甚至认为挖矿成本就是Token价值的支撑点。CarBlock“挖矿”奖励算法在前文“挖矿”与贡献证明章节已经探讨，虽然我们并不完全认同“挖矿成本”和“Token价值”的关联性，但以下我们就将从“车主汽油消耗”的经济角度来粗略探讨一下CarBlock的“挖矿”成本：

从汽油消耗的角度，**1CAR的“挖矿”成本 = (Driver数量 x 人均每日汽油消耗 x 汽油价格)/每日Token发行量；**

根据Motley Fool在2017年的报道，美国平均每个驾驶员2015年的汽油消耗是656加仑，即折合每天每人汽油消耗1.8加仑-我们假设这个用户驾驶习惯在数年内不会产生大的变化；

根据CNBC新闻报道[15]，美国在2018年1月平均油价是$2.54-我们就取这个数字来作为汽油价格来参与计算；

nonda将在其所有用户中推荐CarBlock，甚至将在其后续App中直接接入CarBlock SDK，提供车主数据获得奖励的“挖矿”功能。nonda在2017年的MAU是40万+，所以CarBlock生态中Driver数量可以用100,000来作为一个非常可行的保底数字；

将以上变量代入公式可得：**1CAR的“挖矿”成本 (USD) = (Driver数量 x 1.8 x 2.54)/200000**。根据100,000作为保底的Driver数量，我们可以绘制以下表格：

Driver数量	1CAR Token的“挖矿”成本 (in USD)	1CAR Token的“挖矿”成本 (in ETH)
100,000	2.29	0.0035
400,000	9.16	0.0062
1,000,000	22.86	0.0352
10,000,000	228.60	0.3523

*这是以2018年3月ETH平均价格$650来计算。

诚然，以上的计算方式不尽完美，一方面驾驶者还要投入大量的时间，这可能比汽油更有价值；另一方面从驾驶者目的来看，他／她付出大量的油耗是因为行程的安排，而贡献数据并获得CAR Token只是顺势之举。所以以上计算只是说明了：如果存在“矿工”想以赚取CAR Token目的来进行驾驶，他／她将付出如何的最低成本，但我们不希望也不认为会存在这样的“矿工”，而且从计算结果来看，从驾驶来赚取CAR Token这个纯“挖矿”行为本身的成本不低。

CAR Token 使用场景

CAR（Utility Token）作为未来智能交通中最重要的角色，将在很多环节中发挥作用。为了便于描绘，我们将使用场景尽量合并，如下图所示：

CAR流通场景

因篇幅有限，以下我们仅选取几个很有意思的场景来展开探讨：

场景1：保险服务

目前，绝大部分的汽车保险是根据汽车型号、车龄、交通违章等静态信息进行报价，也有极少部分保险公司（如前文提到的Metromile）开始根据行驶里程来修正保费价格。但是当车联网数据在CarBlock生态中自由流动后，会发生什么？

汽车型号、车龄一样，但车况完全不同的情况很常见。对，创新的保险公司可以完全扔掉汽车型号、车龄这些笼统信息，直接精确根据车况来计算－保养更好的车辆理应获得更好的报价；

个人驾驶风格不一样，出险概率也有很大不同。对，交通违章信息也可以扔掉了（和当地警力有关），创新的保险公司直接分析驾驶习惯，甚至针对驾驶习惯推出特定保险；

出险概率是不是和当地的气候、路面情况有关？根据用户的活动区域变化（出差、搬家等），未来的气象分析，路面变化等，能否进一步计算出险风险的调整？甚至提醒驾驶员未来潜在的风险，进一步降低出险概率？

所以在CarBlock生态中一定会出现大量有趣的新保险服务，给出的保险服务完全颠覆现有的车险行业。最颠覆的车险甚至可能是取消现在的年费模式：为什么车险要一年一次性付一大笔钱，而不能像飞机险这样根据实际行程需要来支付？在CarBlock生态中完全可以做到保险从汽车发动开始计费，到发动机停止后终止，保险费用根据当时实际情况计算（本地/外地行车都有不同保费），自动从用户钱包中扣除CAR（Token）结算，不是吗？

保险服务里面另一个有意思的变化在车主端：

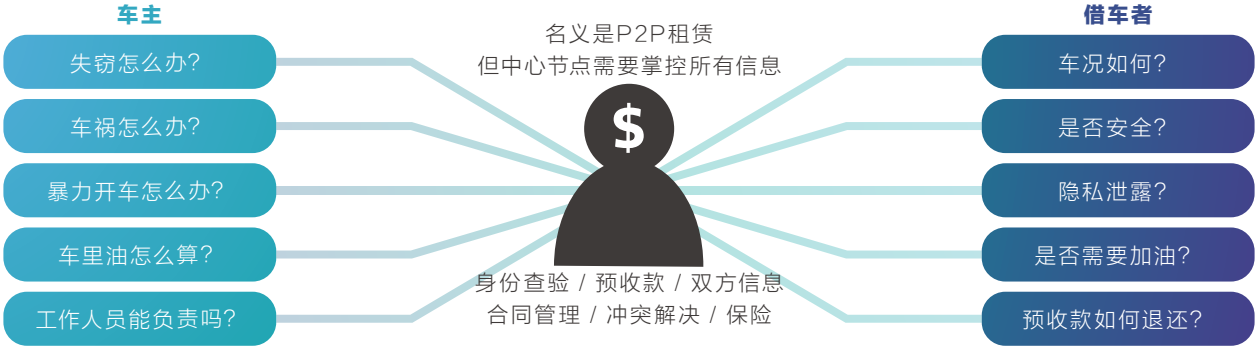
一部分的车主由于更好的实际情况，会获得更优惠的保险条款，而且由于CarBlock生态能让更多保险公司参与竞争，获得优惠的车主只会更多；

另一部分车主由于糟糕的车况或驾驶习惯，可能会要求支付更高的保费。但是，这时候一定会有第三方来为车主提供分析服务，告诉车主哪些不良车况和习惯将他置于风险之中，所以最终导致了保费的上涨。这些服务一方面可以让第三方开发商从用户获取了CAR（Token），另一方面也将促成这些车主反思并修正自己的车况或行驶问题，降低车主的生命/财产损失风险，最终也使车主收益。

综上，我们深信在CarBlock这个开放性生态中，商业合作比现有的“旧世界”做到更多的“双赢”、甚至“多赢”，是完全现实的一个结果。

场景2: P2P租车

现在中心化的P2P租车虽然名义是“P2P”，但在所有场景里我们都可以看到中间人很忙，而两边是信息不对称和大量顾虑：



中心化的P2P租车场景

而在CarBlock生态中，仿佛P2P租车就是为去中心化量身定制的业务：

真正P2P，双方隐私信息都不需要担心外泄，而区块链就是为了解决在非信任关系下的交易；

车主的车况信息、借车者的使用状况，对双方都可以做到透明、真实、公平；

支付走智能合约，租车开始自动计算，回到约定地点交还后自动结算；

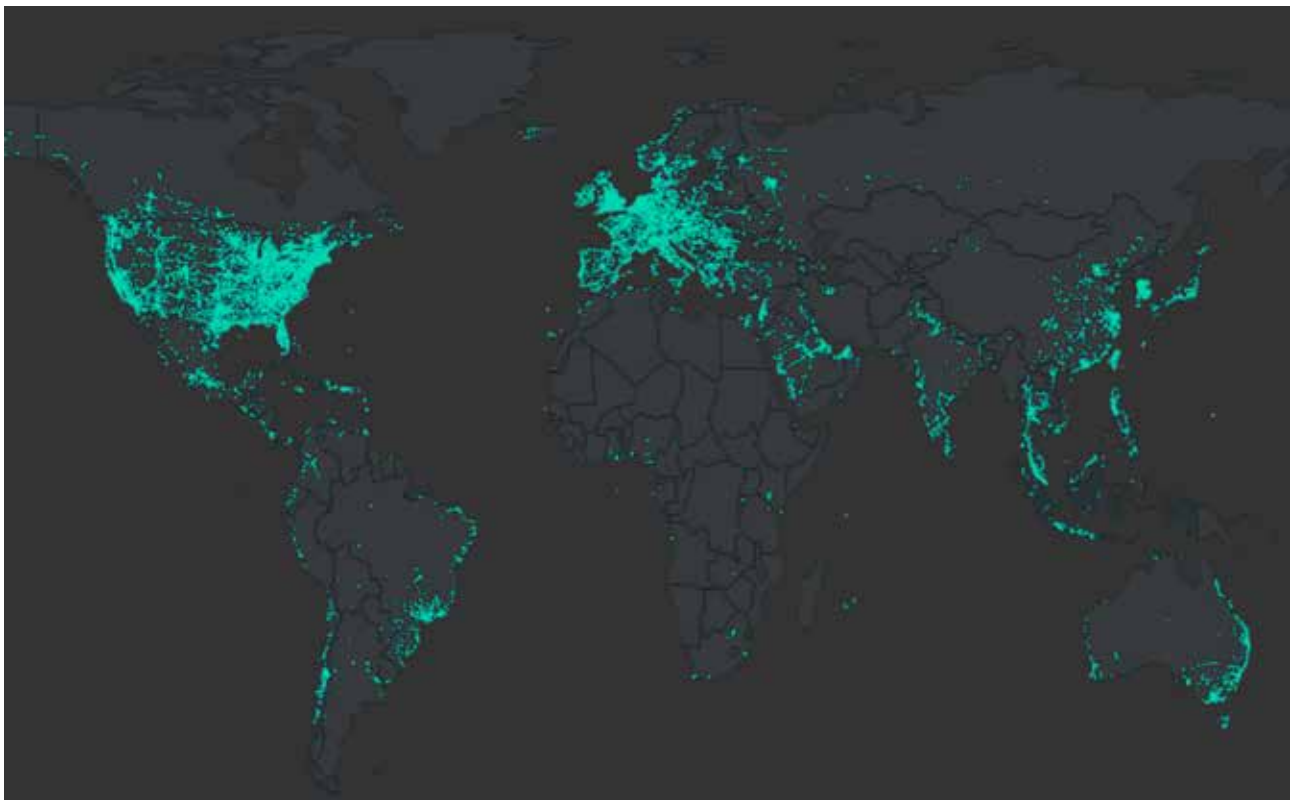
第三方服务（身份认证、保险、防盗、维修、救援）无缝对接，无需中间人工作人员决策；

所有CarBlock生态的车主都可以成为P2P出借方，实现充分市场供给；

如何建立CarBlock生态

CarBlock是一个交通数据生态的协议及落地应用标杆，通过标准的开放协议，将数据从线下所有的汽车/出行业务都引导到这个生态中来，并以此打造创新的去中心化应用。在这个生态中，在数据的“润滑”作用下，用户可以享受到更个性化、更精准、更价优的服务；服务提供商可以更精确的评估成本、推出更多样化的服务、更低成本的接触到目标用户；而创新者将面对更低的进入门槛，给生态带来更多的竞争、更多角度的服务。

首先，我们通过与北美第一个车联网智能硬件企业 nonda 合作，快速建立起了五十万左右的车主群体，以及成熟的硬件数据收集解决方案，保证了 CarBlock 在发展初期能够顺利避免多数项目冷启动的窘境，尤其对于建立一个双边市场，CarBlock 现有的业务基础能够快速打破先有鸡还是先有蛋的问题，并利用 nonda 现在的用户、产品、渠道及品牌影响，将业务快速落地，为日后技术产品的成熟以及生态的扩大提供巨大的帮助。



nonda公司的全球用户分布图

其次，我们认为，建立这个生态的核心循环是：

更多车主加入生态，提供更多的数据，并吸引更多的汽车及其产业相关厂商；

更多的汽车及其产业相关厂商包括创新者）加入生态，在合理获取及利用数据的前提下，为车主提供更多的个性化、精准、价优的服务和产品，并吸引更多的车主加入生态；

从吸引车主加入生态的角度来看，CarBlock有以下优势：

对于车主： CarBlock项目的诉求“你掌控自己的数据”、“获得更个性化、更精准、更价优的服务”也正是车主的诉求，利益充分一致。同时，“通过提供（储存）数据来获得奖励”也是极其有效的激励车主使用的手段。

对于nonda等第三方车联网智能硬件及IoT解决方案公司： 产品方将真正成为尊重用户隐私，符合大众利益及法律法规的公司，同时也享受CarBlock生态带来的额外卖点和流量，从而更愿意将自身用户导入CarBlock生态。

对于汽车厂商： CarBlock的解决方案可以提供免费的数据存储、基于加密与证书的数据访问和授权，并帮助厂商解决数据隐私的法律问题。这对于厂商来说是一个免费的开源的解决方案，可以大大降低厂商自己的工作量和成本。作为代价，厂商只需要承认用户（车主）也对数据拥有所有权，车主加入CarBlock后可以用自己的秘钥来管理和授权第三方的访问；

对于汽车后市场服务类厂商： 其用户在加入CarBlock生态后，将获得更为精准，更有竞争力的服务的产品，厂商在升级创新的同时，也将为CarBlock生态注入更多的流量。

从吸引服务提供商（包括创新者）及相关厂商加入生态的角度来看，CarBlock有以下优势：

从行业发展看，基于用户画像（profile）的精准服务和报价已经成为一个趋势，重要性和价值已经不需要CarBlock团队进行普及；

CarBlock的使命就是让数据尽可能低成本的在生态中流动，鼓励服务商基于数据来进行业务决策，这完全符合服务商的利益和诉求；

CarBlock生态中的大量车主可以使服务商更低成本的接触到用户，节省大量广告开支投入到个性化产品研发、或回馈用户。

此外，CarBlock可以在生态中快速引入很多服务于车主或服务提供商的创新服务。例如，在2018年3月，Facebook爆发了Cambridge Analytica丑闻[16]，除了大量个人Facebook数据被盗用之外，令人震惊的是Facebook公司在2014年了解此事后的不作为。我们想：如果有类似非法使用数据的事件发生在CarBlock中会怎么样呢？非常简单，CarBlock基于本身生态发展的最大利益，一定会毫无犹豫地去惩罚生态系统的破坏者，其次，所有生态内的研发者、创新者、服务者，都会自发进入系统，针对性提供免费或收费的服务或工具，或自动请求代表用户发起群体诉讼，配合CarBlock快速来解决问题或降低风险。

最后，CarBlock是一个独立运作的区块链项目，运作方（CarBlock Foundation）不与任何一个合作伙伴存在业务竞争或利益冲突、合作姿态开放 – 生态利益的最大化即CarBlock Foundation利益的最大化。从动机和诉求的角度，CarBlock相比任何传统公司结构都更适合来发起并完成这个生态；而多年的行业经验、跨国业务经验、及移动互联网背景又能帮助CarBlock团队更深刻去理解这个行业、找到各方的痛点和需求、发起并完成商业合作。以上即CarBlock团队的信心来源，并希望通过这个项目来颠覆汽车/出行行业的生产关系，实现一个更高效率、更精准、更个性化、更多样化的新世界。

发展路线

2018 Q1

CarBlock项目正式启动

核心团队组建完成

2018 Q2

CarBlock募资完成

首款支持挖矿功能App上线

首款硬件产品支持挖矿功能

底层技术方案确认

2018 Q3

第二款硬件产品支持挖矿功能

确认业务层POC需求确认

2018 Q4

完成业务层POC开发

完成第一条基于区块链的车数据真实交易

完成协议层原型测试

2019

扩展和接入更多合作伙伴

挖矿设备进入大众市场

在CarBlock生态内发布维修保养业务

CAR在真实商业环境内形成闭环

协议层开发完成并支持多公链接入

在CarBlock生态内发布保险业务

在CarBlock生态内发布二手车交易业务

2020

整车厂合作并支持整车挖矿

CarBlock 协议层接入更多去中心化应用

CAR在真实商业环境内大规模流通

免责声明

本文档只用于传达信息之用途，并不构成买卖项目股份或证券的相关意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策，或具体建议。

本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不 组成也不理解为提供任何买卖行为，或任何邀请买卖、任何形式证券的行为，也不是任何形式上的合约或者承诺。

本文档此文中所有的收益和利润举例仅为展示目的，或代表行业平均值，并不构成对用户参与结果的保证。

CarBlock明确表示相关意向用户明确了解平台的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。
CarBlock明确表示不承担任何参与项目造成的直接或间接的损失包括: (i) 本文档提供所有信息的可靠性 (ii) 由此产生的任何错误，疏忽或者不准确信息 (iii)或由此导致的任何行为。

CAR是以CarBlock生态为其使用场景之一的数字Token。CAR不是一种投资。我们无法保证CAR将会增值，其也有可能在某种情况下出现价值下降。 鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书 的所有目标，所有购买CAR的个人和团体将自担风险。CAR不是一种所有权或控制权。控制CAR并不代表对CarBlock或其应用的所有权，CAR并不授予任何个人任何参与、控制、或任何关CarBlock及其应用决策的权利。

风险提示

数字资产投资作为一种新的投资模式，存在各种不同的风险，潜在投资者需谨慎评估投资风险及自身风险的承受能力。

Token销售市场风险

由于Token销售市场环境与整个数字货币市场形势密不可分，如市场行情整体低靡，或存在其他不可控因素的影响，则可能造成Token本身即使具备良好的前景，但价格依然长期处于被低估的状态。

监管风险

由于区块链的发展尚处早期，包括我国在内全球都没有有关ICO过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规文件。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的投资与流动性产生不确定影响。而区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则CarBlock应用或CAR可能受到其影响，例如法令限制使用、 销售Token诸如CAR有可能受到限制、阻碍甚至直接终止CarBlock应用和CAR的发展。

竞争风险

随着信息技术和移动互联网的发展，以“比特币”为代表的数字资产逐渐兴起，各类去中心化的应用持续涌现，行业内竞争日趋激烈。但随着其他应用平台的层出不穷和不断扩张，社区将面临持续的运营压力和一定的市场竞争风险。

人员流失风险

CarBlock集聚了一批在各自专业领域具有领先优势和丰富经验的技术团队和顾问专家，其中不乏长期从事区块链行业的专业人员以及有丰富互联网产品开发和运营经验的核心团队。核心团队的稳定和顾问资源对CarBlock保持业内核心竞争力具有重要意义。核心人员或顾问团队的流失，可能会影响平台的稳定运营或对未来发展带来一定的不利影响。

资金匮乏导致无法开发的风险

由于创始团队筹集的Token价格大幅度下跌或者开发时间超出预计等原因，都有可能造成团队开发资金匮乏，并由此可能会导致团队极度缺乏资金，从而无法实现原定开发目标的风险。

私钥丢失风险

购买者的CAR在提取到自己的数字钱包地址后，操作地址内所包含内容的唯一方式就是购买者相关密钥(即私钥或是钱包密码)。用户个人负责保护相关密钥，用于签署证明资产所有权的交易。用户理解并接受，如果他的私钥文件或密码分别丢失或被盗,则获得的与用户帐户 (地址) 或密码相关的CAR将不可恢复，并将永久丢失。最好的安全储存登录凭证的方式是购买者将密钥分开到一个或数个地方安全储存，且最好不要储存在公用电脑。

黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断CarBlock应用或CAR功能的可能性，包括但不限于拒绝服务攻击、Sybil攻击、游袭、恶意软件攻击或一致性攻击等。

未保险损失的风险

不像银行账户或其它金融机构的账户，存储在CarBlock账户或相关区块链网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保。

核心协议相关的风险

CarBlock平台目前基于以太坊开发，因此任何以太坊发生的故障，不可预期的功能问题或遭受攻击都有可能导致CAR或CarBlock平台以难以预料的方式停止工作或功能缺失。

系统性风险

开源软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

漏洞风险或密码学加速发展的风险

密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给CarBlock平台，这可能导致CAR的丢失。

应用缺少关注度的风险

CarBlock应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对 CAR和CarBlock应用造成负面影响。

不被认可或缺乏使用者的风险

首先CAR不应该被当做一种投资，虽然CAR在一定的时间后可能会有一定的价值，但如果CarBlock不被市场所认可从而缺乏使用者的话，这种价值可能非常小。有可能发生的是，由于任何可能的原因，包括但不限于商业关系或营销战略的失败，CarBlock平台和所有的众售资金支持的后续营销将不能取得成功。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对本项目而言是非常不利的。应用存在的故障风险

CarBlock平台可能因各方面可知或不可知的原因故障(如大规模节点宕机)，无法正常提供服务，严重时可能导致用户CAR的丢失。

应用或产品达不到自身或购买者的预期的风险

CarBlock应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何CAR自身或购买者对CarBlock应用或CAR的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

无法预料的其它风险

基于密码学的Token是一种全新且未经测试的技术，除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。

参考文献

[1] “Top 6 Digital Transformation Trends In The Automotive Industry”, Daniel Newman
https://www.forbes.com/sites/danielnewman/2017/07/25/top-6-digital-transformation-trends-in-automotive/#2fffb3e54e1e

[2] “Metromile”, Wiki
https://en.wikipedia.org/wiki/Metromile

[3] “Connected vehicle Succeeding with a disruptive technology”, Andreas Gissler
https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_21/Accenture-digital-Connected-Vehicle.pdf

[4] “国信证券行业研究报告”, 国信证券
http://pg.jrj.com.cn/acc/Res/CN_RES/INDUS/2016/12/16/ed422d0b-176c-4c65-8cc8-2864fbb81d70.pdf

[5] “Equifax profits by selling your personal data”, THE EDITORIAL BOARD
https://www.dailynews.com/2017/09/12/equifax-profits-by-selling-your-personal-data/

[6] “还有多少App在窥视个人隐私 支付宝年度账单事件背后”, 新浪综合
http://tech.sina.com.cn/i/2018-01-11/doc-ifyqnick7174902.shtml

[7] “Waymo says it has logged 3 million miles of self-driving on public roads”, Chance Miller
https://9to5google.com/2017/05/09/waymo-miles-3-million-may/

[8] “Merkle tree”, Wiki
https://en.wikipedia.org/wiki/Merkle_tree

[9] “Filecoin”, Wiki
https://en.wikipedia.org/wiki/Filecoin

[10] “Proof of Replication Technical Report”, Protocol Labs
https://filecoin.io/proof-of-replication.pdf

[11] “Exponential function”, Wiki
https://en.wikipedia.org/wiki/Exponential_function

[12] “Cumulative distribution function”, Wiki
https://en.wikipedia.org/wiki/Cumulative_distribution_function

[13] “Proxy re-encryption”, Wiki
https://en.wikipedia.org/wiki/Proxy_re-encryption

[14] “NuCypher KMS: Decentralized key management system”, Michael Egorov, MacLane Wilkison, David Nuñez
https://www.nucypher.com/assets/whitepapers/english.pdf

[15] “Average US gas price jumps 3 cents to $2.54 for regular”, CNBC
https://www.cnbc.com/2018/01/08/average-us-gas-price-jumps-3-cents-to-2-point-54-for-regular.html

[16] “Facebook's Mark Zuckerberg finally addresses Cambridge Analytica scandal”, Julia Carrie Wong
https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica