DACH 车链

基于分布式技术的汽车生态圈

White Paper v3.0

May 2020

目录

摘要

艾媒咨询统计，全球每年生产约 8000 万辆汽车，目前全球有约 13 亿辆汽车存量，汽车行业的规模体量达 10 万亿美元。

当然，这两年随着全球经济的下行，2018 年全球新车销量出现历史性拐点，首次出现负增长。

2019 年 7 月初，摩根士丹利研究报告中预测，2019 年全球汽车产量将下降 4%。德国杜伊斯堡埃森大学汽车研究所在 6 月份发布的一份报告中认为，2019 年全球汽车销量将为 7950 万辆，与 2018 年相比减少了 420 万辆，同比减少 5%。

2018 年中国汽车的产量和销售量均下滑，分别为 2780 万辆和 2808 万辆，同比下降了为 2.8%和 4.2%，结束为期 28 年的汽车销量增长。

虽然，近两年全球和中国市场汽车销售增长减缓，但中国汽车保有量保持年均 10%以上的增长；截止 2018 年底中国汽车保有量已达到 2.4 亿辆，有望在 2020 年超越美国成为汽车保有量全球最大市场。

同时，中国有上百个汽车厂家，加上进口汽车，覆盖全球上千个汽车品类，随着汽车车龄的增加、汽车改装、汽车租赁、共享汽车、汽车智能服务、二手车交易量的发展，更多的市场资本逐渐投向了汽车后市场，这一定程度上给汽车后市场提供了一个黄金发展期。

但是，中国汽车后市场各个环节大多是碎片化经营，数据相互割裂，标准难统一，品质良莠不齐、车主体验差，汽车保险、汽车金融缺乏数据支持成本高，无法更好的跟上时代发展趋势，无法更好满足消费者需求。

DACH 基于区块链的透明、可信、不可逆等技术特点，所建立的一个去中心化的汽车生态数据服务平台。DACH（Dash Car Chain）通过供应链、数据链、价值链多维度数据的分布式存储与流通，实现配件标准互通、整车生产、车辆流通、车主消费、车辆消耗、行驶行为、车辆残值、汽车金融等数据的上链、转换、溯源、数据触发等应用，为汽车产业赋能，助力汽车消费升级，推动汽车产业发展。

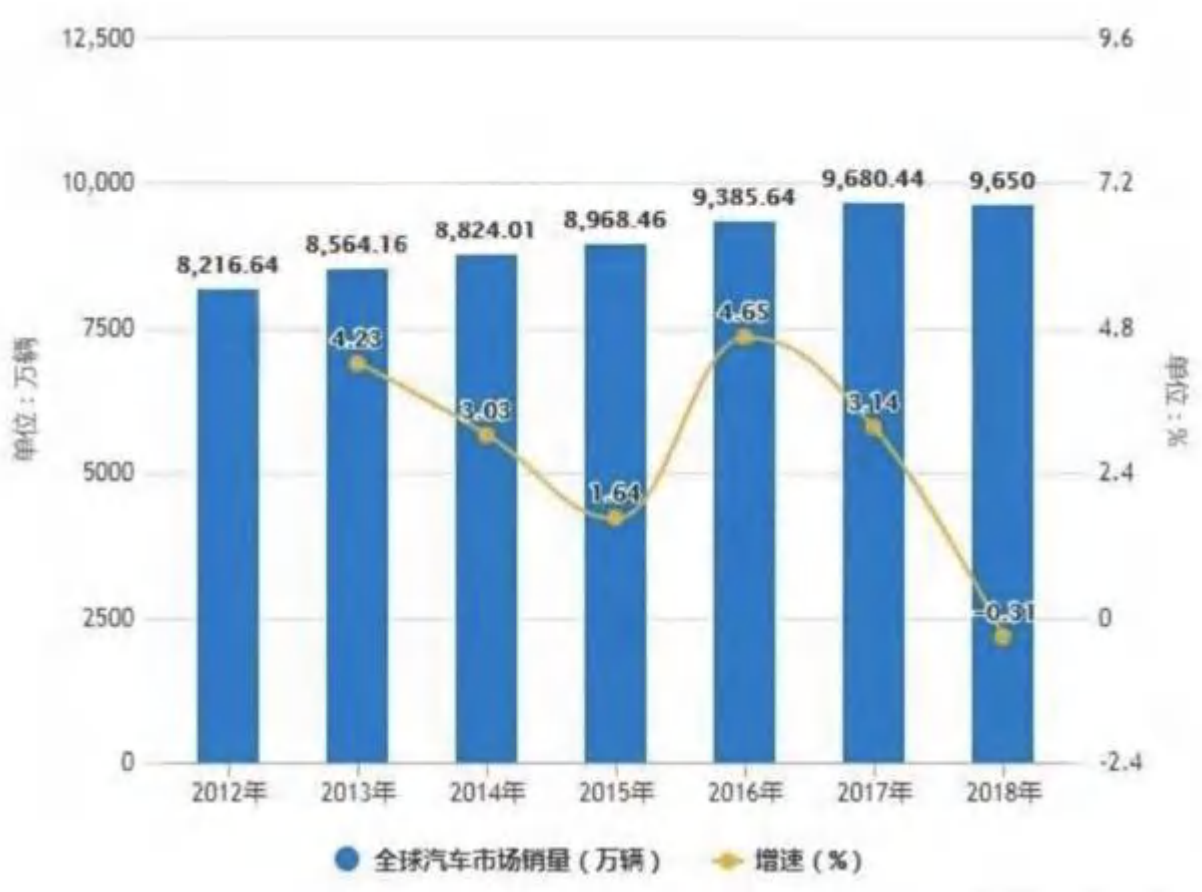
DACH.VIP

1. 项目背景

1.1 全球汽车销量首次连续两年下跌

据前瞻产业研究院发布的《中国汽车整车制造行业需求前景预测与理财战略规划分析报告》统计数据显示：受全球经济形势影响，全球汽车市场遇冷，结束了连续 7 年上涨趋势，2018 年首次出现全球汽车销量下滑。2018 年全球汽车市场销量达到了 9560 万辆，较上年同比下降 1.24%。2018 年的上半年，全球市场表现相对出色，保持了一定增长势头。但从下半年开始，欧洲和中国两个最大汽车市场开始出现了销量下滑情况，最终导致全球汽车销量七年来首次下滑。

2012-2018 年全球汽车市场销量统计及增长情况



1.2 中国汽车销量下滑，但保有量将成为第一，后市场大有可为

（1）2018 年中国汽车产销量均有所下滑 13%

据《日本经济新闻》统计，2019 年二季度，全球汽车销量最大的 5 个单一市场，中国、美国、欧盟、印度、日本的汽车销量总计约为 1600 万辆，同比减少了 13%，创下了单季度销量降幅历史新高。和 2018 年相比，这些国家和地区汽车销量下降的速度正在加快，而且更多的市场加入到销量下滑的行列。

2018 年全球主要的汽车市场中，日本、美国、印度都保持增长，仅欧洲和中国下滑。但今年二季度，中国、印度、美国和欧洲都出现了销量下滑，而且中国和印度两国汽车销量下滑幅度都超过了 13%。

7 月初，摩根士丹利在一份研究报告中预测，2019 年全球汽车产量将下降 4%。德国杜伊斯堡埃森大学汽车研究所在 6 月份发布的一份报告中认为，2019 年全球汽车销量将为 7950 万辆，与 2018 年相比减少了 420 万辆，同比减少 5%，原因是美国的贸易政策将会对全球汽车消费产生影响。该报告认为全球汽车销量下滑的状态将延续四年，直到 2022 年才能恢复增长。

（2）2018 年中国汽车市场依然是全球最大的单一国家市场

2018 年以来，中国汽车市场产销量均出现一定程度上的下滑，但在 2018 年中国汽车销量依然达到 2800 万辆，中国汽车市场依然是全球最大的单一国家市场。

（3）中国汽车市场保有量每年 10%增长，汽车后市场空间巨大

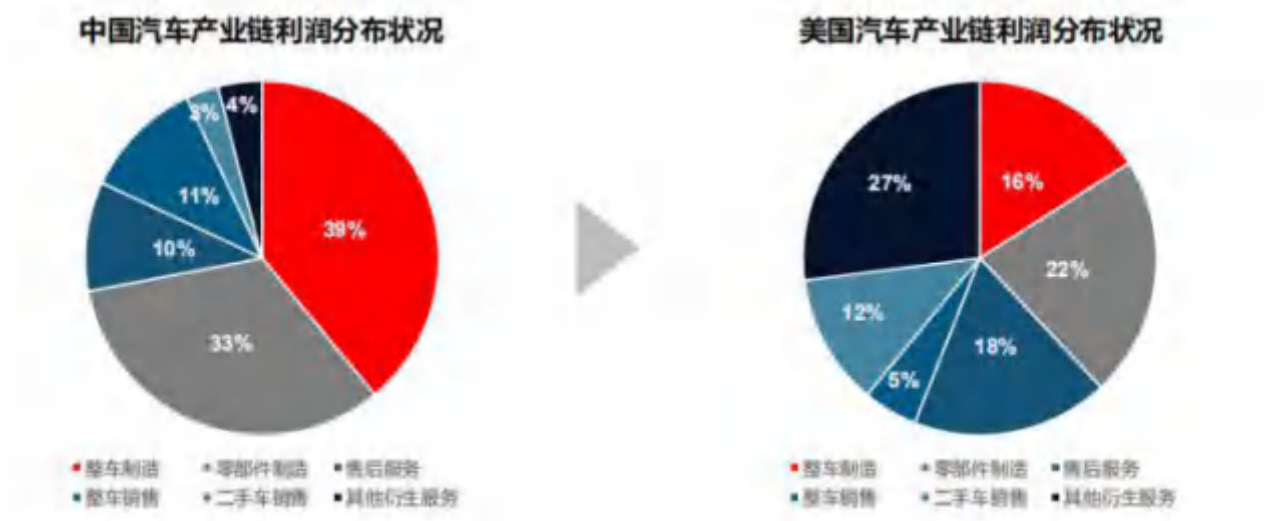
从市场发展来看，中国汽车保有量保持年均 10%以上的增长，至 2018 年已达到 2.4 亿辆；同时，有望在 2020 年超越美国成为保有量全球最大市场。

后市场因历年汽车保有量的增加，其规模越来越大，2018 年后市场规模达 12900 多亿；

目前，中国现有保有车辆平均车龄约 4.9 年，并随着市场存量车辆的车龄还在持续增长，对照国际市场用车经验，车龄超过 5 年后将迎来大型维修保养高峰期。

（4）中国与成熟汽车市场相比，在后市场方面依然有较大的增长空间

从中国汽车市场与美国等成熟汽车市场的利润分布对比来看，虽然中国汽车市场利润50%分布在后市场中，但与美国等成熟的后市场利润相比，还有一定的差距，如美国后市场利润占比能够达到 80%左右，未来还有巨大的增长空间。



（5）技术驱动：互联网+汽车，促进后市场产业发生变革

随着移动互联网的快速发展，以车联网、智能化、大数据等为代表的新技术将逐渐应用与售后服务相关的领域，服务于汽车后市场的各个业务层面。

在线养护：

自营型养护电商	综合电商	品牌连锁店	导流/上门服务平台

在线二手车：

二手车售卖	二手车评估	二手车检测

在线汽车租赁：

在线预订	在线支付	分时租赁	车辆共享

在线金融：

金融公司线上平台	独立第三方平台	互联网金融公司

在线保险：

保险公司线上平台	独立第三方平台	互联网保险公司

1.3 麦肯锡预测：汽车产业未来将发生惊人变化

未来几年，汽车产业将迎来根本性变化：

渠道及其入口的数字化，产业需要新的配套能力

以区块链、大数据分为代表的软件技术愈发重要，将成为新的价值

行业整合将加速，专业化汽车管理将愈发重要

新兴市场和服务意识将进一步提升

下一代汽车兴起，电气化将缩小利润池

自动驾驶的发展将减少事故和维修量

谷歌、亚马逊、eBay、中国的 BATJ 等新玩家将进入市场，将赢得重要的市场份额

这些变化必然引起汽车后市场的价值链重塑、终端客户获取方式转变、利润池的转移。

1.4 汽车产业现状

1) 传统汽车服务对象正在由“车”转变成“人”

传统汽车服务的对象主要是“车”，不管是车贷、车险、维修、保养、用品销售，还是汽车美容，汽车服务的着力点都在汽车上。然而，在智能互联蓬勃发展的今天，上述每一个环节都正在、或者即将被互联网和人工智能等新技术所改变，汽车作为制造的商品，越来越透明。

越来越多的人意识到要尽快升级汽车服务，以适应于即将爆发和到来的以人为中心的智能互联与自动驾驶等发展大趋势。

现在，Uber、滴滴出行等打车服务的日益普及，就是因为他们解决了闲置汽车的数据和用车客户的需求数据进行协同。

Vendy 公司 CEO 萨洛蒙·霍洛维茨认为：“我们在车内花费的时间会越来越多，我们将变得越来越依赖汽车。 汽车服务将像互联网一样，为电商、社交媒体和约会服务带来新的发展机遇，为车内售货机、广告和数据收集提供新的平台”。

2) 中国汽车服务市场现状不容乐观

服务市场混乱

中国消费者较为偏好到 4S 店进行汽车维修、保养美容等消费，但 4S 店客户消费不透明，缺乏成本优势。

街边中小型服务店的专业性与技术性不到位。

管理落后

汽车服务市场鱼龙混杂，产能过剩。

进行专业汽车维修和保养的人才培养体系不健全。

汽修管理的不规范，服务和流程标准化程度低，行业体系发展不完善。

门店数虽多但规模小

汽车后市场各种业务项目较为分散，例如汽车配件和用品供应、汽车改装、美容养护、汽车维修、汽车保险等分散经营，无法形成一体化服务。

车主需求得不到满足

汽车耗材使用成本高

掌握汽车技能的学习成本高

汽车泊车等操作费时费力费钱

汽车保险等服务成本高

汽车社交难信任

1.5 汽车产业的痛点分析:

信任不能相通

在现代商业，人、组织之间彼此缺乏信任的基础，更多行为都是在验证彼此信任，最大的成本就是信任的成本，无异于阻碍了商业活动和人际交往。这也是第三方服务企业兴起的原因，就是解决信任起到桥梁作用。

数据不能联通

传统商业都是各自独立的个体，所有思维逻辑和底层算法都是中心化设置，缺乏数据共享的激励机制和工具，导致各个中心化组织之间很难实现数据的联通。比如：车主消费数据和汽车厂家数据无法联通。

价值不能流通

每一个模块和各个维度的数据无法连通，也难以建立多维度统一的数据价值评估和交易体系，更多的价值认可只能局限在各自独立的生态体系，在其他体系就无法使用，比如银行与商城之间的积分无法互通使用。

需求不能畅通

如果人、企业之间缺乏信任，彼此数据无法联通，价值交易无法实现，更多的车主需求也无法得到满足。

当然，诸多企业已嗅到汽车服务市场的发展变化，并做出了积极的调整与尝试，传统的汽车服务已发生了重大改变。虽然汽车服务趋势以消费者服务为中心，但是，我们也发现这些服务都是碎片化，数据相互割裂，车主作为被动消费者角色没有太多改变，消费者真正的潜在需求没有得到真正激活与满足。

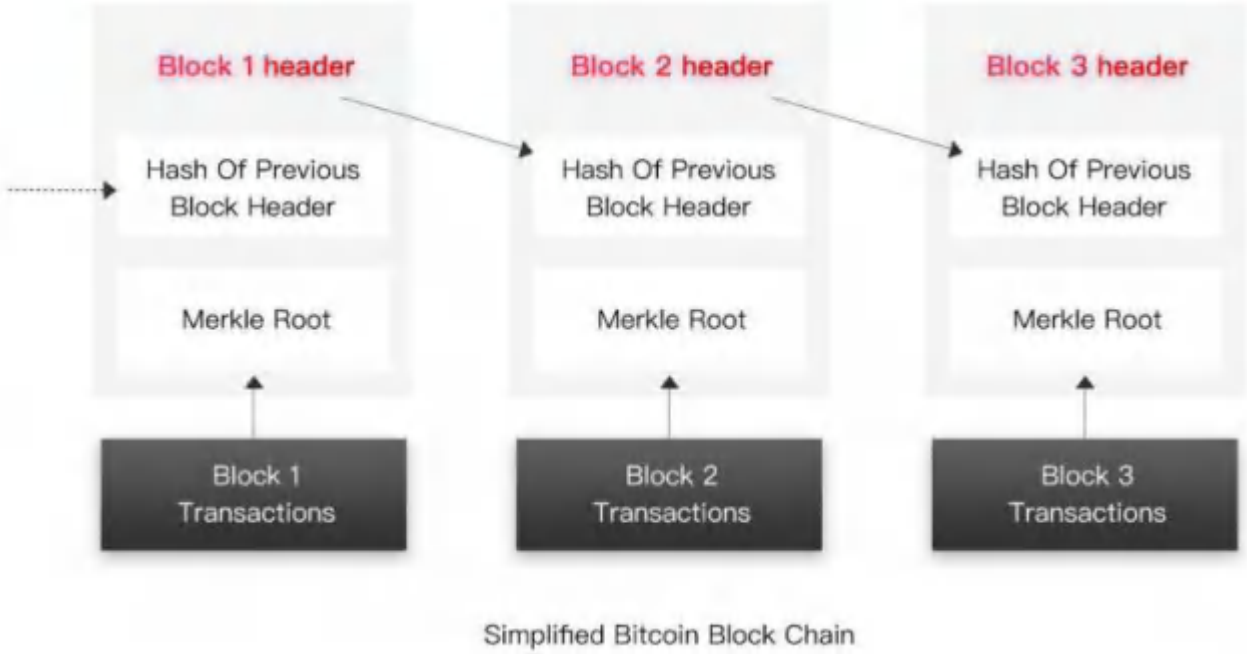
2. 区块链让汽车产业消费升级

事实上，汽车服务的对象已经慢慢由“车”在向服务“人”转变，也就是更多向人提供人、车、环境、场景体验等多维度的智能互联和数据协同。汽车不再是交通工具，而是作为数据的入口和载体，通过 5G、物联网 LOT、人工智能、VR/AR、大数据、云计算等技术，链接和集成所产生的所有数据，从而更好的洞察和满足客户的各种需求，推动产业发展。

随着区块链的诞生与发展，以人为中心的汽车服务，为以上“四通”的解决提供了可能。

2.1 区块链技术简介

上世纪 70 年代以来，随着密码学技术、分布式网络、共识算法以及硬件存储计算能力的飞速发展，通过技术手段实现多主体间共识机制建立的条件日趋成熟，为解决多主体环境下的中介机构信任风险、降低交易成本、提升协同效率提供了全新的解决思路。



Simplified Bitcoin Block Chain

中本聪于 2008 年发表了名为《比特 Token：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，详细描述了如何创建一套去中心化的电子交易体系。这种体系不需要创建在交易双方相互信任的基础之上，首次通过技术手段实现了交易主体间共识机制的建立，而“区块链”技术正是构成这种电子交易体系的基础技术。

以太坊（Ethereum）是继比特 Token 之后的又一个开创性的区块链项目，于 2013 年末发布白皮书。以太坊开创性地将智能合约（Smart Contracts）和区块链结合起来，在交易主体间共识机制建立的基础上，通过自动触发可执行的电子合约，解决了交易主体间承诺履行的问题，有效推动了区块链产业化应用的进一步发展。

近年来，区块链技术的不断发展和随之而来的 Token 热潮，引发了从极客到 IT 技术圈、金融领域、产业经济、政府和公共组织、媒体舆论等的广泛关注，围绕区块链技术研究、产业化应用、政策监管等开展了广泛而有益地探索实践。区块链技术的成熟应用尚需时日，但它所带来的多主体共识协同机制的思想，将对社会治理和商业运作产生深刻的影响。

2.2 什么是区块链

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。简单来讲，在区块链系统中，每过一段时间，各参与主体产生的交易数据会被打包成一个数据区块，数据区块按照时间顺序依次排列，形成数据区块的链条，各参与主体拥有同样的数据链条，

且无法单方面篡改，任何信息的修改只有经过约定比例的主体同意方可进行，并且只能添加新的信息， 无法删除或修改旧的信息，从而实现多主体间的信息共享和一致决策，确保各主体身份和主体间交易信息的不可篡改、公开透明。

区块链发展到今天，已经涌现出许多形形色色的区块链项目，我们梳理了这些区块链项目在技术上的共性：区块、账户、共识、智能合约这 4 个主要部分构成了目前的区块链系统的通用模型。

通过链式结构记录数据变更历史，这部分被称为“区块”；

通过非对称密钥表示参与者身份，以某种形式的状态数据库记录当前的信息，这部分被称为“账户”；

通过链上编码定义参与者之间的承诺，这部分被称为“智能合约”；

通过某种算法在多节点之间达成状态一致，这个过程被称为“共识”。

2.3 区块链有哪些特点

事实上区块链并不是一个全新的技术，而是结合了多种现有技术进行的组合式创新，是一种新形式的分布式加密存储系统。

区块链本质上是一种健壮和安全的分布式状态机，典型的技术构成包括共识算法、P2P 通讯、密码学、数据库技术和虚拟机。这也构成了区块链必不可少的 5 项核心能力：

存储数据

源自数据库技术和硬件存储计算能力的发展，随着时间的累积，区块链的大小也在持续上升，成熟的硬件存储计算能力，便得多主体间同时大量存储相同数据成为可能；

共有数据

源自共识算法，参与区块链的各个主体通过约定的决策机制自动达成共识，共享同一份可信的数据账本；

分布式

源自 P2P 通讯技术，实现各主体间点对点的信息传输；

防篡改与保护隐私

源自密码学运用，通过公钥私钥、哈希算法等密码学工具，确保各主体身份和共有信息的安全；

数字化合约

源自虚拟机技术，将生成的跨主体的数字化智能合约写入区块链系统，通过预设的触发条件，驱动数字合约的执行。

3. DACH 生态圈介绍

3.1 DACH 是什么

中国清华大学汽车工程系主任杨殿阁教授接受《中国汽车报》记者采访时曾表示：“未来汽车行业将不再是一个传统的制造业，而是一种全新的、更高价值的社会生态体系。这不再仅仅是汽车行业上的技术变化，而是一场由汽车带来的社会变革。”

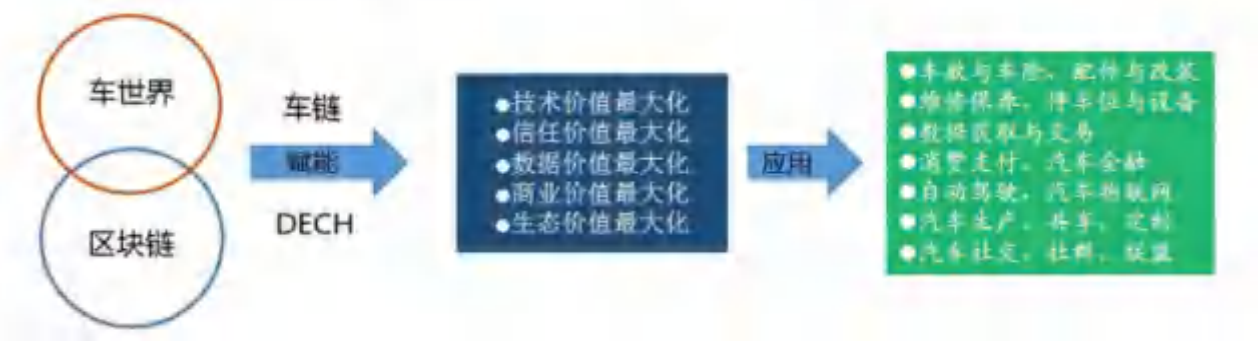
达世车链，简称 DACH ，是新加坡 DAG 基金会研发的区块链全球开源项目。DAG 基金会秉承网络与实体结合，产业与金融一体的理念，突破汽车市场上下游的产业布局，重新定义汽车，打造行业新业态。

DACH 基于区块链的透明、可信、不可逆等特点，所建立的一个去中心化的汽车生态数据服务平台。DACH（Dash Car Chain）通过供应链、数据链、价值链多维度数据的分布式存储与流通，实现配件标准化、整车生产、车辆流通、车主消费、车辆消耗、行驶行为、车辆残值、汽车金融等数据的上链、转换、溯源、数据触发等应用，为汽车产业赋能。

DACH 它基于区块链技术，通过数据上链、溯源查询、智能合约、智能触发、Token 流通、社区建设、Dapp 生态等，连接汽车服务的诸多要素，依托 DACH 的一站式服务平台，构建人、车、交通和生活方式互联互通、开放共享的生态圈。

DACH 以 DACH Token 为介质构建数字金融生态，通过金融资本与产业资本相结

合，可有力的助推汽车产业的“研发、生产、流通、营销、消费、社交、共享、创业”等多环节的数据与价值进行流通，实现汽车产业的智能化、数据化、资产化、商业化。



3.2 DACH 使命

DACH 的使命：汽车让生活更美好

DACH 的远景：区块链时代汽车第一品牌

DACH 的价值观：新技术、新商业、新财富

3.3 项目亮点

行业数据整合，打造汽车行业新业态

利用区块链技术达到汽车产业大数据整合，革新汽车制造企业的生产管理，实现汽车销售行业的精准式营销，利用数据跟踪和挖掘技术改善经营管理，优化产业结构。

利用大数据分析，降低成本

会员用车习惯数据、汽车维修数据、配件调配数据等分析 。

分析数据可了解会员市场需求，为汽车前后端市场解决未来发展方向的重要参考依据，达到去库存去产品，降低成本的作用。为汽车市场发展提供强大市场支持 。

产融一体，汽车行业整合

汽车产业资本结合数字资产金融生态，以金融的商业运作推动实体汽车产业发展，加速汽车产业生态落地。

一站式汽车服务

整合汽车后市场上下游产业链布局，打造汽车市场一站式服务平台。

优化信息结构，保障用户隐私

基于区块链的链上信息加密，保证用户数据的稳定与安全，实现商家与消费者之间的互利共赢。

信息溯源，优化服务

基于区块链技术打造的分布式底层信息网络，所有用户数据产品信息链上存储，信息可追溯，让每一个会员都能享受到专属服务。

3.4 DACH 的优势

DACH 全球第一个提出“区块链+去中心化+全球汽车服务数据共享”的系统服务平台

DACH 它是集互联网、区块链技术、大数据、人工智能等多种技术与金融结合的跨界结晶。DACH 利用区块链的分布式数据库，为传统汽车企业上下游等经济要素进行“赋能”，通过产品和服务数据上链，整合线上线下商业资源，为车主、消费者、商家、汽车生产等实体企业提供强大的数据和交易支撑。

DACH 全球第一个基于区块链技术的提出的“社交+社群+社区”三维度可匿名的汽车社交商业系统

传统汽车制造型企业，以汽车等产品为中心构建营销体系和配置营销资源，客户的忠诚度和粘性不够，整个行业都是中心化的分布，缺乏底层数据协同。

DACH 依托区块链技术赋能行业诸多要素，建立“社交+社群+社区”三维度的社群生态体系节点，通过生态圈 Token 的流通与激励引导，让更多的消费者参与到企业的营销资源配置，实现区域化营销、定制化营销、精准化营销。最终有效推动生态圈中数据的流动、更好的显现价值贡献、更好的体现各环节的财富收益。

同时，在 DACH 分布式匿名网络中，每个人通过全网主节点作为服务器传递这些交易或数据等信息，在这个过程中信息不仅是加密的，这些主节点的 IP 是隐藏的，而且遍布在全球各个角落中。没有人可以知道聊天双方的真实身份。从而捍卫每个人的社交隐私，因为没有隐私就不会存在自由。

DACH chain 链接众多公链

区块链领域最激烈的竞争在于“主链”，每条主链都在竭尽全力成为区块链底层的龙头，进而成为领域内的 ios 系统与微软。在这种氛围中，各条公链之间从底层架构到上层 Dapp 之间壁垒森严，将原有不多的区块链用户进一步分割为 ETH 用户、EOS 用户等等。这必然会带来公链发展的“囚徒困境”。DACH 希望透过 DACHID，将原有分散在各条公链的用户账户进行整合，并将范围进一步向传统平台推广，让更多用户无感进入区块链，解决用户基数的问题。这样，开发者也能够突破公链间的壁垒与区块链圈的限制，获

得更多的用户。

DACH 的核心在于运营，而不是制造

对于 DACH 平台，以追求更好的用户体验为宗旨，在汽车硬件的基础上，对软件平台、操作系统、智能应用、信息娱乐、数据确权与流通等软件进行规范和整合，激活先有商业要素，最终建立起智能汽车的生态。

一站式软件开发平台

DACH 平台最大的特点在于开放、可定制，其目标是基于标准化的 SDK、API 接口，可方便开发者快速的开发各种业务应用。DACH 支持多种语言编写智能合约，使业务开发过程更符合企业级软件开发惯例和范式。另外全球汽车服务企业、制造厂商和中介均可通 DACH chain 构建的 API (应用程序编程接口)和 SDK (软件开发工具包)实现各种线上场景及应用。

“主链+子链”高性能高保密驱动应用

商业应用对性能的要求极高，DACH 致力于解决现有区块链的性能受限问题，采用平行扩展技术，通过主链加多个子链的运行机制，分离主链和子链的业务，每个子链负责各自的业务，主链负责子链之间数据交换和数据安全等服务，以满足千万级 TPS 需求。同时也保障了数据透明与商业保密的平衡。

4. DACH Token 模型

4.1 DACH Token 说明

DACH Token 是 DACH 平台数字通政，发行总量为：3.913 亿枚，属于通缩型经济模型且永久不可增发，Token 被用于达世车链平台的支付，是生态系统中流通的 Token。

DACH Token 代表了平台数据的价值，共识价值。用以实现平台信息的共享与传播，实现平台数字价值的转换，并能更好的激励平台内在价值的提高。Token 不仅代表了数据和价值，更代表了一种权益，这种权益还可以在不同链中进行流转，并支持用户之间、企业之间的流转，让数据生态变得更活跃和生机勃勃。

DACH Token 的合理分配有利于促进 DACH 生态系统健康的发展。具体如下：

DACH 社区及早期理财人 20%

用于 DACH 所有社区成员及早期理财人的贡献奖励。其中 10%用于前期项目研发投入；剩余 10%的锁定期为 48 个月，以确保项目能够持续推进

社区与开发者奖励 25%

用于推动社区生态发展，为了让项目更快的进入市场，奖励社区推动的贡献者，并资助开发者执行有意义的开发计划，对开发任务进行代码审核和任务质量评估

DPOS 40%

应用于 DACH 生态 DAPPS，搭建节点的基础设施，奖励节点贡献者，鼓励更多的企业、机构和用户参与达世车链大数据的生态建设和共识体系的维护。

市场推广及运营 15%

DACH 保障体系，维持项目的持续经营和发展，商业落地，服务于市场运营推广的过程中对市场资源整合、通证置换、商业活动产生的各类费用。

4.2 DACH Token 通缩经济模型

随着达世车链的应用场景不断增加，DACH 将逐渐进入一个通缩型经济时代，DACH 智能合约将履行通证的销毁机制，减少 DACH 在市场的流通量，促进市场价值。

DACH 销毁计划：最终销毁至发行总量的 10%

每季度执行销毁一次，以公告的形式在官方和社区内发布。销毁的 Token 将通过智能合约永久转入一个未知的地址，合约每完成一期的销毁，社区将区块链的 hash 值公开发布，任何人都可以访问这个地址查询销毁数量，销毁时间，确保销毁的公证属性。

5. DACH 应用场景

DACH 基于区块链的透明、可信、不可逆等特点，所建立的一个去中心化的汽车生态数据服务平台。DACH（Dash Car Chain）通过供应链、数据链、价值链多维度数据的分布式存储与流通，实现配件标准化、整车生产、车辆流通、车主消费、车辆消耗、行驶行为、车辆残值、汽车金融等数据的上链、转换、溯源、数据触发、Token 流通、社区建设、Dapp 生态等，连接汽车服务的诸多要素，依托 DACH 的一站式服务平台，构建人、车、交通和生活方式互联互通、开放共享的生态圈。等应用，为汽车产业赋能。

DACH 可广泛应用在汽车全产业链的各个领域：汽车生产 、汽车销售 二手车市场 ，平行进口车 、配件用品、维修保养、救援、汽车租赁、汽车改装、二手汽车、违章查询洗车、停车、广告会展、汽车俱乐部、信息咨询、驾驶培训、汽车租赁、汽车金融、车辆保险等。

5.1 数据上链、确权与交易

众所周知，制造一辆汽车需要上万个零部件，其中大部分零部件由外包供应商提供，供应商数量巨大又分布在全球各地，信息透明度很低，摩擦成本高昂。

汽车行业是一个多方参与的复杂，包括设计、生产、分销、流通、市场营销、销售、和车辆服务、维修保养、二手车买卖、保险理赔、汽车共享、汽车租赁、汽车金融等多环

节全流程以区块的形式记录下来，信息公开透明、不可篡改，可追溯，一旦出现问题，可以对相关信息进行精准追溯确认，使得产品信息高效准确存储与溯源得以实现，提升整条供应链的运转效率。

同时，未来的汽车将实现智能化和无人驾驶，车主或乘客在汽车内有更好的体验，比如：看电影、听歌曲、直播、分享、培训、办公、商业交易、汽车文化 IP 创造与分享等活动。但是因为牵涉到个人隐私，无法确权和维权，很多人不愿意提供更多有价值的内容或者相关数据/经验。

在 DACH，区块链利用“去中心化”、“数据不可篡改”、“永久记录”为特征，把 IP 内容提供者或者数据提供者通过储存散列（Hash）的方式，将所有相关信息完整地保存。区块链下的 DACH 版权上链， 其目的是通过区块链技术为更多的汽车 IP 创作人创造公平透明的行业环境，让更多的人愿意创造和分享自己的创意、数据等。将文字、视频、音乐、图片版权保护、个人相关数据等；同时汽车服务企业可以把对应服务上传至 DACH 主链，车主和第三方在注册后之后都可以查询相关数据，降低时间和不可信成本。

DACH 平台中 Token 经济模型机制是建立未知双方的信用基础，从而促成双方的交易。智能合约则起到了第三方监督的作用。在 DACH 提倡的是所有用户的行为都是有价值，不管是数据 IP 内容的生产、还是内容的转发与分享等，都是有价值，因此，所有的行为都将被标注成数字资产，可获得平台给以的 Token 奖励。DACH 将所有人纳入价值网络，赋予普通人众多的机会入口， 为数据生产者赋能。通过区块链实现由中心化向去中心化的转变，从而解决人与人在生活、经济等交往中的信任问题。

5.2 实现汽车配件质量追溯

区块链可以帮助汽车制造商、汽车服务商和车主追溯汽车生命周期的全过程，快速找到谁对汽车做出了什么，可以跟踪到汽车生产过程中整个供应链的产品和零部件的出处，可以将整个车辆分解成所有进入其中的组件，并识别每个组件的来源。如果汽车零件出现问题，区块链技术可以确定谁制造了这个有缺陷的零件。通过这种模式，一方面可以大大降低汽车制造商的召回成本；另一方面让汽车后市场服务商可以实时掌握汽车健康状况，通过累积的历史数据对汽车状况进行分析，提前预防汽车可能出现的故障，增强汽车行驶的安全性。

5.3 实现二手车信息对称

通过区块链技术可以建立全行业的汽车维保联盟，不管车辆在什么地方进行维保服务，都会将产生的信息记录到车辆健康“病历”中。那些外表漂亮，内饰清洁，看似保养记录良好的车辆，未必是好车辆，使二手车交流不再光看表面。二手车公司和“接盘者”可以通过区块链上汽车维保数据，真正了解车辆的实际状况，使交易双方信息对称。在汽车的全生命周期，特别是一些特殊事件，通过区块链技术不可篡改的记录下来，通过公开的方式让交易者在所有节点能够公平使用、公平交易。

5.4 实现生态互利互信

目前，在汽车维保服务方面，车主方、汽车维保方、汽配提供方三者心态完全是个悖论。对于车主，他们需要高品质，低成本，而汽车维保方却是需要车主有粘性，快速建立服务口碑，作为汽配提供方则是追求高利润和高销售量，这些使得他们互相之间忠诚度和互信度都非常低，流量不稳定，数据不精准，经营也就比较累。在区块链技术背景下，建

立基于信任和互利的闭环汽配、汽修及相关服务的生态系统，打造彼此互信认同的价值共享平台，能够更加广泛的促进汽车维保行业的健康发展，实现三者之间良性可持续的互惠互利，使整个汽配行业杜绝假货，利润合理，彼此互信，可促进行业共同发展。

5.5 实现车辆保险精准定价

汽车保险业是汽车后市场服务中最稳定的“蛋糕”。对于车主而言，他们抱怨的是：我一年中从来没有发生事故，凭什么还要交那么多保费，我们需要优惠政策。而对于保险公司，由于国内交通环境和汽车产品的复杂性，加上车主对保险漏洞的深刻领会，让很多保险公司有苦难言。随着信息技术手段升级，如果通过区块链技术建成汽车全生命周期管理，不但可以实现对汽车零部件追溯，最重要的是可以记录汽车理赔发生的场景数据。这样使保险公司即可以非常有效的降低保险运营成本、理赔成本，又可以根据车主的驾驶水平、习惯等分析出险的可能性，做到车辆保险 “一车一策” 精准定价，提升车主对保险公司的认可度。图 5 为汽车后市场区块链数据模型。

5.6 实现有效停车服务

停车难几乎困扰着每一位车主和城市管理，成为最为突出的城市病之一。据调查统计，中国停车位总缺口超过 5,000 万个，北京缺口 250 万个，深圳缺口 200 万个，上海和广州缺口均在 150 万个以上，停车难已经成为城市发展的瓶颈。DACH 可以把车主、消费者、车库经营者、车库及其硬件等服务要素整合起来，通过 APP 和数据上链与智能合约，让数据、价值、合约自动运作。

车库管理者通过 DACH APP 把停车位数据及时上传，消费者通过 APP 获得对应信息 ，通过消耗 Token 购买对应车位使用权，并获得对应 Token 奖励，交易双方所有交易

信息都将上链，智能合约自动执行。

DACH 将实现立体机械车库解决停车位空间限制，通过爱码停车移动端 APP 实现大众车主共享停车的需求，以及汽车后汽车市场服务。提供创新的技术整合方法，开放性，便利性和易用性，使停车行业及其利益相关者能够将发达城市生活质量提高到一个全新的水平。

基于车链 DACH 的开放平台，联盟商家可以将自己的线上商城，线下实体店，渠道批发，跨境贸易，成品销售等业务接入车链，实现业务互通，数据共享，商机互助，全球车位通证 DACH 助力各商业机构实现资源互助，流量共享。

5.7 实现网约车隐私安全

网约车安全问题的根源首先是人为作恶，其次是平台审核存在漏洞，车主注册门槛太低，第三是隐私保护问题，第四是缺乏警方联动机制和应急能力。DACH 为这些问题的解决提供可能。

在 DACH，可以把其他平台的信用体系链接到打车平台，比如，可以把芝麻信用作为车主注册的一个参考，对于信用差的车主，平台可以拒绝注册。滴滴车主伪造了假车牌，根本查不到。在 DACH 运用区块链技术，用户在审核过程中，车牌是可以追溯源头的，也就是说车牌也无法造假，如果是假的就无法通过审核，也就没办法进行交易。而且，基于区块链分布式存储、不可篡改的特性，可以把车主和乘客双方打车信息记录在区块链上，形成平台自己的信用体系，对于信用评分低的司机或乘客，可以取消其使用平台的权利。更重要的是，根据这些信用信息，乘客可以优先选择信用评分高的车主，而对于评分低的乘客，车主也同样可以选择拒绝。

在 DACH，乘客和司机的订单一旦约定成功就立马被打包成一个信息区块，这个区块

里包含着乘客的身份信息、司机的身份信息、车牌号、行程信息、大约所用时间等，并设置查看密码。这个带有密码的信息区块会作为一个独立的项目上传到区块链上，全网都能见这比交易的诞生。每一个乘客乘车的信息在确认上车后，信息会被自动传到区块节点当中，信息都被记录，其真实性和不可篡改性都有所保障。那么如果有危害发生，亲友们可以在平台上第一时间确认信息，从而将会省去一些不必要的中间环节。

DACH 的加密特性可以把车主和乘客双方的信息进行加密处理，保护乘客的个人信息；为了解决隐私保护问题，我们可以运用最新的零知识证明或类似的匿名技术，这样的情况下，没有查看私钥的外人，就无法获取到乘客及司机的信息。比如，乘客结算后，对车主不满意，给了低分评价，车主无法得知是谁给出的评价，也无法得知乘客的电话信息，也就降低了车主骚扰、报复乘客的可能性。

在 DACH 交易过程中，可以公开司机的行车路线和时间，利用开放式节点的设计，让车主、消乘客、网约车机构、警方都对信息有一个准确详实的掌握。

在 DACH 信息区块及密码同步给公安机关系统，并根据订单信息实时监控车辆行驶动态，确保用户安全到达目的地后关闭交易信息；如果行车明显偏离了出行轨迹，紧急情况下平台可以通知警方。可以在用户到达地点后，平台马上为车主派发下一单，环环相扣，以防心怀不轨者尾随乘客。

5.8 DACH 生态应用延伸

6. 技术原理

6.1 DACH 主要的技术解决方案

DACH 公链是由 DAG 基金会社区完全自研的一条高性能公链，兼容 EVM 和 WASM 格式的智能合约，具有双层架构，稳定的根链及可定制的子链系统。

DACH 采用的是 DAG + DPOS 的共识方案。DACH 采用 DAG+DPOS 技术，区块生成时间不到 3 秒，TPS 最高可达百万级。DAG(Directed Acyclic Graph) 有向无环图在设计上有别于默克尔树结构区块链（传统的 block chain）。通过“DAG+DPOS”能很好的解决区块吞吐量低、交易确认时间缓慢、节点挖矿等问题。

DACH 提出的智能管道技术（Smart Pipeline）可以在区块链虚拟机和外部应用之间传输数据，提升批量数据处理能力，高效率、强拓展、零 Gas，解决智能合约（Smart Contract）无法解决的现实需求。

为实现数据串联和隐私保护，DACH 会设计去中心化 ID 系统，形成一个主 ID 加多个子 ID 的分层体系。允许用户通过 DACH 客户端，对中心化及去中心化平台上的数据和资

产，进行一站式管理。

为提供 DACHID 的长期持有价值，DACH 推出了声誉系统，包括通用声誉协议、声誉管道接口、声誉数据上链与算法库、声誉激励机制、声誉账户管理与虚假检测等。

为降低技术使用门槛和教育成本，DACH 研发了 API、Plug-in（插件）及针对垂直行业的 SDK，可支持 Dapp 社区一键发布多公链资产支持版本，内置孵化器及资产交易平台，基于共享 DACHID 获取多公链用户，无感转化各类数字资产持有者成为其平台用户。

6.2 技术原理

6.2.1 DAG 算法

DAG(有向无环图)是不同于主流区块链的一种分布式账本技术，把同步记账提升为异步记账，被不少人认为可以解决传统区块链的高并发问题，是区块链从容量到速度的一次革新。

6.2.2 什么是 DAG？

DAG：Directed Acyclic Graph，中文意为「有向无环图」。

DAG 原本是计算机领域一种常用数据结构，因为独特的拓扑结构所带来的优异特性，经常被用于处理动态规划、导航中寻求最短路径、数据压缩等多种算法场景。

6.2.3 传统区块链和 DAG 的区别

1）单元：区块链组成单元是 Block，DAG 组成单元是 TX（交易）；

2）拓扑：区块链是由 Block 区块组成的单链，只能按出块时间同步依次写入，好像单核单线程 CPU；DAG 是由交易单元组成的网络，可以异步并发写入交易，好像多核多线程 CPU；

3）粒度：区块链每个区块单元记录多个用户的多笔交易，DAG 每个单元记录单个用户交易。

6.2.4 传统区块链技术存在的几个问题

1）效率问题：传统区块链技术基于 Block 区块，比特币的效率一直比较低，由于 BlockChain 链式的存储结构，整个网络同时只能有一条单链，基于 POW 共识机制出块无法并发执行；例如比特币每十分钟出一个块，6 个出块才能确认，大约需要一个小时；以太坊大幅改善，出块速度也要十几秒。

2）确定性问题：比特币和以太坊存在 51%算力攻击问题，基于 POW 共识的最大问题隐患，就是没有一个确定的不可更改的最终状态；如果某群体控制 51%算力，并发起攻击，比特币体系一定会崩溃；考虑到现实世界中的矿工集团，以及正在快速发展量子计算机的逆天算力，这种危险现实存在。

3）中心化问题：基于区块的 POW 共识中，矿工一方面可以形成集中化的矿场集团，另一方面，获得打包交易权的矿工拥有巨大权力，可以选择哪些交易进入区块，哪些交易不被处理，甚至可以只打包符合自己利益的交易，这样的风险目前已经是事实存在。

4）能耗问题：由于传统区块链基于 POW 算力工作量证明，达成共识机制，比特币的挖矿能耗已经与阿根廷一个国家耗电量持平，IMF 和多国政府对虚拟 Token 挖矿能源消耗持批评态度。

DAG 技术被用于尝试解决区块链的上述问题。

6.2.5 DAG 起源

最早在区块链中引入 DAG 概念作为共识算法是在 2013 年，bitcointalik.org 由 ID 为 avivz78 的以色列希伯来大学学者提出，也就是 GHOST 协议，作为比特币的交易处理能力扩容解决方案；Vitalik 在以太坊紫皮书描述的 POS 共识协议 Casper，也是基于 GHOST POW 协议的 POS 变种。后来 NXT 社区有人提出用 DAG 的拓扑结构来存储区块，解决区块链的效率问题。区块链只有一条单链，打包出块无法并发执行。如果改变区块的链式存储结构，变成 DAG 的网状拓扑可以并发写入。在区块打包时间不变的情况下，网络中可以并行打包 N 个区块，网络中的交易就可以容纳 N 倍。

此时 DAG 跟区块链的结合依旧停留在类似侧链的解决思路，交易打包可以并行在不同的分支链条进行，达到提升性能的目的。此时 DAG 还是有区块的概念。

2015 年 9 月，Sergio Demian 发表了 《DagCoin: a cryptocurrency without blocks》一文，提出了 DAG-Chain 的概念，首次把 DAG 网络从区块打包这样粗粒度提升到了基于交易层面。DagCoin 的思路，让每一笔交易都直接参与维护全网的交易顺序。交易发起后，直接广播全网，跳过打包区块阶段，达到所谓的 Blockless。这样省去了打包交易出块的时间。

一句话来概括：DAG 是面向未来的新一代区块链，从图论拓扑模型宏观看，从单链进化到树状和网状、从区块粒度细化到交易粒度、从单点跃迁到并发写入，这是区块链从容量到速度的一次革新。

6.2.6 DAG+DPOS 共识算法

共识机制是指分布式系统中的一致性问题， 其核心是在某个协议（共识算法）保障下，在有限的时间内，使得指定操作在分布式网络中是一致的、被承认的、不可篡改的。在区块链系统中，特定的共识算法用于解决去中心化多方互信的问题。为适应不同的应用场景，区块链共识机制集中于优化系统的可扩展性、运行效率和容错等方面。

DACH 采用 DAG+DPOS 共识算法，它分为两部分。一部分是 DAG 算法，确保各个节点之间的数据绝对一致，用于解决可信节点间网络通信问题的算法等。另一部分是 DPOS 算法，则是通过经济利益和算力，鼓励对系统的贡献及提高不可信节点成本的算法，这类算法通过提供算力或持有权益来平衡利益。

6.2.7 分层架构

任何一个曾经开发过 Dapp 的程序员都必须考虑到当前公共区块链的局限性，其中区块链局限性的最重要和最明显的问题就是有限的吞吐量，比如，每秒处理的交易量过少。为了运行一个能够处理实际吞吐量需求的 Dapp，区块链就必须具有可扩展性，进行区块链扩容的一个答案就是分层技术。

1) 传统区块链基本框架

区块链基本框架从下至上包括数据层、网络层、共识层、激励层、合约层和应用层共六层；基础数据传输到数据层，在区块主体中组成数据列表，用区块主体中的 Merkle 树记录，区块主体与存储 Merkle 根、父哈希、时间戳等数据的区块头共同形成区块，多个区块通过区块头的数据形成链式结构；网络中的节点收到上传数据后，通过 P2P 网络向全网广播，各节点自动对其验证。

要系统的考虑区块链技术可扩展方案，首先必须理解区块链技术框架，如图所示：

当前主流的区块链架构包含六个层级：网络层、数据层、共识层、激励层、合约层和应用层。图中将数据层和网络层的位置进行了对调，主要用途将在下一节中详述。

●网络层：区块链网络本质是一个 P2P（Peer-to-peer 点对点）的网络，网络中的资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行，可以无需中间环节和服务器的介入。每一个节点既接收信息，也产生信息，节点之间通过维护一个共同的区块链来同步信息，当一个节点创造出新的区块后便以广播的形式通知其他节点，其他节点收到信息后对该区块进行验证，并在该区块的基础上去创建新的区块，从而达到全网共同维护一个底层账本的作用。所以网络层会涉及到 P2P 网络，传播机制，验证机制等的设计，显而易见，这些设计都能影响到区块信息的确认速度，网络层可以作为区块链技术可扩展方案中的一个研究方向；

●数据层：区块链的底层数据是一个区块+链表的数据结构，它包括数据区块、链式结构、时间戳、哈希函数、Merkle 树、非对称加密等设计。其中数据区块、链式结构都可作为区块链技术可扩展方案对数据层研究时的改进方向。

●共识层：它是让高度分散的节点对区块数据的有效性达到快速共识的基础，主要的共识机制有 POW（Proof Of Work 工作量证明机制），POS（Proof of Stake 权益证明机制），DPOS（Delegated Proof of Stake 委托权益证明机制）等。

●激励层：它是大家常说的挖矿机制，用来设计一定的经济激励模型，鼓励节点来参与区块链的安全验证工作，包括发行机制，分配机制的设计等。这个层级的改进貌似与区块链可扩展并无直接联系。

●合约层：主要是指各种脚本代码、算法机制以及智能合约等。第一代区块链严格讲这一层是缺失的，所以它们只能进行交易，而无法用于其他的领域或是进行其他的逻辑处理，合约层的出现，使得在其他领域使用区块链成为了现实，以太坊中这部分包括了EVM(以太坊虚拟机)和智能合约两部分。这个层级的改进貌似给区块链可扩展提供了潜在的新方向，但结构上来看貌似并无直接联系。

●应用层：它是区块链的展示层，包括各种应用场景和案例。如以太坊使用的是 truffle 和 web3-js.区块链的应用层可以是移动端，web 端，或是是融合进现有的服务器，把当前的业务服务器当成应用层。这个层级的改进貌似也给区块链可扩展提供了潜在的新方向，但结构上来看貌似并无直接联系。

2) DACH 分层架构

Layer 1 层改进是指通过对某条公链本身的改进来提升它的可扩展性，即 On-Chain 链上改进；Layer 2 层改进是指不影响该公链本身，通过其他方式来实现可扩展性的提升，即 Off-Chain 链下改进（此处链下的含义仅仅指脱离该公链）。

在这个理解的基础上，我们借鉴计算机网络分层管理、各层标准化设计的思想，建立区块链技术可扩展方案分层模型：Layer 1 层 On-Chain 公链自身（底层账本）层和 Layer2 层 Off-Chain 扩展性（应用扩展）层。具体如图的划分：

Layer 1 层 On-Chain 公链自身改进

Layer1 层 On-Chain 公链自身改进的主要思路的出发点是将区块链技术底层账本和上层应用分离，底层账本的重心放在安全性和去中心化上，在性能上有所取舍。只是将需要共识确权的数据上链，从而降低对 TPS 的需求，从目前技术发展来看，可能千位级别（1000~3000）TPS 即可满足。结合前文介绍的区块链的架构可以看出，能够提升的地方有共识层的机制改进和数据层的数据区块大小调整、链式结构的优化以及网络层的验证机制改进等方法。

所以，Layer 1 层改进的思路是做好一条底层账本公链，将其他的事情交由 Layer 2 层来互补处理。这里对于隐私加密技术的需求对 Layer 1 层会是一个不错的附加属性，但不属于可扩展方案讨论范畴，在没有很好的处理方案前，在 Layer 2 层考虑也是个能接受的

选择。

Layer 2 层 Off-Chain 扩展性改进

Layer2 层 Off-Chain 扩展性改进是基于区块链的底层账本技术之上的应用型扩展，可以是基于区块链技术的应用，也可以是中心化的应用结合，它的重心放在性能和安全上，对去中心化有所取舍。最终关键数据传输给 Layer1 层上链，本身利用高性能处理大量数据，达到现实世界对性能的需求。该类型的改进有跨链是基于区块链技术的多链生态扩展；状态通道是链下数据处理来提升性能；Plasma 通过一系列的智能合约，来构建多种应用场景达到多链并行的结果；Truebit 一种帮助以太坊在链下进行繁重或者复杂运算的技术等。所以，Layer 2 层作为 Layer 1 层的互补来解决与现实世界的需求，并将必要的数据上链到 Layer 1 层。

6.3 DACH 智能神经管道

智能合约（Smart Contract）在 Ethereum 等平台得到广泛应用的同时，其数据容量、Gas 消耗、缺乏主动调用功能等诸多问题为开发者所诟病，限制了大型 Dapp 的开发。

智能神经管道是 DACH 社区提出的一种崭新的区块链应用模式，在不影响安全性的基础上，具有高效、拓展性强的诸多优势，解决智能合约无法解决的现实需求。

DACH 智能神经管道是数据传输的“管道”，在区块链虚拟机和外部应用之间传输数据：区块链客户端将实时数据通过智能神经管道传输给外部应用，外部应用执行后将结果通过智能神经管道实时返回给区块链客户端。这些智能神经管道能够被插入于区块链执行区块的各过程中，并且可以根据需要选择插入的位置执行相应代码，提升执行效率。智能神经管道的优势：

更“智能”

智能神经管道部署上链后，可以根据条件自动触发执行，相比智能合约条件范围更加广泛，执行更难受到干扰，非常利于复杂事务的执行。

零 Gas 消耗

智能神经管道的应用在执行时，相比智能合约的一大优势是无需消耗 Gas。零 gas 消耗并非零责任，所有智能神经管道运行代码需要开源接受监督。同时智能神经管道消耗计算资源主体并不在相应子链上，而是由智能神经管道代码提交方提供计算资源，即便出现漏洞，也不会影响相应子链的性能。

编程语言无局限性

智能神经管道采用 WASM 虚拟机进行交易的执行，用户可以使用多种编程语言进行代码编写，之后转成 WASM 指令。随着 WASM 的不断改进，其支持的语言种类将逐步增加，代码效率也会得到相应提升，不会影响区块链的执行。

满足复杂应用的需求

智能神经管道的应用没有受到 Gas 等限制，可以支持区块链实现更复杂的逻辑。在精心设计后，带有智能神经管道的区块链可以和其他应用或者服务进行交互，满足大型复杂应用的需求，制作已有区块链无法支持的应用。

6.4 零知识证明

零知识证明(Zero—Knowledge Proof)，是由 S.Goldwasser、S.Micali 及 C.Rackoff 在 20 世纪 80 年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协

议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。

DACH 在零知识证明上采用 zk-SNARK 技术。zk-SNARK 的全称是 zero-knowledge Succinct Non-Interactive Arguments of Knowledge （零知识，简洁，非交互的知识论证）。它是一种非常适合区块链的零知识验证技术，可以让别人在不知道具体交易内容的情况下验证交易（或者是智能合约函数调用）的有效性。有了 zk-SNARK，我们既保留了区块链互相不信任个体间的共识达成问题，又保护了交易隐私，简直就是在众目睽睽下原地隐身。zk-SNARK 在实现零知识验证的同时还具有以下几个特点：

Succinct （简洁性）：验证者(verifier)只需要少量计算就可以完成验证。这对于区块链非常重要，因为区块链上为了能够快速达到共识，每一个计算步骤不能过于复杂。

Non-interactive (非交互性)：示证者(prover)和验证者(verifier)之间只需要交换极少量的信息即可完成整个验证过程。这对于区块链同样至关重要，因为区块链上节点众多，并且每个节点都需要每一笔对交易进行验证，所以验证过程必须只涉及极少量的信息交换，否则通信成本会非常巨大。

6.5 抗量子攻击

传统的区块链，如比特币和以太坊，使用了经典的公钥密码哈希生成的地址来减轻破解威胁。这个安全性的附加层，意味着公钥只有在其参与第一笔交易发生后，哈希接收方密钥地址就被暴露。

6.5.1 以下区块链场景易受量子攻击：

●地址重用 ：当一笔交易被签名时，公钥就会被揭露。

●被遗弃的 Token/资产：如果它们的相关地址不是通过哈希生成的，这些旧地址的公钥就会被暴露。

●正在进行当中的交易：一旦一笔交易广播到网络上，并且它还没有被区块链所接受，那么这些交易就很容易受攻击。

●交易被拒/失败：如果签名的一笔交易没有通过，例如，由于给出的交易费过低，或者有恶意方阻止交易中继，那么密钥将会受到攻击；

●多重签名交易/混合交易：如使用 CoinJoin 协议 ，这会在交易完成之前向其他方揭示公钥；

●单个地址的公告：公告和使用相同的地址，例如筹集资金，将会暴露第一次消费交易的公钥，使后续资金收益置于风险之中。

6.5.2 BPQS 协议

BPQS 较传统非量子签名方案（例如 RSA、ECDSA 以及 EdDSA）会更具一些优势，它可以提供更可靠的量子安全性，这是因为它的加密哈希函数会更安全。

●更短的签名、更快的密钥生成，当签名只进行一次或少数次数时，其签名和验证时间会比 XMSS 和 SPHINCS 系列后量子（PQ）协议也会更短，可以实现更好的匿名性；

●它在计算上与非量子方案相当。人们可以利用易于应用的多哈希链 WOTS 并行化和缓存，以提供几乎即时的签名和更快的验证；

●其可扩展性属性，允许多次签名，它也可以很容易地进行定制，如果需要的话，它也可以回滚到另一种多次签名方案；

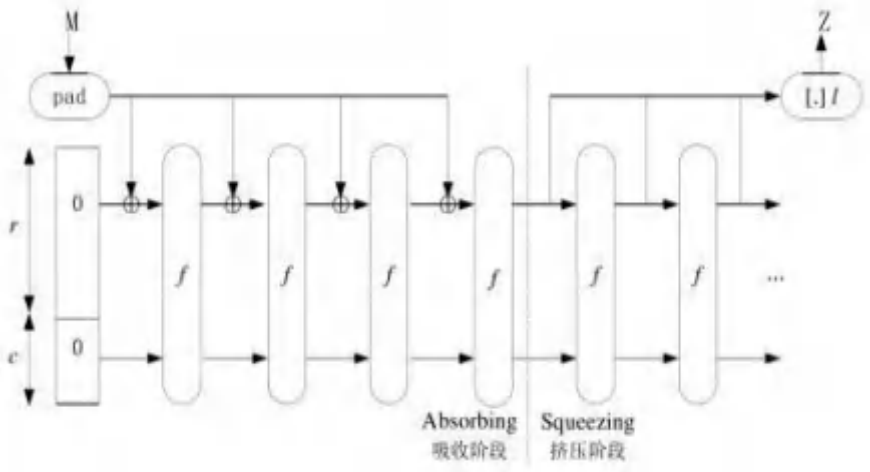
●在区块链和分布式账本应用时，它可以通过引用先前的交易（其中相同的密钥会被重用），从而利用底层链或图结构的优势。这可能意味着，每个新的 BPQS 签名，只需要一次 OTS 方案的努力，因为其余到根的签名路径已经在账本当中了，因此可省略它们；

●它可被用作一个构建块，用于实施新颖的 PQ 方案，例如同时的“有状态和无状态”方案，其可能会使集群环境受益，当共识消失时，其中的节点可回滚到无状态方案；另外，这样的方案可以用于向前和向后兼容的目的，或者当要求在两个独立和不兼容的区块链中重用一个密钥时。

6.5.3 抗量子攻击算法

在当前以比特币为代表的区块链系统中，SHA-256 哈希计算和 ECDSA 椭圆曲线密码构成 了比特币系统最基础的安全保障，但随着量子计算机技术不断取得突破，在量子计算机下针对 ECDSA 签名算法非常高效的 SHOR 攻击算法。

可将任意长度的输入比特映射成固定长度的输出比特，该算法速度非常快速，在英特尔酷睿 2 处理器下的平均速度为 12.5 周期每字节。



如上图所示，在海绵结构的吸收阶段，每个消息分组与状态内部的 r 比特进行异或，然后与后面固定的 c 比特一起封装成 1600 比特的数据进行轮函数 f 处理，然后再进入挤压过程。在挤压阶段， 可以通过迭代 24 次循环产生 n 比特固定输出长度的 Hash 值，每个循环 R 只有最后一步轮常数不同，但是该轮常数在碰撞攻击时经常被忽略不计。

6.5.4 抗量子攻击的数据签名算法

哈希算法可以保证交易数据不被篡改，但是无法保证对数据和摘要同时的替换攻击，同时也不能保证交易数据的不可否认性，数字签名算法涉及到公钥、私钥和孵化器等工具，它有两个作用：一是证明消息确实是由信息发送方签名并发出来的，保证不可否认性，二是确定消息的完整性。数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用哈希算法对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性并保证信息的不可否认性。

现有区块链系统大都采用椭圆曲线数字签名方案 ECDSA，但是量子计算机下针对 ECDSA 签名算法非常高效的 SHOR 攻击算法，Shor 算法适用于解决大整数分解、离散对数求逆等困难数学问题，导致 ECDSA 签名算法在量子攻击下相当不安全。

目前抗量子 Shor 算法攻击的公钥密码体制主要包括基于格理论的公钥密码、以 McEliece 公钥密码为代表的基于编码公钥（Shor 算法适用于解决大整数分解、离散对数求逆等困难数学问题），导致 ECDSA 签名算法在量子攻击下相当不安全。在下图中目前主流加密算法在量子计算机面前的的安全程度，所以需要需找一个抗量子的加密方法，以此来替换 DACH 链的基于 ECDSA 算法的加密方法。

密码学中的哈希算法又称为散列函数或杂凑函数，它在现代密码学中扮演着重要的角色。哈希算法是一个公开的函数 H，它将任意长的消息 M 映射为较短的、固定长度的值 h。h 称为消息摘要，也称为哈希值、散列值或杂凑值。哈希算法的结构如下图所示：

量子计算机下针对哈希算法目前最有效的攻击方法是 GROVER 算法，该算法可以将对 Hash 算法的攻击复杂度从 0(2 n)降低为 0（ 2 n / 2 ）,因此，目前比特币系统采用的哈希算法 PIREMD160 算法由于输出长度只有 160 比特，在量子攻击下是不安全的。抵抗量子攻击的有效手段是通过增加哈希算法的输出长度来有效降低 GROVER 算法威胁，目前普遍认为只要哈希算法输出长度不少于 256 比特时，是可以有效抵抗量子攻击的。另外，除了量子攻击威胁外，一系列在实践中被 广泛应用的 Hash 函数如 MD4、MD5、SHA-1 和 HAVAL 等受到差分分析、模差分和消息修改方法等传统方法的攻击，因此区块链中的哈希算法也需要考虑的是对传统攻击的抵抗能力。DACH 采用 SHA-3 算法 Keccak512，该算法蕴涵许多杂凑函数和密码算法最新的设立理念和思想，且设计方式简单，非常方便硬件实现。McEliece 公钥密码体制的安全性基于纠错码问题，安全性强，但计算效率低。 MQ 公钥密码体制，即多变元二次多项式公钥密码体制，基于有限域上的多变元二次多项式方程组的难解性，在安全性方面的缺点比较明显。相比之下，基于格理论的公钥加密体制算法简洁、计算速度快、占用存贮空间小 。

6.6 多链与侧链

如上所述，DACH 作为公有链实现企业数据价值传递，在实际应用中会存在多个这样的链共同运行于网络中，联盟链和私有链则作为独立的链，整体架构会复杂起来。在

DACH 的多链系统中，采用侧链技术来实现多链，主链为 DACH 公有链，其他为侧链。

采用主侧链技术的思想在于，主链只提供上层架构可信交易服务和数据安全以及可扩展性，侧链则负责具体的数据交易逻辑实现，包括普通交易和合约交易的执行等操作。优点在于解决了单链结构下随着节点数量增加整个网络结构越来越大、越来越长，由网络延迟导致的交易时间滞后以及其他风险增大的情况。

在主侧链技术中，交易转账是最核心的部分，从主链向侧链转账，意味着要把主链资产转变为侧链资产，转账目标地址是对应侧链在主链上的联合签名地址，转账过程需要保证转账交易能够自动被侧链识别并为转账人在侧链对应账号充值对应价值的侧链 Token。通过随机秘密以及对应的哈希，我们可以构造必须提供秘密才能解锁的交易脚本。

下面是转账过程的示意步骤：

1)转账用户 A 生成一个随机秘密，以及对应的哈希；

2)用户 A 在主链上构造给侧链在主链上的联合签名地址转账的交易，交易的解锁条件除了需要提供联合签名地址的私钥签名，还要提供用户生成的秘密；

3)用户 A 将上面的交易以及秘密对应的哈希发送给侧链转账处理节点；

4)侧链转账处理节点在侧链上生成给用户 A 在侧链上的发 Token 交易，这个发 Token 交易的锁定脚本要求用户 A 提供秘密哈希对应的秘密本体以及用户 A 在侧链上的私钥签名；

5)用户 A 提供秘密，从侧链上获得 Token；

6)侧链在主链上对应的联合签名地址根据上面提供的秘密，从主链获得 Token。

从侧链向主链转账的过程逻辑和上面的相似，不再阐述。而对于多链来说时间确认是一个难题，在 DACH 链中，主链时间戳可以辅助确认侧链向主链交易的时间值，而主链向侧链交易则由侧链时间戳进行辅助确认，主链时间戳和侧链时间戳不同于区块头中的时间戳，该值会允许在一个时间缓冲期内完成交易的数据被认为有效，当然这其中也包含其他机制来保证主链和侧链数据的最终一致性。

6.7 多重签名

在企业应用中，一个文件需要多个部门共同的签署才能生效。所以同一个文件由多个部门使用自己的私钥对其签名，如果想获取此文件内容则必须由多个部门同意才行（也就是使用多个部门的私钥对其进行验证），从而保证了文件的管理的规范性和安全性。这种机制类似于一个保险柜由 5 把钥匙才能打开，而 5 把钥匙分别在 5 个人手中，所以申请人需要同时持有 5 个人的钥匙才能打开保险柜。

E 能链使用采用单向散列函数实现多种签名，以下是 Alice、Bob 和 Carol 的多重签名的过程。

(1)Alice 对文件的散列签名。

(2)Bob 对文件的散列签名。

(3)Bob 将他的签名交给 Alice。

(4)Alice 把文件、她的签名和 Bob 的签名发给 Carol。

(5)Carol 验证 Alice 和 Bob 的签名。

Alice 和 Bob 能同时或顺序地完成第(1)步和第(2)步；在第(5)步中 Carol 可以只验证其中一人的签名而不用验证另一人的签名。

关于 MultiSig（多重签名），从原理角度上讲，多重签名本身并不复杂，简单来说，

一句话就够了：“用 m 把钥匙生成一个多重签名的地址，需要其中的 n 把钥匙才能花费这个地址上的代 Token，m >= n，这就是 n/m 的多重签名”。

在实际的操作过程中，一个多重签名地址可以关联 n 个私钥，在需要转账等操作时，只要其中的 m 个私钥签名就可以把资金转移了，其中 m 要小于等于 n，也就是说 m/n 小于 1，可以是 2/3, 3/5 等等，是要在建立这个多重签名地址的时候确定好的。

6.8 DACH 跨链协议

DACH 的跨链协议突破了传统跨链只能进行资产转移的思维定式，将声誉（征信/忠诚度）等重要个人身份相关的行为数据也进行跨链同步与迁移，通过同态加密进行安全保护与使用。根据不同需求，DACH 采用同构与异构两套跨链方案，以应对不同架构下性能和成本的平衡：

同构跨链：DACH 主链与子链之间通过轻量化同构跨链协议相互连接，用户可以通过孵化器即时看到不同跨链平台之间的状态变化。

异构跨链：分布式私钥控制技术将 DACH 体系之外的链甚至传统平台跨链连接到 DACH 生态中，达成安全的异构跨链，将声誉协议的应用范围拓展到多种平台。

6.9 跨链交易

在跨链中，每个链都是独立存在链，拥有完全的独立的网络和 Token。目前主要的跨链技术包 括三种：公证人机制、侧链/中继、哈希锁定。

公证人机制是指由一 组可信的节点作为公证人向链 X 的节点验证链 Y 上的特定事件是否 发生。典型的公证人机制包括瑞波实验室提出的 Interledger。如果链 X 能够验证来自链 Y 的数据，则称链 X 为侧链。

侧链通常以锚定某种 原链上的代 Token 为基础，其它区块链则可以独立存在。目前侧链很难做 到在其上建立跨链智能合约，所以很难实现各种金融功能，这正是现 有区块链在股票、债券、衍生品等领域尚未取得进展的原因。

哈希锁定是 一种通过时间锁定让接收方在某个约定的时刻前生成支付的密码学 哈希值证明来完成交易的机制，最早起源于闪电网络。然而哈希锁支 持的功能比较少，能够支持跨链资产交换，大部分场景能够支持资产 抵押，但不支持跨链资产转移和合约。以上三种技术的比较如下表：

跨链技术	公证人技术	中继/侧链技术	哈希锁定技术
互操作性	所有	所有（需要所有链上都 有中继，否则只能支持 单向）	只有交叉依赖
信任模型	多数公证人诚实	链不会失败或受到 51% 攻击	链不会失败或受到 51%攻击
适用跨链交换	支持	支持	支持
适用跨链资产转移	支持（需要共同的长期公证人支持）	支持	不支持
适用跨链预言机	支持	支持	不直接支持
适用跨链资产抵押	支持（需要共同的长期公证人支持）	支持	支持，但有难度

6.10 DACH 隐私保护设计

DACH 引入了基于多重签名的 PBFT 机制。传统 PBFT 协议需要参与者将信息的签名传给 Leader，然后 Leader 将这些签名放进区块头。但存储多个签名将增加区块头的大小，影响网络传输效率。DACH 使用了基于 Secp256k1 椭圆曲线的 Schnorr 多签名算法，明显提升了区块链效率。不同于其他签名形式，Schnorr 多重签名最终只产生一个签名，大大减小了签名的长度，从而减小了区块头大小，减轻了存储开销和网络传输开销。

另外，当未来需要增强隐私性交易需求时，除了环签名之外，Schnorr 签名亦可提高隐私性。

同态加密与隐私保护 DACH 链的运行过程中，必然会遇到将信息传递给第三方的情况——如内部的智能管道和外部的数据共享。在这些过程中，有可能会出现用户隐私在环节内被泄露等情况，不利于用户的 ID 安全。为此，DACH 采用同态加密的方式，在用户认定为隐私的信息进行数据处理中，保护数据本身的隐私安全。

6.11 数据链上存储

去中心化存储，即将数据分块存储于区块链网络节点中。相较于传统的集中式的云存储服务，去中心化存储无需依赖于对于存储服务提供商的信任，从而避免集中式于存储方案中的安全威胁，如中间人攻击、恶意软件、以及服务漏洞所导致的信息泄漏问题。因此，去中心化存储的出现使具有去信任、防篡改及防数据丢失的分布式存储平台成为可能。

IPFS（INTER PLANETARY FILE SYSTEM）协议是一种通用的去中心化的存储设施，用户可以基于 IPFS 构建文件存储的版本控制、区块链去中心化应用等。结合 IPFS 做为区

块链平台底层的存储服务，单一节点可以不用全量存储去中心化应用内的数据，从而达到数据分区及分片的效果，提高系统吞吐性能。另一方面，区块链不仅成为去中心化应用平台，亦可以成为一种去中心化存储服务平台，实现去中心化计算的目标。

7. 里程碑

一期（2019 年 Q3-2019 年 Q4）

- 项目启动，顶层设计，整合关键资源
- DAG 基金会成立
- 公布发展计划
- 发布白皮书 V2.0
- 成立汽车生态联盟，完善生态体系
- 基于 DACH chain 一次性创设数字通证 DACH Token
- 节点部署
- 搭建跨国（区）交易的结算环境
- DAPP 孵化器上线，区块链浏览器上线

二期（2020 年 Q1-Q4）

- 完成分布式客户端应用，推出全球节点计划
- 汽车联盟生态圈发布会
- 开发 DACH Token 区块链网络
- 移动端应用上线
- 建立汽车 Dapp 生态自治社区
- 主网测试发布及上线
- 打造共识车载节点，发布车载矿机等硬件，支持更大规模的用户需求
- 设计可稳定运行的智能终端及区块链节点网络硬件，保证开发环境的稳定
- 公布主网应用接口文案
- 生态区域内实现的 DACH 结算
- 持续优化 DACH 平台的产品、服务、盈利能力

8. 基金会

8.1 DAG 基金会

DAG 汽车联盟基金会（以下简称“DAG 基金会”或“基金会”）是 2019 年 4 月在新加坡成立的基金组织。

DAG 基金会通过区块链数据结构，实现企业、用户、平台的交易区块链化，实现用户、企业、合作伙伴、第三方、政府等相关方的共赢利益，保证项目管理的有效性、可持续性和安全性，推进 DACH 区块链技术的发展推广。

DAG 基金会将 DACH 区块链技术与更多场景结合，通过通用推广奖励、营销激励、电子商务、活跃奖励等一系列措施，实现 DACH Token 的生成、赠送、交易等功能，推动 DACH 区块链的生态系统建设。

DAG 基金会的初步资金将主要来自于 DACH Token 的售卖。DAG 基金会筹集的 DACH Token 根据透明、可审计和效率的原则进行保管和经营。资金主要用于 DACH 的设计与研发、运营管理、DACH 相关项目收并购以及综合治理等方面。

DAG 基金会在服务与推进 DACH 项目本身之外，同时也致力于将项目所产生的价值

用于生态成员的成长扶持上。基金会每年将拿出额度不等的项目资金扶持，以帮助开发者能够更加快速地成长；同时，基金会设立了专项种子孵化资金，用以帮助初创社区能够快速将想法落地，让车链以获得更快的成长。

DAG 基金会接受年度审计，由国际顶尖会计事务所对基金会的运作和风险进行评估。基金会将根据事件特性，例如事件影响程度、影响范围、影响 Token 量和发生的概率进行分级，按照优先级进行决策, 对于优先级高的事件,尽快组织基金会相关委员会进行决策。

DAG 基金会的合作伙伴已与国际知名律师事务所建立合作，其作为 DACH 项目法律顾问, 为 DACH 项目提供运营合规化、法律风控体系设计、国际法律咨询等方面提供全面的法律服务。

8.2 基金会组织架构

为了在公开和透明的原则下，合理高效地利用基金会的资金和资源，为了推动 DACH 的快速发展，为了更多结合了 DACH 的行业、场景、应用的落地，基金会由产品人员、开发人员、市场人员、运营人员和职能部门组成，组织架构包含决策委员会、产品设计、技术研发、市场推广、运营管理、财务与人力管理。

决策委员会

决策委员会是 DACH 的最高决策机构，承担最终决策职能，决策委员会委员无职位高低之分，由联合创始人、顾问、大小节点发起人选举组成，负责对基金会战略规划、年度计划、预算等重大事项进行审议和审批，并代表基金会对 DACH 的生态重大议题做出表决。

决策委员会设立首席执行官，由 DACH 创始社区及决策委员会票选产生，对决策委员会负责。

基金会成立初期，决策委员会由基金会主席、创世社区核心成员、超级使用者和基石机构组成，每届理事成员任期为二年。

执行负责人

执行负责人由决策委员会选举产生，负责基金会的日常运营管理、各下属委员会的工作协调、主持决策委员会会议等。执行负责人定期向决策委员会汇报工作情况，其职责相当于公司 CEO，CEO 的任命由决策委员会产生。

公共关系委员会

公共关系委员会的目标是为基金会及全球社区服务，负责 DACH 全球市场的法律、法务、技术知识产权、开源项目、品牌推广和全球战略联盟。

8.3 社区介绍

为了保证项目的顺利实施与推进，同时考虑到企业未来的事业布局和持续的行业竞争力以及战略性的商业理财和并购，DACH 主要理财人和创始核心社区主要强调在数字支付行业、商业金融、区块链技术、机密技术、互联网技术、社区管理等方面的人才，他们是基金会运营的核心要素。

Gleb Wikeny　　CEO

金融硕士/通讯工程硕士，资深理财人，有丰富的商业阅历，大型 IT 平台 20 年以上管理经验，区块链运营与开发管理经验。

Mikhail Zarutskiy　　CTO

EOS 高级研发工程师，15 年大型技术项目开发经验，丰富的区块链开发管理经验，擅长加密算法、人工智能系统，打造了能够将神经网络计算和其他机器学习算法相结合的百万计 TPS 请求。

Oleg Romanenko　　CSA

AdSniper 实时服务架构师，AlfaBank 在线银行系统分析师， 能够在 1 个节点每秒处理超过 1 百万请求的高负荷网络创始人。

Maria Agranovskaya　　法律部总监

资深律师, 区块链项目律师事务所总监，具有 20 年以上工作经验的律师。新技术、媒体和知识产权领域的法律实践超过 15 年，从 2010 年开始处理加密 Token 问题。

Dmitry Borisenko　　测试主管

首席 C++开发者；Hadoop 系统替代系统的创建者，其速度为同类系统速度的 100 倍以上。

Eugenia Sigacheva　　公共事务合作伙伴

在国际营销、公关、IT 和创新方面有超过 18 年的经验。

Andrey Akimov　　首席传播官

在娱乐和 IT 商业领域拥有超过 15 年的营销和公关经验，曾任 Game Insight 等公司公关主管。

Anton Agranovsky

IT 公司建立和发展领域的理财者、专家及意见领袖，Plastic Media 和 SMX Communications 董事会成员。

Vitaly Golban

经验丰富的企业家、加密基金经理，在全球企业拥有 10 年以上的运营管理经验

9. 合规与风险提示

9.1 合规与信息披露

DACH 项目将严格遵循国家相关政策法律法规，并主动接受政府相关监管，DACH 将在所在国家及地方政府授权的区域落地，并遵守各类监管相关要求，争取将 DACH 相关交易平台打造成为全球区块链产业的示范样板项目。举措如下：

1.参与者充分知悉本项目存在的风险；对于没有鉴别风险能力或风险承担能力的参与者，本项目有权拒绝接收；

2.向主体公司所在监管机构或产业园区所属地的地方政府，主动披露项目的资料，包括本白皮书、社区成员、商业模式、经费使用计划、项目特色、发展目标、发展策略、风险评估、相关计划等；

3.积极了解全球相关政策法律法规，推进区块链合规化发展进程。为切实保护参与者合法权益，DACH 社区将对经费使用和重大进展进行定期披露，以保护参与者的合法权益。

9.2 风险提示

DAG 基金会认为，在 DACH chain 的开发、维护和运营过程中存在众多风险，这其中很多都超出了 DACH chain 基金会的控制。每个 DACH Token 参与者应仔细阅读、理解并考虑下述风险，慎重决定是否参与 Token 互换计划。若参与到 DACH Token 互换计划则将视参与者已充分知晓并同意接受下述风险:

9.2.1.交易安全

法律政策和监管风险 区块链技术受限于全球多个不同的监管组织的监督与控制。DACH 或受限于他们所提出的要求或行动， 包括但不限于限制数字 Token 的使用，例如 DACH 可能减慢或受限制 DACH 在未来的功能或回购。Token 买家必须自己进行尽责的调查，确保他们遵循所有他们当地关系到加密数字通政、税务、债券及其他监管的法律。

9.2.2.安全风险

在天使或私募阶段收集到的资金都不经保险保障。若遗失了它们或它们失去了价值，买家或无法得到任何私人或公众保险的协助。

9.2.3.技术风险

DACH chain 仍在开发阶段，由于 DACH chain 底层公链开发的技术复杂性，出售方可能不时会面临无法预测和/或无法克服的技术困难。因此，DACH chain 的开发可能会由于任何原因而在任何时候失败或终止。

9.2.4.未经授权认领 DACH 的风险

任何通过解密或破解 DACH 购买者的密码而获得购买者注册邮箱或注册账号访问权限

的人士，将能够恶意认领在本次公开发售中所购买的 DACH。据此，购买者在本次公开发售中所购买的 DACH 可能会被错误发送至通过购买者注册邮箱或注册账号认领 DACH 的任何人士，而这种发送是不可撤销、不可逆转的。

每一购买者应当采取如下的措施妥善维护其注册邮箱或注册账号的安全性：使用高安全性密码；不打开或回复任何欺诈邮件；严格保密其机密或个人信息。

9.2.5.源代码漏洞风险

无人能保证 DACH chain 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞。可能将损害 DACH chain 的可用性、稳定性和安全性，并因此对 DACH 的价值造成负面影响。开放源代码以透明为根本，以促进源自于社区对代码的鉴定和问题解决。

9.2.6.流动性风险

DACH 既不是任何人、实体、中央银行或国家、超国家或准国家组织发行的 Token，也没有任何硬资产或其他信用所支持。DACH 在市场上的流通和交易并不是出售方的职责或追求。DACH 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 DACH 持有者处对话或购买任何 DACH，也没有任何人士能够在任何程度上保证任何时刻 DACH 的流通性或市场价格。

9.2.7.价格波动风险

若在公开市场上交易，加密 Token 通常价格波动剧烈，短期内价格震荡经常发生。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、悟空的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。DACH 交易价格所涉风险需由 DACH 交易者自行承担。

9.2.8.信息披露不足风险

截至本白皮书发布之日，DACH chain 仍处于开发阶段，其哲学理念、共识机制、算法、代码等技术规范和参数可能会经常不断更新与变更。尽管白皮书包含 DACH chain 的特定信息，但其并不绝对完整，且出售方可能会根据特定目的不时对这些信息做出调整与更新。出售方无法，也无义务随时告知参与者 DACH chain 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让参与者及时且充分地获悉 DACH chain 开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

9.3 免责声明

除本白皮书所明确载明的之外，基金会不对 DACH chain 或 数字通证 DACH Token 作任何陈述或保证(尤其是对其适销性和特定功能)。任何人参与数字通证 DACH Token 的售卖计划及购买数字通证 DACH Token 的行为均基于其自己本身对 DACH chain 和数字通证 DACH Token 的相关知识、法律法规、本白皮书的信息认知。在无损于前述内容的普适性的前提下，所有参与者将在 DACH chain 项目启动之后按现状接受数字通证 DACH Token，无论其技术规格、参数、性能或功能等。

基金会在此明确不予承认和拒绝承担下述责任：

1.任何人在购买数字通证 DACH Token 时违反了任何所在国家的反洗钱、反恐怖主义融资或其他监管要求；

2.任何人在购买数字通证 DACH Token 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法使用或无法提取数字通证 DACH Token ；

3.由于其他原因，数字通证 DACH Token 的售卖计划被放弃；

4.DACH chain 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；

5.DACH chain 及其数字通证 DACH Token 源代码的错误、瑕疵、缺陷或其他问题；

6.DACH chain 平台、数字通证 DACH Token 的故障、崩溃、瘫痪、回滚或硬分叉；

7.DACH chain 或数字通证 DACH Token 未能实现特定功能或不适合任何特定用途；

8.未能及时且完整的披露关于 DACH chain 开发的信息。