Vedacoin 加密货币
中文版白皮书 1.0 版本

前言

区块链技术给数字货币经济时代带来了巨变的曙光。

这种巨变在互联网近 50 年的历史上曾发生过两次。第一次巨变是全球性的互联网自 1969 年阿帕网（Advanced Research Projects Agency Network，ARPANET，美国国防部高级研究计划局组建的计算机网，又称 ARPA 网。现在的 Internet 是在 APRA 的基础上才建立起来的）诞生以来，全世界主流国家逐渐接入互联网，开启了全球互联网的征程。 第二次巨变是全球性的应用，自 1989 年万维网论文问世后，互联网应用全面开花，实现了应用全球爆发。

第三次巨变正在酝酿。2009 年比特币诞生是个标志性事件。在区块链技术的支持下，比特币打破了传统纸币的“暗黑”盒子。作为实体的纸币的流通是看不见的，没有人知道一张纸币从哪里来到哪去，而区块链却可以让数字货币的每一笔动向都清清楚楚有“链”可查，同时还可以保护参与者的隐私。人们发现区块链的意义在于可以构建一个更加可靠的互联网， 这样才能从根本上解决价值交换与转移中存在的欺诈问题和寻租现象。越来越多的人相信，随着区块链技术的普及，数字经济将会更加真实可信，经济社会由此变得更加公正和透明。

区块链技术具备有简化流程，降低一些不必要的交易成本及制度性成本。这种能力应用于许多社会领域中，对于改善当前低迷的经济环境更有现实意义。

区块链的诞生，标志着人类开始构建真正可以信任的互联网。通过梳理区块链的兴起和发展可以发现，区块链引人关注之处在于，能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开信息又保护隐私，既共同决策又保护个体权益，这种机制提高了价值交互的效率并降低了成本。 从经济学意义来看，区块链创造的这种新的价值交互范式基于“去中心化”，但这并非意味着传统社会里各种“中心”的完全消失，未来区块链将会出现多种区块链体系并存，以联盟链、私有链和混合链、公有链为主。

公有链

公有链是指全世界任何人都可读取、发送交易且交易能获得有效确认的、也可以参与其中共识过程的区块链。

公有链特点：

1、保护用户免受开发者的影响，在公有链中程序开发者无权干涉用户，区块链可以保护其用户；

2、访问门槛低，任何人都可以访问，只要有一台能够联网的计算机就能够满足基本的访问条件；

3、所有数据默认公开，公有链中的每个参与者可以看到整个分布式账本的所有交易记录。

私有链

私有链是指其写入权限仅在一个组织手里的区块链，目的是对读取权限或者对外开放权限进行限制。

私有链特点：

1、交易速度非常之快一个私有链的交易速度可以比任何其他的区块链都快，甚至接近了并不是一个区块链的常规数据库的速度。这是因为就算少量的节点也都具有很高的信任度，并不需要每个节点来验证一个交易。

2、给隐私更好的保障私有链使得在那个区块链上的数据隐私政策像在另一个数据库中似的完全一致;不用处理访问权限和使用所有的老办法，但至少说，这个数据不会公开地被拥有网络连接的任何人获得。

3、交易成本大幅降低甚至为零私有链上可以进行完全免费或者至少说是非常廉价的交易。如果一个实体机构控制和处理所有的交易，那么他们就不再需要为工作而收取费用。

4、有助于保护基本的产品不被破坏，银行和传统的金融机构使用私有链可以保证它们的既有利益，以至原有的生态系统不被破坏。

联盟链

联盟链是指其共识过程受到预选节点控制的区块链。只针对某个特定群体的成员和有限的第三方，其内部指定多个预选节点为记账人，每个块的生成由所有的预选节点共同决定。

联盟链的特点：

1、是交易成本更便宜。交易只需被几个受信的高算力节点验证就可以了，而无需全网确认。

2、是节点可以很好地连接，故障可以迅速通过人工干预来修复，并允许使用共识算法减少区块时间，从而更快完成交易。

3、是如果读取权限受到限制，可以提供更好的隐私保护。四是更灵活，如果需要的话，运行私有区块链的共同体或公司可以很容易地修改该区块链的规则，还原交易，修改余额等。

1.0 区块链的特征和类型

区块链作为一项创新技术体系，以分布式账本、加密授权技术、共识机制和智能合约等技术为主轴，形成了由技术直接支撑的几个重要特征。

A 去中心化

去中心化是区块链最基本的特征，意味着区块链应用不依赖于中心化的机构，实现了数据的分布式记录、存储与更新。由于使用分布式存储和算力，不存在中心化的硬件或管理机构，全网节点的权利和义务等，系统中的数据本质是由全网节点共同维护的。在传统的中心化网络中，对一个中心节点实行攻击即可破坏整个系统，而在一个去中心化的区块链网络中，攻击某个节点无法控制或破坏整个网络，掌握网内超过 51%的节点也只是获得控制权的开始而已。

B 透明性

区块链系统的数据记录对全网节点是透明的，数据记录的更新操作对全网也是透明的，这是区块链系统值得信任的基础。由于区块链系统使用开源的程序、开放的规则和高参与度，区块链的数据记录和运行规则可以被全网节点审查、追溯，具有很高的透明度。

C 开放性

区块链的开放性是指，除数据直接相关各方的私有信息被加密外，区块链的所有数据对所有人公开（具有特殊权限要求的区块链系统除外）。任何人或参与节点都可以通过公开的接口查询区块链的数据记录或者开发相关应用，因此整个系统是开放的。

***D* 自治性**

区块链采用基于协商一致的规范和协议，使整个系统中的所有节点能够在去信任的环境下自由安全地交换、记录以及更新数据，把对个人或机构的信任改成对体系的信任,任何人为的干预都将不起作用。

***E* 不可篡改性**

区块链系统的信息一旦经过验证并添加至区块链后，就会永久存储，无法更改（除具有特殊更改需求的私有区块链等系统外）。除非能够同时控制系统中超过 51% 的节点，否则单个节点上对区块中记录的修改是无效的，因此区块链的数据的稳定性和可靠性极高。

***F* 匿名性**

区块链系统中虽然所有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仍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。由于节点之间的数据交换遵循固定且预知的算法，因而其数据的交互无需双方存在相互信任的前提，可以通过双方地址而非身份的方式进行，因此交易双方无须通过公开身份的方式让对方产生信任。

1.0.1 区块链的核心技术

随着科技的发展，区块链技术从最初的版本从而具有更多的技术特点，其最核心的技术表现在以下几个方面：

分布式账本

分布式账本技术 DLT(DistributedLedgerTechnology)本质上是一种可以在多个网络节点、多个物理地址或者多个组织构成的网络中进行数据分享、同步和复制的去中心化数据存储技术。

相较于传统的分布式存储系统，分布式账本技术主要具备两种不同的特征：

传统分布式存储系统执行受某一中心节点或权威机构控制的数据管理机制，分布式账本往往基于一定的共识规则，采用多方决策、共同维护的方式进行数据的存

储、复制等操作。面对互联网数据的爆炸性增长，当前由单一中心组织构建数据管理系统的方式正受到更多的挑战，服务方不得不持续追加投资构建大型数据中心。

共识机制

区块链是一个历史可追溯、不可篡改，解决多方互信问题的分布式（去中心化）系统。分布式系统必然面临着一致性问题，而解决一致性问题的过程我们称之为共识。

分布式系统的共识达成需要依赖可靠的共识算法，共识算法通常解决的是分布式系统中由哪个节点发起提案，以及其他节点如何就这个提案达成一致的问题。我们根据传统分布式系统与区块链系统间的区别，将共识算法分为可信节点间的共识算法与不可信节点间的共识算法。前者已经被深入研究，并且在现在流行的分布式系统中广泛应用，其中 Paxos 和 Raft 及其相应变种算法最为著名。对于后者，虽然也早被研究，但直到近年区块链技术发展如火如荼，相关共识算法才得到大量应用。而根据应用场景的不同，后者又分为以 PoW（ProofofWork）和 PoS（ProofofStake）等算法为代表的适用于公链的共识算法。

密码学

信息安全及密码学技术，是整个信息技术的基石。在区块链中，也大量使用了现代信息安全和密码学的技术成果，主要包括：哈希算法、对称加密、非对称加密、数字签名、数字证书等。此外，区块链中还应用了现代密码学最新的研究成果，包括同态加密、零知识证明等，在区块链分布式账本公开的情况下，最大限度地提供隐私保护能力。这方面的技术，还在不断发展完善中。区块链安全是一个系统工程，系统配置及用户权限、组件安全性、用户界面、网络入侵检测和防攻击能力等，都会影响最终区块链系统的安全性和可靠性。区块链系统在实际构建过程中，应当在满足用户要求的前提下，在安全性、系统构建成本以及易用性等维度，取得一个合理的平衡。

智能合约

智能合约（Smartcontract）是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易。这些交易可追踪且不可逆转。其目的是提供优于传统合同方法的安全，并减少与合同相关的其他

交易成本。随着区块链技术的出现与成熟，智能合约作为区块链及未来互联网合约的重要研究方向得以快速发展。

基于区块链的智能合约包括事件处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约，数据的状态处理在合约中完成。事件信息传入智能合约后，触发智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状态机根据预设信息选择合约动作的自动执行。因此，智能合约作为一种计算机技术，不仅能够有效地对信息进行处理，而且能够保证合约双方在不必引入第三方权威机构的条件下，强制履行合约，避免了违约行为的出现。

1.1 区块链——从摆脱第三方制约起步

起初，人们将区块链视为点对点网络上的一个分类账本，每笔交易自诞生起，所有转账、交易都将被记录在“区块”上，区块与区块之间首尾相连，形成链式的结构，并且公布给该网络上所有的节点，节点之间通过共识机制形成共识。节点成员可根据权限查阅相关交易记录，但任何单个节点都无法轻易控制和更改整个网络的数据。

这种设计来源于 2008 年中本聪发表的论文《比特币一种点对点的电子现金系统》。文章提出，希望可以创建一套新型的电子支付系统，这套系统“基于密码学原理而不是基于信用，使得任何达成一致的双方能够直接进行支付，从而不需要第三方中介参与”。 该论文催生了比特币，标志着人类社会的货币体系向前迈出了一大步。比特币采用了公开的分布式账本的设计思路，摆脱了第三方机构的制约。 比特币的匿名性对传统金融监管提出了挑战，比特币是一种巨大的实验。

1.2 从比特币跃迁到区块链

区块链的诞生，标志着人类开始构建真正的信任互联网。 有一种新的观点认为，区块链技术可以构建一个高效可靠的价值传输系统，推动互联网成为构建社会信任的网络基础设施，实现价值的有效传递，我们注意到， 区块链提供了一种新型的社会信任机制，为数字经济的发展奠定了新基石，“区块链+”应用创新，昭示着产业创新和公共服务的新方向。 多个发达国家认识到区块链技术在公共

服务和社会机制优化上存在着巨大的应用前景，开始设计区块链的发展道路。

1.3 愿景

构建 Web3.0 互联网流量来源，分布式的流量引擎。

1.3.1 背景介绍

2008 年，中本聪提出的比特币和区块链打开了新一代互联网——Web3.0 的大门。从比特币出现至今，区块链应用已经呈现出多种不同的形态。从分布式账本，到分布式计算平台，再到各类金融工具，区块链正在用一种去中心化的方式逐步解决越来越多的问题。 虽然当前的区块链应用普遍执行效率较低，因此只能在一定层面作为账本进行数据的保存，短时期内无法对外界提供计算能力。但是按我们的预期，随着区块链基础设施的逐步发展，运行在区块链上的计算能力将逐步增强。

web 的发展

web 1.0:基本 HTML,e-mails

web 2.0:信息与交互式（中心化）

web 3.0:去中心化，隐私和安全（以用户为中心）

Web 1.0

这些网站是用 HTML、CSS、JavaScript 创建的，互联网上没有很多的网络应用程序，没有互动，也无法播放音乐和视频。

Web 2.0

web2.0 与 web1.0 相比发生了重大变化。它始于人人喜爱的交互界面和内容，各种流行媒体消费平台的兴起，如优酷、微博、YouTube 等。任何人都可以分享信息。

Web 3.0

web3.0 更关注以人为本，将 web 体验向前推进了一步。它将更倾向于保护个人隐私，反对大机构的控制。是一个更加透明和公平的网络，每个人都可以参与其中，而不必担心隐私和安全的的损失。随着技术的发展，web 正在从 2.0 转变到 3.0 时代。人工智能、大数据等技术将使提供比以往更多的个人网络体验。

互联网正在开始向 Web3.0 过渡

Web3.0 的目标就是在重塑互联网去中心化初心的同时，提供诸如价值转移、透明开放、高度信任、隐私保护以及互操作性等特性。 互联网上信息流动的过程中，用户兴趣点和注意力的迁移称为互联网流量。早期互联网和网络的倡导者都支持去中心化、互操作性和开放性。然而，随着时间的推移，互联网流量逐渐被集中以及控制在少数人的手中。在这种情况下，互联网流量生态环境不断恶化，中间成本不断增加、用户隐私数据被侵犯、恶意欺诈行为泛滥等，这导致参与方的利益都受到不同程度的损害。

互联网广告当前正在走向急速下降的趋势，核心原因有几个方面：

1：互联网的发展趋势造成存量市场新增用户量降低，新增应用无论是互联网网站还是移动 app 都在争夺已存在市场，造成用户选择减少，需求降低。

2:中间商对于广告的采购成本 急剧增加，头部市场过于强势造成头部流量来源议价能力过强，长尾流量采购成本过高，资金占压严重。

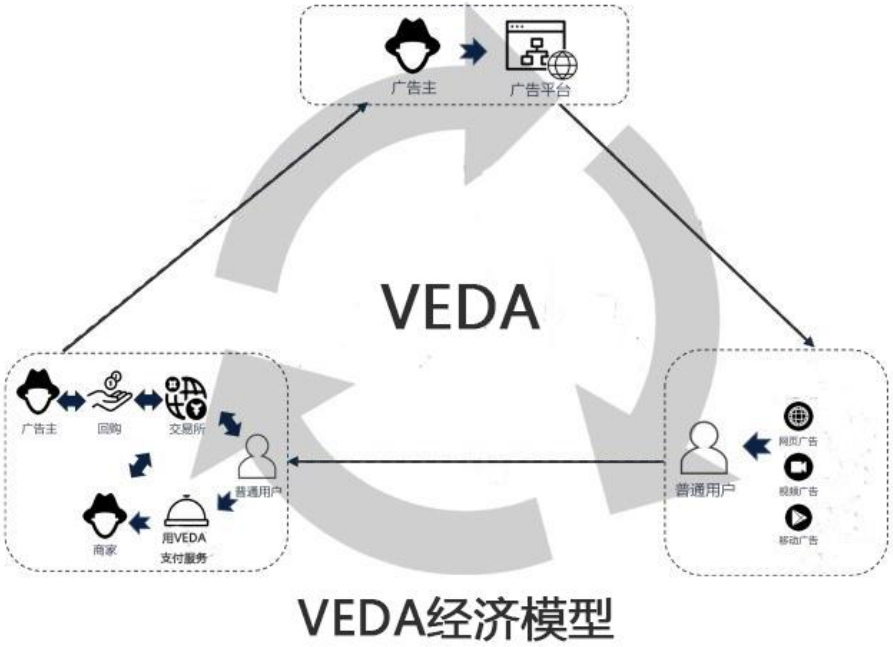
3：市场恶劣的情况下，流量数据造假扣量、内部回扣等黑幕在互联网广告行业常有发生。

4：流量来源方为了拉低成本，不惜进行难以追踪的作弊造成流量质量逐年降低为了实现精准匹配提高广告价格，用户隐私被严重侵袭。

5：用户体验恶劣，广告平台提供的 SDK 使得多数应用强制用户看广告后才能继续使用实质功能，平台为了实现利益最大化，往往不考虑用户的体验感。在搜索方面，用户搜索问题搜出来的答案页面广告就占三分之一，使得广告在用户层面口碑极差，极大拉低用户留存率。

面向互联网的发展趋势，我们计划实现一个在区块链上进行去中心化互联网流量交换的引擎，并以主链加密货币——Vedacoin 作为经济支撑，实现其中的流量交易服务。

VEDA 网络经济闭环设计，如下图：



VEDA经济模型

在我们的经济系统里：商家购买 VEDA，投放广告->用户在各种媒介中浏览得到 VEDA->用户把得到的 VEDA 用于支付有偿服务和商品或者在交易所套现->商家回购 VEDA 用于投放广告->依此持续循环……

1.4：目前互联网流量环境

互联网的存在基础是内容的获取，其次才是沟通和交流。在以上的过程中，用户兴趣点和注意力的迁移就转变为流量。研究表明，用户的注意力是很容易被引导和迁移的，因此拥有流量的控制权，在过去的二三十年里，全球的互联网经历了巨大的发展。互联网的基础架构自出现至今，始终是基于“浏览器 - 服务器”和“客户端 - 服务器”的形态。在传统 PC 互联网时代，各类浏览器作为流量的基本入口，广告通过 URL 进行流量的跳转及统计分析。到了移动互联网时代，两大巨头 Apple 和 Google 占据了移动互联网唯一的两个操作系统入口：iOS 和 Android，形成了实质性的垄断。移动互联网的流量也从之前浏览器的 URL 跳转，变为只能通过激励的方式引导用户下载 App。巨头们通过此种方式，迅速抢占流量入口，并迅速建立起基于广告流量的商业模式。

过去的这二十年里，逐步有越来越多的公司 进行互联网流量的引流和输出，第

三方流量平台虽然不像巨头那样可以从更高维度进行流量的整合，但是也在一定层面对流量的价格和倾向性进行一定程度的控制，可以通过拉高利润率，再通过洗流量的方式进行推广和销售。 随着互联网注意力的逐步迁移，市场上还将出现更多的全新产品和服务，也能够提供更多的流量来源。互联网的流量和注意力将作为永久的话题，无论技术形态和业务形态如何改变，都会始终以不同的形式存在。

1.4.1 流量被巨头把持

目前，多个互联网传统巨头的商业来源都是互联网广告。互联网广告是推动用户流量的一种形态， 但不是唯一形态。 流量应当像流动的水，允许用户根据自己真正的兴趣进行随意流动，而不应当被限制在单一产品或者单一服务中。而互联网巨头将商业模式构建在互联网广告之上，实际对用户的潜在伤害是巨大的。互联网巨头拥有的海量数据能力，意味着用户是可以被分析的，用户的注意力是可以被操控的。这些利益都属于用户的基础利益，而巨头商业的目的是为股东负责，因此，对利益的把持和操纵造就了今天的互联网广告环境。

在这种环境下，用户隐私难以被保护，某一些机构平台为了利益倒卖用户的个人信息，导致了用户经常被各种电话信息骚扰。

1.5 VEDA 希望解决的问题

流量”这一词，本身就是分散的。互联网上成千上万的用户，在不同服务、内容之间的跳转，本质是分散的，去中心化的，应当以用户真正的意志为转移，而不应被操控。传统互联网存在的种种限制让流量的控制权逐步汇聚到了巨头手中。区块链的发展，必然和以往的行业发展一样，会经历递进的过程。流量作为互联网的基础， 在区块链的去中心化时代应当首先被解决。发展的必然路径将是从流量去中心化先行，逐步带动各类区块链基础设施，进而再带动基础应用。 未来 10 年，互联网的应用都将向去中心化转变，VEDA 有机会搭建和传统互联网广告模式完全不同的全新流量推动模式，让用户也参与其中，不会被单一商业力量操纵，系统的整体设计并非为中心化利益服务，而是使得参与在其中的各个角色

共赢。 VEDA 不仅仅能够作为一个基础的流量平台，除了作为最佳的应用示范，引擎基础链本身还将作为一个流量引擎，使得其他服务商也可以在其上构建自己的流量应用。

1.6 分配方案

	Veda币
中文名	吠陀硬币
英文名	Vedacoin
简　称	VEDA
共　识	PoS
供应量	1.4亿
区块时间	60秒
区块大小	1M
	分配方案
挖　矿	1亿
基金会	2000万
创世者	1000万
社区经费	500万
开发团队	500万

免责条款

本白皮书中的所有内容仅供参考，不得依赖本文中的任何陈述作为任何决策的前提。本白皮书描述的信息并非完全详尽，也不包含构成合同关系的内容。不得将本白皮书视为投资要约，它既不以任何方式也不应被解释为在任何司法管辖区提供证券。本白皮书不包含任何可被视为建议或可作为任何投资决策基础的信息或建议。

2019 年 11 月 10 日