

TAK DATA LINK

以边缘计算核心带动的物联网大数据解决方案



白皮书

【构建数据共享和万物互联的新范式】

二〇一九年八月二日



目录

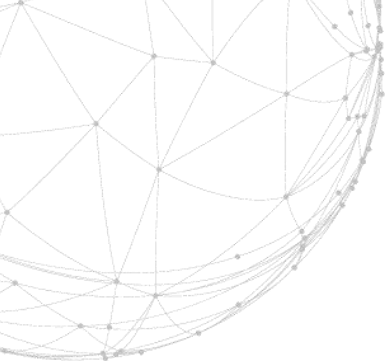
第一章 项目背景	5
1.1 区块链背景简介	5
1.2 物联网的兴起与趋势	7
1.3 大数据产业的物联应用趋势	11
第二章 TAK DATA LINK 物联解决方案	13
2.1 区块链与物联网	13
2.2 TAK DATA LINK 物联解决方案	15
2.3 IoT 应用数据开放与收益	20
2.4 IoT 应用数据交易流程	20
2.5 TAK DATA LINK 系统特性	21
第三章 TAK DATA LINK 技术架构	23
3.1 概述	23
3.2 零知识证明	24
3.3 同态加密	25
3.4 安全多方计算	27
3.5 复合决策闪电网络模型	28

第四章 TAK DATA LINK 应用场景	29
4.1 主要场景 - 数据开放平台	30
4.2 应用示例 - 健康大数据	31
4.3 应用示例 - 汽车物联网	33
4.4 其他应用 - 农业 & 工业	33
第五章 代币分配计划	36
5.1 TAK DATA LINK 代币	36
5.2 代币分配方案	37
5.3 发行计划	37
第六章 团队和基金会	38
第七章 免责声明	41
第八章 参考文献	43

版权声明

本白皮书由 TAK DATA LINK 团队主导编制，严禁抄袭，如需转载，请注明出处。同时本白皮书中所涉及到的所有的产品设计理念、技术设计方案以及技术解决方案，其知识产权均属于 TAK DATA LINK 团队，对于任何侵犯知识产权的行为，团队将通过法律手段保护权益。

TAK DATA LINK 团队

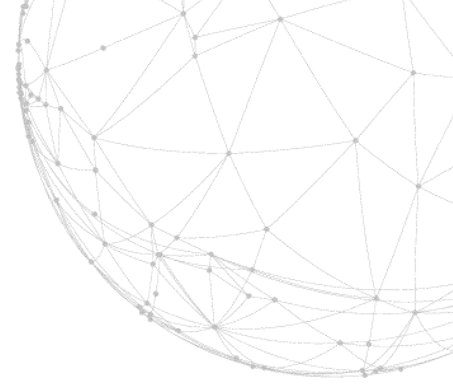


第一章 项目背景

1.1 区块链背景简介

2008 年匿名人 Satoshi Nakamoto 发表了一篇名为 “Bitcoin: A Peer-to-Peer Electronic Cash System” 的论文，之后比特币成为世界第一个去中心化的电子货币。比特币的去中心化是基于对于区块链，一个分布式账本的应用。

自从 1969 年 10 月份互联网诞生以来，人们从未停止对于电子货币的创造研究，美国国防部于 1985 年就展开对于发行电子货币的可能性的探究，但是直到 2008 年中 Satoshi Nakamoto 创造比特币，去中心化的电子货币一直是一个未完成的课题。数据或者信息在互联网内是自由传播的，但是基于这一特性也产生出许多问题，例如，如果一张图片被分享给另外一个人，那收到图片的人可以立刻对这张图片进行复制然后分享给其他人，图片的发送者也可以再复制图片一次然后分享出去，这样就造成了数据所有权极难管理和维护。货币有两点基本属性，不可被复制以及不可被二次花出，任何电子货币也都需要满足这两点，所以传统的电子货币是通过一个中间机构来进行清算以此保证其不能被复制以及不能被花出两次。区块链技术的诞生让互联网里任意两个个体直接进行价值传递而不需要第三方（中间）机构介入。拜占庭将军问题，是由莱斯利提出的点对点通信中的基本问题。在分布式计算上，不同的计算机透过讯息交换，尝试达成共识；但有时候，系统上协调计算机或成员计算机可能因系统错误并交换错误的讯息，导致影响最终的系统一致性。区块链技术是除了量子通信之外解决此问题的有效方案。现在区块链已经不再仅仅局限于“公共账本”，而是“公共电脑”。任何人不仅可以在上面存储非常可靠无法被恶意篡改的重要数据，还可以在上面运行程序，所



有被运行程序的逻辑是所有用户达成共识后一致认可的，不会因为个人的意志而被改变。

区块链具有以下显著优势：

● 分布式

区块链分布式的特征也称去中心化，是区块链最基本的特征。在传统的中心化网络系统中，对一个中心节点的破坏即可瘫痪整个系统，而对于区块链网络，由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据由整个系统中具有维护功能的节点来共同维护，此时攻击某个节点无法破坏整个网络。

● 开放式

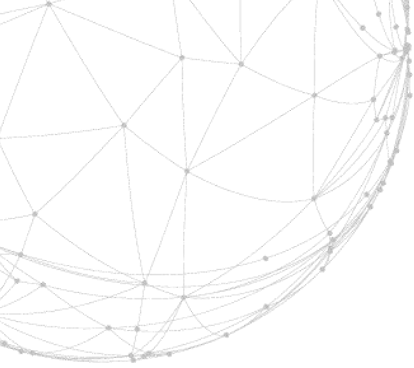
基于区块链系统使用开源的程序、开放的规则和高参与度，除交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，整个系统信息高度透明。

● 难以篡改/唯一可信

区块链系统的信息一旦经过验证并添加至区块链后，链上数据在每个网络节点中均有备份，且不会删除，导致攻击整个网络的成本代价极高，从而保证区块链网络中的数据难以篡改，且唯一可信。

● 隐匿性/安全性

区块链系统中虽然所有的数据记录和更新操作过程都是对全网节点公开的，但其交易者的私有信息是通过哈希加密处理的，即数据交换和交易都是在匿名的情况下进行的。加密简单而言就是通



过一种算法手段对原始信息进行转换,信息的接收者能够通过密钥对密文进行解密从而得到原文的过程。区块链运用了许多成熟的加密算法来保证系统的可靠性和安全性。

区块链技术已成为全球创新领域最受关注的话题,被称为最有潜力触发第五轮颠覆性革命浪潮的核心技术。目前,区块链的应用已延伸到金融、物联网、智能制造、供应链管理等多个领域,将为云计算、大数据、AI等新一代信息技术的发展带来新的机遇,有能力引发新一轮的技术创新和产业变革。

经济增长的第一原动力是科技创新,其成长效率由这个社会结构中的资金流、信息流和物流等共同决定。区块链及加密数字货币的成长和发展为其带来三个底层的改变:第一是实现了信息即价值,产业即金融;第二是涌现出更多去中心化、社区化和自由化的协作组织;第三是实现协作机制中的成本降低和效率提升。

正如《经济学人》杂志中所定义的那样,区块链是信任的机器。它将会重新定义生产关系,使得整个生态更加可信。

1.2 物联网的兴起与趋势

1、物联网吹响战略爆发前奏

全球物联网应用增长区势明显,万物互联时代开启。全球新一轮科技革命和产业变革正在孕育兴起,信息通信技术以前所未有的速度转化为现实生产力,深刻改变着全球经济格局、利益格局、安全格局。物联网作为信息通信技术的典型代表,在全球范围内呈现加速发展的态势。



不同行业 and 不同类型的物联网，应用的普及和逐渐成熟推动物联网的发展进入万物互联的新时代，可穿戴设备、智能家电、自动驾驶汽车、智能机器人等，数以百亿计的新设备将接入网络，**预计到 2020 年全球联网设备数量将达到 260 亿个，物联网市场规模达到 1.9 万亿美元。到 2018 年，全球车联网的市场规模将达到 400 亿欧元，年均复合增长率达到 25%，2018 年全球智能制造及智能工厂相关市场规模将达 2,500 亿美元；截止 2019 年，全世界智慧城市总投资将达到 1200 亿美元。**

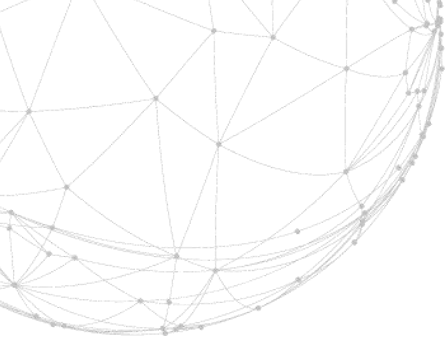
万物互联在推动海量设备接入的同时，将在网络中形成海量数据，预计 2020 年全球联网设备带来数据将达到 44ZB，物联网数据价值的发掘将进一步推动 物联网应用呈现爆发性增长，促进生产生活和社会管理方式不断向智能化、精细化、网络化方向转变。

2、基于边缘计算建立的新物联

(1) 边缘计算概念

边缘计算和云计算两者都是处理大数据的计算运行的一种方式

- 云计算：一种利用互联网实现随时随地、按需、便捷地使用共享计算设施、存储设备、应用程序等资源的计算模式，**一种中心化的大数据处理服务中心**，所有数据处理集中于云端数据服务商的大数据处理服务中心上。
- 边缘计算：利用靠近数据源的边缘地带来完成的运算程序，是常用云端协同中的“端”口，**一种去中心化的边缘式大数据处理服务**，边缘计算数据无需消耗时间传送至云端，在边缘侧既能完成计算任务，对云计算的一种补充和优化。



(2) 边缘计算特点

● 分布式和低延时计算

边缘计算聚焦实时、短周期数据的分析，能够更好地支撑本地业务的实时智能化处理与执行

● 更加智能化

AI+边缘计算的组合出击让边缘计算不止于计算，更多是智能化

● 更加节能

云计算和边缘计算结合，成本只有单独使用云计算的 39%

● 缓解流量压力

在进行云端传输时通过边缘节点进行一部分简单数据处理，进而能够设备响应时间，减少从设备到云端的数据流。

(3) 边缘计算下的物联网

未来构成物联网的设备将超过数万亿台，世界将迎来物联网席卷所有行业的临界点。未来物联网应用关键在于：降低成本、保护用户隐私、物联网自治的解决方案等，从根本上重新思考技术战略，利用产业的水平核心环节构建完善的产业生态，建立高效的数字经济模型和价值。物联网现阶段的主要发展模式呈现以下特征：

● 平台化服务：

利用物联网平台打破数据孤岛效应，大规模应用数据，增值数据；

● 广泛化连接：

广域网和短距离通信技术扩大物联范围，实现大规模连接能力

● 智能终端化：

通过设备智能化及互联网支持不同设备本地协同，应用场景灵活

为了消除人们对物联网隐私的担忧，建立对物联网的信任，使得物联规模从数十亿台设备增长到数万亿台设备，降低成本 的“设备民主”



(democracy of devices) 将成为主流，同时它将通过为顾客和企业提供更好的产品和用户体验，促成新的数字经济和创造新价值。

在新兴的设备民主中，物联网的权力将从中心转移到边缘。当设备可以实时地进行竞争和交易，它们将从物理世界中创建出流动的市场。在由数以千亿计的设备构成的物联网中，“连接”和“智能”将会成为产生更好的产品和用户体验的手段。

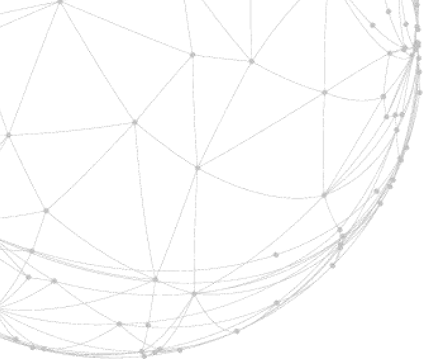
3、现在物联网存在的问题

物联网技术诞生于 20 世纪 90 年代。物联网的里程碑事件发生在 2016 年 6 月，当时 3GPP 发布了 release 13，定义了物联网连接统一标准协议，解决了传统物联网由来已久的四大问题：

- 连接数量受限；
- 覆盖范围受限；
- 待机时间短；
- 成本高。

从 2016 年 9 月开始，各家移动通讯设备厂商陆续发布了可商用的物联网连接方案，针对不同的应用可以选择 eMTC、NB-Iot 和 EC-GSM 等不同的技术。通过对以上四大问题的改进，物联网产业开始在全球蓬勃发展，拥有了大量应用案例、应用、产品和解决方案，但仍存在三个重大问题，有望通过区块链技术来解决：

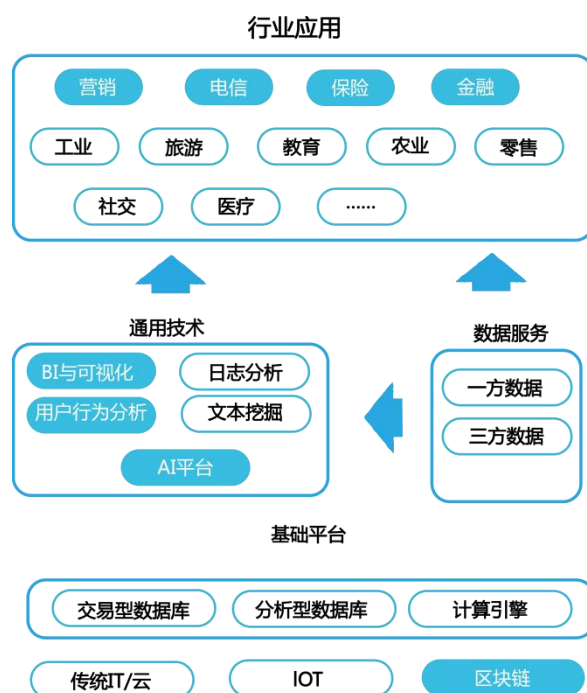
- 标准通讯协议的碎片化；
- 开发、部署和维护成本太高；
- 安全隐私无法确保。



1.3 大数据产业的物联应用趋势

随着互联网的充分发展，大数据全面进入塔克链的生活。大数据已经成为现代经济的最重要基石，产业规模巨大。在无形的数据资产价值逐步超越有形资产的今天，谁拥有更多更优质的数据，谁就是未来的主人。伴随 5G 时代的到来，大数据产业也面临着质的突破，打破空间距离的限制，以万物互联为理念，实现大数据产业的物联应用时代；

当前，典型大数据产业结构如下图：



大数据产业典型特征是全行业以数据为基石。但当前的大数据产业分散，多家厂商在数据孤岛上各自为战，万亿的行业产值分散到多个厂商。造成这种行业分散格局的主要原因是：

- 行业对中心化的数据平台的数据安全普遍存有疑虑，如平台是



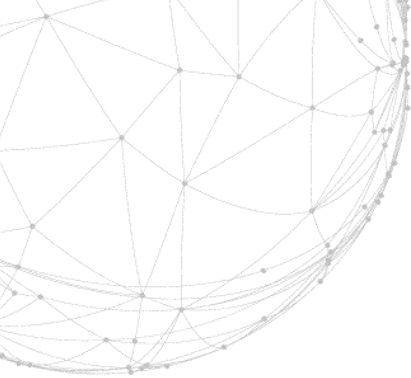
否会沉淀数据，平台上存储的数据是否会被暴力破解。同时，行业普遍担心中心化的数据平台有可能被巨头操纵，从而失去中立性。

- 电子数据不同于实体物品，其天然具有复制成本低、复制无差异性、没有唯一且明确的所有权约束等特征。在数据资产的确权 and 溯源，以及数据流通环节的信任和安全问题得到有效解决前，行业各方将无法积极参与数据流通。

区块链的本质是生产关系和信任关系的变革。在大数据领域，最有可能带来的变革机会是利用区块链技术重构全产业的沟通关系，构建基于物联网的立体化信息采集网络。这包括：

- 以去中心的数据开放交易平台代替中心化数据平台，解决中立和信任问题。
- 可确权可溯源的可信数据流通机制。
- 跨行业跨设备构建信息采集网络，提升生产能力，推动服务化转型。

以去中心的、自治的数据开放平台为基石，以可信的数据流通机制为轴线，建立跨行业跨设备构建信息采集网络，将有可能建设一个横贯数据服务商、行业应用商、通用技术商、平台应用商、传统设备商、全体用户的全新生态体系。



第二章

TAK DATA LINK 物联解决方案

2.1 区块链与物联网

关于物联网 (IoT , Internet of Things) 的概念 , 第一次是由英国学者 Kevin Ashton 于 1999 年在 MIT 提出 , 经过与多位企业高管的访谈和讨论 , Ashton 将 IoT 定义为 :

“一个包含了所有 ‘智能’ 设备的网络 , 具有某种传感机制 , 可以在没有人工干预的情况下通过互联网与其他智能设备或云进行通讯。”

关于物联网技术和区块链上的智能系统 , 目前已经有很多探索。当应用于物联网时 , 区块链开辟了创新的无限可能性 , 区块链技术有助于 :

1. 记录、跟踪和验证设备的历史记录 ;
2. 保管设备的数字认证和所有权 ;
3. 保证设备的真实性、隐私性和安全性 ;
4. 进行设备与设备之间 , 设备与人之间的智能活动.

TAK DATA LINK 认为物联网技术和区块链技术在应用中密不可分 , 物联网技术在设备之间建立信息连接乃至商业连接 , 此过程通常需要三个步骤 :



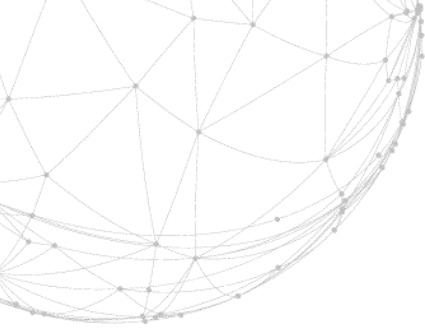
1. 要想建立设备之间的通用通讯协议，就要有通用语言。这就要求设备之间有统一的通讯协议，即便厂商和所有者不同。换言之，设备需要可以用一种语言交流。3GPP 发布的物联网标准给物物相连提供了一种统一语言；

2. 一旦设备能够相互对话，下一步就是实现设备的统一识别。换言之，各方需要访问并认同统一的 ID，这些 ID 不能被任何人控制或操纵。这就像不限实体或制造商的通用序列号。区块链是在各方之间构建这种可信任和许可机制的完美解决方案；

3. 有了通用的语言和身份识别之后，设备之间需要进行进一步的合作和开展商业活动，那么就需要智能合约和智能货币的支持。

区块链可以确保数据的完整性，物联网可以确保数据收集并记录到区块链时的客观性。事实上，三大最具前景的技术将实现合作：

1. 物联网就像双眼和双手，负责接触世界并收集数据；
2. 区块链就像心脏，负责保护数据和提供信任；
3. 人工智能就像大脑，负责处理和分析数据。



2.2 TAK DATA LINK 物联解决方案

TAK DATA LINK (塔克链) 即是为了解决上述问题而设计的。TAK DATA LINK (塔克链) 是针对行业垂直领域物联的应用, 基于区块链技术、边缘大数据计算、智能合约及共识机制形成的一个去中心化的万物互联数据平台, 实现可接入海量 Dapp、海量数据、海量物联网设备关联的大型数据共享和开放平台, 打造以边缘计算核心带动的物联网大数据解决方案, 构建数据共享和万物互联的新范式。

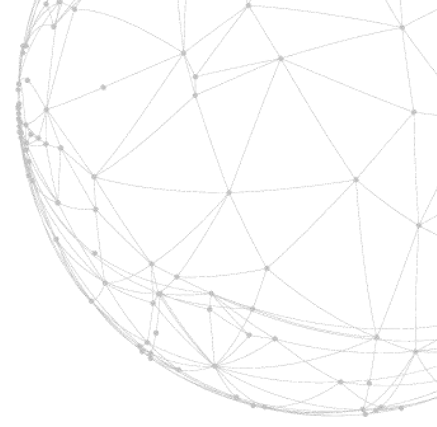
在这个平台内, 所有行业与用户基于公平、开放、透明的共识规则、可信的密码学、数学算法及边缘大数据计算, 形成一个物联应用数据共享和开放平台, 从而实现不同垂直场景物联应用的数据应用共享、开放、交易和变现。

1、TAK DATA LINK 4 大核心能力：

1 . 强大的物联网连接与整合能力

TAK DATA LINK (塔克链) 支持海量、多样的物联网数据的接入、集成与分发, 是万物互联数据平台的入口。基于区块链共识协议实现的复合决策闪电网络能够在不同的网络环境下, 极其稳定、高效地完成物联网数据的网络传输, 使得物联网的大数据分析成为可能。

TAK DATA LINK (塔克链) 针对大量的物联网设备产生的不同形式的大数据, 提供特定的有效的存储方式, 具备高度的安全性、规范性、整合性和可扩展性。此外, 该平台还提供相应的应用场景, 实现物联网系统与现有系统及数据的整合。



2 . 丰富的物联网大数据分析能力

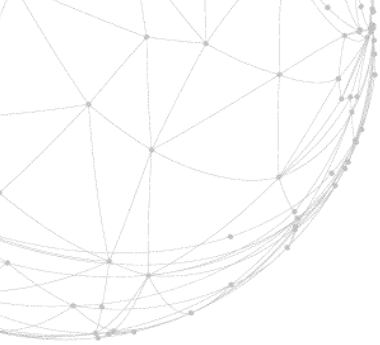
物联网真正的价值来自对海量数据的分析洞察，由大数据驱动的物联网才是有价值的物联网。TAK DATA LINK (塔克链) 开发以边缘计算为核心的大数据分析能力，包括实时流式计算(StreamingComputing)、指导性分析 (PrescriptiveAnalytics)、业务智能分析 (BusinessIntelligence)，和最新的认知计算(CognitiveComputing)等。从而帮助相关行业客户从多种数据源中洞察、获取、支撑整个企业甚至价值链的相关业务决策。

3 . 推动价值链整合与业务创新的 PaaS 能力

万物互联数据平台是 TAK DATA LINK (塔克链) 基于开放式技术构建的 PaaS (PlatformAsAService , 平台即服务) 平台。 通过提供多种技术与业务服务以及托管功能来实现快速、组装式、规模化应用开发，从而简化应用程序的交付过程，使得开发者能够轻松地进行应用程序开发。在 TAK DATA LINK (塔克链) 上，物联网基础服务(IoTFoundation)提供了对物联网设备和数据的应用程序访问，可以简单方便地注册与管理物联网设备。

4 . 完善的物联网安全保障能力

TAK DATA LINK (塔克链) 不仅高效地保护其上的应用与数据免受



各种安全威胁，并使其符合法规要求，同时也简化了云应用程序的管理。分布全球的塔克链安全运营中心每天都会帮助 TAK DATA LINK（塔克链）客户解决每个安全事件问题。TAK DATA LINK（塔克链）将汇集诸多行业数据，打造世界上最大的“威胁和漏洞数据库”，对各种安全威胁进行实时分析和历史分析，能够为客户所面对的安全威胁和事件做好充分准备并做出更为快速的响应。

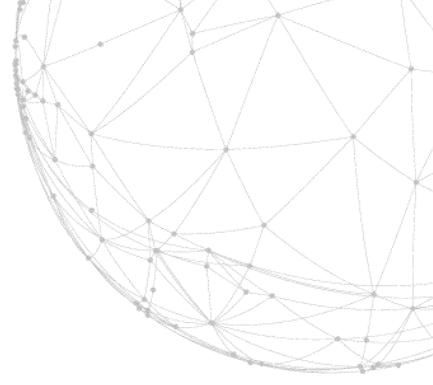
2、TAK DATA LINK 技术特征：

- 跨行业跨设备构建信息采集网络
- 身份公平，没有特权身份存在。
- 用技术保障平台是完全自治的，没有任何人和组织可以绝对控制平台以及平台上的数据。
- 数据可被确权和溯源，数据供应方的权益可被保护。
- 终端用户隐私安全，用户绝对控制隐私数据。

TAK DATA LINK（塔克链）的目标是以一个去中心化的万物互联数据平台为基石，以海量垂直场景物联应用及物联设备关联组成核心数据供应方，以可信可确权的数据流通为轴线，基于区块链技术及边缘大数据计算，提供数据计算的隐秘性，改造大数据产业的生产关系和信任关系，建设全新的物联大数据共赢生态社区。

3、TAK DATA LINK 解决方案：

TAK DATA LINK 物联解决方案通过整合区块链、物联网和大数据



应用等各种技术而形成的。物联网是塔克链团队的一大关键技术能力。

塔克链拥有专注于物联网开发和区块链协作解决方案的物联网团队，**该团队提出的解决方案包括但不限于：**

- 1．标签技术和加密芯片组；
- 2．物联网传感器的识别和数据隐私；
- 3．物联设备系统的安全和授权模块；
- 4．相关行业数据的存储与分析。

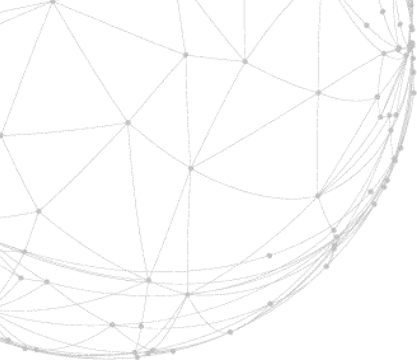
塔克链在传统物联网系统的基础上进行了创新，加入了基于区块链的设备 ID 和非对称密钥算法：

设备 ID：

每个物联网设备在区块链网络上都需要唯一且通用的身份。在应用案例中，网络中其他参与者，只要获得授权，可按需访问和识别该设备 ID。此外，该 ID 还需要通过特定的智能合约和应用（如 VeVID 中的模块）来验证设备，以证明其原始生产商和所有权。

非对称密钥算法：

非对称密钥算法是区块链的基石。如果算法得当，便可以一种绝对安全的方式实现设备的鉴权和授权。为每个设备分配一个公钥和私钥，其中公钥是识别码，私钥是安全签名。在塔克链区块链的设计中，私钥存储在每个设备的安全位置，且完全无法读取，而加密和解密算法将在 CPU 或 mCPU 的安全模式下执行，以确保安全。通过实施该方案，应用案例可以覆盖设备的访问控制、设备认证、数据源验证、智能合约执行控制等。



4、TAK DATA LINK 影响：

TAK DATA LINK（塔克链）将成为物联产业发展的制高点，功能和服务模式将不断完善

- TAK DATA LINK 加速产业价值向软件和基于数据的服务转移

TAK DATA LINK（塔克链）汇聚海量终端设备的数据信息，利用大数据分析等技术挖掘潜在价值，推动物联网行业形成“数据衍生创新服务”的新业态，基于 TAK DATA LINK（塔克链）提供远程故障诊断、生命周期管理等增值服务等，丰富服务内容

- 利用共性能力覆盖垂直行业，加速产业发展

TAK DATA LINK（塔克链）整合不同行业分散的信息、用户、设施等资源及外部的开发资源，利用通用功能和接口开发适用不同行业的应用，降低投入成本，提升开发效率，并实现跨行业、跨领域资源互通，推动大规模开源应用的发展。

- 推动服务模式转变

TAK DATA LINK（塔克链）吸引设备供应商、网络运营商、系统集成商、应用开发商等产业链上下游企业，形成互利共赢的生态圈，既可以满足用户多样化需求，也能够利用快速迭代的开发模式短时间响应行业用户的特定需求，实现向集成服务模式转变。



2.3 IoT 应用数据开放与收益

垂直行业物联设备接入 TAK DATA LINK(塔克链) 会获得 TAK DATA LINK Token 做为奖励。在万物互联数据平台提供的数据越多，被使用的优质数据越多，获得的 Token 奖励就越多。

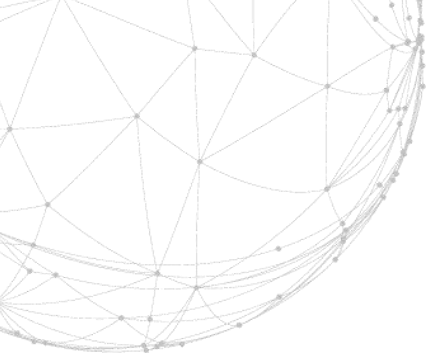
为了公平交易，TAK DATA LINK (塔克链) 的数据开放平台采用透明定价的原则。每条数据定价对所有成员可见，交易按照定价交易。

开放平台中数据的定价和结算使用 TAK DATA LINK Token，参与数据聚合等交易的节点会收到 TAK DATA LINK Token 做为奖励。数据交易涉及的用户和运营商均会收到 TAK DATA LINK Token 奖励。

2.4 IoT 应用数据交易流程

数据交易流程：

1. 数据购买方向数据开放平台发出购买请求（智能合约），请求的智能合约中带有自己的公钥，并用私钥签名。平台 DApp 验证此用户为平台的认证用户，并且通过签名验证合约正确
2. 平台广播此购买请求
3. 相关数据提供方查询数据源，获得需要的数据
4. 如果涉及隐私数据，平台要获得用户授权，才能继续此交易
5. 数据提供方用购买方的公钥加密后，通过 P2P 网络发送数据给



购买方

6. 数据购买方完成付款，智能合约交易完成

2.5 TAK DATA LINK 系统特性

1、公平、透明、开放和自治

区块链技术和思想的引入，可以让所有机构或个人在无须任何中心机构背书的前提下公平地参与到物联数据的收集共享和开放运动中来。所有的机构或个人只需认同这些基于密码学和数据规则，即可加入到万物互联数据开放平台中，成为 TAK DATA LINK（塔克链）上的一个节点，数据平台的开放、交易或使用，没有任何人可以掌控。

2、数据可确权、可溯源

通过区块链的分布式账本，能够安全透明地记录所有数据上传、更新、交易或使用行为，这些行为记录一经确认就不可被篡改，使得开放平台上的所有数据具有可确权、可溯源的功能。

3、安全可信数据交易

点对点方式数据交易，从根本上避免了平台沉淀数据的可能性。应用智能合约，数据透明公开定价，保证交易的公平性。

购买的数据由数据提供方用数据购买方的公钥加密传输，只有购买方的私钥才能解密，

从而避免数据泄露。平台上的数据都有唯一的签名，如果数据购买方对数据进行转售，收益会记入初始数据提供方。基于智能合约和社区共识的数据评分机制。

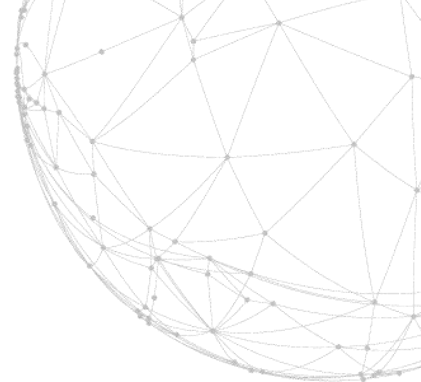
4、多维度大数据整合

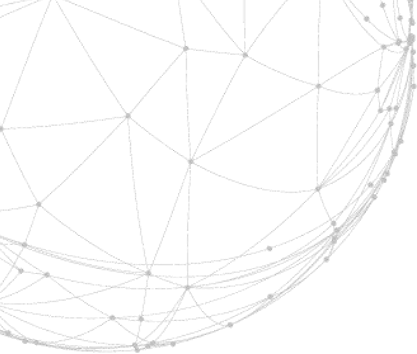
由海量垂直应用分别基于共识机制共享数据，形成大数据共享开放平台，从而实现更完整、更精准的多维度数据画像。

5、用户隐私保护与用户数据确权

使用统一数字身份对用户在网上多个设备多个场景的不同身份进行统一映射。可以用于用户数据的跨屏跨应用合并，及统一登录。

用户的个人数据完全由用户所有，用户完全掌握私钥，并由用户自己决定向谁开放授权以及如何收费，全程可跟踪。





第三章

TAK DATA LINK 技术架构

3.1 概述

TAK DATA LINK 引擎提供运行隐私保护去中心化应用的环境，核心目标是能够让参与者在完全掌控 IoT 应用数据所有权的情况下实现多方协作计算，主要包含三个组件：

1) OVM (TAK DATA LINK Virtual Machine):

智能合约代码的执行引擎，支持动态加密等密码学原语；

2) OOP (TAK DATA LINK Oracle Protocol):

智能合约与外部世界进行安全数据交换的标准协议；

3) OAF (TAK DATA LINK Application Framework):

隐私保护去中心化应用开发框架和密码函数库等。

简而言之，TAK DATA LINK 引擎是在区块链技术基础上，高度抽象并整合零知识证明、同态加密、安全多方计算、边缘计算等密码学机制来支撑安全数据计算，实现隐私保护智能合约和去中心化数据计算应用的快速构建和部署。



3.2 零知识证明

零知识证明是由 S.Goldwasser、S.Micali 及 C.Rackoff 在 20 世纪 80 年代初提出的[10]，指的是证明者可以在不泄露任何有用信息的前提下，使验证者相信某个论断是正确的。

零知识证明系统是实现隐私保护安全协议的有效手段，首先塔克链给出交互式证明系统的定义：

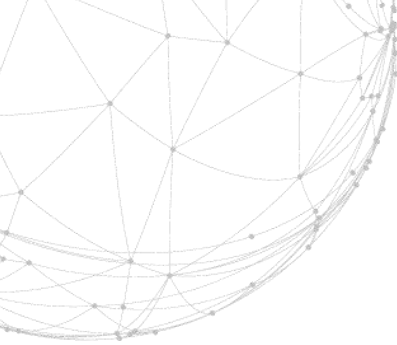
交互式证明系统：称一对交互机器 $\langle P, V \rangle$ （其中 P 和 V 分别为证明者和验证者）是语言 L 的交互式证明系统当它满足：

- 1) 机器 V 是多项式时间的；
- 2) 完全性 (Completeness) : $\forall x \in L$ ，那么存在诚实的证明者 P ，使得 V 与 P 交互后，输出 “ $x \in L$ ”；
- 3) 有效性 (Soundness) : $\forall x \notin L$ ，那么对于任意的证明者 P ， V 与 P 交互后，输出 “ $x \in L$ ” 的概率很小。

零知识证明系统可以认为是符合零知识要求的交互证明系统，必须满足以下四个属性：

- 1) 验证者无法从协议中获得任何信息；
- 2) 证明者无法欺骗验证者；
- 3) 验证者无法欺骗证明者；
- 4) 验证者无法同时伪装为其他零知识证明系统中的证明者。

零知识证明极其适合隐私保护业务场景，Zerocash 就是其典型的应用



案例。Zerocash 是首个使用零知识证明机制的区块链系统，它在比特币的基础上提供完全的支付保密性，能够自动隐藏区块链上所有交易的发送者、接收方以及金额等，并允许选择性披露查看密钥给他人来实现交易详情查询的访问授权。

TAK DATA LINK 引擎通过高度抽象零知识证明协议，在智能合约和去中心化应用底层提供零知识证明安全服务层，支撑 TAK DATA LINK 数据计算对隐私保护的需求，如零知识身份认证、交易数据保密等。

3.3 同态加密

同态加密的问题最早是由 Ron Rivest、Leonard Adleman 和 Michael L. Dertouzos 在 1978 年提出，而第一个全同态算法到 2009 年才被 Graig Gentry 证明。同态加密是指具有同态性质的公钥加密体制，允许对密文进行处理后仍然得到加密的结果，即对密文直接进行计算，同对明文进行计算后再加密，得到的结果是等价的。假设 $E(m)$ 表示 m 的加密密文，如果已知 $E(a)$ 、 $E(b)$ ，任何人都可以通过某种运算得到 $a \oplus b$ 的密文 $E(a \oplus b)$ 将这个过程表示为 $E(a) \otimes E(b)$ (\oplus 和 \otimes 分别表示明文空间和密文空间的二元运算符)，由此可以将同态性质笼统表示为：

$$E(a \oplus b) = E(a) \otimes E(b)$$

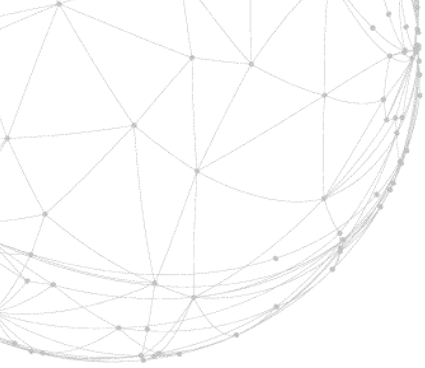
同态加密包括加法同态、减法同态、乘法同态、除法同态等。同时满足加法同态和乘法同态，意味着能完成全部运算，称为代数同态即全同态。

同态加密对于区块链时代的意义非常重大。目前，从安全的角度

讲，用户并不敢将敏感信息直接放到区块链上进行运算，如果有足够实用的同态加密技术，则大家就可以放心地使用区块链服务而不用担心信息的泄露。

尽管当前的同态加密尤其全同态加密技术需要消耗大量的计算时间，还远达不到大规模应用的水平，但对于数据规模较小且需求较迫切的业务场景，同态加密技术在智能合约层面的实现依然具有极强的现实意义。TAK DATA LINK 引擎在 OVM 底层原生支持同态加密运算符，实现加法同态算法 Paillier、Benaloh 以及乘法同态 RSA、ElGamal 等算法，便于快速构建隐私保护去中心化应用。





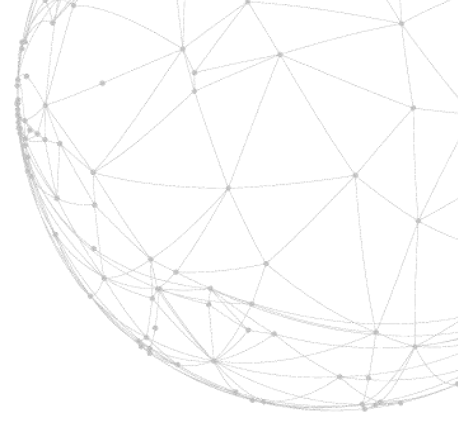
3.4 安全多方计算

传统方式下，为了能够完成某个计算任务，往往把所有参与者的数据都集中到某一个参与者进行集中计算。这种传统方式虽然能够解决一些问题，但如果所有参与者中没有任何一方能得到足够的信任去知道所有的输入，那么对于每个参与者的输入，即他的私有信息如何得到保护，就成了一个首要问题。这样的情形在现实生活中有很多，比如：

1) Alice 觉得自己可能患有某种遗传病。她知道 Bob 有一个包含各种疾病的 DNA 原型的数据库。Alice 当然可以把自己的 DNA 序列样本送交给 Bob，让 Bob 来诊断她是否患病。但是如果 Alice 关注自己的隐私，不想透露自己的 DNA 信息和诊断结果，那么上面的方法是无能为力的；

2) 经过一段时间的市场调研，A 公司决定在某些地区扩展市场份额以获得更大的盈利。但是 A 公司担心竞争对手 B 公司也正打算在那些地区扩展市场。简而言之，A 公司和 B 公司不想在相同的地区内竞争，所以他们想知道在他们的扩展计划里，是否有重叠的地区；而同时他们都不想泄露各自计划中地区的具体定位。因为这样的泄露会给双方带来巨大的损失，另一个公司 C 可能抢在 A 或 B 之前占领市场，或者房地产商在知道 A 或 B 对某块地感兴趣后会提高价位，所以他们需要一个途径来解决这个问题，同时保护自己的隐私。

以上两个例子的共同点是：两方或多方想在他们的私有输入的基础上进行合作计算，但是没有任何一方愿意泄露自己的输入给其他任何一方。问题是如何完成计算任务，同时保护了参与者的私有信息。该问题称为安全多方计算问题(Secure Multi-party Computation Problem)，简称为 SMC 问题。



安全多方计算由图灵奖得主 A.C.Yao 于上世纪 80 年代提出[13]，其主要目标是完成以下计算任务：在一个互相不信任的分布式网络中，两个或多个参与者能够在不泄露各自隐私数据的前提下合作计算某个约定函数并获得计算结果。安全多方计算在隐私保护的合作科学计算、隐私保护的数据库查询、隐私保护的数据挖掘、隐私保护的计算几何问题、隐私保护的数据分析等领域都有大量应用。

尽管 O. Goldreich、S. Micali 和 A. Wigderson 提出了密码学安全的可以计算任意函数的安全多方计算协议，但是由于使用了大量的零知识证明，协议参与者之间需要传输大量数据，其适用性受到很大限制。因此，提高安全多方计算协议的关键是针对特定场景设计特定的协议，TAK DATA LINK 引擎对安全数据计算的场景进行归类，高度抽象了多种安全多方计算协议并提供区块链计算模型下的底层解决方案，满足各个行业对隐私保护数据协作计算的需求。

3.5 复合决策闪电网络模型

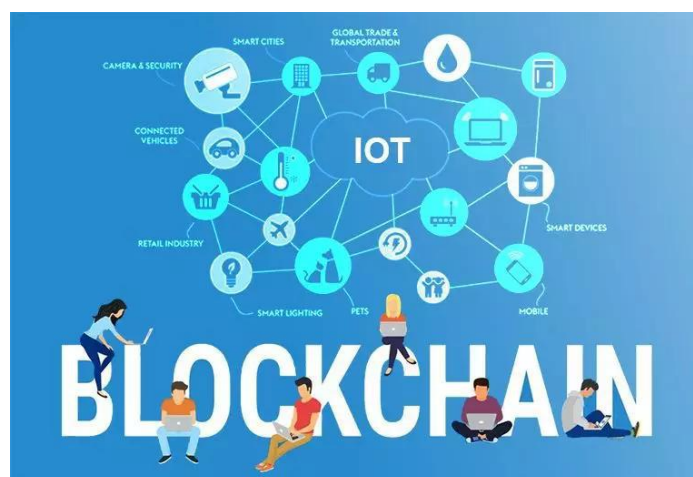
闪电网络是基于 BOLT 协议实现的分布式网络的统称，经典闪电网络设计只能实现加密货币的链外点对点交易，一旦涉及到法币交易的匹配就无能为力。

TAK DATA LINK 抽象出的复合决策闪电网络通过将一个决策层网络和一个执行层网络融合到同一套分布式系统中，共用节点的同时可以做到深度联动，让闪电网络更智能，从而实现交易请求与支付请求的匹配等高级路由功能，还可以通过规则设计让网络拓扑保持健康高效，避免出现中心化节点。

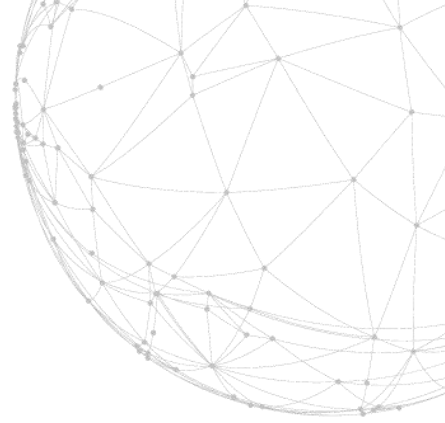
第四章

TAK DATA LINK 应用场景

物物相连，万物万联，物联网，就是实现我们梦想中科技世界的基础。科幻片中智能管家，从其低沉有礼貌的问好开始，每一步都是科技堆积，空调自动开启调温，灯光逐步亮起，提前点好的晚饭余温正好；当您出门时，无人汽车悄然打开车门，您设定好目的地，坐稳闭目休息，车内遮光并让您躺好舒适位置，直到温馨提醒先生，您到啦。当您在外时，管家收整房间，除尘打扫，并准备好您接下来的行程，以及衣物搭配。



这些就是物联网的未来一角，也是物联网最微弱的影响表现之一。TAK DATA LINK 从不低估物联网的巨大潜力，在工业，医疗，农业，汽车，物流，企业管理，城市建设，人类生活等各个方面，它都将以革命性的趋势去改变。这就是 TAK DATA LINK 选择物联网的原因。



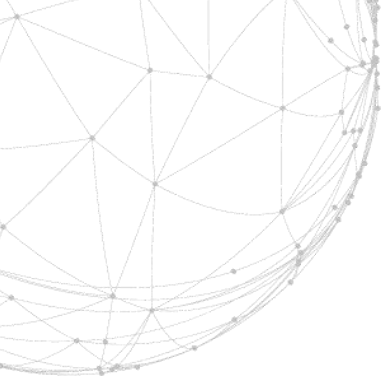
4.1 主要场景 - 数据开放平台

大数据是支撑现代企业发展的信息基础，谁拥有更多更广更全面的大数据，就会在商场战争中夺得一分天下，因此，TAK DATA LINK 万物互联数据开放平台的成立是必然。TAK DATA LINK 万物互联数据开放平台作为 TAK DATA LINK 生态中的 DAPP 应用方，其 DAPP TOKEN 是 TAK DATA LINK 系统中交易的重要基础。TAK DATA LINK 实现设备用户，设备厂商和数据购买方三方的平衡，各有所得，良心循环，使 TAK DATA LINK 数据交易平台可持续性稳定发展。

■ 行业级万物互联数据开放平台

行业级万物互联数据开放平台，是 TAK DATA LINK（塔克链）的基础，也是最核心的应用平台。基于智能合约：设备，对象，数据，逻辑方法，凭证等可以完美的在 TAK DATA LINK 上进行组织和执行，并为 TAK DATA LINK 其他应用提供运行环境和执行系统。

作为全球首家区块链平台将物联网设备智能合约投入实用场景，使现实生活合同去纸化，签订合同无人化，对于时间精力，人力物力的巨大节省，TAK DATA LINK 拥有无可比拟的前景。对于 TAK DATA LINK 支持多种不同的数据类型，以及多样化物联网设备的数据采集，更支持超小额支付和超低手续费交易，方便小额支付，满足数据碎片化的交易需求，这更是手机支付在区块链行业的展开发展，是货币支付多样化的体验。



4.2 应用示例 - 健康大数据

从 2008 年到现在，随着医疗数据从纸质记录向电子记录迁移，信息化的医疗数据、医疗研究数据、病人特征数据以及移动设备、社交网络和传感器产生的医疗健康相关的数据为医疗健康从业人员提供了新的思路，利用大数据技术可以从中发现潜在的关系、模式，从而帮助医师提高诊断精度、预测治疗效果、降低医疗成本，帮助医药公司发现潜在的药物不良反应、帮助公共卫生部门及时发现潜在的流行病。

这种现状主要来源于以下几个方面的发展：

- 1) 病人需要一个更好的端到端的医疗服务体验
- 2) 医疗卫生领域的低数据需求的开发和研究已经越来越少
- 3) 病人们对于医疗数据的安全和隐私保护等问题越来越关注

针对上面的问题，基于 TAK DATA LINK 系统可以开发出全新的解决方案。

以去中心化的结构（高效率、低成本），做到数据信息完整透明（符合法律和便于追踪），分布式记账与存储（高容错性），智能合约可编程（没有负担的进化模型），全球一个数据库（高包容性业务模式），透明世界背后的匿名性（保护隐私）。由于这些特点，区块链+物联网的技术在医疗信息化领域的核心应用优势十分显著：

- 去中心化的分布式结构应用于现实中可节省大量的信息收

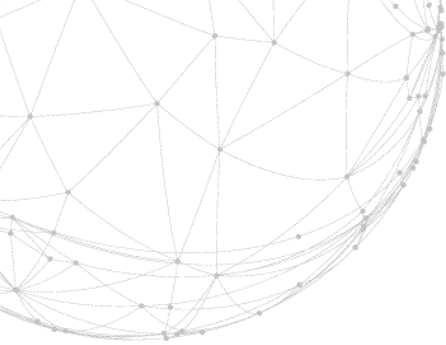
集成本；

- 不可篡改的时间特征可解决数据追踪与信息防伪问题；
- 安全的信任机制可解决现今医疗信息化技术的安全认证缺陷；
- 物联网设备信息灵活的可编程特性可帮助医院建立拓展应用。

项目应用案例：智能床垫

以智能床垫为例，智能床垫可以实时采集人体的生命体征，包括心率、脉搏、呼吸频率、睡眠状态、体动次数等等，遇到异常情况可以在手机端推送警告信息。同时这个床垫也可以作为一个采集用户健康数据的设备，如果用户量达到一定的量级，可以形成极具价值的数据库，作为医药制造业、社会保险业、公共卫生系统等行业参考的重要数据依据。

而在传统模式中，数据的收集是一个非常繁琐并且费用高昂的过程。通过 TAK DATA LINK 系统可以构建一个在隐私保护的前提下的去中心化的数据交换场所，TAK DATA LINK 通过智能床垫对接系统所开放的数据池，实现数据分享，出售相关的数据给相关信息需求方。



4.3 应用示例 - 汽车物联网

■ 汽车信息收集

通过物联网设备采集汽车行驶状态、运动轨迹、驾驶员驾驶习惯、汽车各个系统的技术参数等信息，可以作为汽车制造业、汽车保险业的重要参考数据。

物联网设备需要不停地进行车辆信息收集与沟通，车辆与车辆之间的信息交流，车辆和基础设施之间的信息交流，车辆和其它设备之间的信息交流，而且这种信息交流要求快捷、安全。“区块链+物联网”给汽车制造商提供了一个很好的解决方案。

通过 GPS、RFID、传感器、摄像头等装置，TAK DATA LINK（塔克链）可以完成对车辆自身环境和状态信息的采集。通过 TAK DATA LINK（塔克链）的边缘计算机制，实现数据在用户端的处理分析，从而总结出适用于汽车行业的价值数据；

基于区块链技术的云计算能够很好的存进加密、传输、分发、和存储物联网汽车每分钟产生的数据。毫无疑问，汽车制造商将会转向区块链技术，将其作为物联网汽车进行数据交换的支柱。

4.4 其他应用：农业 & 工业

TAK DATA LINK 不仅仅可以用于上述的场景，开发者可以针对 TAK DATA LINK 区块链或者 TAK DATA LINK 引擎开发各种去中心化的应用。根据使用场景，开发者还可以自由选择所开发的应用是否需要特别的隐私

保护和数据分析处理，如农业&工业等。

■ 农业物联网

即通过各种仪器仪表实时显示或作为自动控制的参变量参与到自动控制中的物联网。可以为温室精准调控提供科学依据，达到增产、改善品质、调节生长周期、提高经济效益的目的。农业物联网一般应用是将大量的传感器节点构成监控网络，通过各种传感器采集信息，以帮助农民及时发现问题，并且准确地确定发生问题的位置，这样农业将逐渐地从以人力为中心、依赖于孤立机械的生产模式转向以信息和软件为中心的生产模式，从而大量使用各种自动化、智能化、远程控制的生产设备。


区块链技术为物联网提供了点对点直接互联的方式进行数据传输，整个物联网解决方案不需要引入大型数据中心进行数据同步和管理控制，包括数据采集、指令发送和软件更新等操作都可以通过区块链的网络进行传输。

■ 工业物联网

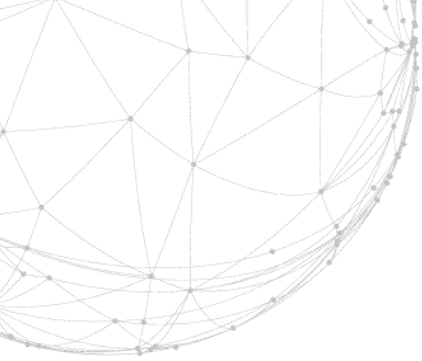
工业物联网是工业 4.0 转型，不是 3.0 时代 MES，ERP，SCM，PLM，CRM 等系统的简单集成或更新换代，而是借助新技术(物联网、大数据等)在多个维度对企业及价值链的革命性整合、重塑与创新。

工业生产中的跨组织数据互信全部通过“区块链+物联网”来完成，订单信息、操作信息和历史事务等全部记录在链上，分布式存储、不可篡改，所有产品的溯源和管理将更加安全便捷。

实现工厂内系统、设备与机器间在物联网的基础上互联互通。逐步



达到全企业内所有工厂间运营、监控和管理决策的完整联系。由此激发主要生产力的提升，并增强运营决策灵活性。最终实现企业全方位供应链的互联互通。包含上游所有各级供应商的相关系统(系统内包含相关设备的物联网信息)以及下游各渠道的系统终端或设备。以此增加生产力，提升效率与灵活性。



第五章 代币分配计划

5.1 TAK DATA LINK 代币

为了防止恶意用户对 TAK DATA LINK 的滥用以及维护系统的安全性和稳定性，所有希望使用系统的用户（转移 TAK DATA LINK 代币或者使用 TAK DATA LINK 来进行数据运算）都需要支付一定的手续费。

TAK DATA LINK 作为平台的自有代币，发行总量上限为 2,000,000,000 枚，在首次发行完成后不再增发。

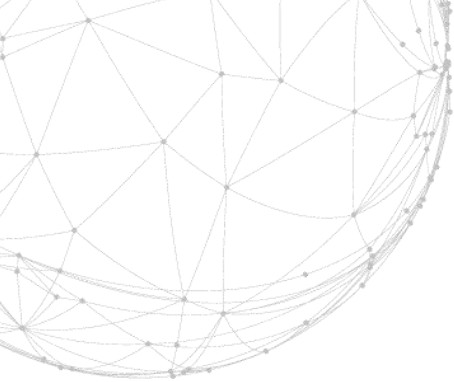
- 代币名称：TAK DATA LINK Token
- 简称：TAK
- 发行技术：ERC20

5.2 代币分配方案

类别	数量	分配方案
发展基金	1,400,000,000 枚	用于项目后续的市场推广和应用落地
用户激励	200,000,000 枚	用于激励用户进行下载、存币、消费等行为
研发团队	200,000,000 枚	创始团队成员早期持有每年释放不超 20%
早期投资人	100,000,000 枚	对早期投资人在项目发展的过程中在财力、资源、人力辅助方面所做的贡献进行奖励！
机构投资者	100,000,000 枚	对于机构合作者在项目发展过程中所作的战略合作和远期规划进行奖励！
TAK 流通及锁仓机制	2,000,000,000 枚	其中 14 亿枚作为发展基金锁仓，不流入二级市场。流通总量为 6 亿枚，研发团队每年释放不超 20%，早起投资者及机构根据项目实际运营情况，每个月释放量不超过 20%。

5.3 发行计划

日期	工作
2019/07/25	白皮书初稿，向潜在投资人演示
2019/08/22	白皮书发布
2019/10/26	开放用户注册和注册送币活动
2019/11/12	平台正式上线，TAK 代币交易上线



第六章 团队和基金会

团队成员	岗位介绍
(1) 约翰·查尔斯	TAK DATA LINK 塔克链团队发起人
	美国 IT Summa 的创办人以及 10 年首席执行官经验。自 2015 年到 2017 年 2 月，共操盘 6 个区块链项目，自 2017 年 3 月起脱离持有的所有区块链项目，全身投入并启动 TAK DATA LINK 塔克链的区块链项目。
(2) 阿尔·丹尼列夫	技术工程师
	俄罗斯软件工程师在商业开发方面有 10 多年经验。参与并管理俄罗斯领先品牌软件开发：Sberbank、RZD、飞机建造公司。构建公司区块链开源库的核心开发人员：exonum-bootstrap，参与项目开发并担任顾问：后离开加入 TAK DATA LINK 塔克链团队，目前为 TAK DATA LINK 塔克链平台及技术主力工程师。

(3) 尼克拉维	核心算法工程师
	<p>基于全球支付的区块链技术及金融契约逻辑的核心定位就是由 Nicolaw 在发起人的理念基础上完善而来的,目前负责 TAK DATA LINK 塔克链复杂的算法制定,同时对平台规则进行测试与运算。</p>

美国富达投资集团

富达投资集团成立于 1946 年,其创始人是爱德华 C. 约翰逊二世,总部设在美国波士顿。公司成立的最初承诺为:每天更加勤奋+更加机敏的工作,帮助小额投资者达到他们的目标。经过半个多世纪的发展,富达集团积累了丰富的投资管理经验,能够为客户提供便捷、专业的服务,已经由纯粹的共同基金公司发展成为一个多元化的金融服务公司,向客户提供包括基金管理、信托以及全球经纪服务在内的全面服务。它是第一家推出“货币市场共同基金账户”的基金管理公司。富达在全球管理的资产达 2,900 亿美元,客户遍布亚太区、欧洲、中东和南美洲 25 个国家。服务的客户包括中央银行、主权财富基金、大型机构、金融企业、保险公司、财富管理公司及个人投资者。除资产管理外,亦在多个国家为雇主福利计划、投资顾问和个人客户提供投资行政管理及指引服务。截至 2016 年 09 月,负责行政管理的资产金额达 850 亿美元。

美国富达投资集团 (Fidelity Investment Group) 目前全球最大的专业基金公司。富达投资集团的分支机构遍布全球 15 个国家和地区。目前为全球 1200 多万位投资者管理的资产高达 1 万亿美元,占美国共同基金总额的 1/8,倍受投资者和基金市场的关注。富达投资集

团注重"自下而上"的选股策略，善于发掘股价被低估或者股价落后于市场涨幅、具有长期投资潜力的公司的股票，因此其基金经理的作用非常重要，而且富达集团也拥有许多世界知名的基金经理，彼得·林奇(Peter Lynch)就是其中最为出名的一个，他管理麦哲伦基金的十三年里，年平均收益率为 29%，而同期标准普尔 500 指数的涨幅平均只为 14%。此后富达集团也出现了许多杰出的基金管理经理，1998 年，它有 4 名基金经理人的表现列于最佳基金经理的前 20 名。

国际金融财经业务中心

所有国际金融、保险业、零售银行业和商业银行业的运作皆由该中心管理。其金融业务划分三大地区：欧洲和拉丁美洲、北美洲、亚澳地区。银行业务则由中心统一管理。

企业及资本市场中心

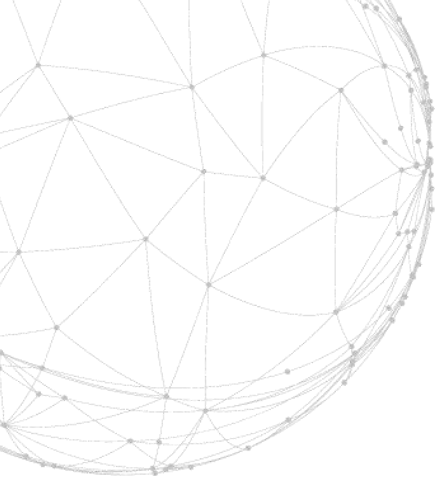
所有国际货币和资本市场管理都由该中心进行。包括国际银行网络以及金融产品、金融贸易、销售、投资银行、企业银行、风险管理及调研的各项业务。

大数据资产管理中心

该中心承担企业投资者的资产和账目管理、提供个人国际银行服务以及基金会的金融业务的资产管理。房地产业务和信托业务也属于这个部门管理。该部门同时管理基金会各个公司的投资基金。

区块链发展研究中心

专注于区块链在实体经济中的发展，其中以物联网、大数据的融合为突破点，实现长效发展。基金会区块链发展研究中心，汇集了全球顶级金融、物联网和区块链底层技术专家，正在构建塔克区块链生态系统，并推动全球落地。



第七章 免责声明

除本白皮书所明确载明的之外，TAK DATA LINK 团队不对 TAK DATA LINK 或项目代币 TAK 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 TAK DATA LINK 的售卖计划及购买 TAK 的行为均基于其自己本身对 TAK DATA LINK 和 TAK 的知识和本白皮书的信息。在无损于前述内容的普适性的前提下，所有参与者将在 TAKE DATA LINK 项目启动之后按现状接受 TAK DATA LINK，无论其技术规格、参数、性能或功能等。

TAK DATA LINK 在此明确不予承认和拒绝承担下述责任：

（1）任何人在购买 TAK 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；

（2）任何人在购买 TAK 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付款或无法提取 TAK；

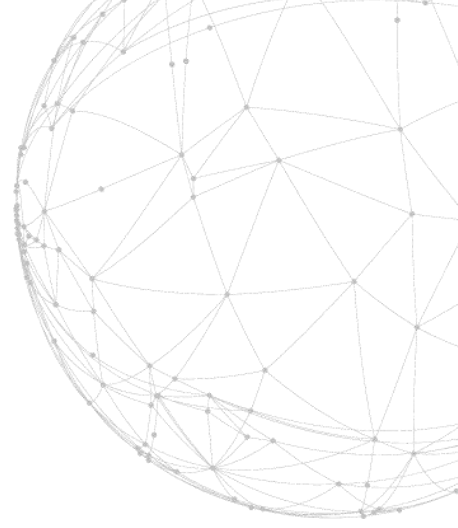
（3）由于任何原因 TAK 的售卖计划被放弃；

（4）TAK DATA LINK 的开发失败或被放弃，以及因此导致的无法交付 TAK；

（5）TAK DATA LINK 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；

（6）TAK DATA LINK 源代码的错误、瑕疵、缺陷或其他问题；

（7）TAK DATA LINK 或以太坊区块链的故障、崩溃、瘫痪、回滚或硬分叉；



(8) TAK DATA LINK 或 TAK 未能实现任何特定功能或不适合任何特定用途；

(9) 对代币售卖所募集的资金的使用；

(10) 未能及时且完整的披露关于 TAK DATA LINK 开发的信息；

(11) 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥（尤其是其使用的 TAK 钱包的私钥）；

(12) TAK 的第三方售卖平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业；

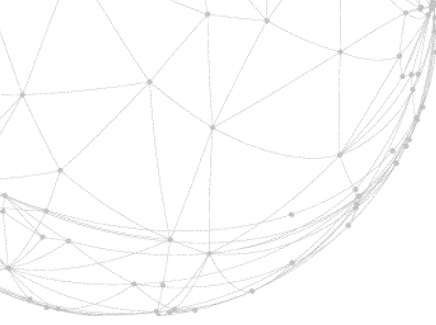
(13) 任何人与第三方售卖平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；

(14) 任何人对 TAK 的交易或投机行为；

(15) TAK 在任何交易所的上市或退市；

(16) TAK 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；

(17) 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致的损害、损失、索赔、责任、惩罚、成本或其他负面影响。



第八章 参考文献

- [1] Nakamoto, SaTAK DATA LINKhi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.
- [2] Vukolić, Marko. "The Byzantine empire in the intercloud." ACM SIGACT News 41.3 (2010): 105-111.
- [3] Duyvendak, Jan Julius Lodewijk. The Book of Lord Shang. Probsthain, 1928.
- [4] Constine, Josh. "Facebook now has 2 billion monthly users... and responsibility." TechCrunch, TechCrunch, 27 June 2017, techcrunch.com/2017/06/27/facebook-2-billion-users/. Accessed 17 July 2017.
- [5] Levy, Steven. Crypto: secrecy and privacy in the new code war. London, Penguin, 2002.
- [6] Antonopoulos, Andreas M. "Blockchain vs. Bullshit: Thoughts on the Future of Money."
- [7] Stephenson, Neal, and Jean Bonnefoy. Cryptonomicon. Paris: Payot & Rivages, 2000. Print.
- [8] Micali, Silvio. "ALGORAND: the efficient and democratic ledger." arXiv preprint arXiv: 1607.01341 (2016).
- [9] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." OSDI. Vol. 99. 1999.
- [10] Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptography"

LINKsystems," Communications of the ACM, Vol. 21, No 2, pp.120-126, 1978.

[11]Gentry C. Computing arbitrary functions of encrypted data[J]. Communications of the ACM, 2010, 53(3): 97-105.

[12]Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. "The knowledge complexity of interactive proof systems." SIAM Journal on computing 18.1 (1989): 186-208.

[13]Yao, Andrew C. "Protocols for secure computations." Foundations of Computer Science, 1982.SFCS'08. 23rd Annual Symposium on. IEEE, 1982.

[14]Goldreich, Oded, Silvio Micali, and Avi Wigderson. "How to play any mental game."Proceedings of the nineteenth annual ACM symposium on Theory of computing. ACM, 1987.

[15]Turner, Michael A. " Predicting Financial Account Delinquencies with Utility and Telecom Payment Data." PERC Results and Solutions. 2015.

