唯链 VeChain
发展计划
与
白皮书

版本 1.0.0.0

2018.5

序言

唯链团队和唯链区块链已经在通向未来的道路上奔跑了两年半。

一路走来，我们遇到过许多志同道合的人士。我们的商业伙伴，无论是企业还是个人，在这条探索新技术的道路上都热情洋溢，充满梦想，信仰坚定，勇往直前。我们在多个行业积累了应用案例的使用经验，在过程中不断的调整策略、解决问题。我们将一如既往，探索这一改变世界的“颠覆性技术”的正确道路。

我们初心未改，赤子之梦一如从前：

旨在建立一个信息透明、协同高效、价值高速传输的可信任分布式商业环境。

唯链距离通证发行已经九个月有余。我们在坚守初心的同时，也紧跟整个区块链行业快速发展的脚步，适时地逐步调整唯链的各项使命。

唯链致力于打造一个区块链平台，为那些基于区块链技术的创造真正经济和社会价值的商业应用提供支持。

在对现有公链平台（包括以太坊）进行全面研究并与多个商业合作伙伴进行无数次讨论和交锋之后，我们找到了企业和以消费者为中心的大型应用尚未采用区块链的原因。最大的障碍不在于技术，而在其他与区块链操作设计相关的关键要素。

我们确定了四个阻碍企业采用区块链技术的主要因素。

其一，多数公链缺乏适当的**治理模型**。尽管去中心化是区块链技术的基石，但它的缺陷也十分明 显，这就导致区块链效率低下，且难以快速迭代。我们认为，区块链的可扩展性并非取决于技术， 而是取决于治理的共识问题。很难想象，一个像比特币这样估值超过 1400 亿美元且通行全球的“软件”或“系统”，在过去的 10 年里鲜有升级。诚然，中本聪最初描绘的愿景非常令人着迷，比特币区块链也如其最初设计的那样发挥着自己的功能。但随着区块链应用案例的不断进化，区块链的特征和功能也无可避免的要随之改变。而一个适当的透明且高效的治理体系将能推动区块链实现持续、快速的创新。

其二，现有公链的**经济模型**几乎全部都将交易成本与相应区块链的总估值直接或间接地联系起来，这就不必要地造成了交易成本高企且难以预测。多数公链都有这样一个矛盾：使用量越大，通证 价值越高，使用该区块链的成本非但未降低，反而越发高企，这就伤害了用户的使用积极性，也 降低了网络总价值。对于任何一个商业伙伴而言，在区块链或其它任何地方，以不稳定的成本运 营应用程序或新业务都是无法接受的。另外一个矛盾在于，通证持有者希望通证的价值不断增加， 而企业用户则希望其价值能保持稳定和/或较低水平。要解决这些问题，必须在下一代公链中引入 适当的经济模型。

其三，一个成熟生态系统的参与者中，不止要有区块链技术专家，还要有许多其他背景的人士。事实上，更多的商业人士关心可行的解决方案，而不仅仅只是技术。通常，他们希望看到的解决方案需**结合多种技术，**如区块链、物联网、大数据和人工智能等。现有的区块链生态也要求商业伙伴更积极主动，深入参与到区块链的创新中来，从而使区块链技术能创造出新的商业价值。当

前的区块链世界缺少能够提供此类解决方案、将技术与商业应用连接起来的人士。因此，区块链本身的通用基础架构服务必须允许技术和商业开发人员建构解决方案，为其业务增加价值。

最后，任何面向应用的区块链都要具备**遵守法规、适应变化**的能力。

为解决上述所有问题，唯链创建了唯链雷神区块链，代表下一代区块链公链的发展方向，我们称之为区块链 X。它具有以下主要特点：

1) 强健的治理架构

2) 完善的经济模型

3) 监管与合规性

4) 唯链雷神主网与相应的基础架构服务

目录

1 背景

1.1 项目启动

一切都始于神秘人中本聪 2008 年 10 月发布的白皮书。白皮书发布后，第一个创世区块于 2009 年 1 月 3 日被创制出来，它的出现也标志着区块链的诞生。旅程始于疑虑、猜测、炒作和恐惧，但最重要的，区块链技术如同所有其它新技术一样，给了我们一个改变世界的机会。比特币被认为是区块链 1.0。

在 2009 年到 2013 年间，尽管投身其中的人不多，但对区块链技术进行的创新实验和探索始终在进行。区块链也被慢慢的向全世界推广。

2014 年，以太坊发布白皮书，2015 年，以太坊上线。它对智能合约及通过虚拟机执行相关合约的机制创造性的引入标志着区块链技术的一次巨大飞跃。以太坊的实践表明，区块链可以通过部署和运行智能合约来描述更为复杂的活动，这些实践也为以太坊赢得了区块链 2.0 的称号。

以太坊的实践表明，区块链不再只是知识分子毫无实际价值的异想天开。突然之间，企业和政府都开始将目光投向建构于智能合约之上的那些全新的应用案例。2015 年 10 月，《经济学人》杂志发表了一篇题为《区块链：信任的机器》的文章，该文广为传播，也将区块链技术带入社会主流人群的视野。

在其后的 2016 和 2017 两年中，比特币在加密货币市场总市值中所占的比例从超过 90%降到不足 40%，这种迅速的变化一方面体现了区块链思想、创新和发展的繁荣，另一方面也表明了人们的恐惧、不确定性、疑虑及猜测。

在 2018 年的今天，企业界的主流观点认为“1995 年的场景又一次出现了”，区块链如同 25 年以来的互联网一样，将会改变世界，只是区块链改变世界的步伐将会更快。尽管公众对区块链的潜力充满热情，但在现有公链上，值得关注的商业应用仍然屈指可数。唯链则致力于彻底改变这一局面。

所谓“站在巨人的肩膀上”，实际表达的是“在前人发现的基础上探索真理”。唯链雷神区块链一直将以太坊（区块链 2.0）和比特币（区块链 1.0）视为自己的前辈。正是由于他们此前的开拓工作，唯链才得以设计出一个功能齐全、组织完备的区块链。唯链区块链由治理架构、通证经济体系、监管合规和社区生态构成，能够持续不断地发展区块链协议，从而吸收各种创新并满足社区、投资者、企业客户、学术和政府合作伙伴等各方面的需求。由此来看，唯链雷神区块链将会是区块链 3.0、4.0、5.0……因此，我们将唯链雷神区块链视为区块链X，而不仅仅是区块链3.0。

此外，根据唯链雷神区块链未来的预期使用率及相关预测，我们认识到，在进行智能支付时，VET 的计算多涉及小数形式。为解决这一问题，在主网发布进行通证置换时，我们将以 1：100 的比例对通证进行兑换。每 1 个 ERC20 VEN 可以置换为 100 个 VET。置换完毕后，各节点的 VET 配置要求也将提升 100 倍。更多细节请参阅后面章节。

1.2 认识区块链技术

1.2.1 协同与价值传导

在传统的商业世界里，包括金融行业在内，对于各种形式的协同合作和商业运作而言，信任都是最大的一项成本。而区块链则天然是“信任的机器”。

区块链的本质就是一种关于信任（ Trust ）的互联网协议和技术集合。

我们可以分别从数据、系统和应用这三个维度来解析区块链的含义。

从数据(Data) 的角度看，区块链是按时间顺序不断增量记录的分布式数据库系统。区块链上的数据只可添加，不可篡改。

从系统(System) 的角度看，区块链是一种分布式且实时同步的系统，允许多方通过共识机制共同参与数据的创建、获取和维护。整个区块链网络就如同一个由多个节点组成的巨型计算机，这些节点遍布整个互联网且都储存有相同的数据。

从应用(Application) 的角度看，区块链是一个允许多方同时接入的标准化全球平台，在这个平台上，各方可以同时管理所有的数字化物品、用户及其与共识协议相关的操作行为。

信息技术和互联网的发展使得协同合作变的越来越便捷和高效。但是由于信任问题依然存在，这 种高效的协同合作多数仍仅存在于企业或组织内部。当不同的企业之间需要进行协同合作的时候， 人们通常仍会使用 40 年前的技术，如电子邮件甚至传真。由于数据安全、商业机密、隐私、法律责任等方面的顾虑，系统整合其实并不是想象中那么简单。

以供应链（图 1.2.1）为例，在供应链这样一个经典的商业协同模式中，有多方参与者，包括品牌商、制造商、分销商、零售商、消费者、监管部门及相关服务 提供商等。各方管理对象相同，均是产品，目标也一致，即在不同的环节创造产品价值。然而由于缺乏充分的信任，各方的合作仍然停留在一个点对点的方式，使用的也依然是传统的工具。如此，数据交换既低效又昂贵。在这样传统的产品生命周期里面，即使物流可以做到相对流畅和高效，也难免造成信息流割裂、财务支持相对低效。

区块链技术可以帮助我们建立一种新型的、可信任的 （Trust-free）、共享性商业协同合作模式（图 1.2.1），让各参与方以更加便捷和通畅的方式保证数据安全。在更加及时准确的信息流支持下，价值传导可以伴随商业活动的开展同时进行，提高每个企业的现金流使用率，极大提升价值的传导速度，从而可以支持更多的商业发展。

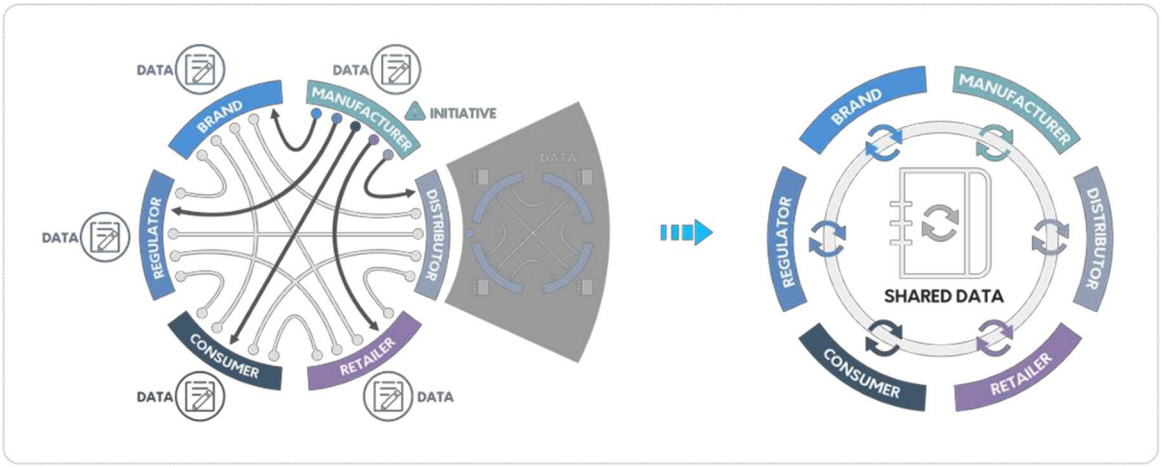


图 1.2.1 传统商业合作模式 vs 区块链上的分布式商业合作模式

回首技术发展史，在第 1 个 100 年中，技术的发展主要在物流技术领域，如交通运输。过去 30 到 40 年中，技术的发展主要在互联网信息流领域。而现在，通过解决信任问题，区块链将会在提升价值流方面实现突破。我们预见，在不久的将来，如同当今的互联网一样，基于区块链技术的使用案例和应用将会改变我们的日常生活。

1.2.2 数据可用性与信息透明

多数企业和个人，或泛言之商业伙伴，都有三种类型的数据：

- 公开数据，如企业在官网上公开发布的企业数据信息。
- 私有数据，如客户信息、研发文档及非上市企业的财务报告等。
- 有权限的共享数据，通常存在于不同的合作方之间，如与标识、物流、供应链、支付信息、售后服务等相关的信息。

前两种数据较易理解。有意思的是，第三种数据通常被参与各方收集用作私有数据。

例如，汽车售出后，其使用过程产生的数据散布于服务提供商、零配件供应商和保险公司等各方的数据库中。如能将这些数据组合起来，将能挖掘出其巨大的潜在价值。现在的问题是，对保险公司和银行这样的数据使用者而言，要想准确且充足地从各处收集到相关数据，以备未来服务之用，不仅困难而且成本高昂。而因收集数据产生的成本最终又将被转移到消费者身上。

区块链技术则可以打破这种信息不对称的局面，让数据的所有权回归真正的所有者，并为所有者赋能。在不同环境间转移数据时，区块链可以大大提高数据可互换性以及数据提取、转换和加载过程的效率。通过这种方式，区块链可以将数据的价值分配给不同的贡献者或服务提供者。例如， 在前述汽车案例中，车主在使用汽车的时候产生的数据自然应该归车主所有。可以通过智能合约 执行精心设计的激励机制，并通过分配共享价值（如保险或汽车交易等应用案例中节省的成本） 来激励数据贡献者。

简而言之，在前述汽车案例中，车主在将车况综合数据授权给保险公司时，也应获得相应价值回报，如减免部分保险费用。由此产生的价值应与数据的维护提供者共享。

此种区块链生态系统，作为区块链使用案例的典范，其价值观可以概括为：

“有所得到就要有所付出，有所分享就会有所收获。”
–雷纳托·格罗托拉（Renato Grottola），挪威船级社管理服务集团（DNV GL）高级副总裁兼全球 M&A 及数字化转型负责人

通过将数据所有权和数据货币化的权益交还数据的生产者，区块链技术将有机会营造一个更美好的新世界。

1.3 唯链和唯链雷神区块链的愿景

唯链和唯链雷神区块链的愿景是打造一个信息透明、协同高效、价值高速传输的可信任分布式商　业环境。

唯链愿景可由以下特质体现。

在唯链生态中，信息相对**透明**对称，大部分利润通过实现真实价值产生。

在唯链生态中，商业参与各方可以大幅降低彼此间的**潜在信任成本**，让商业合作变得更加简单、高效、低成本。如此，就可以将资源集中投向更先进的技术、更优良的产品和更优质的服务，从而产生更大的价值。

在唯链生态中，每个商业伙伴（包括企业和个人），都能根据各自的贡献和价值找到自己的位置，并获得相对公平的奖励。

在唯链生态中，每一项商业活动就如同区块链平台上一个个独立运行的点。通过商业应用和商业创新，把区块链的特性最大化，发掘出各点之间的新连接，如此便可以在整个生态的各点之间搭建一个互联网络。

在唯链生态中，增长的价值源自各点之间连接的建立，形成群体价值。以车企和消费者之间的联 系为例。从创造出的价值中可以发现，有机增长得益于新发现的连接，通过新集群的点和连接之 间的高速价值传输来实现。创造和服务的价值可以表现为商品、产品、服务、资产和资金等形式。

唯链雷神区块链平台通过强大的区块链底层架构、配套的基础设施服务、合理的治理模型和经济　模型、不断壮大的社区和商业合作来打造这一引领未来的生态系统。

1.3.1 分布式商业生态环境

在唯链所设想构建的生态环境中，主要有以下几类参与方：

1) 商业伙伴

在唯链雷神区块链上开展、运营业务以向用户提供产品和服务的各种实体，包括企业、个人、组织、政府机构及监管机构等。

2) 应用服务提供商

应用服务提供商为不具备独自开发应用能力的商业伙伴提供服务，帮助他们在唯链雷神区块链上搭建必要的应用开发和服务。

3) 智能合约服务提供商

智能合约服务提供商指那些有能力为商业伙伴提供专业、高效智能合约开发技术服务的企业和个人。

4) 基础架构服务提供商

直接参与到唯链区块链网络的企业和组织，通过生成和验证区块，维持所有节点的正常运行，并保障整体网络安全。他们开发并运行特定功能节点，以提供配套的基础架构服务，如审计服务、钱包服务、KYC 服务、投票服务、智能合约认证服务、智能合约库服务等。

5) 唯链基金会

唯链基金会（又称“基金会”）是由去中心化的唯链社区组成的中心化组织，负责日常运营工作，包括唯链雷神区块链的开发和维护、社区建设和管理、商业开发、技术研发设计、公共服务提供等。唯链基金会负责整个唯链社区的组织工作，也是整个唯链社区的代表，基金会同时负责战略决策委员会的设立，该委员会负责领导唯链的核心团队，现有七名成员，成员数可随基金会的扩大而增加。

6) 唯链社区

唯链社区由所有志愿参与唯链生态系统的开发并为之做出贡献的实体组成，并可获得相应的奖励。在主网发布、通证 1：100 拆分后，将按持有通证的数量分为以下几类：

- 雷霆战锤(15,000,000 VET)与雷霆战锤 X 节点(15,600,000 VET)
- 雷霆闪电(5,000,000 VET) 与雷霆闪电 X 节点(5,600,000 VET)
- 雷霆力量(1,000,000) 与雷霆力量 X 节点(1,600,000 VET)
- 雷霆 X 节点(600,000 VET)

以及一般的通证持有者或应用程序用户。

1.3.2 分布式生态系统的“血液”——唯链通证（VET）与 唯链雷神之能——VeThor（VTHO）

如果把整个分布式商业生态系统比作一个生命体，那么区块链底层架构就是骨架，其上的各种应用服务则是肌肉和器官；只要是生命体就一定要有血液，而唯链雷神区块链的血液就是唯链通证——VET 和唯链雷神之能—— VTHO，它们承载着在唯链雷神区块链网络上促成价值传导和交易执行的功能。

VET 是唯链雷神生态系统中的“智能货币”或“智能价值”，可在智能合约中编程和执行，从而推进唯链雷神区块链上运营商业活动，完成价值传导。此外，VET 可被视为在生态系统内各点之间建立联系的关键元素。

唯链基金会已通过非公开发售、公开发售、宣传推广、商业合作、市场营销、研发项目等形式向社区发放了超过 60%的唯链通证，其中一部分（总计 132,837,655.34 枚 ERC20 VEN）已在退币过程中销毁。未来几年，唯链基金会将通过各种活动持续、逐步地将唯链通证发放给社区。

同时，VTHO 作为执行转账交易和智能合约交易的能量或费用，由 VET 随时间推移而生成。更多细节请参见下文中的经济模型部分。

当然，生态系统的发展总会经历多个阶段，也要灵活应对各种可能性。将区块链技术与传统商业世界更好地融合在一起，将有助于传统商业活动的转型。企业发现新的商业模式后，将逐步形成分布式商业生态系统。这一过程需要包括企业、个人、商业伙伴及服务提供商在内的所有社区参与者的投入、创新和贡献。

唯链将为杰出的商业和技术合作伙伴提供支持、赞助和激励，充分利用各行业的最佳应用案例，来帮助正确的人做最正确的事，使他们加入到我们创造未来、改变世界的征程中。

根据过去两年推进区块链技术商业落地的经验，我们将开发区块链应用的要点总结如下：

1) 与最具前瞻性和影响力的战略伙伴一道，发现各行业中最有前景的突破性应用；

2) 应用案例要聚焦解决现实问题，或能创造新价值；

3) 商业应用场景需有多方参与，且应有进一步扩展的空间；

4) 目标企业、目标案例在某行业或多个行业内应有相当的影响力；

5) 应当具备在独立运作的各点间建立联系的可能性。

开发时，为实现应用的纵向和横向扩展而需使用的策略：

1) 横向方面，将成功案例复制到更多相似的应用案例中去；

2) 纵向方面，使开发完成的应用案例覆盖更广泛的人群。

参与者数量越多，合作就会越广泛，价值流转效率也越高，同时会有更好的机会创建新的耦合商业模式，并最终一步步的打造出分布式商业生态系统。

1.3.3 唯链对区块链技术的理解

历史一再证明，任何新技术的发展通常都要经历以下几个重要阶段：

1) 第一阶段，**技术壁垒阶段**，在此阶段，区分因素在于是否有能力使用新技术；

2) 第二阶段，**商业壁垒阶段**。在此阶段，技术突飞猛进，同时也吸引越来越多的社会资源和相近行业的人才流入该领域。越来越多的技术理论和技巧得到传播和分享，技术壁垒变得越发模糊。此时，凸显出的问题变为能否通过相关技术提供优质的产品和服务。这一阶段的关键不再是技术能力，而在于是否能将技术巧妙合理地转化成商业应用和商业价值；

3) 第三阶段，**规模壁垒阶段**。在此阶段，滚雪球效应颇为明显，规模优势变得越来越重要。这一时期，随着商业和社会活动、参与者和玩家以及应用开发数量等的增加，整个生态系统加速成长；

4) 第四阶段，**细分阶段**。在此阶段，行业规模和格局基本形成。新的突破来自资源优势更加集中的细分领域，进一步提升产品和服务的效率和价值；

5) 第五阶段，**新技术革命诞生，产生下一个新的循环**。当现有技术发展到极限时，新技术将会诞生并颠覆现有体系，进而进入到下一个循环。

一般而言，区块链技术也不会脱离此“规律”而成为特例。

时至今日，虽然区块链技术还有很长的路要走，也还有很大的改进空间。然而就上述标准来看，我们的区块链技术已经发展到了第二阶段早期。

因此，作为一本白皮书，这一份发展计划不仅涉及算法和技术细节的内容，还重点介绍了商业生态系统的理念和设计以及进一步发展所需的技术支持。

无论是在过去、现在还是未来，在看待区块链技术和其他事务的重要性及其发展时，我们都将始终保持谦卑的态度。同时，我们通过提供全面的区块链底层技术，打造由物联网专家和人工智能专家组成的多元化技术团队，并搭建由商业应用驱动的迭代机制，为目标的最终实现开创了良好的局面。

2 治理模型与设计

尽管去中心化是区块链技术的基石，但实践证明，完全的去中心化在实际应用中存在明显缺陷，无论对比特币还是以太坊而言都是如此。尽管这些项目在启动时，都有理想化的去中心设计，但现阶段，中心化的趋势却自然而然地日益走强，通过持有大量通证的钱包所有者、比特币矿机的主要制造商、大比例占有总哈希算力的矿池、主要的钱包服务提供商、社区中影响力最大的用户等，区块链变得越发中心化。理想主义的去中心化只能是乌托邦，即便在加密货币和区块链的世界也是如此。

我们认为，应该在去中心化和中心化之间找到平衡点，唯链雷神平台的治理模型设计也正是基于这一理念。在区块链技术、生态系统发展的不同阶段，唯链雷神平台也会对这种平衡做出相应的调整，从而打造一个能够持续迭代、不断发展的治理模型。

唯链基金会通过了以下治理原则和章程，作为协助战略决策委员会（简称“SC”）履行职责的灵活框架。下述治理原则体现了战略决策委员会对于监督基金会政策和决策的公平性及有效性的承诺，且应在全部适用法律、唯链基金会章程文件及其它监管法律文件的范围内进行解释。战略决策委员会可适时对下述治理原则进行修改。

2.1. 治理架构的原则与理念

治理架构及原则的初衷是打造一个可见、包容、透明、高效的平台，促进唯链雷神区块链生态系统的开发、创新、协调和进步。

2.2 治理架构

作为非营利性实体，唯链基金会将致力于唯链平台生态系统的开发、治理及进步。区块链技术的去中心化运营机制赋予基金会以独特治理架构。图 2.2.1 为基金会当前治理架构图。

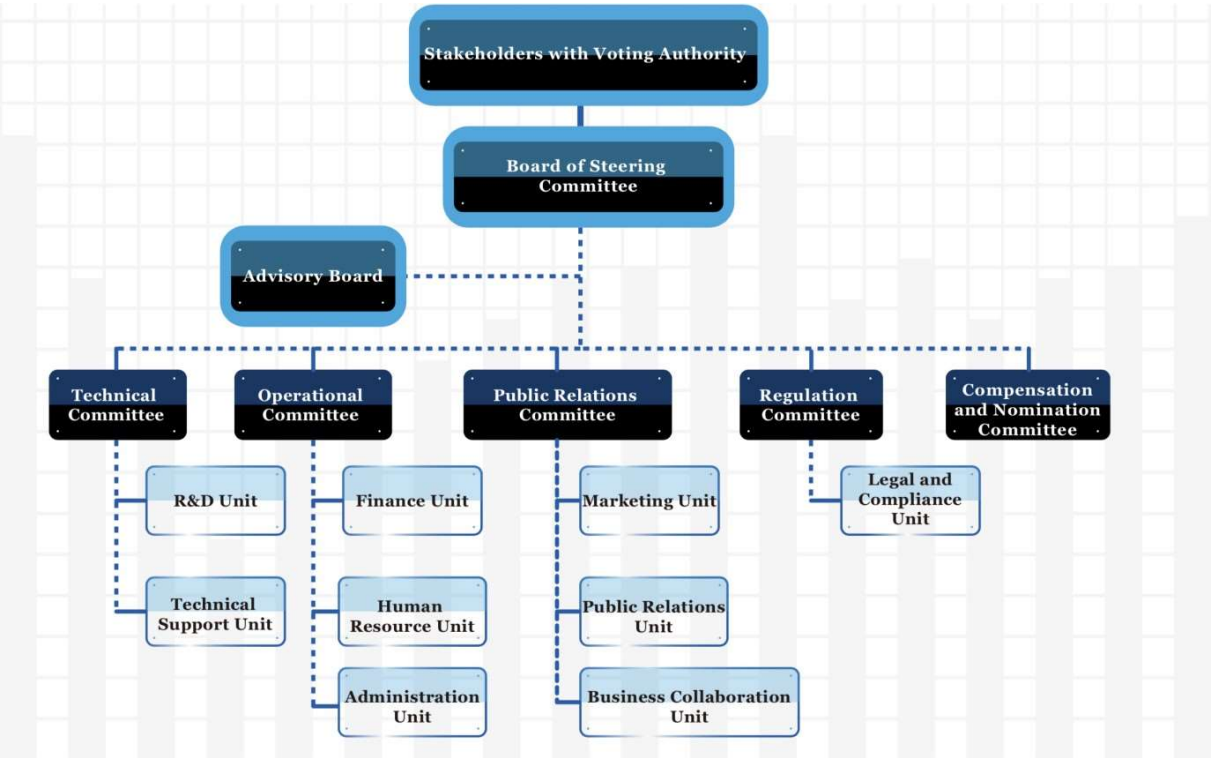


图 2.2.1 唯链基金会治理架构

战略决策委员会为唯链基金会的理事机构，由身份明确且具有 VET 投票权的利益相关者选举产生。战略决策委员会负责制定重大战略事项，并选派职能委员会负责人对基金会的各运营部门进行监管。

2.3 拥有投票权的利益相关者

2.3.1 利益相关者

唯链雷神平台上的利益相关者指 VET 持有者，其中部分持有者拥有特定角色，如智能合约所有者和超级权益节点持有者。每名利益相关者均拥有经投票权益模型算定的投票权。利益相关者可以是具有合法身份的个人、公司、政府机构、非营利实体及其他机构。投票机制的设计可以确保实现对唯链雷神区块链生态系统中所有指定利益相关者的全覆盖。

2.3.2 利益相关者、区块链运营节点与多层认证

下表总结了各类利益相关者所需持有的最低VET 数额（主网发布并完成 1：100 通证拆分后）及其相应投票权。

	持有 VET 最低数量要求	拥有投票权的利益相关者类别	投票权
1	1,000,000	未执行 KYC 的 VET 持有者(**VEOK**)	20%
2	1,000,000	已执行 KYC 的 VET 持有者(**VEK**)	30%
3	5,000,000	个人智能合约所有者(**SO-I**)	20%
4	15,000,000	企业智能合约所有者(**SO-E**)	
5	25,000,000	个人超级权益节点持有者(**AN-I**)	30%
6	25,000,000	企业超级权益节持有者(**AN-E**)	

利益相关者如想获得相应身份（VEOK 除外），除需持有超过最低要求的 VET 外，还需在唯链入口递交申请，并按要求提交验证信息。通过唯链入口KYC 验证的VET 持有者将获得一个VeVID，拥有 VeVID 即获得了申请成为智能合约所有者或超级节点持有者的资格。唯链雷神区块链平台上有 101 个活跃的超级权益节点持有者。在此，候补超级权益节点持有者的投票不包括在这一分类的投票权内。

注：具体申请和验证要求将在唯链入口发布时公布。

2.3.3 投票机制

2.3.3.1 VET 持有者 (VE)

1a. 未执行 KYC 的 VET 持有者(VEOK)

在投票权计算日当天，每个未执行KYC 且账户中拥有超过 1,000,000 枚 VET 的持有者拥有一票投票权；

未执行 KYC 的 VET 持有者（VEOK）所拥有的投票权总量占全部投票权的 20%（$\omega_{VEOK} = 20\%$）。

1b. 已执行 KYC 的 VET 持有者(VEK)

在投票权计算日当天，每个已执行KYC 且账户中拥有超过 1,000,000 枚 VET 的持有者拥有一票投票权；

已执行 KYC 的 VET 持有者(VEK)所拥有的投票权总量占全部投票权的 30%（$\omega_{VEK} = 30\%$）。

2.3.3.2 智能合约所有者(SO)

在投票权计算日当天，每个满足最低 VET 持有数额要求（ 个人 5,000,000 枚 VET，企业 15,000,000 枚 VET）的智能合约所有者拥有一票投票权。

智能合约所有者(SO)所拥有的投票权总量占全部投票权的 20%（$\omega_{SO} = 20\%$）

2.3.3.3 超级权益节点活跃持有者 (AN)

在投票权计算日当天，每个持有不低于 25,000,000 枚 VET 的超级权益节点活跃持有者拥有一票投票权。

超级权益节点活跃持有者(AN)所拥有的投票权总量占全部投票权的 30%（$\omega_{AN} = 30\%$）。

2.3.3.4 求和

最终投票结果V 可 依下式计算：

$$V = \omega_{VEOK} V_{VEOK} + \omega_{VEK} V_{VEK} + \omega_{SO} V_{SO} + \omega_{AN} V_{AN}$$

$V_{VEOk}, V_{VEk}, V_{SO}$ and V_{AN} 分别代表 VEOK, VEK, SO 及 AN 等各组的投票结果。各组权重满足 $\omega_{VEOK} + \omega_{VEk} + \omega_{SO} + \omega_{AN} = 1$，战略决策委员会可适时调整相应数值。单一地址的投票只能根据其最高状态计入相应类别。在本式中，VEOK 的投票结果可能是 14%选“是”，6%选“否”。

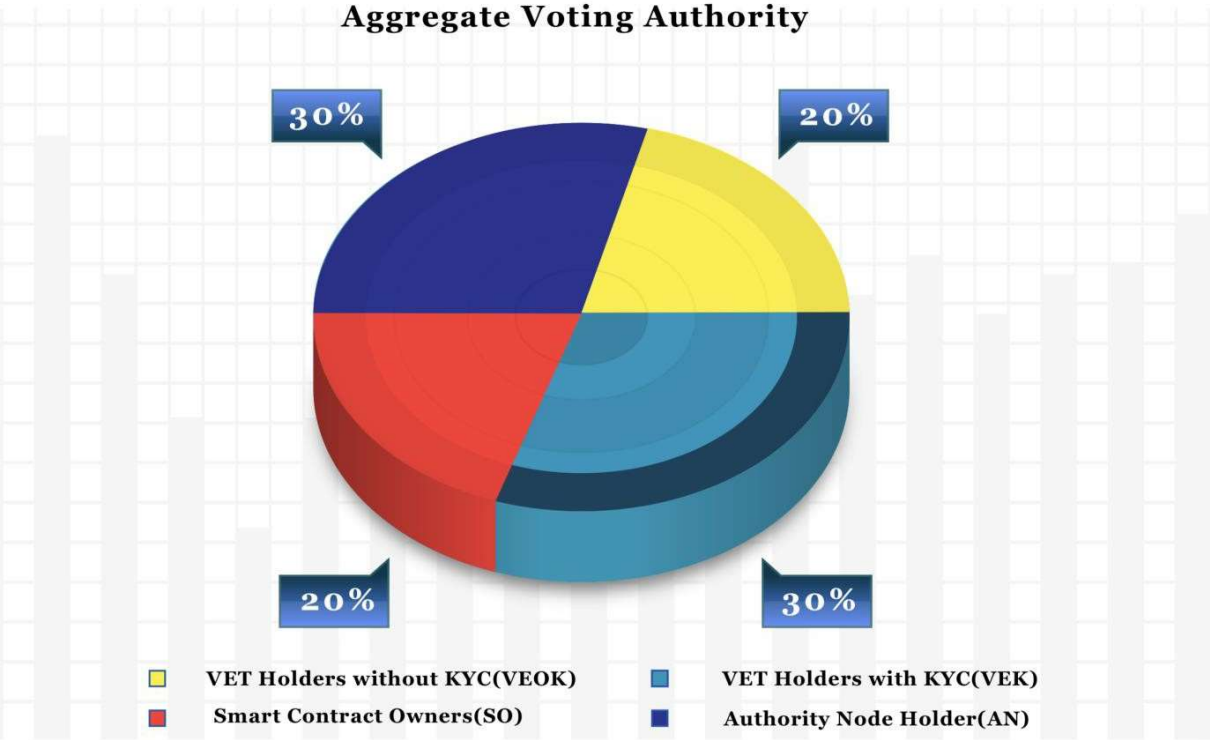


图 2.3.3 唯链合计投票权

2.3.4 全网投票

2.3.4.1 事项

以下核心事项需由利益相关者依各自投票权投票决定：

1) 新一届战略决策委员会成员的选举；

2) 基本共识机制或技术参数的修改；

3) 其它战略决策委员会认为需要进行全网投票的事项。

2.3.4.2 投票权计算日与投票日

投票举行前，基金会将公布具体的投票规则，如投票权计算日、投票日的日期及对最低参与率的要求等。利益相关者如计划参加即将举行的投票，需在投票权计算日进行登记，唯链将检查其 VET 持有量及相关状态，以决定其是否可以获得投票权。投票日当天，所有报名参加投票的利益相关者均可通过 VeVote 服务进行投票。对于定期举行的投票活动，如战略决策委员会成员的选举，基金会将在投票日前至少一个月公布相关信息。对于临时举行的投票活动，基金会将根据具体情况发布公告。

2.3.4.3 投票平台与步骤

全网投票应通过 VeVote 服务进行，该服务可以确保投票匿名、准确，并防止有人操纵投票。

在选举新一届战略决策委员会成员时，提名委员会将在行政部门的协助下，发布提名名单、投票权计算日及投票日日期等信息。依照事先确定的战略决策委员会人数，获得最高票数的候选人将成为战略决策委员会成员。提名委员会将在投票结束后 48 小时内公布新一届战略决策委员会成员的选举结果。

对于上文列出的其它事项，应采用得票最高之选项。投票进行前将公布投票的详细规则。战略决策委员会将在投票结束后 48 小时内公布相应事项的投票结果。

此外，任何投票要想具备效力，各类投票人的参与率或总投票人数占登记人数的比例需高于投票公告事先规定的标准。否则，将由战略决策委员会做出决定。详细信息将在 VeVote 服务中发布。

2.4 战略决策委员会

2.4.1 使命

唯链基金会是一个非盈利机构，致力于唯链雷神区块链的开发、治理和进步。战略决策委员会是唯链基金会的理事机构，负责重大战略的制订以及各职能委员会负责人的选派。唯链基金会致力于打造一个可见、包容、透明、高效的平台，促进唯链雷神区块链生态系统的开发、创新、协调和进步。

战略决策委员会认为，委员会全体成员代表整个唯链雷神区块链各方利益相关者的利益平衡。

战略决策委员会代表唯链雷神区块链各方利益相关者在技术基础架构长期建设、业务拓展和 VET 增值等方面的利益。战略决策委员会同时也认识到基金会在区块链生态系统中发挥的重要作用，基金会进行主动治理，对于确保唯链雷神区块链运营的安全性和稳健性具有重要意义。战略决策委员会负责总体监督和确立框架，包括设计区块链运营规则，以实现相应的目标。

战略决策委员会的主要职能包括：

1) 为唯链雷神区块链上的重大事项发起并组织全网投票，如对共识机制或技术参数的根本性调整、新一届战略决策委员会成员的选举及战略决策委员会认为需要进行全网投票的其它事项；

2) 审查、批准及监督基金会的重大战略、技术、财务及业务活动；

3) 审查、修改及批准基金会的治理原则；

4) 审查、批准及监督基金会的年度预算、财务状况（包括 VET 持有情况）、所得款项用途及其主要交易；

5) 审查、批准及监督战略决策委员会成员、各职能委员会负责人及基金会秘书长的提名和选举流程；

6) 审查、批准及监督 VTHO 的运营模型（唯链雷神区块链的运营成本基础）和 VET 的估值模型（包括市场政策制订）。

2.4.2 成员资格

2.4.2.1 规模、组成及标准

战略决策委员会的规模。委员会成员人数由战略决策委员会视情况决定，可以是 7、9、11 或 13 人。提名委员会或任一战略决策委员会成员均可就委员会规模提出建议。战略决策委员会的规模应确 保其具有适当的专业技能及多元化，并能代表不同利益相关者的利益，从而使其能够在遵守相关 法律法规的同时对基金会的运营进行有效监管。

战略决策委员会的组成。基于区块链的多利益相关者特质，战略决策委员会由两类成员组成：

1) 利益相关者成员指拥有投票权的不同利益相关者（见 2.3.1 节定义）的代表。战略决策委员会中的利益相关者成员来自唯链基金会、最终客户、开发者、超级权益节点持有者及 VET 持有者等单一利益相关者。属于同一实体的利益相关者成员不得占据超过 50%的战略决策委员会席位；

2) 独立成员指不为任何利益相关者（见 2.3.1 节定义）全职工作的个人。独立成员在战略决策委员会中至少应有一个席位。

战略决策委员会的成员标准。战略决策委员会寻求实现成员专业背景的多元化，专业技能涉及面越广，越有利于其为基金会提供战略指导。战略决策委员会成员应具有以下重要特征，包括但不限于：

1) 正直、客观，并具备良好的判断力及领导力；

2) 具备相关专业技能、经验，能够为基金会的发展战略提供建议和指导；

3) 具备独立分析调查、高效协作的能力，并能为战略决策委员会的讨论和审议作出建设性贡献；

4) 致力于为各利益相关者提升唯链雷神区块链的长期价值；

5) 对唯链基金会及区块链的运营、战略和挑战有深刻认识；

6) 有意愿且有能力付出足够的时间和精力履行作为战略决策委员会成员的职责，完成战略决策委员会安排的相应职能委员会的工作；

7) 非下方定义的不符合要求人员。

“不符合要求人员”指任何被官方判定违反刑法、或不符合KYC 认证要求、或依其它相关法律法规被起诉的人员。

秘书长(GS). 秘书长经战略决策委员会选举产生，担任战略决策委员会的联络人及责任代表。秘书长必须是战略决策委员会成员，负责指导和协调各职能委员会与战略决策委员会之间的沟通。如上所述，秘书长不得为战略决策委员会的雇员成员。

第一届战略决策委员会成员和秘书长由创始人选定，并受战略决策委员会的章程约束。

2.4.2.2 任期、退职与任期终止

任期：战略决策委员会成员任期固定为两年。

退职： 战略决策委员会不主张设置强制退职年龄。如某位战略决策委员会成员在其任期内无法继续履职，则其应向战略决策委员会递交书面辞职申请，说明其无法继续履职的原因。如战略决策委员会的利益相关者成员从利益相关者公司辞职或退休，或被利益相关公司辞退，则其将被计为

战略决策委员会的独立成员。如战略决策委员会的利益相关者成员从一个利益相关者处离职，到另一个利益相关者处工作，则其将被计入后者的配额中。

任期终止：如出现下述情况，则战略决策委员会成员资格立即终止：1）丧失任职资格，成为前述不符合要求人员；2）无故缺席两次战略决策委员会会议；3）无故缺席年度会议。

如出现任期终止或主动辞职的情况，则由顾问委员会成员依预定顺序递补进战略决策委员会，直至任期结束。除非在如下提名过程中得到提名，否则递补进战略决策委员会的成员不可自动成为新一届战略决策委员会候选人。

2.4.2.3 新一届战略决策委员会的提名与选举

提名：为确保基金会的稳定性，战略决策委员会现成员自动视为新一届战略决策委员会候选人。如某现成员不愿参加竞选，其应向提名委员会递交书面退选通知。

选举新一届战略决策委员会成员时，如新一届规模与现在相同，提名委员会可最多提名 3 名候选人，如新一届战略决策委员会规模扩大，可最多提名5 名候选人。同时，个人也可通过书面申请书申请成为候选人，基金会将确定申请人资格的评估流程，并由社区投票选出候选人，将其列入候选人名单。

候选人总人数不得超过新一届战略决策委员会建议人数的两倍。被提名人的组成应与新一届战略决策委员会的组成成正比。提名委员会应在选举举行两个月前公布候选人名单。

选举：现战略决策委员会成员任期结束两个月前，由拥有投票权且符合资格的利益相关者选出新一届战略决策委员会成员。被提名者将按得票数排序，并根据事先确定的战略决策委员会规模和组成规则，由得票最高的候选人当选战略决策委员会成员。选举结果将由提名委员会公布。

2.4.3 召开战略决策委员会会议

2.4.3.1 会议次数

每年，战略决策委员会至少应举行四次定期会议。除定期会议外，战略决策委员会可在妥当通知后，随时召开临时会议以解决基金会的特定事项。各职能委员会负责人、战略决策委员会成员均可通过秘书长协调召开临时战略决策委员会会议。

2.4.3.2 议题选择

秘书长应在辅助行政人员的协调下确定战略决策委员会会议的议程。战略决策委员会、职能委员会和顾问委员会的成员均可要求在会议议程中加入某项议题。四次定期战略决策委员会会议中， 有一次被定为年度会议，年度会议召开日期定在基金会当前财年结束前一个月。

战略决策委员会年度会议议程：

1） 审查并批准基金会的一年与五年战略计划；

2） 审查并批准下一年度的技术、运营与公共关系发展提议；

3) 审查并批准基金会的年度预算；

4) 审查并批准对治理原则内容的调整；

5) 审查并批准对各职能委员会新成员与职能单位负责人的任命；

6) 审核并批准VTHO（唯链雷神区块链运营收费基准）的运营模式和VET的估值（包括市场政策制定）；

7) 其它议题。

其它定期举行的战略决策委员会会议议程：

1) 审查基金会的新进展与长期战略计划的实施情况；

2) 审查技术、运营、公共关系和法律等职能委员会取得的新进展及面临的挑战；

3) 其它议题。

2.4.3.3 会议出席

战略决策委员会全体成员均应出席并参与所有战略决策委员会会议及各自所属职能委员会的会议。除非有特殊情况确实无法出席，全体成员均应亲自出席年度会议。确实无法亲自出席年度会议时， 该成员应在年度会议举行前提前将相应情况告知指定的辅助行政人员或秘书长，并通过电话参加 会议。

举办其他定期或临时战略决策委员会会议时，成员可亲自出席，也可通过语音或视频电话参加。如某成员无法亲自出席会议，也无法通过语音或视频电话参加会议，其应事先书面告知指定的辅助行政人员或秘书长，解释相关情况。

2.4.3.4 材料发放与战略决策委员会演示

战略决策委员会成员务必在会前就需要充分讨论的主题提供一定的材料。战略决策委员会成员通常可以在会议前的几个工作日收到简报和/或幻灯片，以便进行适当的准备。会员应审阅在此类会议之前分发的材料。如果战略决策委员会迫切需要在短时间内召开会议，或者这些材料将包含高度机密或敏感的信息，则可在会议前不提供书面材料。

对于每一项议程，相关负责人应使用辅助材料和幻灯片向战略决策委员会做出清晰的阐述。

2.4.3.5 非战略决策委员会成员列席会议

战略决策委员会认为，重要顾问及各职能委员会、各部门的负责人列席会议能够推进会议进程，提升会议效率。收到秘书长邀请后，顾问委员会成员、职能委员会成员和其他职能部门的雇员可以列席战略决策委员会的某些会议。

受邀人员应提前做好准备，以便回答战略决策委员会成员提出的专业领域问题，让最了解情况的负责人同战略决策委员会直接沟通。

2.4.3.6 会议记录

战略决策委员会及职能委员会所得出的结论、做出的决定及对职能部门的指示均应记录在会议记录中。战略决策委员会及职能委员会每次会议的记录应在下次会议上呈交战略决策委员会或相应职能委员会批准。委员会会议记录在委员会批准并由相应负责人和秘书长签署后应尽快归入战略决策委员会档案。

2.4.4 战略决策委员会薪酬

战略决策委员会的利益相关者成员和雇员成员不得因其在战略决策委员会供职而获得额外现金报酬。

委员会的独立成员可获取比类似实体具有竞争力的报酬。战略决策委员会将定期审查委员会独立成员获取报酬的水平和形式。

为保证公平，激励战略决策委员会成员，应在薪酬委员会审核后，向战略决策委员会所有成员（来自唯链基金会的成员除外）和职能委员会负责人发放固定数额的 VET。

基金会应负责报销会议期间外地战略决策委员会成员的差旅费和住宿费。

2.5 顾问委员会

2.5.1 组成

基金会会寻求实现顾问委员会成员专业背景的多样化。顾问的人数不应超过战略决策委员会成员的人数。顾问由战略决策委员会基于多样化、专业化的原则选定。

2.5.2 成员资格

顾问必须具有独立性，不得与基金会的任何利益相关者有直接关系。如某顾问与利益相关者产生关系，其应在关系产生时辞去顾问委员会成员的职位。

顾问委员会成员是战略决策委员会候补成员，当现任战略决策委员会成员任期终止或主动退出时，顾问委员会成员按预定顺序递补。递补进战略决策委员会的成员将任职至本届任期结束。除非得 到提名委员会提名，否则递补进战略决策委员会的成员不可自动成为新一届战略决策委员会的候 选人。

顾问委员会成员每年应获得固定的 VET 报酬，因出席会议产生的差旅费应予报销。

2.6 职能委员会

2.6.1 委员会

战略决策委员会下设以下委员会：技术委员会、日常运营委员会、公共关系委员会、监督管理委员会、薪酬委员会以及提名委员会。各委员会应由战略决策委员会成员或顾问委员会成员担任负责人，并将各职能单位的关键管理人员列为成员。薪酬和提名委员会应由战略决策委员会的独立成员或顾问委员会的成员担任负责人。委员会的工作分配及其负责人的任命应基于成员的知识、兴趣和专业领域。

战略决策委员会可适时视情况组建新的职能委员会或解散现有委员会。战略决策委员会也可适时视情况设立特别委员会或工作组，并决定相应委员会的组成和职责范围。

2.6.2 职能委员会会议

各常设委员会均应定期举行会议，并就涉及委员会工作的发展事项听取基金会工作人员报告。委 员会负责人应视需要确定委员会会议的频率和时间。委员会成员应准备、出席并参加全部委员会 会议，并尽力亲自出席。如某位成员无法亲自出席，情况合适且必要时，其可通过电话参加会议。如某位成员无法亲自出席并希望通过电话或视频参加会议，其应在会议开始前告知委员会主席。

2.6.3 委员会向战略决策委员会报告

战略决策委员会议程应包括各职能委员会负责人对其工作进程和研究的定期报告。委员会应将其认为意义重大的事项和决定提请战略决策委员会审议。各委员会还应在当前年度内向战略决策委员会提交有关其主要活动的书面年度报告。该报告可证实委员会已履行章程所规定的全部义务。

2.6.4 职能委员会

2.6.4.1 技术委员会

技术委员会由唯链区块链底层技术开发人员组成，其职责如下：

1) 为唯链雷神区块链当前和未来的发展制定规划，按计划开发及测试新技术，并向战略决策委员会报告其开发进展；

2) 向个人开发者或企业开发者提供技术文档与开发工具，为其在唯链雷神区块链上开发应用程序提供支持；

3) 监控唯链雷神区块链的状态，出现紧急状况时及时分析、处理，保持系统稳定性；

4) 监控唯链雷神区块链的使用情况，收集使用数据及市场数据，与经济学家合作，共同改进经济模型，就模型参数调整提出可行建议，并向战略决策委员会报告；

5) 确定未来区块链相关研究领域，内部开展研究，与研究机构合作开展联合研究项目，并将

成果发表于国际会议及期刊上。

2.6.4.2 日常运营委员会

日常运营委员会职责如下：

1) 制订报告制度，细化各职能单位职责。该委员会负责监督以下部门：财务部门、人力资源部门和行政部门；

2) 与财务部门主要管理人员一道，起草预算方案、财务方案、分配方案及财务报告，并向战略决策委员会汇报；

3) 与人力资源部门的主要管理人员一道，设定基金会各职能部门的人力资源结构。在人才招募、薪酬和激励等方面提出建议。为薪酬委员会和战略决策委员会提供建议；

4) 与行政部门的主要管理人员一道，设定各部门的职能结构和职责；

5) 协助职能部门与战略决策委员会沟通；

6) 其它战略决策委员会批准的职责。

2.6.4.3 公共关系委员会

公共关系委员会职责如下：

1) 在社区、利益相关者、商业联盟和公众中推广唯链雷神区块链及唯链基金会；

2) 为基金会的法务与合规部门提供指导；

3) 与政府监管部门保持良好沟通；

4) 设定规程，确保报告透明度；

5) 在战略决策委员会认为适当的时机，向唯链雷神区块链社区、利益相关者、商业联盟和公众发布重要文件和公告；

6) 其它战略决策委员会批准的职责。

2.6.4.4 监督管理委员会

监督管理委员会负责确保基金会运营活动符合相关法律法规的要求。如有任何重要的风险、挑战或问题，均应列入战略决策委员会会议议程。

监管委员会同时负责监督日常运营的内部审计，一旦发现任何不当行为或不合规的情况及时汇报。

2.6.4.5 薪酬及提名委员会

薪酬及提名委员会负责设立适当的激励制度，激励基金会各职能部门的重要管理人员。委员会应制订规程，经战略决策委员会批准，对管理层的业绩进行评估，并采取相应的激励措施。

提名委员会同时负责新一届战略决策委员会成员候选人的提名工作，提名工作应在本届战略决策委员会成员任期结束六个月前进行。

2.7 沟通与披露

2.7.1 与战略决策委员会沟通

相关各方如希望与战略决策委员会取得联系，可发送电子邮件至 foundationboard@vechain.com。您也可以发送电子邮件给基金会执行秘书，通过基金会执行秘书与战略决策委员会个别成员、全 体成员、特定委员会或其独立成员进行沟通。

所有来信将由基金会行政部门整理， 并按季度或视情况提前提交战略决策委员会。foundationboard@vechain.com 收到的电子邮件经筛选后标记为垃圾邮件或一般性咨询邮件。如信件不涉及下述一般业务事项，并且指定某一战略决策委员会成员查收，则将其转发给该成员。为了提高一般业务事项的响应速度，战略决策委员会已授权指定工作人员视具体情况代表我们的成员（包括特定成员或其非雇员成员）接收、查看并回复有关申请或服务的“一般业务事项”信件。战略决策委员会任何成员均可审查此类来信及回复。

2.7.2 披露

为确保基金会运作的公开透明，战略决策委员会将按季度、年度发布报告，总结基金会的运营状况、新发展、业绩以及潜在风险。战略决策委员会的组成和高管成员名单将在年报中披露。基金会的运营、战略及战略决策委员会组成如出现重大事项或变化，也将通过沟通平台及时披露。

2.7.3 道德与利益冲突

战略决策委员会已通过利益冲突政策。该政策包含适用公司法、条例及基金会通过的其它规定， 以确保战略决策委员会的决定不受利益冲突的影响。根据利益冲突政策和基金会通过的规章制度， 战略决策委员会成员应避免与基金会的利益发生冲突的任何行动、立场或利益，亦不得表现出有 冲突迹象。

当面临潜在利益冲突时，战略决策委员会成员应向法务部门法律事务总顾问或法律事务总顾问指定的外部律师征求意见。

3 经济模型与设计

3.1 背景

区块链生俱来具有金融特性。适当的经济模型是区块链生态系统的一大基本要素，也是其成功的关键。

在研究了大多数公链网络的经济模型，并与我们的商业合作伙伴，特别是各类企业进行了多次讨论之后，我们发现在区块链上大规模使用应用的最大障碍是：区块链的使用成本与通证的估值直接挂钩。一方面，通证估值通常会随着区块链使用量的增加而上升，另一方面，区块链的使用成本也存在显著差异，具体取决于参与者是希望进行支付交易，还是进行智能合约操作。这还没有考虑投资者和交易者的投机和炒作行为对于区块链价值的影响。对于任何一个商业伙伴而言，在区块链或其它任何地方，以不稳定的成本运营应用程序或新业务都是无法接受的。

本节将介绍唯链雷神区块链经济模型，内容涵盖：VET 生成 VTHO 的模式、VTHO 的市场供需情况预估，以及 VTHO 的价格建模原则。总之，VTHO 是因持有 VET 而生成的，生成速率为 u VTHO 的设立是为了让持有 VET 的用户在不产生额外成本的情况下进行交易，但前提是用户持有 VET 的时间足够长。

在 VTHO 生成模型的基础上，我们可以在唯链主网正式发布后预估每天 VTHO 的供需情况，并动态跟踪一年。 按当前速率v计算,VTHO 的总供应量为每天 37,459,858 个。对 VTHO 的需求分两种情况：执行智能合约和支付交易。前者对 VTHO 的需求根据业务开发团队的预测得出，后者对 VTHO 的需求根据过去三个月可比较的加密货币交易数据得出。为了稳定 VTHO 价格，保持 VTHO 的供需平衡，基金会可能会在需求接近 VTHO 总供给时调整经济模型的变量。

在第 3.5 节，我们将提供通证价格的一个通用增长模型。一般情况下，VET 的价格由三部分组成：所有未来生成的 VTHO 的现值；作为加密货币的 VET 的现值；以及在唯链区块链上作为价值转让媒介（或智能货币）使用的 VET 的现值。

3.2 模型设计理念

设计该模型的基本原则是防止交易费受到通证价格波动的直接影响，从而使唯链雷神区块链更好地满足个人和企业用户的业务/财务活动需要。

在我们的设计中，唯链区块链（下称“唯链”）分两个层级。较低层级涉及区块链层面的操作，如通证的转账和智能合约的执行，而较高层级涵盖执行复杂商业和财务活动的应用。

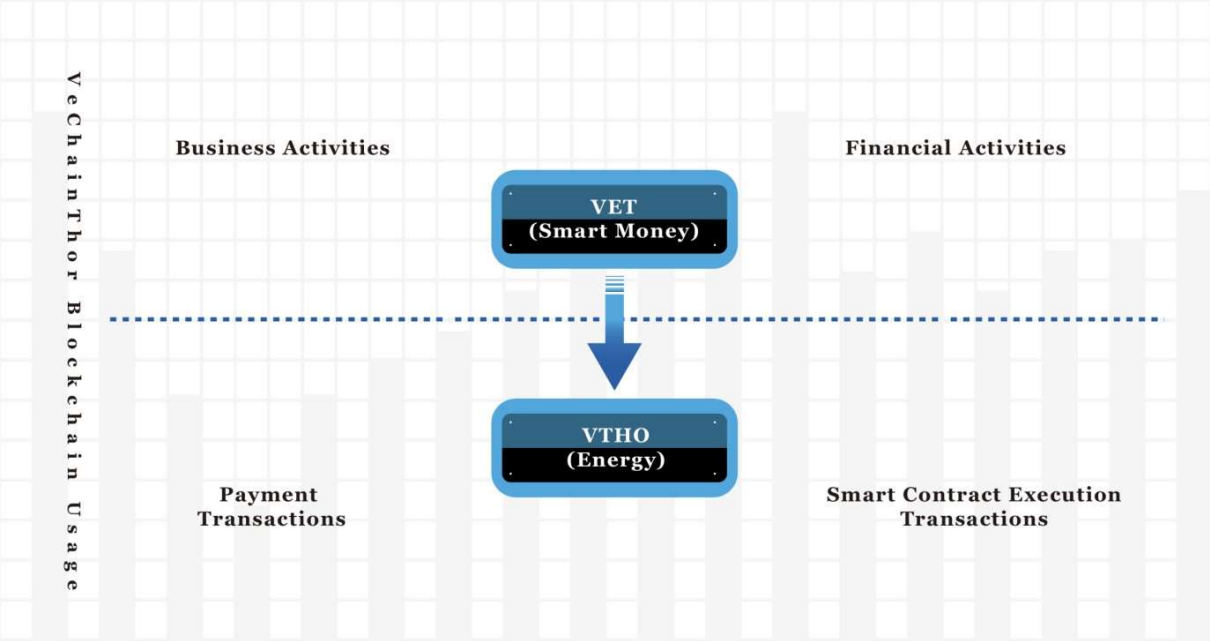


图 3.2.1 唯链区块链的两个层级

在模型中，我们设计了一个双通证系统来促进VET 和 VTHO 两个层面的活动。VET 的功能是充当价值转移媒介（智能货币），以便在唯链的基础上实现生态内的快速价值流通。另一方面，VTHO 代表使用唯链的底层成本，并且在执行某些区块链操作后将被消耗/销毁。

由于 VET 实际上是一种唯链使用权，因此该模型的设计是为了让用户通过持有 VET 自动生成 VTHO。换言之，VET 持有者将免费获得 VTHO，并且只要执行操作所消耗的 VTHO 低于其生成量，就可以免费使用唯链。VTHO 通证可以转让或交易，这样一来，用户也可以获取更多 VTHO 来执行更大规模的操作，例如运行在唯链雷神区块链上托管的应用。

3.3 模型设置

首先我们来定义一些变量，来描述我们的模型设置。

：VET 的数量
E：VTHO 的数量
G：gas 的数量（以 1000 个 gas 为单位），其中 gas 是唯链的内部单位，用于为各种区块链操作定

：因持有 VET 而积累 VTHO 所用的时间。请注意，t 是以区块的数量而不是常规时间单位计算的。
p：以 VTHO 衡量的 gas price
v：因持有 VET 而生成 VTHO 的速率

我们的模型可以用以下数学公式来表示：

$$v \quad V * t \qquad (1)$$
$$E = p * (\qquad (2)$$

公式 1 告诉我们，每产生一个区块，1 个 VET 就会产生v个 VTHO。公式 2 展示了VTHO 通证在系统中的使用方式。具体而言，当交易被放入一个区块时，系统首先计算所需的G，然后用方程 2 计算E，即耗费E个 VTHO。请注意， 是由交易发起者设定的，每笔交易都可能不同。 值越大，交易被处理的优先级越高，耗费的 VTHO 也越多，反之亦然。

我们预计，初期唯链区块链的使用量不会很大，但在未来两年内会迅速增长。我们初始化了模型参数v和p，使 100 万个VET 每天生成的VTHO 数量足以进行二十次支付交易。根据我们的设计，唯链将每隔 10 秒产生一个区块，每笔支付交易需要 21,000 个 gas。参数v的当前设置为每个区块每个VET 生成 $5x10^{-8}$ 个 VTHO。因此，在 24 小时内，共产生$6 \times 60 \times 24 = 8{,}640$个区块，每 1 万个 VET 会生成 4.32 个 VTHO。

理想情况下，生成的 VTHO 通证大部分将用于在唯链上进行交易。在我们的模型中，我们允许用户在提交交易时灵活调整p值。理论上讲，用户可以将p值设定得小一些，以使交易消耗的 VTHO 趋近于零。但如果大批用户照此行事，会造成大量 VTHO 无法消耗，从而增加唯链雷神区块链的不稳定性。

为了防止p值低于最低交易成本，用户选取的范围将限定于$[p^{基础值}, 2 \times p^{基础值}]$区间内，其中我们当前设定$p^{基础值} = 1$ VTHO/1000 个 gas。我们预计，p的均值与唯链上运行的应用数量以及定期交易的活跃用户数量相关。该取值区间的设置是为了防止有人独占区块链资源并伤害其他交易发起者，gas price 一旦超出限定范围，交易将被延迟或不执行，作为系统的惩罚。

3.4 VTHO 的供需估算

3.4.1 VTHO 的供应

根据 v=每 1 万个 VET 每天生成 4.32 个 VTHO 的基线设定，每位持有 1 万个 VET 的用户每天将获得 4.32 个 VTHO。在整个唯链雷神区块链中，每天由VET 生成的VTHO 有 37,459,858 个，此外，全网每天所消耗的VHTO 中有 30%将奖励给超级权益节点。我们将 VTHO 的每日市场供应用以下数学公式表示：

$$S_{Th,d} = \rho \cdot (v_d \cdot V \cdot (1-\gamma) + 30\% \cdot D_{Th,d}) \qquad (3)$$

其中
$S_{Th,d}$是 VTHO 的每日市场供应；
v_d是每 1 万个 VET 每天生成 VTHO 的速率；
V是 VET 的总数；
ρ是每天使用 VTHO 进行交易的活跃用户（“活跃交易者”）的占比；
γ
$_{Th,d}$是每天 VTHO 的总使用量，其中 30%授予超级权益节点持有者，假定他们的参与度ρ相同。

注：在该计算方法中，所有 VET 都有一个基础生成速率。

3.4.2 对 VTHO 的需求

对 VTHO 的需求分两种：企业用户通过应用程序部署在唯链雷神区块链上的智能合约，和个人的交易支付。

因使用智能合约导致的 VTHO 需求可通过以下公式进行估算：

$$D_{Th,d,SC} = K \cdot p_{TH/KG} \cdot \sum_{i=1}^{N} ID_i \cdot \theta_{i,d} \cdot L_i \qquad (4)$$

其中
D
$_{Th,d,SC}$是每天因执行智能合约产生的对 VTHO 的市场需求；
ID_i是每个应用具有的 ID 的平均数量；
$\theta_{i,d}$是每天每个 ID 关联交易的平均数量；
L_i是应用程序 i 运行的可能性；
K是每次智能合约执行的平均 gas 使用量；
$p_{TH/KG}$是每 1000 gas price 的 VTHO。

在个人交易支付的基线模型中，我们将使用以下公式进行估算：

$$D_{Th,d,TX} = TX_d \cdot K_{TX} \cdot p_{TH/KG} \qquad (5)$$

其中
$D_{Th,d,TX}$是 VTHO 的每日市场需求量；

TX_d是预计每日交易次数；
K_{TX}是每笔交易付款固定使用的 2.1 万个 gas；
$p_{TH/KG}$是每 1000 gas price 的 VTHO。

因此，对 VTHO 的总需求可以用以下公式进行估算：

$$D_{Th,d} = D_{Th,d,SC} + D_{Th,d,TX}, \qquad (6)$$

3.4.3 交易成本

双通证模型的设计是为了保持因使用唯链雷神区块链而产生的一些可持续交易成本。基金会将根的据 VTHO 市场的参与度和 VTHO 的供需情况调整p 的最低值，以实现其目标。如果出现明确长期趋势，或调整$p_{TH/KG}$的最低值仍不能有效地稳定交易成本，则基金会将调整 VTHO 的生成速率 v。

VTHO 的供应基于当前的生成速率。未来六个月的 VTHO 需求可以通过计量经济预测模型加上业务发展和营销团队的投入调整进行估算。在比对可用数据的基础上，预测技术也将不断接受检验。可以考虑采用不同的模型来估计支付交易和智能合约对 VTHO 的需求，并根据历史数据对市场参 与度进行估算。

3.5 通证价格建模

我们的通证价格模型是以金融行业广泛运用的股票价格模型为基础构建的，这可能是我们可以从以往经验中借鉴的最为接近的模型。一般而言，可将 VTHO 视为因持有 VET 而获得的一种新型效用。特别是，我们认为VET 的价格来源于三部分：1）持有VET 可产生VTHO；2）VET 在未来的升值；以及 3）VET 通证可用作智能货币。

VET 估值的通用模型设计如下：

$$P = \frac{E}{r-g} + PVG_c + PVG_B \qquad (7)$$

其中
P是 VET 的市场价格；
E是 VTHO 的市场价格；
r是贴现率，与持有 VET 的回报率相关；
g是 VTHO 生成速率的增长率；
PVG_c是目前和预期未来作为加密货币使用的 VET 的现值。可以根据整个加密货币行业或几个类似货币的增长前景进行估算；
PVG_B是目前和预期未来在唯链上作为智能货币使用的 VET 的现值。可以根据未来应用开发和商业战略合作的增长进行估计。

为了了解这些变量的数值，我们选取了当前十大高科技公司的股票价格数据，计算后得出以下结果：$\frac{PVG}{P} = 80\%$，以及$r - g = 0.05$。 对于PVG_B，我们不能妄加猜测，需要更多未来数据才能评估。

定价模型背后的假设是以理论研究为基础的，我们认为实际价格将由也应当由市场来决定。之所以这样认为，是基于以下基本理念：唯链雷神区块链将可做到稳定、可控和可预测，以支持在平台上运行的应用，而 VTHO 将用作唯链雷神区块链的使用成本。唯链基金会将在近期公布和实施一系列宏观调控措施。

3.6 经济节点

唯链经济节点是在区块链经济中体现优待和权利分配，并维持生态系统稳定性的节点。唯链经济节点在生态系统中拥有投票权。对于经济节点而言，每个持有 100 万个 VET 的节点，在多数共识中均享有一票的投票权。与超级权益节点不同，经济节点不生成区块和记账。

为获得经济节点资格，您必须持有超过 100 万个 VET，并按以下最低 VET 持有标准（在主网发布和 1:100 通证拆分后）进行分类：

- 雷霆战锤 - 15,000,000 VET
- 雷霆闪电- 5,000,000 VET
- 雷霆力量- 1,000,000 VET

基金会将预留一个 VET 奖励池，奖励池生成的 VTHO 有一部分将作为奖励分发给经济节点。奖励池中的 VET 每 6 个月减少 25 亿个，直到 2019 年另行发布通知*。基金会预留的 VET 如下（在主网发布和 1:100 通证拆分之后）：

阶段	VTHO 奖励池中的 VET
主网发布 - 2018.12.31	150 亿个 VET
2019.1.1 - 2019.6.30	125 亿个 VET
2019.7.1 - 2019.12.31	100 亿个 VET
……	……

这些奖励将分配给经济节点，并且不会取代因持有 VET 而获得的 VTHO 基础奖励。

假设如下（在主网发布和 1:100 通证拆分之后）：

B =持有 1 个 VET 的 VTHO 基础生成速率（0.000432 个 VTHO/每天）；
FR =分配至基金会奖励池中的 VET 数量（150 亿个 VET）；
F =基金会奖励池每天生成的 VTHO 数量（150 亿 VET×0.000432 = 6,480,000 个 VTHO）；
A =超级权益节点圈定的 VET 数量（101 个节点×25,000,000 = 2,525,000,000 个 VET）；
M =雷霆战锤节点圈定的 VET 数量（变量）；
T =雷霆闪电节点圈定的 VET 数量（变量）；
S =雷霆力量节点圈定的 VET 数量（变量）；
NB =所有节点奖励的基础生成速率。

经济节点额外的 VTHO 奖励计算公式如下，其中 F、M、T、S 已知，NB 待估：

F =(A*NB*(1+100%))+ (M*NB*(1+100%)) + (T*NB* (1+50%)) + (S*NB* (1+0%))

3.6.1 节点成熟期

“节点成熟期”是唯链生态中使用的一个术语，意指：一旦钱包拥有足够的通证，符合成为某个

节点的条件，且唯链钱包内置功能“VTHO 铸造”中存储的 VET 数量达到相应要求，则节点成熟

期启动计时。

成熟期结束时，若存储在“VTHO 铸造”中的 VET 数量在规定时间内的任何时刻都未曾降到阈值以下，则节点身份将被正式确定，并开始生成节点奖励。

雷霆战锤节点成熟期：唯链雷神区块链主网启动后 30 天；要求最少 1500 万个 VET；

雷霆闪电节点成熟期：唯链雷神区块链主网启动后 20 天；要求最少 500 万个 VET；

雷霆力量节点成熟期：唯链雷神区块链主网启动后 10 天；要求最少 100 万个 VET。

在主网启动后，若因 VET 数量变化导致节点类型发生变化，则同样会激活相应的节点成熟期。例如，若节点在钱包“VTHO 铸造”中的通证数量从 100 万个 VET 增加到 500 万个，则该经济节点会进入 20 天的成熟期，成熟期过后，除正常生成的VTHO 基础奖励外，还会获得新的经济节点奖励。

3.6.2 X 节点

X 节点是专为早期支持者预留的另一个 VET 奖励池。如需了解向早期支持者提供的额外待遇，请阅读关于 X 节点的公告。

4 唯链雷神区块链底层技术

唯链雷神区块链是一条公链，旨在促进区块链技术的大规模商业应用。唯链基金会致力于通过健全的治理架构与完善的经济模型，为实现这一目标提供坚实的基础。在此基础上，打造一个可持续、可扩展的生态系统。

自 2014 和 2015 年以来，以太坊[1,2]代表了区块链公有链技术的发展水平，其创意包括：引入账户模型，使基于交易的基础状态机模型可以存储余额等状态信息；提出“智能合约”的概念，区块链可以通过基于共识的计算以及以太坊虚拟机（EVM）和支持智能合约的EVM 代码等发明来描述真实世界中更复杂的对象和活动。

尽管以太坊是一个重大的技术里程碑，但尚不适合搭载日常活动所需的大规模商业去中心化应用（DApps）。一大原因是，以太坊从一开始就没有一个有效的治理架构，来实现自身高效、透明的转型（升级），从而适应新挑战。其次，以太坊未能提供合适的经济模型，让企业以可控、可预测的成本运行他们的 DApps。考虑到以太币价格的波动幅度，企业几乎不可能预测以太币的未来价格，也无法预测一段时间内基于以太坊的 DApps 的运行成本。

唯链雷神区块链旨在解决上述问题。它不仅提供纯技术解决方案，而且还推出了新型治理模型和经济模型，我们认为，这些新模式有助于推动区块链技术更广泛的应用，打造更加可信、高效的生态系统。唯链雷神区块链并非从零开始构建，而是基于以太坊的一些基础模块（如帐户模型、EVM、改良版帕特里夏树和 RLP 编码法）。但最重要的是，它具有专为企业和个人用户的实际需求而量身定制的技术功能。我们相信这些新功能为用户和开发者提供了更多的灵活性和更加强大的工具，帮助他们通过唯链雷神区块链实现自己的目标。

4.1 支付模式

普通人乃至企业使用公链的一大障碍是加密资产处理的不确定性和复杂性。一方面，用户在从市场获得加密货币时不得不面对剧烈的价格波动；另一方面，他们需要先了解相关概念并熟悉各种工具才能使用和管理加密货币。

那么，我们是否能够找到解决这些问题的方法？对于比特币和以太坊等现有区块链网络而言，已无可能，因为我们在使用区块链服务时，无论是转账还是执行智能合约，都必须向相关网络发送交易请求，并使用自己的帐户余额来支付交易费用。

我们意识到了这一问题的重要性，于是在唯链雷神区块链中设计了一种新的多层支付模式，如下图所示。

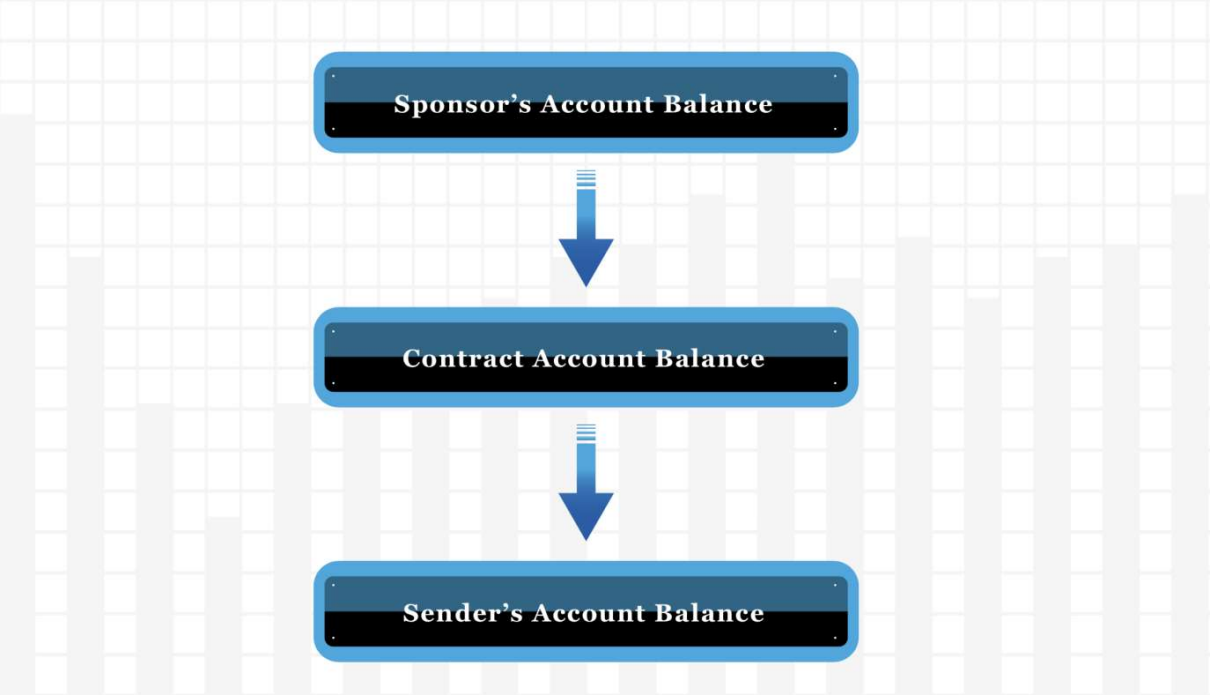


图 4.1.1 唯链雷神区块链支付模型

可以看出，唯链雷神区块链交易可由三方支付。从下到上，他们分别是交易发起方、交易接收方和智能合约的赞助方。在收取交易费时，系统执行以下操作步骤：

1) 系统会检查 a）发起方是否被允许放弃支付交易费用，b）智能合约赞助方是否同意支付费用。如果两个答案都是肯定的，系统就会尝试从赞助方的帐户余额中扣除费用。如果扣费失败（例如，由于资金不足）或第二个答案为“否”，则进入步骤 2。
2) 如果问题a）答案为“是”，系统会尝试从智能合约的帐户余额中扣除交易费用。如果扣费失败或答案为“否”，则转到步骤 3。
3) 系统会尝试从发起方帐户余额中扣除交易费用。如果扣费失败，则返回错误提示。

就支付结构而言，该模式为企业在唯链雷神区块链上开发 DApps 提供了极大的灵活性和便利性。例如，有了赞助方机制，企业可以更好地与无意处理加密资产的业务伙伴合作。同时，企业也能够

更有效地管理多个 DApps，因为它可以使用主账户来支持多个智能合约，并且只需确保主账户

有足够的资金来支付交易费用。此外，该支付模式使得普通人可以使用唯链雷神区块链上运行的DApps，就像使用非去中心化应用一样，只需要处理公钥和私钥对即可，这并不困难，因为我们大多数人每天都要处理数十个用户名/密码对。

4.2 交易模型

唯链雷神区块链采用新的交易模型，来解决阻碍区块链更广泛使用的一些基本问题。具体而言，唯链雷神区块链交易包含以下字段：

- **链标（ChainTag）** - 用于防止交叉链重放攻击的创始区块 ID 的最后一个字节；
- **Tx 随机数（txNonce）** - 可由用户设定的交易随机数值；
- **子句（Clauses）** - 一组“clause”对象，各子句均包含“To”，“Value”和“Data”等参数值，单个“from”可匹配多个“to”参数值；
- **依靠 （DependsOn）** - 用于当前交易的先决条件交易 TxID；
- **区块索引（BlockRef）** - 特定区块的索引，表明区块高度和部分 ID；
- **到期（Expiration）** - 用于指定交易何时到期的区块数量；
- **燃料费系数（gasPriceCoef）** - 用于计算总燃料费用的系数；
- **燃料（gas）** - 交易发起方愿意为交易支付的最高 gas 数额；
- **保留（Reserved）** - 保留字段，用于向后兼容；
- **签名（Signature）** - 交易主体 Ω 的哈希签名，$signature = sign(hash(\Omega), private\_key)$。

下面我们将结合一些问题详细解释我们的设计。

4.2.1 交易 ID 与帐户 Nonce 值

在以太坊账户模式中，用账户 nonce 值计数，确保每个交易只能使用一次。虽然这种方案可以防止重放攻击，但实践证明，这种机制过于繁琐，对企业用户而言尤其如此。例如，如果用户同时发出多个交易（例如，当企业用户注册产品或更新记录时），一旦一个交易失败，那么 nonce 值更大的所有交易都将被以太坊节点拒绝。

我们取消了帐户 nonce 值机制，引入了交易 ID 的概念。在唯链雷神区块链中，每笔交易都有一个唯一的 ID（*TxID*），可以用如下公式计算：

$$TxID = hash(hash(\Omega), signer\_address)$$

其中，Ω是包含上面列出的所有字段（“Signature”除外）的集合。

在唯链雷神区块链中，验证某一交易时，系统不是检查当前的帐户 nonce 值，而是计算其 *TxID* 值并检查其是否曾被使用过。现在让我们回到刚才的问题：1）如何防止重放攻击；2）如何同时安全地发起多笔交易。假设 Alice 签署了一笔交易，要向 Bob 发送 10 个 VET，Bob 想要重复利用该交易从 Alice 处收取更多资金。显然，Bob 不可能成功。因为这两笔交易具有相同的 ID，因此由 Bob 发出的其中一笔交易广播将被拒绝。

关于第二个问题，对于任何两个交易，只要字段的值不同，交易 ID 就不同。而且，我们可以随时调整交易 nonce 值来生成新 ID。通过这种机制，用户可以轻松地使用不同的 ID 进行多笔交易，也就是说，交易请求可以同时发出，但由唯链雷神区块链分别处理。

4.2.2 交易依赖性

每笔唯链雷神交易都包含与交易依赖性相关的新字段 *DependsOn*、*BlockRef* 和 *Expiration* 。

- *DependsOn* 字段存储着当前交易赖以进行的 ID。 换言之，若 *DependsOn* 指向的交易未能**成功**，则当前交易也无法得到验证。这里的“成功”是指交易不仅被纳入到了区块链中，而且得到了成功执行（系统没有返回任何错误）。

- *BlockRef* 存储着指向某个特定区块的参考地址，该特定区块是指最先打包当前交易的区块的前一个区块。参考地址（八字节数组）包括两部分：前四个字节包含区块高度（编号），后四个字节是相关区块 ID 的一部分。在实际运用中，*BlockRef* 的第二部分在区块不可用时（例如将来的某个区块）不必为其赋值。

- *Expiration* 字段用于设置交易过期/失效时间，以块为单位。具体而言，*Expiration* 加上 *BlockRef[:4]*（*BlockRef* 前四个字节的整数值）规定了可以最晚打包该交易的区块的高度。

有了 *DependsOn* 字段，我们便可以正式定义唯链雷神区块链上一系列交易的顺序，而且这种顺序受区块链共识机制的保护。在以太坊中，只有通过同一个帐户发出的交易才能以确定顺序（即 nonce 值定义的顺序）进行配置。在此系统中，nonce 值较小的交易必须在nonce 值较大的交易之前执行。但是，对于来自不同账户的交易，没有一种简单的方法可以确保某笔交易在另一笔交易之前执行。此外，唯链雷神区块链要求，一笔交易如有先决交易，则先决交易不仅要包含在一个经验证的区块中，而且执行后系统不能返回任何错误提示。而在以太坊中，只需要在已验证的区块中包含先决交易即可，不需要验证交易执行状态。

综上所述，*BlockRef* 字段有两种使用方式。它可用于证明交易的创建时间。相比之下，在大多数区块链系统中，尽管交易广播到网络的时间是已知的，但却无法知道交易是何时创建的。在这种情况下，很难确定交易创建后，是否过了一段时间才被发送到区块链网络之中。在唯链雷神区块链上，发起方需要根据当前可用的区块填写 *BlockRef* 的所有字节。

BlockRef 还可用于设置未来的区块高度来延迟交易的验收。在这种情况下，*BlockRef* 的后四个字节可以留空，因为指向的区块尚不可用。例如，Alice 可能想在未来的某个时间点向 Bob 转一些钱。她可以设置适当 *BlockRef*，然后发起交易，或将签署好的交易交给 Bob。

通过使用 *Expiration* 字段，我们可以终止已发出的交易。有了这么方便的功能，我们在交易陷入迟滞，需要等待几个小时甚至几天才能得到处理时，不会再束手无策。*Expiration* 字段的引入也使得交易更加安全，因为它可以避免因交易遭劫持并重复而引发的问题。

4.2.3 交易内工作量证明

很多人都遇到过这种情况：以太坊交易停滞长达数小时甚至数天，令人备感受挫。有时，我们必须设置一个相当高的 gas price，才能吸引矿工将交易打包到下一个区块。难道我们只有提高 gas price（相当于支付更高的交易费）才能提升交易优先级么？

答案当然是否定的，因为唯链雷神区块链出现了。我们允许单笔交易执行 PoW（工作量证明）机

制[1-3]，如此一来，交易发起方便可选择以挖矿的方式获取额外的 gas price，换言之，交易发起方可以利用其本地算力来增加交易的 gas price，而不必支付更高的交易费用。特别是，发起方可以通过交易字段“Nonce”来证明其已完成相应的计算工作，类似于现有区块链系统中实施的 PoW 机制。工作量之后被转换为一个系数，用以计算交易总 gas price。

请注意，交易发起方用以搜索理想 nonce 值的时间并不是无限的。数学运算需要将交易字段“BlockRef” 考虑在内。如上所述， BlockRef 可用于指向特定区块。验证 PoW 时， 系统将 BlockRef 字段的后四个字节与前四个字节标识的区块 ID 进行匹配。若匹配成功，则计算索引区块和当前区块之间的高度差（区块数）。只有在双方高度差低于规定的阈值时，PoW 方可生效，并计入交易的总 gas price。

4.2.4 多任务交易

唯链雷神区块链另一项新的内置功能是允许单笔交易执行多项任务。为此，我们明确了代表某个区块链任务的“Clause”结构。一笔交易可以包含零个或多个 Clause 子句 ，每个 Clause 包含三个字段：

- To – 接收方地址；
- Value – 转让给接收方的金额；
- Data –用于帐户初始化的 EVM 代码或某些输入的数据[2]。

然后，我们将“Clause” 定义为交易模型中的一组子对象， 以便交易可以执行多个任务。“Clause”模型可能会让人想起经典的比特币“UTXO”模型[3]，因为这两种模型都允许单笔交易拥有多个输出。但是，有了 Clause，用户可以输出的将不仅仅是余额信息。

多任务机制有两个主要特点：

- 由于单笔交易包含多个任务，因此任务的执行可视为原子操作，即要么全部成功，要么全部失败。
- 在交易执行过程中，所有任务按 Clause 规定的顺序逐个处理。

由此可以看到，多任务机制为我们提供了很大的能力和灵活性来处理实际应用中的复杂情况。例如，在需要进行资金分配、批量产品注册或任何其他需要整体执行多个任务的操作的时候，它可以提供简单、系统的解决方案。此外，第二个特点（即所有任务按 Clause 规定的顺序逐个处理） 使得它可以用一种安全有效的方式来描述多步流程。我们预计多任务交易的设计将大大简化唯链雷神区块链上许多应用的开发步骤。

4.3 权威证明（PoA）

设计区块链系统时需要做的一大决定就是选择并实施共识协议。共识协议不仅规定了如何在分散网络内就区块链状态达成共识，而且体现了为区块链系统所设计并实施的治理模型。回想一下， 我们的治理模型基本设计理念是：

完全的中心化或完全的去中心化都不可行，我们要在两者之间寻求折中和平衡。

工作量证明（PoW）、权益证明（PoS）和委托权益证明（DPoS）等主流协议均不适用于我们的系统。相反，唯链雷神区块链创建了符合我们治理需求的权威证明（PoA）共识协议，由此可以防止匿名区块生成者的出现，只有唯链基金会和唯链社区授权的 101 个已知验证者（超级权益节点）才能生成区块。

“建立好名声需要20 年，而只消五分钟就会让名声毁于一旦。如果你能想到这一点，那么你处理事情的方式就会有不同。”——沃伦·巴菲特

要成为唯链雷神区块链上的超级权益节点，个人或实体需自愿披露其身份和声誉，方有权申请成为验证和生成区块的节点[4]。事关身份和声誉，所有超级权益节点都会更有动力来保证网络的安全。在唯链雷神区块链中，每个超级权益节点都必须经过严格的身份认证（KYC）流程，并满足基金会设定的最低要求。

PoA 协议的主要特点总结如下：

1) 算力要求低；
2) 无需超级权益节点间通讯即可达成共识；
3) 系统连续性不受实际可用超级权益节点数量的影响；

4.3.1 协议详情

设计任一区块链的共识机制时，设计者都必须解决三个基本问题：

1. 区块何时生成？
2. 区块由谁来生成？
3. 如何从两条标准（合法）的区块链分叉中选择出唯一正确的那条（区块链主链）？

4.3.1.1 何时生成区块

在唯链雷神区块链中，区块每 Δ 秒产生一块。根据对区块链正式发布后的使用量预估，我们当前将 Δ 设置为10秒，设 t_0 为创世区块的时间戳，则高度 $n>0$ 的区块的时间戳 t_n 必须满足 $t_n = t_0 + m \cdot \Delta$，其中 $m \in N$ 且 $m \geq n$。

4.3.1.2 由谁生成区块

雷神区块链 PoA 协议确保每个超级权益节点被选择成为区块生成者的机会相同。但出于系统安全考虑，我们希望各超级权益节点生成区块的顺序具有一定的随机性。为此，雷神区块链结合使用确定性伪随机过程（DPRP）和 “活跃/非活跃”状态概念，以确定a是否是生成区块$B(n,t)$（n 为区块高度，t 为区块时间戳）的合法超级权益节点。其中，t 必须满足$(t - t_0)\ mod\ \Delta = 0$ 。为确定

由谁来生成区块，我们首先定义 DPRP 通过下方等式生成伪随机数$\gamma(n,t)$：

$$\gamma(n,t) = DPRP(n,t) \triangleq hash(n \circ t)$$

其中符号$\circ$表示将两个字节数组关联起来的操作。

A_B表示具有与B相关 “活跃”状态的超级权益节点集合。为验证a是否是生成区块$B(n,t)$的合法超级权益节点，我们首先定义：

$$A^a_{B(n,t)} = A_{PA(B(n,t))} \cup$$

然后用下方等式计算$i(n,t)$：

$$i^a_B(n,t) = \gamma(n,t) \bmod \|A^a_{B(n,t)}\|$$

$PA(\cdot)$ 返回父区块。当且仅当$i^a_B(n,t)] = a$时，a 为生成区块 $B(n,t)$ 的合法超级权益节点。请注意，我们在“活跃”二字上加了双引号，是为了强调这个状态并不直接反映某个超级权益节点当时是否实际在线，而仅仅是表明它们在网络上生成区块的有效性状态。

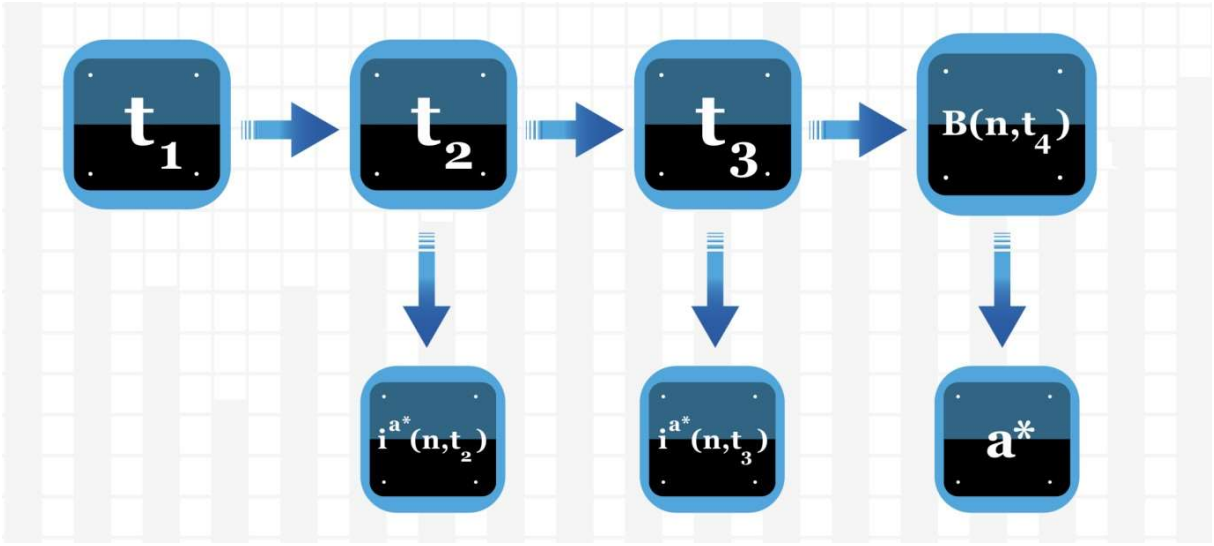


图 4.3.1 PoA 中的超级权益节点正在生成区块

为讨论超级权益节点的状态更新情况，我们先看一下上图示例。图中是四个允许生成区块的时隙$\{t_1,t_2,t_3,t_4\}$。实线部分表示已按时生成的已验证区块，而虚线部分表示缺失区块。对于每个时隙，系统可以用上述等式计算责任超级权益节点指数。系统会将所有未能按时生成区块的超级权益节

后，会将与$B(n,t_4)$相关的超级权益节点状态更新为：

- $A_{B(n,t_4)}[i^{a^*}(n,t_2)] \leftarrow$ *不活跃*
- $A_{B(n,t_4)}[i^{a^*}(n,t_3)] \leftarrow$ *不活跃*
- $a \leftarrow$ *活 跃*

a^* *是*$B(n,t_4)$. 的签名人 （signer）

从上述描述中可以看出，在合法区块时间戳t前，任何缺失区块均会彻底改变其后生成区块的超级

权益节点的顺序。这样一来，对于攻击者而言，想要找出未来由哪个超级权益节点负责生成哪些区块就更困难了。此外，唯链基金会还能特意赋予超级权益节点间或跳过生成某一区块的能力， 以此来增加不可预测性。

4.3.1.3 如何选择主链？

我们需要回答的最后一个问题是如何在两条标准的区块链分叉中选择“主链”。由于 PoA 没有算力竞争，所以“最长链”规则[1,3]不适用。相反，雷神区块链选择被更多超级权益节点见证的分叉作为两者 中的主链 。为此， 协议按下方等式计算区块 $B(n,t)$ 的累计见证量（AWN）：

$$\pi^{B(n,t)} = \pi^{PA(B(n,t))} + \|A^{B(n,t)}\|$$

由于$\|A \quad \|$负责计算与$B(n,t)$相关的活跃超级权益节点数量，可将其视为见证$B(n, \ )$的超级权益节点的数量。因此， AWN 最大的分叉将被选作主链。如 AWN 相同，雷神区块链将选择长度较短的分叉作为主链。

形式上 ，假定分支B和B'的最新区块分别为$B(n,t)$ 和 $B'(n',t')$，协议首先计算 AWNs$\pi_{B(n,t)}$ 和 AWN$\pi_{B'(n',t')}$。然 后系统做出如下决定： 如 $\pi_{B(n,t)} > \pi_{B'(n',t')}$，选 择$B$ 作为主链； 如 $\pi_{B(n,t)} < \pi_{B\ (n\ ,t\ )}$，则选择$B$ 作为主链。如$\pi_{B(n,t)} = \pi_{B\ (n\ ,t\ )}$，当$n < n'$ 时选择B作为主链，$n > n'$ 时则选择B' 作为主链，$n = n'$时保留当前主链。

4.3.1.4 系统连续性

在考量系统性能时，一定要测试其连续性，换言之，要弄清系统在什么情况下会宕机。从上述 PoA 协议可以看出，与 PBFT [5]协议相同，本系统对于实际可用验证人的数量没有最低要求，且能够执行多轮节点间通信以达成共识。超级权益节点可以免受外部因素影响，基于其从网络接收的信息连续执行 PoA 协议，并就当前区块链状态达成共识。通过这种方式，PoA 协议保障雷神区块链具有充分的鲁棒性和稳定性。

4.3.2 51%攻击问题

理论上，PoA 协议容易受到所谓的“51%攻击”的影响。该术语最初用于描述对比特币和以太坊等以 PoW 为基础的区块链系统的攻击。在上述系统中下，“51%”指超过一半的算力。共识机制不同，“51%”的含义自然也不同。在 PoA 中，

> *“51%”意味着目前可用的超级权益节点中，超过一半串通了起来。*

要发动这种攻击，不仅对攻击中受控超级权益节点的数量有要求，更重要的是，还要假定反叛超级权益节点会互相勾结。实际上，PoA 共识机制大大增加了进行这种 51%攻击的难度。

4.3.3 远程攻击

远程攻击是最常见的区块链系统攻击方式之一。攻击发生时，攻击者会先占据一个旧区块，并就此创建一个新分叉，然后尝试将其广播到全网以取代现有主链。通常，生成的新分叉比主链长得多，以此欺骗共识协议。

一般情况下，远程攻击无法用于攻击拟定的 PoA 协议。下图演示了对于 PoA 的远程攻击，其中白色区块表示主链，而灰色区块表示伪造分叉。一方面，由于两个连续区块之间必须有 Δ 秒间隔，所以攻击者不可能产生更长的分叉。另一方面，PoA 基于“活跃”超级权益节点的累计数量来选

择主链。在这种情况下，要想用伪造分叉替换当前主链，攻击必须掌握超过一半的可用超级权益节点，才能生成一条比现有分叉更大的分叉。如此，远程攻击就变成了上述 51%攻击。

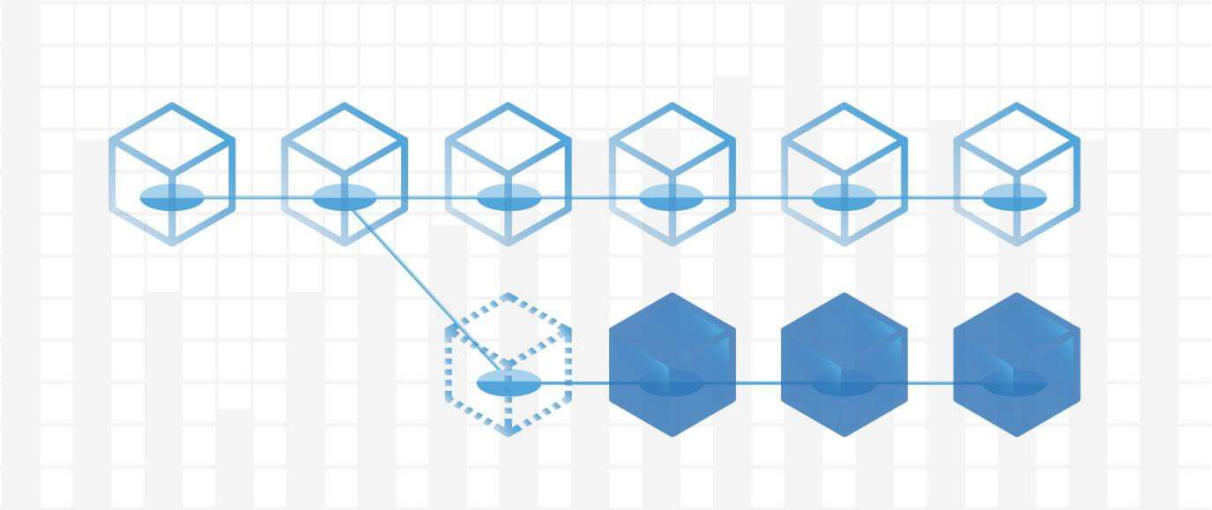


图 4.3.3 远程攻击

5 平台架构及应用开发

5.1 开发方法

从始至今，唯链一直初心未改，我们始终致力于通过解决问题、不断进步来实现区块链技术的落地，并提供更具商业价值的应用。唯链未来的整个生态系统将发展成为一个网络，以新兴商业应用为点，以新兴商业模式和服务为线，连点成线，形成网络。

区块链是“信任的机器”，是可信任生态系统的基石。未来的区块链世界将对其上运行的每个元素（如人员、物体和资金）都进行数字化。 唯链想要通过以下步骤改变现实的商业世界：

1) 将任何参与者可以识别、访问和管理的对象数字化。唯链借助物联网标签或传感器，使用统一的唯链 ID（VID）来标记对象，从而将对象的物理实体与区块链上的数字化虚拟身份连接起来；

2) 在 VID 和对象的哈希数据之间建立不可更改的连接，以此表明对象已经通过认证，而且可以共享；

3) 用智能合约来描述对象的可信任商业活动，如生产、授权、所有权转让、商业协议和交易等；

4) 将可编程 VET 应用在不同的业务活动中充当价值载体，实现高效、高速的价值转移；

5) 通过适当的产品和服务发掘和打造一种全新的万物可信互联的商业模式；

6) 将商业应用、资产、产品、服务、社区参与者和活动联系起来，共同构成一个可信任的商业生态系统。

在这种方法论的指导下，唯链能够将目标产品、参与者和商业活动从现实的商业世界转移到区块链的世界。通过这种方式，我们可以将合作关系数字化，实现各行业、企业和个人之间更大规模的系统化运作。信任和合作的成本将大大降低，对于单个实体如此，对于行业、国家乃至整个世界亦是如此。人人参与，便可优化资源，新的商业模式也将随之诞生。

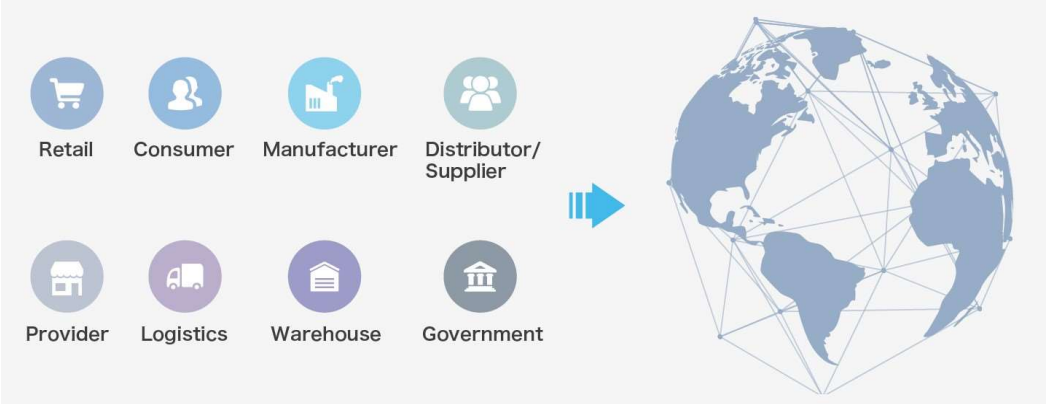


图 5.1 传统世界中的标准数字化

5.2 唯链雷神区块链架构

唯链技术开发的基本规则将由应用驱动。我们认为，应用案例将推动产品开发，而产品开发推动技术发展，而非相反。

唯链的技术发展路径几乎就是区块链技术发展的一个缩影，并与之紧密相连。最初的想法是在 2015 年中产生的，从那时起，唯链就开始了一系列技术概念验证（TPOC）。在不同行业用例需求和项目需求的推动下，技术交付在过去三年中经历了几轮大的迭代和更多小的迭代。

如果我们将未来的唯链雷神生态系统比作全功能高速公路，那么区块链底层网络就像路网。在这条路上还有其他的服务和功能，如免费通道、加油站、休息站、应急路线和服务等。唯链不仅是在为平台构建区块链底层技术，还提供配套的基础架构服务、公共工具和通用应用，如此一来， 任何人都能以方便且专业的方式开发、部署和使用区块链应用。

从应用的角度来看，所有的商业伙伴都将更加关注解决方案，而不仅仅是技术。因此，唯链雷神区块链的技术组合不仅包括区块链技术，还包括开放协议（如物联网、人工智能等），以提升互连性。

5.2.1 唯链雷神平台的四层技术架构

唯链雷神平台的四层技术架构如下：

触点：将真实世界的信息数字化。我们使用 NFC 和 RFID 芯片对产品和传感器进行数字化，通过传感器来捕获环境、惯性、气体和位置信息。触点是唯链雷神的双手和双眼，用于连接世界并收集数据馈送。

连接：连接单元传输经传感器捕获的数据。连接单元和传感器共同构成了唯链雷神区块链平台中的物联网技术组合。

区块链底层：区块链底层负责进行交易，并存储以上收集到的数据。在区块链上部署并运行智能合约可以支持多方协作活动。

应用和服务：区块链内置的应用和公共服务可以提供基础架构服务，简化和标准化应用开发以及常见协议和接口，如用于 KYC 的 VeVID、用于投票的 VeVOT、用于智能合约认证的 VeSCC、用于智能合约库的 VeSCL 和其他一系列技术协议，如侧链、交叉链、数据馈送、预言机等等。

5.2.2 唯链雷神区块链平台架构

唯链雷神区块链的平台架构以应用案例的商业应用为驱动。这种架构的基本规则如下：

1) 独立与派生的技术层；

2) 能够实现标准化、模块化，灵活度高，可快速迭代；

3) 开发方便、快捷；

4) 向其他技术和系统开放的协议.

下图展示了唯链雷神区块链平台的整体架构：

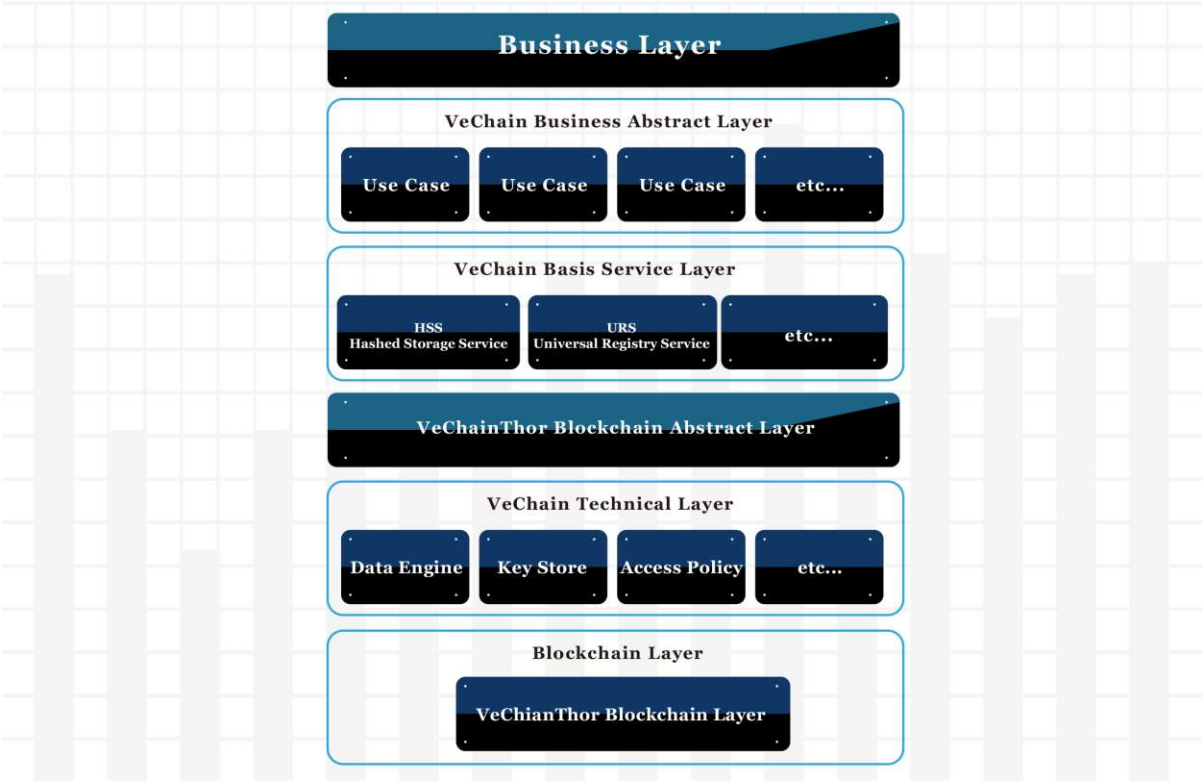


图 5.2.2 唯链雷神区块链平台架构

关键层有两个：区块链抽象层和业务抽象层。

5.2.2.1 区块链抽象层

最底层为基础架构层，包括区块链底层技术，具体有以下内容：

1) 区块安全协议（BSP）：通过 BSP 实现在每个数据区块上签名的功能，保证超级权益节点和 PoA 共识的安全性。只有具备授权签名的数据区块才会被开采和接受；

2) 数据组嵌入协议（DGIP）：DGIP 可以通过批处理将数据组嵌入到区块链；

3) 分层归档协议（LACP）：LACP 可用于不同层级的数据存储，以增强数据的可伸缩性和可索引性。

4) 多交易协议（MTxP）：一次交易操作多个对象，换言之，在一个交易中，一个“from”可以执行多个“to”；

5) 分布式跨链同步通讯协议（DCCP）：DCCP 是用来实现在不同的区块链网络之间进行数据

同步和互相操作的一种跨链解决方案；

6） 交易数据隐私协议（TxDP）：TxDP 可以确保交易和数据的隐私性。

7） 更多内容，敬请期待。

上一层是智能合约抽象层。实现各种场景下的技术抽象，构建标准化、模块化的智能合约模板，进一步整合和定制不同行业、企业和应用案例的智能合约。目前智能合约库包括 VID 注册、数据绑定、状态数据嵌入、数字所有权、所有权转让、授权申报、授权转让、多重授权等。

智能合约库（SCL）是唯链雷神基础架构服务套装的一部分。我们计划同社区一道启动该项目，为开发人员构建并丰富一般性、模块化、经认证的智能合约，促进商业应用开发和智能合约开发。

5.2.2.2 业务应用抽象层

基本服务抽象层是该层分类的底层，其目的主要是建立包括哈希存储服务（HSS）、通用上链注册服务（URS）等基本服务模块的标准智能合约。此层还包含唯链雷神服务的公共服务模块，包括唯链雷神区块链浏览器的索引服务、审计节点的通用数据审计服务（UDAS）、区块链数据监视服务（BDMS）、分布式内容寻址存储系统（DCASS）、合约名称服务（CNS）、数据分组服务（DGS）、隐私信息保护服务（PIPS）、创世纪合约服务（GCS）等。这些公共服务加上基本模块，有助于降低智能合约开发的难度，更容易进入智能合约开发。

我们将继续加强这一层，重点开发更便捷的工具，如可视化智能合约开发工具包、更多语言支持、智能合约连接器等。通过这些工具，来自不同行业且具有不同背景和不同专业知识的开发人员， 甚至是几乎没有区块链经验的开发人员都可以轻松开发和部署智能合约，满足商业应用的需要。

中间层用于基本服务层与业务应用层之间数据交互的标准应用程序接口。此层主要是对不同业务系统的系统接口进行标准化，特别是广泛使用的大型企业系统或互联网平台。我们已经推出了与 SAP、WMS 和 Salesforce 等主要企业应用相对接的接口，以及常见网络和移动应用接口。我们将继续开发此类接口。

顶层是业务应用抽象层，随业务场景和应用的变化而变化。该层的开发人员甚至不需要具备区块链开发能力，但应该知道如何连接到唯链雷神区块链，并通过标准协议来调用智能合约。

5.2.2.3 架构详解

在商业应用和唯链雷神生态系统建设的推动下，我们将唯链雷神区块链的详细技术架构设计如下：

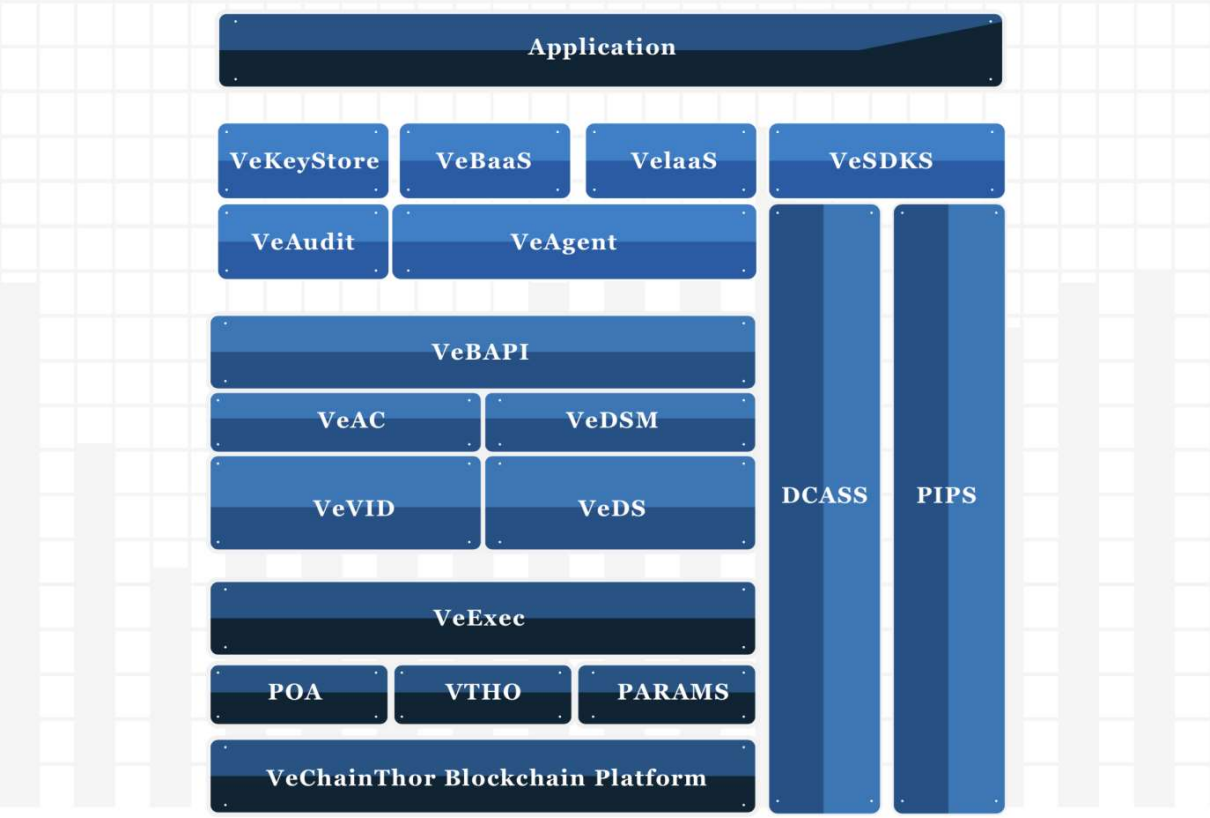


图 5.2.2.3 唯链雷神区块链技术架构

- VeKeystore - 这是应用层负责私钥管理的一项公共服务。企业用户可以选择自行管理密钥或委托给唯链雷神区块链公共服务。

- VeBaaS - 唯链雷神区块链平台上的“区块链即服务”（BaaS），是企业用户的区块链服务管理门户。每个商业伙伴都能够根据行业、业务场景和具体需求选择或创建自己的区块链解决方案。

- VeIaaS - 唯链雷神区块链平台上的“实施即服务”，属于“一键部署”模块，允许商业伙伴通过预定义的软件包在不同的云平台中部署唯链雷神区块链节点。我们同世界各地的知名云服务商开展合作，不断丰富我们的产品组合，为终端用户提供更多选择。

- VeSDKS - 唯链雷神区块链平台的软件开发工具包套装，包括但不限于以下内容：

  ✓ VeSDKS.DB，用于集成云服务商的传统数据库（如 mysql、oss / s3）的 SDK。

  ✓ VeSDKS.DCASS，用于集成唯链雷神区块链平台的分布式存储服务、分布式内容地址存储系统的 SDK。

  ✓ VeSDKS.Privacy，用于隐私保护的 SDK，可用于多种商业场景，如 KYC 应用程序 VeVID。唯链一直与DNV GL 等多家知名安全服务提供商合作，落实不同的选择和解决方案。唯链计划研究和开发信誉良好的开源解决方案，例如斯坦福计算机科学系推出的 Bulletproof 协议。

- ✓ VeSDKS.AA，用于访问授权的 SDK，可用于智能合约、数据、文件、系统等多种访问场景。

- VeAudit - 唯链雷神区块链网络、智能合约、交易等的基本审计服务。
- VeAgent - 用于调用在唯链雷神区块链上部署和运行的智能合约的接口。
- VeBAPI - 连接区块链的初始 API。
- VeAC - 用于数据集和 VeVID 的访问控制。
- VeDS - 用于定制数据的存储。
- VeExec - 以下智能合约的执行器：
  - ✓ POA，为超级权益主节点管理智能合约，包括活跃列表、备用列表、签名控制等。
  - ✓ VeThor，管理 VTHO 的智能合约，如管理 VTHO 的生成速率。
  - ✓ PARAMS，包括以下参数：
    - 奖励率 30%，可调整；
    - 被认定为超级权益节点要求持有 2500 万个 VET，可调整；
    - gasPrice，支付和智能合约交易实际消耗的 VTHO，可调整；
    - GrowthRate，可调整。
- DCASS，分布式内容处理存储系统。
- PIPS，隐私信息保护系统。

5.3 更多技术细节

下面我们更深入地了解一下应用案例中相关功能的更多技术细节。

5.3.1 VID 的生成和哈希运算

唯链雷神区块链使用了SHA256 哈希加密算法用于VID 的生成，VID 可以通过自主开发的 VID 生成器并行被写入 NFC、RFID、二维码等各种 IoT 标签和设备，不同类型的标签对应不同的商品，从而实现区块链 ID 与现实世界商品一一对应关系。 IoT 标签是根据用户的需求和产品的功能设计的。

用于唯链 ID 加密的 SHA256 公式为 **SHA256(domain + '.' + ID)[12:]**。其中，domain 是指唯链ID 所在数据库数据结构表的域名，如“**com.VeChain.dbname.tablename**”。

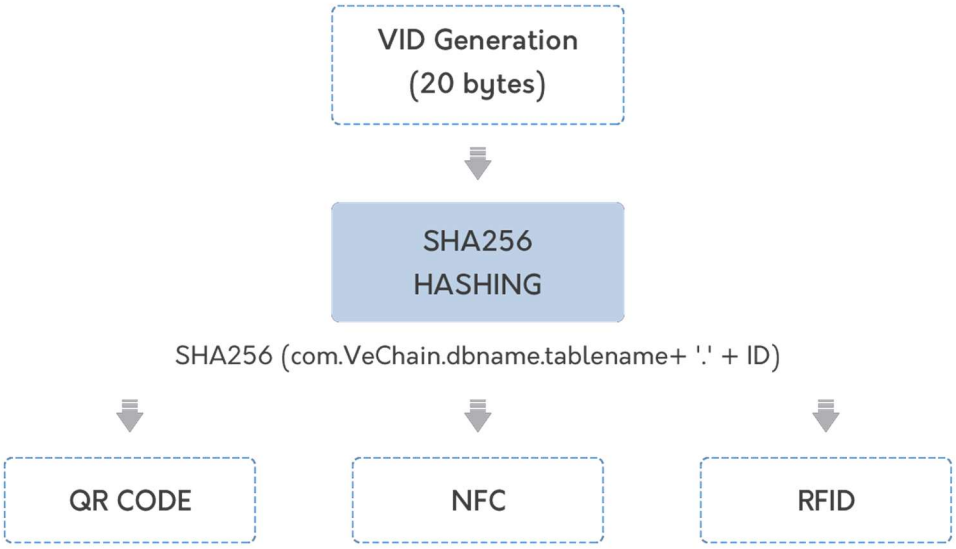


图 5.3.1 VID 的生成和哈希运算

5.3.2 VID 在区块链上的存储

如上所述，经过哈希的 VID 可以根据客户的需求写入不同的标签介质内。标签备好后，需要经过测试才能“激活”。通过一款客制化的支持移动端和PC 端的软件“V-Operation”进行唯链 ID 激活操作。激活后，唯链ID 就被写入区块链中，并于全网节点进行广播同步。

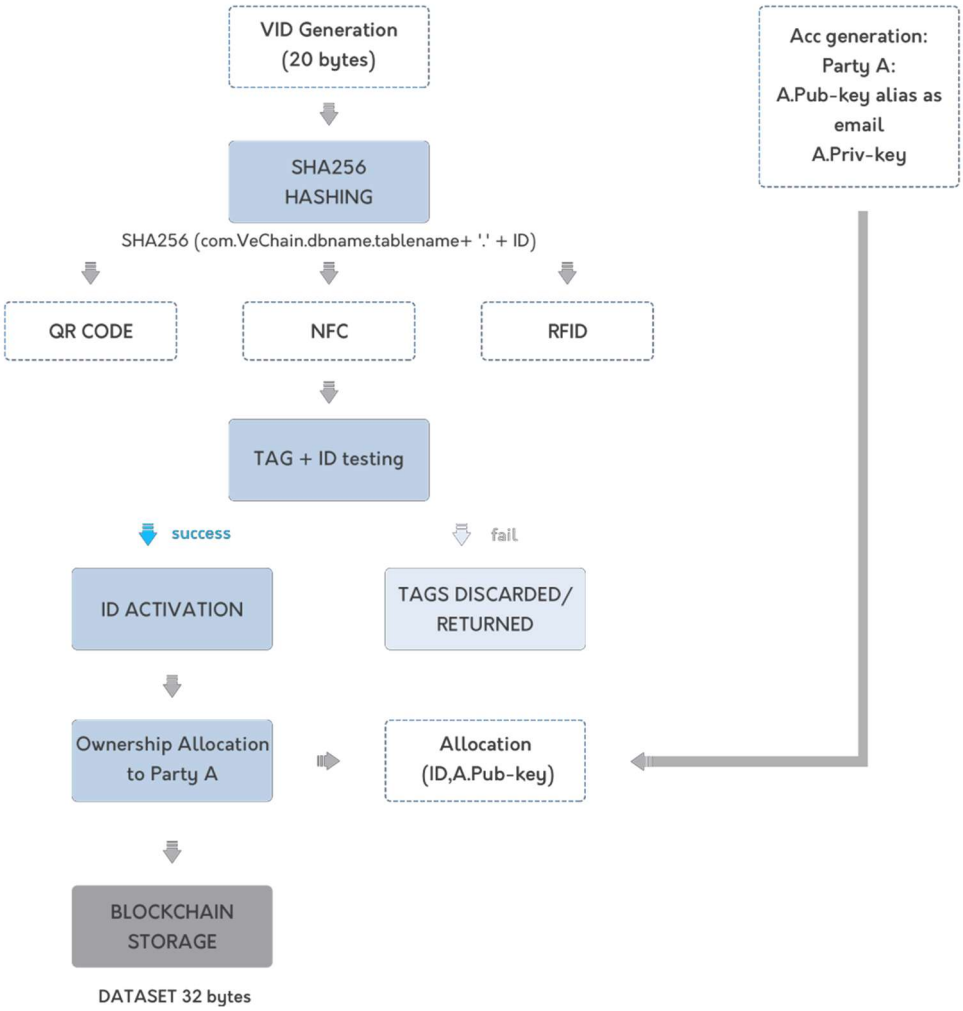


图 5.3.2 VID 在区块链上的存储

5.3.3 区块链上的数字所有权

唯链利用特殊客制化的智能合约**进行基于授权的数字所有权管理。**唯链 ID 通过公私密钥对表示对物品的所有权，并与某一账户相关联。

公钥信息是面向大众公开的，就像是邮箱地址一样，任何人皆可识别、访问。而私钥类似于密码，代表拥有对物品进行操作的权限。基于授权的数字化所有权管理就是在物品 ID 和控制相应私钥的所有者的公钥之间建立连接。

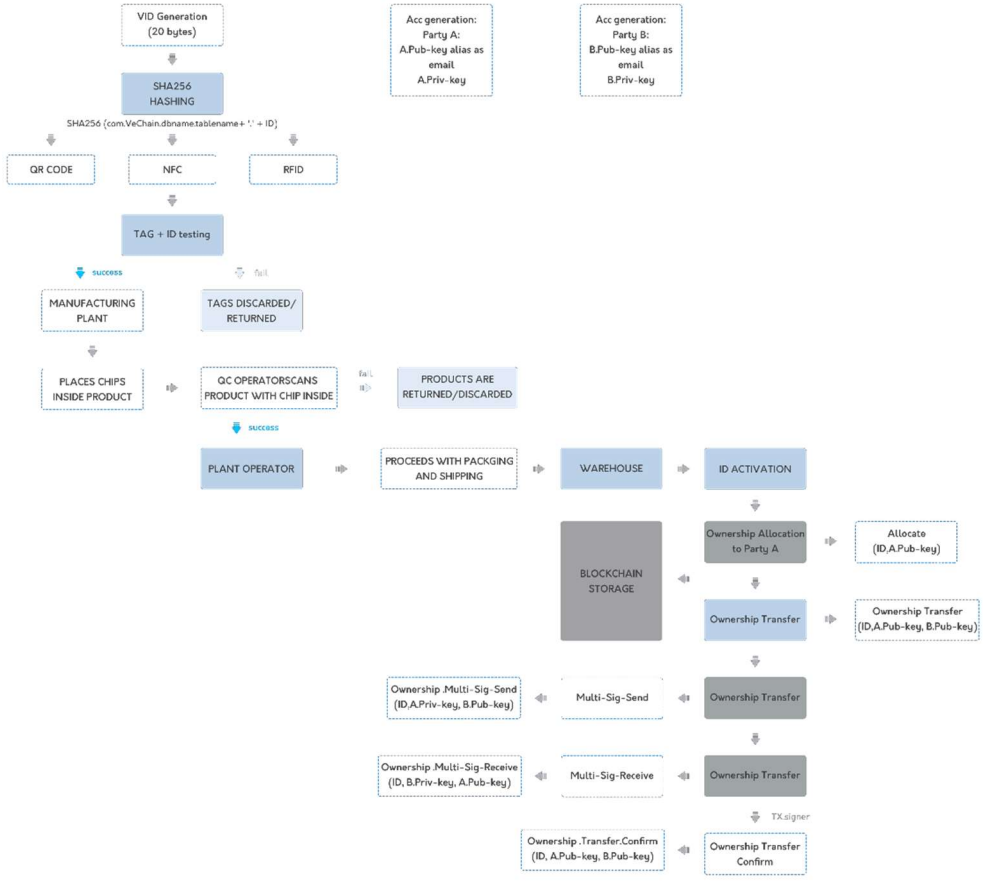


图 5.3.3 区块链上的数字所有权

5.3.4 数据哈希存储（数据证明）

唯链接受任何形式的数据：（字符串、数字、布尔值等），数据通过其哈希值（SHA256 哈希运算）进行识别，通过RESTFUL API 进行数据访问举例：

- **数据存储**
- 上传 https://domain/hss/
- **数据检索**
- 获取 https://domain/hss/{hash}

数据可以进行自验证。提取数据后，可以通过验证其哈希值来达到验证数据的目的。

图 5.3.4 数据哈希存储

5.3.5 标准 API 网关

通用应用程序体系结构接口专为复杂进程设计。API 网关是所有 API 请求的统一入口，它封装了应用程序的内部架构，上层应用只需与网关进行交互即可，无需调用某个特定服务。当区块链、智能合约或服务升级或迭代时，其内部架构是完全透明的，只需保证交换协议的正确性，而无需关心接入方式的变化。

API 网关网络拓扑图、部署图和功能图如下：

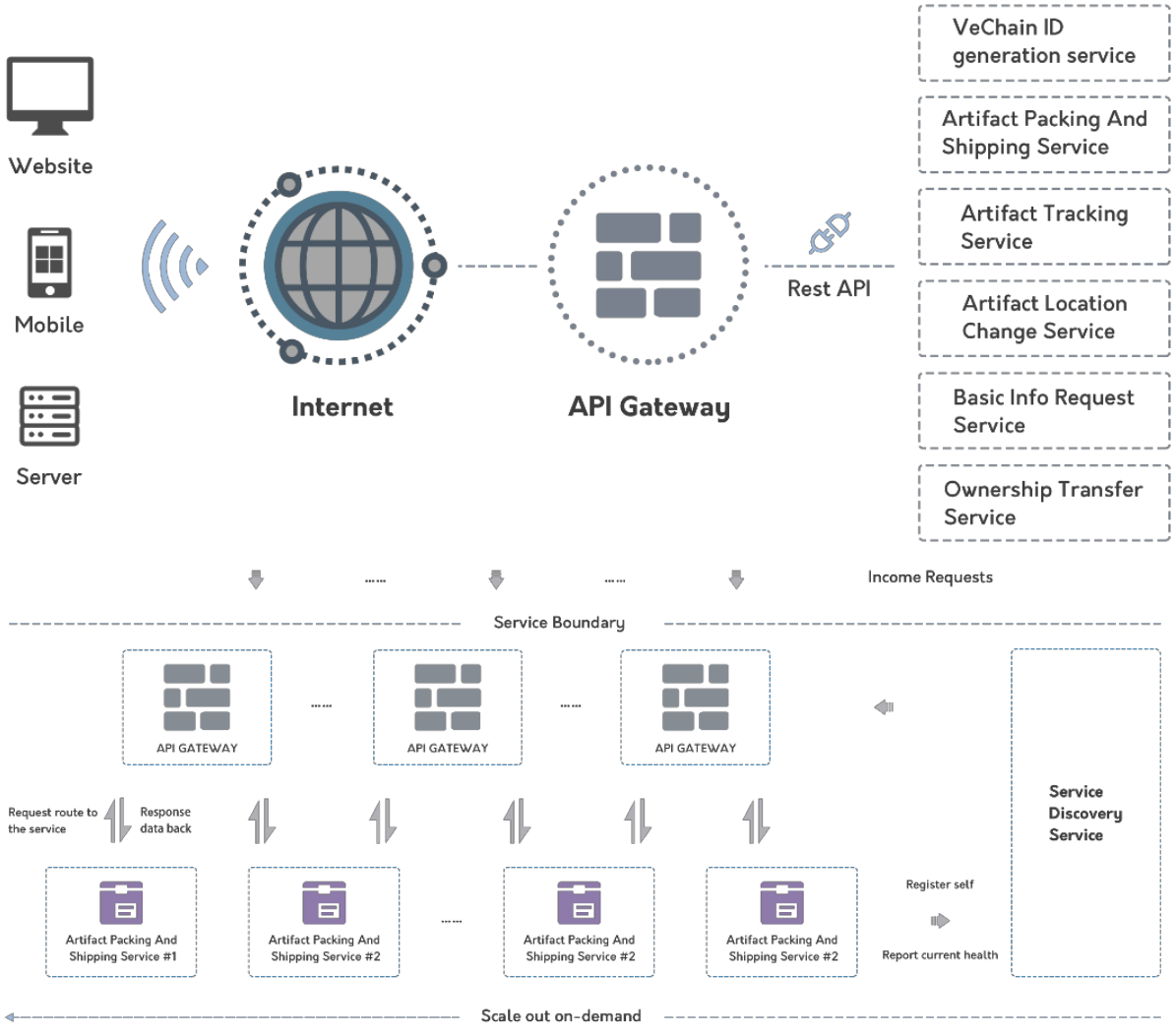


图 5.3.5.1 API 网关-1

服务器的资源是有限的，不过特定功能节点的横向扩展特性也方便大规模的访问。对于同一服务 的不同应用，API 网关可以保证将服务请求进行适当分流。API 网关支持包括一致哈希、IP-hash、随机访问以及优先访问等不同访问策略。与此同时，服务发现以及 API 网关服务可以根据实际需求进行相应拓展。

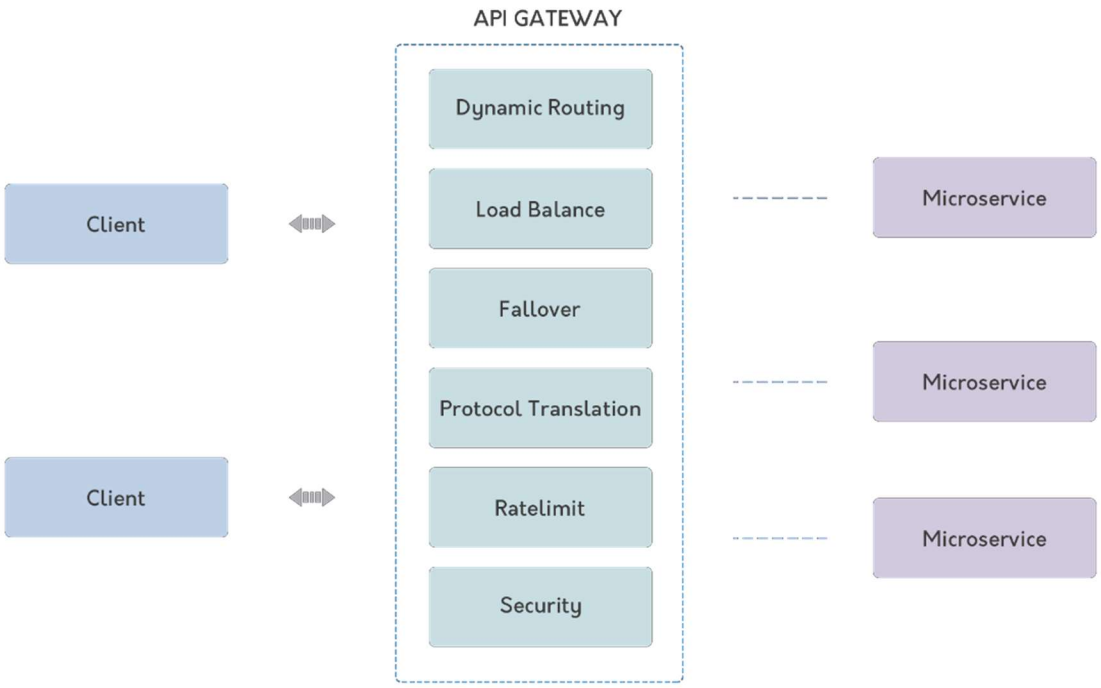


图 5.3.5.2 API 网关

5.3.6 服务发现协议（SDP）

API 网关需要知道与其通讯的每个微服务的“地址”，即 IP 地址和端口号。在传统的应用中，地址定位与连接已较为困难，而基于云存储的微服务应用的地址连接也并非易事。基础架构服务通常有一个静态地址，由 OS 环境变量定义。然而，确定应用程序服务的地址并不容易，因为应用程序服务地址是动态分布的，并且会进行自动容量调整或定期升级。

服务发现协议主要有两个模式：客户端发现模式和服务器端发现模式。唯链雷神区块链平台选择了后者。用户可以通过 API 网关发起一个服务请求，API 网关检查服务注册信息，并将服务请求转发至可用的服务实例。服务器端发现模式的优势在于用户不必关注服务的细节，只需要专注于服务请求本身，这就简化了发现服务所需编码的逻辑流程。

服务注册是发现服务的核心，其功能是构建和维护内含服务实例网络地址的数据库。服务注册需要保持高可用性，并能实时进行更新。

自注册模式适用于服务实例，服务注册的登入和登出都由服务实例执行。此外，服务实例还会发送一个心跳包以保证注册信息的实时性。我们在后端使用 ETCD 提供高可用性、分布式、一致性的密钥存储，用于配置共享和服务发现。

5.3.7 微服务

微服务是唯链雷神区块链所有后台服务的统称。微服务可以根据应用案例的不同要求进行量身配置，从而保证不同业务之间的隔离性。微服务可以保证服务的灰度发布（软件新版本和更新版的平稳过渡），实现快速升级或降级。在唯链雷神区块链的 API 网关中，微服务提供以下基本功能：

注册与注销
微服务器在启动时必须主动注册服务发现服务（SDS），关机时必须进行注销。 SDS 可以保存实例状态 30 秒，如果在关机时未进行注销，则 30 秒后SDS 自动进行服务注销。

服务健康度报告
SDS 无法主动获知后端实例的可用性。因此微服务必须每隔 30 秒报告其健康度信息。

微服务比传统服务更为复杂，特别是后端服务之间的通讯。由于 SDS 需要实例进行自注册，因此所有的实例需要遵循统一的注册规则。将来可能考虑接入第三方注册服务，这些服务可以部署微服务实例，加入一些配置信息，并且可以检查实例健康度并报告给 SDS。如此一来，微服务就成了一个纯粹提供API 服务的应用。

5.3.8 数据哈希存储服务（HSS）

哈希数据存储服务（HSS）是一个提供数字文件、图片、文档及其他类型文档的分布式存储服务。HSS 服务与唯链深度结合，保证存储数据的安全性、完整性和隐私性，同时对数据进行所有权及权限管理。

HSS 主要包含两个部分：数据存储服务和操作存储服务。数据存储服务负责外部数据存储、访问控制和授权管理；操作存储服务负责计算数据存储路径、数据子集和存储。

随着存储服务规模化发展，考虑到系统可靠性，需要经常进行数据备份。为了保证数据的高可用性，常常需要预留多个备份，这种备份方式浪费了大量的存储资源，存储成本也变得愈发高昂。

分布式存储系统的出现很好地降低了传统数据备份的成本。通过创建分布式存储系统，可以简化数据备份程序，降低磁盘利用率，同时提高数据的可用性和耐久性。存储系统还运用了抹除码（Erasure Code）和纠删码（Reed Solomon ）技术。其中，抹除码主要使用数学运算的方式进行原始数据验证，从而满足系统容错率，抹除码可以用作丢失或损坏数据的重建。纠删码经常嵌套在存储系统的抹除代码中使用。我们的HSS 服务使用纠删码对数据进行分片处理，数据可以被细分为若干分片，即使部分分片丢失仍可以通过剩余部分还原原有数据。

此外，HSS 服务还适配亚马逊 S3 接口调用。考虑到大多数开发者对亚马逊 S3 服务及其 API 熟悉度较高，HSS 允许较低级别数据通过亚马逊S3 接口进行调用，从而降低了外部数据接入的成本。

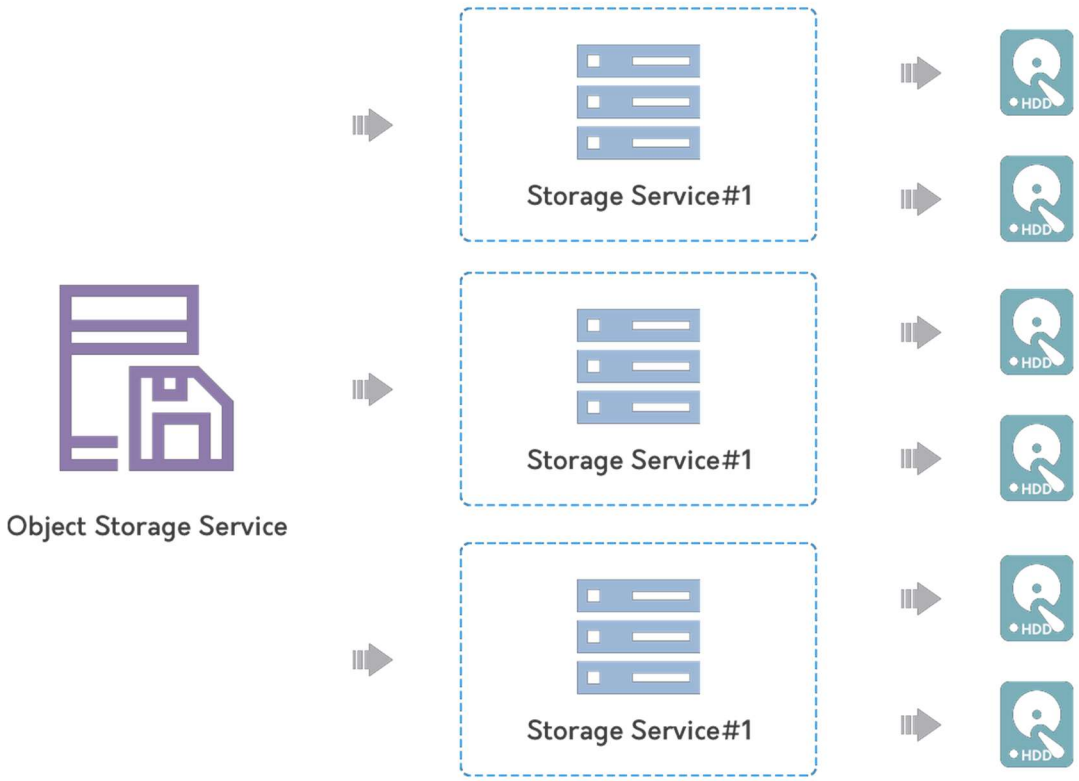


图 5.3.8 哈希存储服务

5.4 区块链与物联网

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。*”

由以上定义可以看出，物联网主要由两部分组成：触点（传感器）和连接。

触点用于真实世界的信息数字化，方式有两种：一是利用标签技术在实体物品和数字化虚拟身份之间建立一种约束性连接；另一种是利用传感器技术收集关键描述性参数，如温度、湿度等环境信息。

连接用于信道和传输协议，比如蓝牙、WIFI、移动互联网、2G/3G/4G/5G 等。

未来的物联网发展特点是应用广、类型多、起量高、发展快，并将对全球产业产生重大影响。从数量上讲，IoT 设备的总量在未来几年有望持续 15%~20%的增长率，IDC （International Data Corporation） 曾经预测全球 IoT 设备总量在 2020 年将达到 450 亿的数量。

5.4.1 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。

5.4.2 区块链与物联网

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.

我们认为物联网技术和区块链技术在应用中密不可分，物联网技术旨在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。

5.4.3 唯链雷神区块链中的物联网开发

大多数致力于开发应用的商业伙伴都不仅仅专注于技术，而会更偏向寻找解决方案，因为解决方案往往是通过整合区块链、物联网和人工智能等各种技术而形成的。

物联网是唯链团队的一大关键技术能力。唯链拥有一个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) NB-IoT 的安全和授权模块。

尽管物联网设备和应用都很复杂，但唯链重点关注以下物联网设备，并从不同角度进行分类：

1) 从供电的角度我们分为：

- **主动模式设备**：传感器、GPS 等有源设备
- **被动模式设备**：NFC、RFID 等无源设备
- **混合模式设备**：有限供电的设备，可通过外部激活

2) 从通讯距离的角度我们分为：

- **近距离设备**：解决距离 10 米以内设备的通讯问题，比如 NFC（1 米以内）、 RFID（10 米以内）、蓝牙（10 米以内）等。
- **中距离设备**：解决距离 1 公里内设备的通讯问题，如 WiFi、sub 1g、lora 等。
- **远距离设备**：解决距离大于 1 公里设备的通讯问题，如 NB-IoT 等

我们在传统物联网设备的基础上进行了创新，加入了基于区块链的设备 ID 和非对称秘钥算法：

1) 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。

2) 非对称秘钥算法：非对称秘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对，其中公钥是识别码，私钥是安全签名。在唯链雷神区块链的设计中，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。

下图是唯链雷神区块链集成的 NB-IoT 安全模块芯片设计示例。

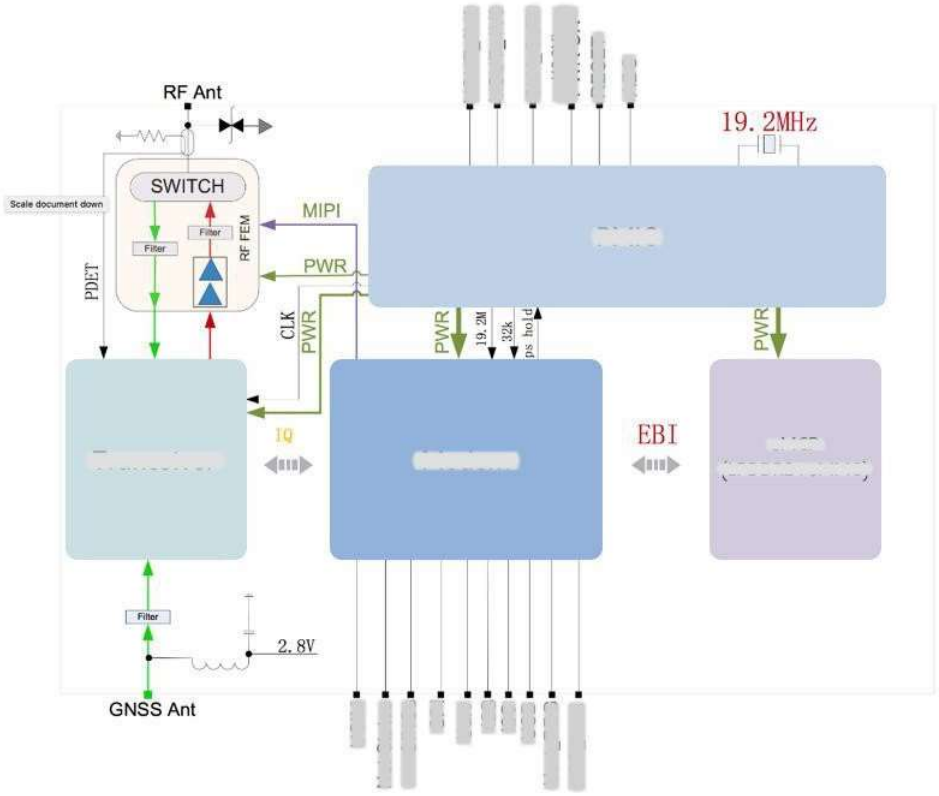


图 5.4.3 NB-IoT 安全模块

5.5 技术测试

唯链团队遵循专业的软件测试流程来评估各项技术交付的测试阶段。软件应当是可预测且稳定的，符合产品定义和设想，不会有预料之外的结果。过去几十年，随着信息系统在复杂性、智能化和 规模上的不断发展变化，软件测试也在不断地发展和迭代，理论和实践逐渐系统化和成熟化，在 保证软件质量的过程中发挥着更加重要的作用。数据显示，在一个成功的软件项目中，测试工作 通常占用超过 **50%的项目时间和成本。**

软件测试最核心的问题是：哪个子集最有可能发现和定位最多的错误或漏洞？我们将测试分为如下几大类：

白盒测试：白盒测试又称玻璃盒测试或结构测试。这种方法把被测软件看成白盒。测试实例根据被测软件的内部结构和逻辑来设计，测试根据程序的路径和流程进行。白盒测试的主要技术有控制流测试、数据流测试、分支测试、语句覆盖、判定覆盖、改良后条件覆盖、主路径测试和路径测试等；

黑盒测试：黑盒测试又称功能测试，被测软件称为黑盒。测试人员必须知道软件的功能，但不知道如何实现相关功能。测试用例是围绕规格和要求构建的。黑盒测试技术主要有结对测试法、等价类划分法、边界值法、因果图法、错误推测法、状态转换测试法等。

灰盒测试：灰盒测试是白盒测试和黑盒测试的结合。灰盒测试员部分了解软件的内部结构，包括有权访问内部数据结构文档及所用算法。灰盒测试多用于集成测试阶段，不仅关注输出、输入的数据准确性，同时也关注软件内部的情况。

唯链建立了一个独立的测试团队，负责软件质量管理，确保软件照其设计运行。需要强调的是，合理有序的文档是唯链雷神平台和应用的测试和整个开发的重要组成部分，这些文档包括但不限于：

1) 主测试计划（MTP）；
2) 层级测试计划（LTP）；
3) 层级测试设计（LTD）；
4) 层级测试案例（LTC）；
5) 层级测试流程（LTPr）；
6) 层级测试日志（LTL）；
7) 测试报告，包括主测试报告（MTR）、层级测试报告（LTR）、异常报告（AR）等。

唯链已在所有技术开发中实施全面的测试管理规则，覆盖区块链底层技术、工具和服务、应用、 物联网（硬件和软件）等领域。唯链和其他软件项目没有区别：测试工作是一个逐步收敛的过程， 严格遵循计划-执行-检查-调整（PDCA）循环。

P（计划）：包括测试方案的确定，包括：单元测试、集成测试、系统测试（功能、性能、安全、兼容性）、验收测试等
D（执行）：根据测试方案执行测试。
C（检查）：总结测试的结果，反馈给开发团队。

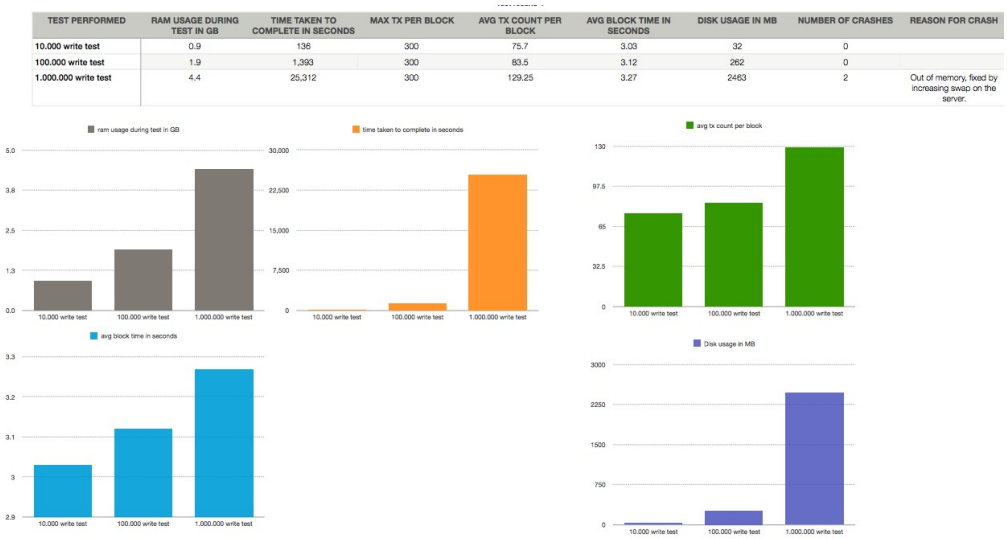
A（调整）：开发团队针对测试结果进行源代码的改善和修正。

唯链测试的主要目标包括：

1) 下位机（PLC）：物联网部分的嵌入式软件；
2) 客户端：PC 端，移动终端（iOS、安卓）和其它终端；
3) 云端和服务器；
4) 区块链节点、应用和数据库；
5) 智能合约；
6) 服务；
7) API 。

下图是唯链雷神区块链部分压力测试数据展示：

TEST PERFORMED	RAM USAGE DURING TEST IN GB	TIME TAKEN TO COMPLETE IN SECONDS	MAX TX PER BLOCK	AVG TX COUNT PER BLOCK	AVG BLOCK TIME IN SECONDS	DISK USAGE IN MB	NUMBER OF CRASHES	REASON FOR CRASH
10.000 write test	0.9	136	300	75.7	3.03	32	0	
100.000 write test	1.9	1,393	300	83.5	3.12	262	0	
1.000.000 write test	4.4	25,312	300	129.25	3.27	2463	2	Out of memory, fixed by increasing swap on the server.



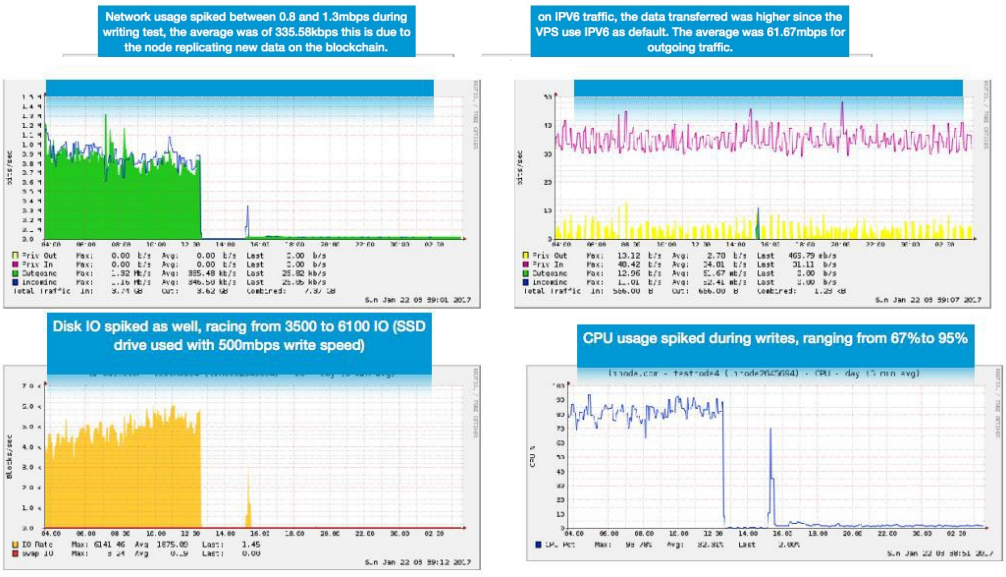


图 5.5.1 部分压力测试数据，测试环境为跨国多地最低配置云服务器。配置参数为 2G 单核 CPU / 4G 内存。

5.6 技术路线图

唯链的技术开发历经两年多，核心发展思路围绕三个方面：应用性、标准性和安全性。唯链团队会继续围绕这三个基本思路进行技术的开发。

唯链技术部门分为几个小组：

1) 研发——侧重于区块链技术的基础架构层，以及物联网、人工智能等新兴技术的研究和实验；

2) 开发交付——在战略计划、商业计划和研发的推动下进行开发和实施；

3) 区块链底层技术；

4) 应用、服务和工具；

5) 物联网 – 触点和连接；

6) 安全；

7) 测试、部署和维护。

下述唯链雷神技术开发路线图体现了唯链雷神区块链的愿景和使命：

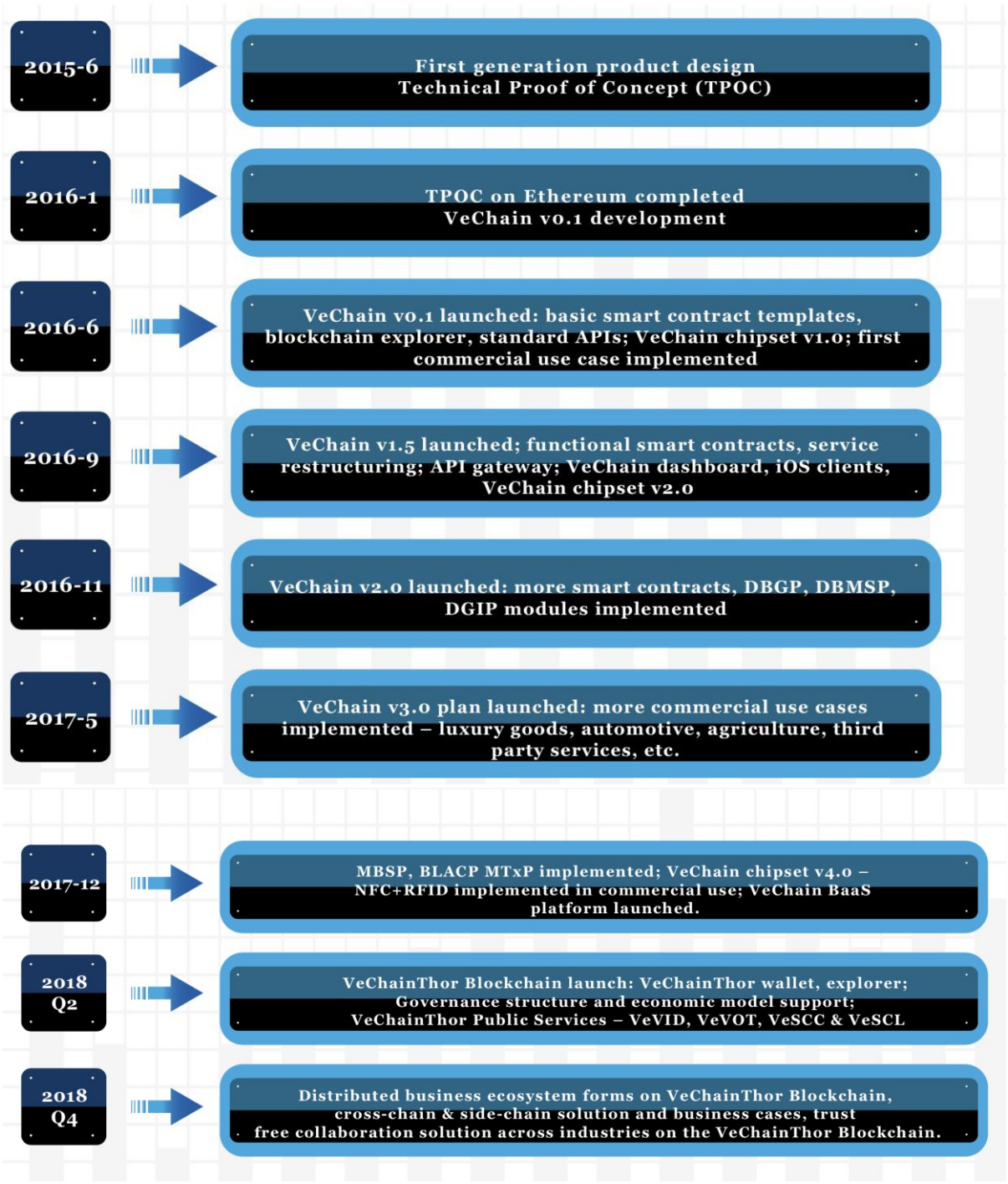


图 5.6.1 技术开发路线图

6 应用案例和应用程序

成为先驱殊为不易，而始终不忘初心、满怀热情则更为艰难。

自 2016 年初推出首代产品和解决方案起，唯链便开始积极探索区块链的商业应用案例。2016 年，我们同全球各大企业合作开发了四种应用案例。2017 年，这一数字达到了 20 多个，涉及一些重要的合作伙伴关系。截至 2018 年初，有超过 210 个应用合作机会正在沟通中。

全球市场正迅速壮大。我们不是孤军奋战，我们不断壮大的社区已经成为一股重要力量，同唯链团队一道，共同致力于唯链雷神区块链的发展壮大。在总计 210 个潜在的应用案例中，有一半以上是社区提供的。社区已经成为唯链团队不可或缺的一部分。

无论是现在还是未来，这一生态均由各种应用和新的连接构成，如同点与线的关系。唯链雷神区块链的使命是同商业伙伴一道打造和推动更具商业价值的应用。唯链雷神区块链平台将承担载体功能，不仅拥有强大的区块链底层基础架构、相匹配的公共服务和工具，还得到了唯链基金会、企业和个人等多方面的支持。

下图显示了唯链雷神区块链应用结构：

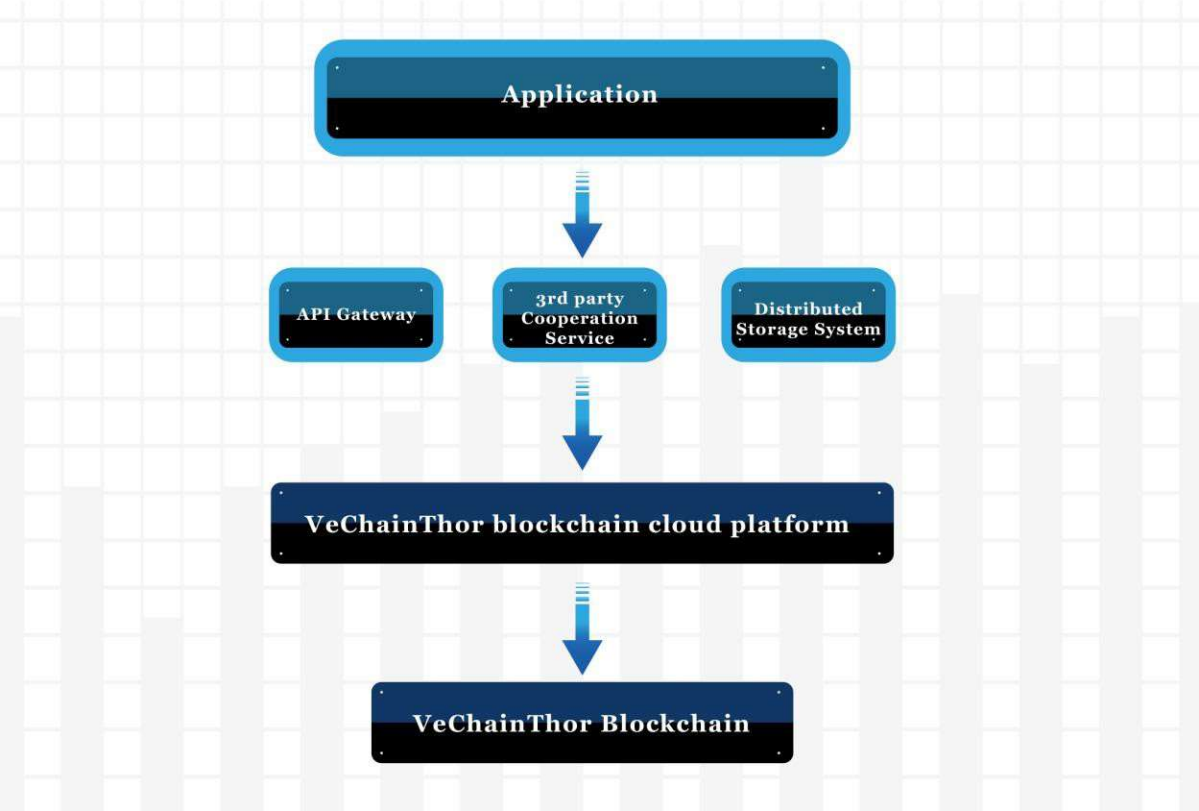


图 6.1.1 工业应用结构

唯链雷神区块链平台将为商业伙伴提供易用的区块链底层架构，同时提供“一键式”部署解决方案，使商业伙伴能够轻松打造和管理自己的区块链节点、智能合约和 API，以改进其商业应用。

除合作伙伴以外，公共服务和工具对于唯链雷神区块链生态的扩展和运行也至关重要。例如，同世界知名会计师事务所一道开展和扩大区块链审计服务，包括整体健康状况、智能合约状态、项

目和商业应用状态等方面的服务。

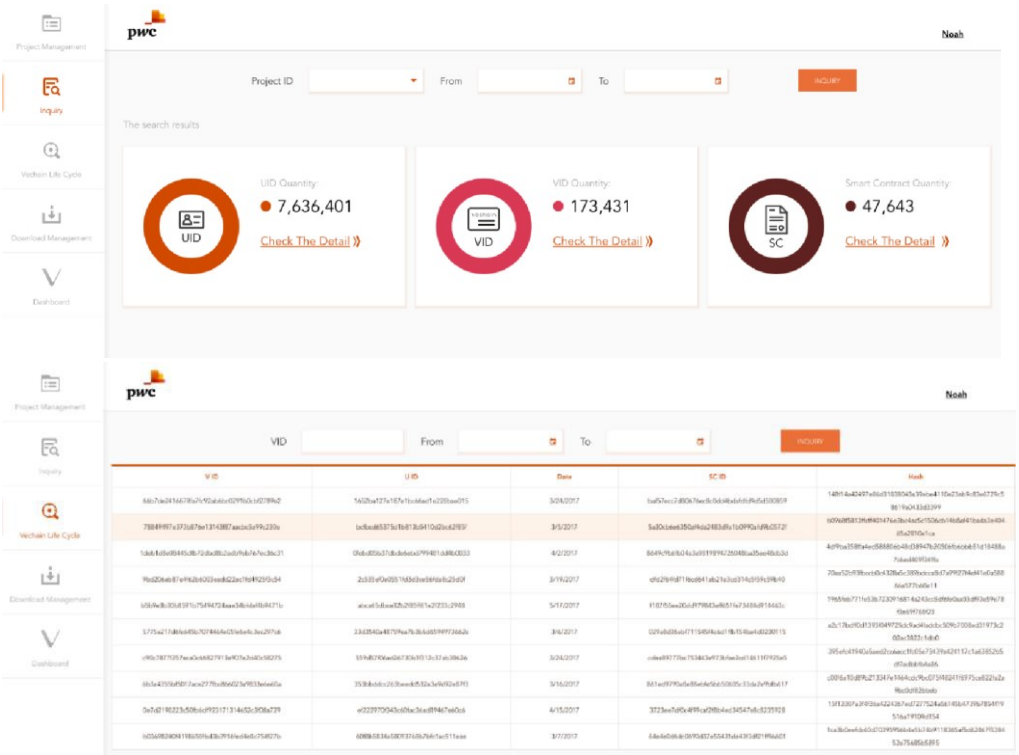


图 6.1.2 第三方服务应用

唯链雷神区块链的基本精神是开放和共享，将于 2018 年 6 月底前开放源代码。我们很乐于分享此前完成且得到合作伙伴认可和批准的应用案例，欢迎所有人复制我们的成功案例并创造新案例。

6.1 时尚与奢侈品行业

根据 2015 年时尚与奢侈品市场调查，欧洲每年的时尚与奢侈品牌总销量中假货占 9.7%。此外，每年还要花费 28.7 亿美金用于打假。假货导致时尚业、制造业和零售业有 36.3 万人因此失业。

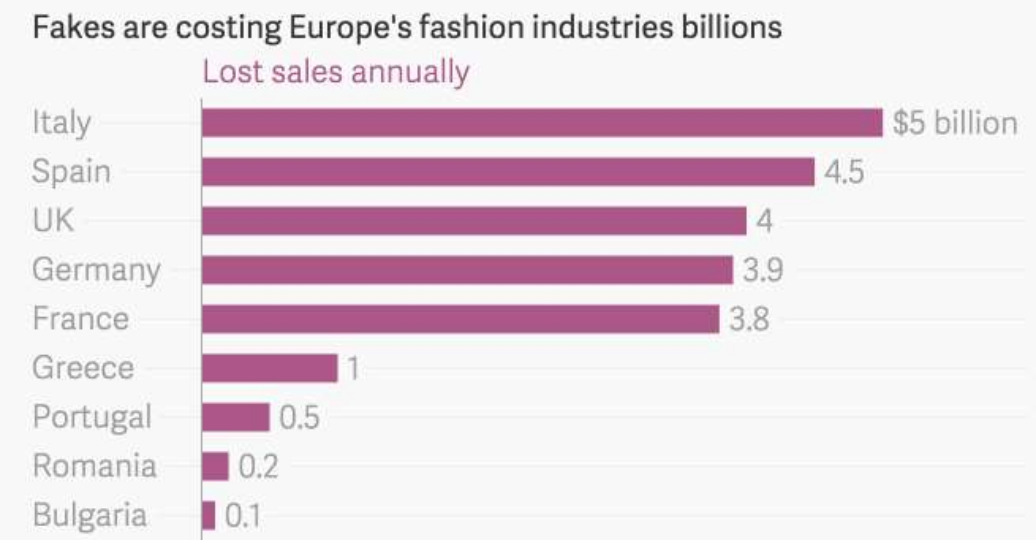


图 6.1.3 假货对欧洲时尚业的冲击（每年销售损失）

唯链致力于开发一种产品全生命周期追溯解决方案，涵盖制造、物流和供应链、批发零售、售后服务等环节，甚至结合物联网技术，让消费者参与区块链打假。时尚与奢侈品牌已经开始采用唯链的解决方案，而假冒活动的大量减少也使得这些品牌获益。

给每个被管理的产品分配一个独特的 VID，用物联网标签注明，并登记在唯链雷神区块链上，使相关方在一件产品生命周期的每一步都能够对其进行访问和识别。该解决方案非常有效，是因为它通过优化现有的 ERP 系统，如生产系统、WMS、SAP 和零售系统（通过 API 与区块链相连），简化了每一步的操作流程。这样就降低了产品交付的总成本。

1) 制造商（通常是第三方供应商）建立产品和标签之间的物理连接，标签记录了产品的生产信息（如位置、时间、原材料、工艺、质量检查等）。
2) 品牌所有者可以控制 VID 注册的智能合约，在质检和验收后再正式“激活”产品，从而杜绝过度生产。
3) 来自物流和供应链运营的数据可通过 WMS 和供应链系统的 API 记录在区块链上。
4) 零售系统可以通过在销售过程中调用智能合约来向终端用户执行所有权转移，就像发送电子邮件一样简单。
5) 消费者可以获取数字化的所有权并进行个人电子签名来创建自己的故事。
6) 在保护消费者隐私且消费者同意的情况下，通过搭建独特的个性化渠道来打造和改进售后服务、客户关系管理和数字体验。

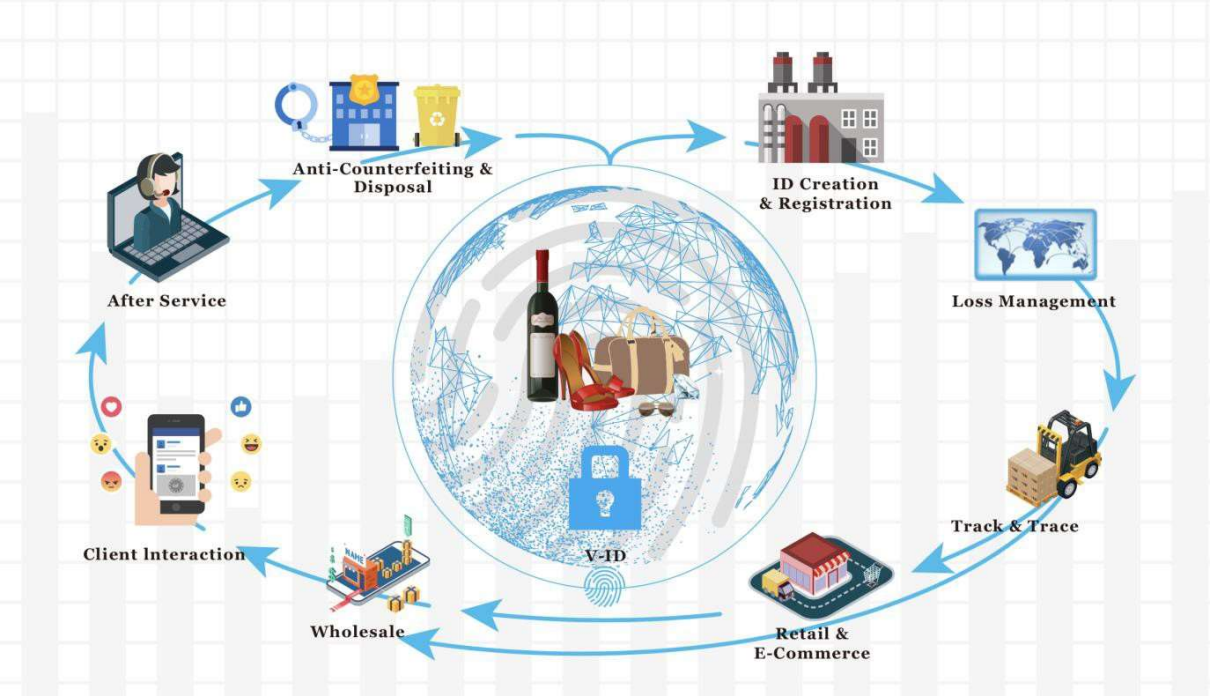


图 6.1.4 唯链雷神区块链平台上奢侈品和时尚品的生命周期

6.2 食品安全

食品安全是全球最迫切需要解决的社会问题之一。传统的食品安全解决方案过于依赖流程控制和企业的社会责任感。在供应链中追踪、追溯、记录和定位食品很困难，因此很难确定是否有问题发生。

区块链技术可为食品行业带来安全可靠的解决方案。中国政府已经宣布并强调，食品认证和供应链有效追踪是迅速找到及消除污染源的关键性步骤。

6.2.1 为 D.I.G.设计海外酒类追溯服务平台

在唯链上搭建的D.I.G.**海外酒类追溯服务平台**可以追踪到葡萄酒生产的源头，当葡萄酒还在海外酒庄的时候便已开始记录。D.I.G.（上海外高桥进口商品直销中心有限公司）是国有企业上海外高桥集团的子公司，上海外高桥集团在中国进口葡萄酒市场占有 30%的份额，在中国证券交易所主板上市，股票代码为 600648。这是中国首个将区块链技术用于生产的成功应用案例。从整个流程的源头开始，葡萄酒的每一个细节便已进行标记和记录。通过这种方式，监管机构和 D.I.G 可以利用智能合约追踪葡萄酒的整个生命周期，并对所有权归属情况进行记录，从海外酒庄开始，历经出口、进口、商检、自由贸易区仓库、配送中心，直到最终抵达各种销售渠道和零售店。

客户可以通过店内触摸屏或智能手机识别和检查葡萄酒信息。高端葡萄酒可以配备物联网芯片，以增加安全性和便利性。唯链的物联网团队将芯片组设计为“贴纸”或“封条”的形式，以免已经消费过并重新灌装的葡萄酒被当作真品。用户可在支持 NFC 功能的智能手机上打开唯链应用程序（支持 iOS 和 Android 系统），只需扫一下酒瓶上的 NFC 标签便可查验产品信息。

图 6.2.1 自贸区葡萄酒中心的唯链应用：后台管理系统、智能前端、手机端展示

该项目在上海市商务委员会组织的上海国际葡萄酒品评赛上进行了展示，被作为酒类追溯服务的标准解决方案向全国推广。

6.2.2 MyStory

MyStory 是一个基于现成区块链的食品和饮料行业数字认证解决方案，依托行业龙头和 DNV GL 的深厚行业经验，提供独立的实体审计、数据收集和验证服务。

MyStory 在意大利葡萄酒行业率先得到使用，有四家葡萄酒生产商——Michele Chiarlo、Ricci Curbastro、Ruffino 和 Torrevento 直接参与到其中。这四家生产商同唯链和 DNV GL 就这款颠覆性解决方案展开合作。到今年年底，这些行业龙头将在门店中推出瓶身上带有 MyStory 标识的葡萄酒，并使用唯链雷神区块链的解决方案和硬件芯片。

图 6.2.2 MyStory 在唯链雷神区块链上的应用

*"MyStory 将产品及其供应链透明化，使得消费者能够即时深入地了解关键产品特性，如质量、真实性、原产地、原料、水和能源消耗等，且整个转化过程全部经过 DNV GL 验证"，***挪威船级社管理服务集团（DNV GL）首席执行官卢卡·克里斯西奥蒂**（Luca Crisciotti）如是说道。

MyStory 解决方案不仅可以应用到葡萄酒行业，还将更进一步应用到多个市场。

6.2.3 冷链认证解决方案

唯链与全球合作伙伴 DNV GL 一道，共同构建与物联网传感器相关的另一种食品安全解决方案：基于区块链的冷链认证解决方案。这一应用率先从一家全球连锁便利店（依据保密协议尚未公开）开始。

依托冷链物流认证服务，客户可以快速查询生鲜食品从工厂，经过冷链物流提供商、门店冷藏室，到最终上架销售的物流状态信息，

从技术角度来看，唯链利用其内部开发的先进物联网设备实时监控和记录冷链物流整个流程中的温度、湿度和位置等数据，并将其上传至唯链雷神区块链。由于 DNV GL 可以确保冷链物流流程满足与食品安全相关的法规，且**业务流程**合规，因而才能保证该解决方案的实现。只有借助唯链雷神区块链，DNV GL 才能确保下一代数字认证服务是公正可靠的。冷链物流是唯链可以完美切入的行业，未来在 DNV GL 的引领下，唯链有望进入到更多行业。

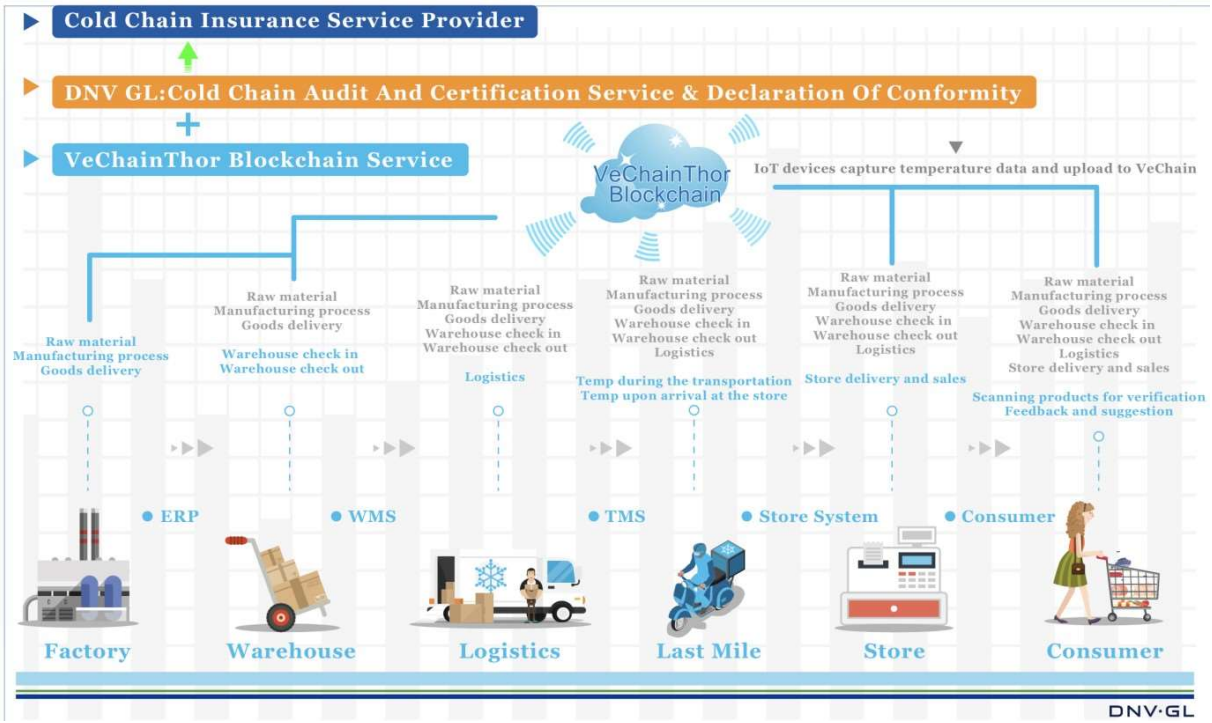


图 6.2.3 与 DNV GL 共同开发的唯链雷神冷链供应链解决方案

6.3 汽车行业

汽车行业是一个复杂的生态，包括制造商、经销商、4S 店、代理商、监管机构、金融服务提供商（保险公司、银行）、技术专家等众多参与方。在车辆的生命周期中，大部分“用户数据”并非消费者或车主所有，这些数据以碎片的形式分别由不同的参与方储存。这些碎片化的数据与完整的数据相比，价值不可同日而语。

唯链已同商业合伙伙伴 Viseo 和微软法国公司一道启动了“车辆数字化账本”项目。在该项目中，唯链团队负责在 Azure 上部署区块链，开发和部署智能合约，并为上层应用提供标准 API， 这类应用包括：

6.3.1 数字维护日志

在数据所有者的授权下，每辆车都可以建立自己的数字记录。车主购车后，可以使用授权及非授权功能向维修服务提供商（如 4S 店或修理厂）提供许可。不同参与者将各自记录数据，同时唯链雷神区块链为每项服务和交易提供保护。一旦所有碎片化数据通过适当的授权控制和经济激励整合在一起，将可以创造出更多价值。

保险公司、银行等数据用户可以使用车主的授权很方便地对汽车信息和历史日志进行查询。查询到的数据是可信的，因为数据来自服务体系中的不同参与者，而且数据在区块链上有副本，可以用来验证数据的完整性。

保险续保或进行二手交易时，传统上会要求进行车辆信息的调查，数字维护日志可以在此方面显著提升效率和大幅降低成本。

6.3.2 “绿色驾驶”

基于此应用的第二个模块是将车载电脑的驾驶数据记录到区块链上，包括加速度、平均速度、燃料消耗等信息，促使驾驶员改进驾驶行为。这些受区块链保护的数据有助于车辆的检查和评估。用户行为还可以与个人征信以及碳减排等其它相应活动挂勾。

通过区块链收集到的数据值得信任，因此也就可以在新业务模型的基础上创建、应用、传输和分配数据价值。

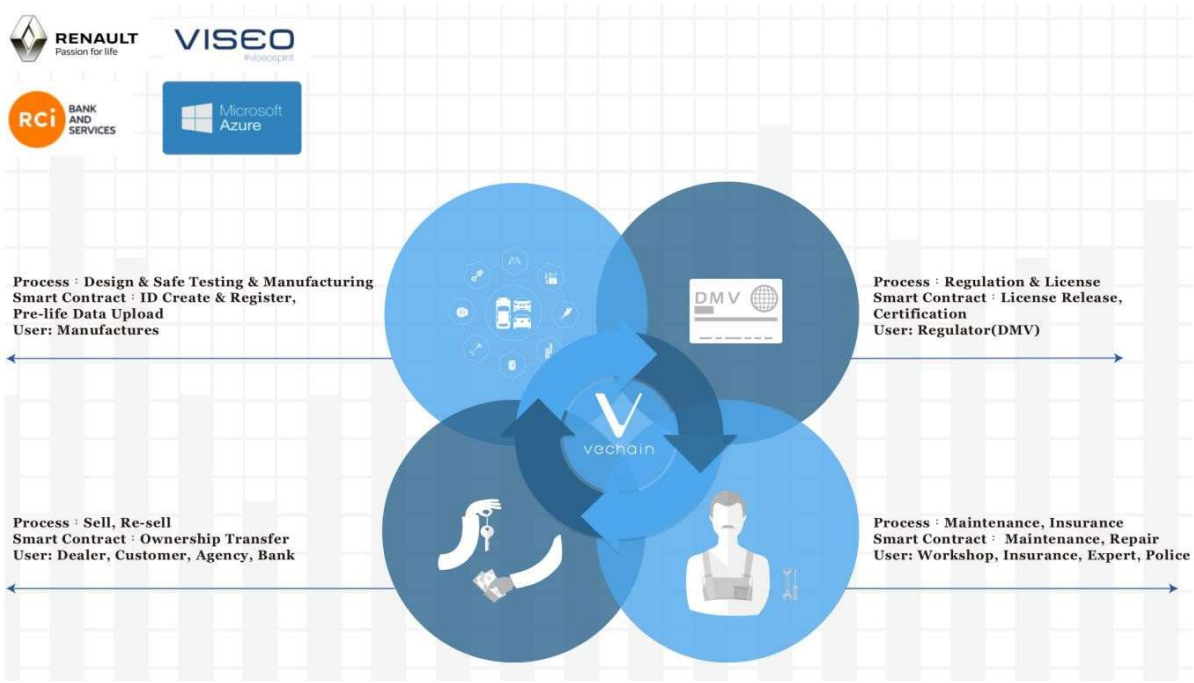


图 6.3.2 为雷诺开发的唯链雷神汽车应用

作为我们的新合作伙伴，宝马集团正在唯链雷神区块链上建立另一个解决方案。更多细节将在准备就绪后由宝马直接公布。

6.4 供应链

传统供应链包括：原材料供应商、制造商、服务代理商、物流、海关和商检机构、仓库、零售和终端用户。

图 6.4-1 传统供应链

人们通常认为，传统的线性供应链能够提供可靠和具有成本效益的结果。交易（实体、信息、财务）通常发生在供应链中的两个参与者之间，这两个参与者在此过程中发生接触。供应链的稳定性本身就是一个信任要素，因而很自然地，不同参与者之间的关系是长期的。因此，选对合作伙伴至关重要。

随着商业和技术的发展，供应链上的节点开始因为技术而越来越紧密的联系在一起，他们呼吁新的合作和交易形式，从而提升贸易效率和价值。这些新的合作和交易形式要求此前鲜有接触的各个参与者更加信任彼此。此外，用户和消费者也需要对他们期望的产品或服务建立起更多的信任，这就要求供应链中的各个节点相互联系在一起。

一种新型供应链即将出现，它具有以下特点：

1) 多个参与者之间的各类交易呈指数增长；
2) 产品和服务的数字内容不断增加；
3) “根据使用情况付费”的复杂商业模式将会出现：参与者需要相信“要想获取就要付出，只要分享就能获利”；
4) 找到具有成本效益的智能方式来标记物理产品并将其连接到数字化虚拟身份的能力，将成为一种关键的竞争优势；
5) 除了人以外，机器之间也可以进行协作和交易。

区块链和物联网的诞生就是为了构建这种新型供应链。

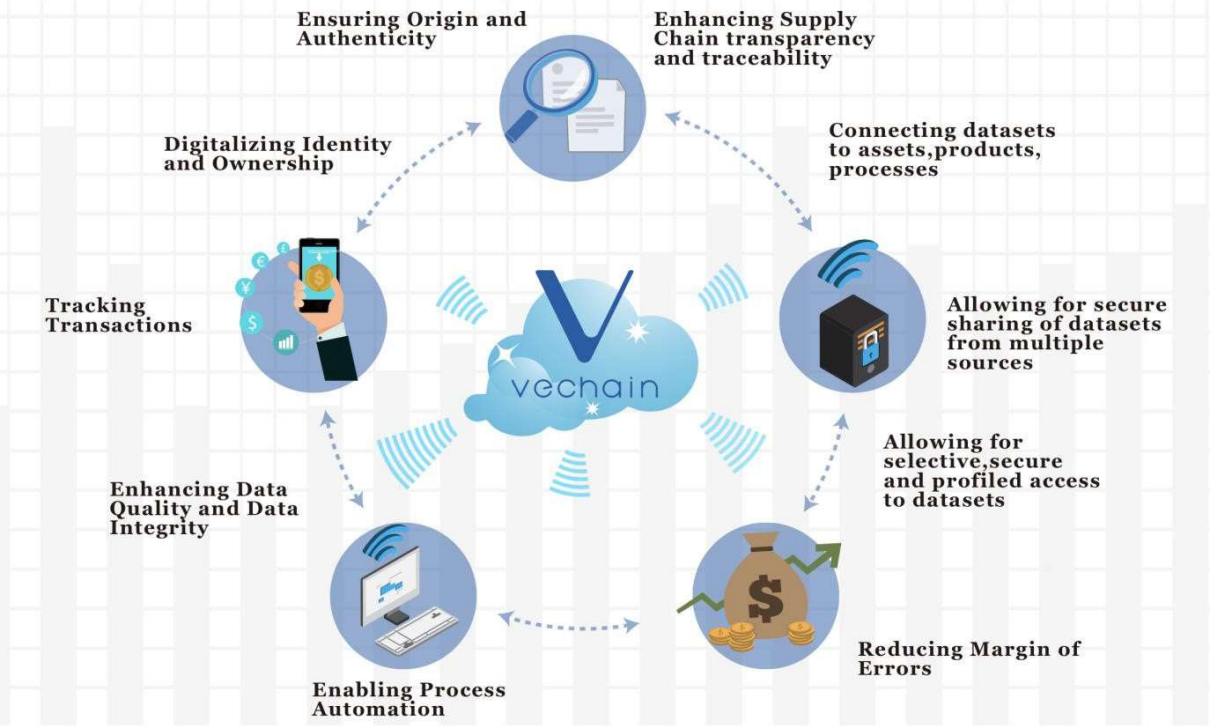
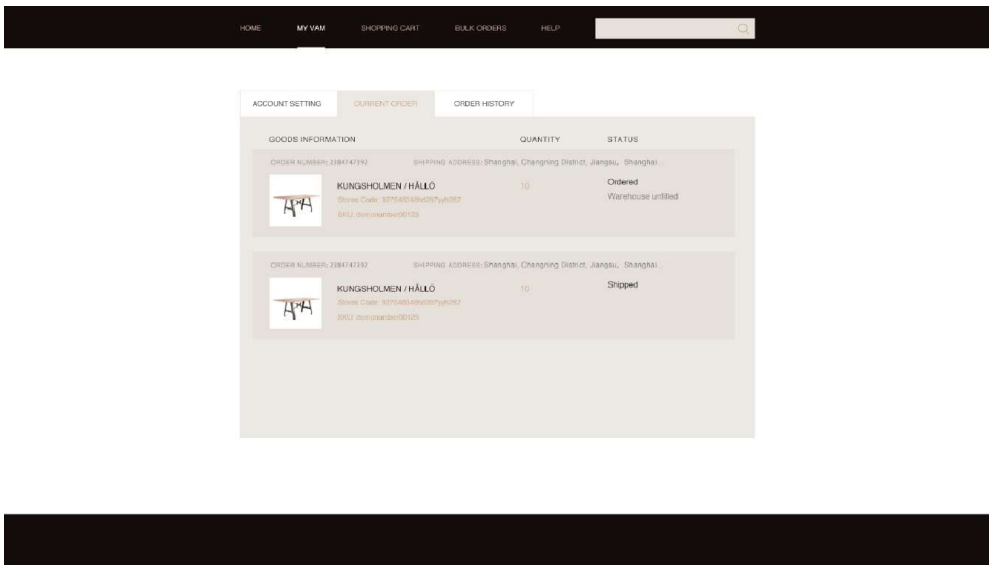


图 6.4-2 唯链打造供应链新模式

6.4.1 帮助德讯进行资产管理

唯链向大型货代公司德讯（K+N）提供 BaaS（区块链即服务）服务，以追踪和管理所有发运货物。为确保数据安全，唯链通过一个通用服务平台实现与不同客户的直接连接。操作人员可以直接使 用手持终端设备完成相关业务操作。



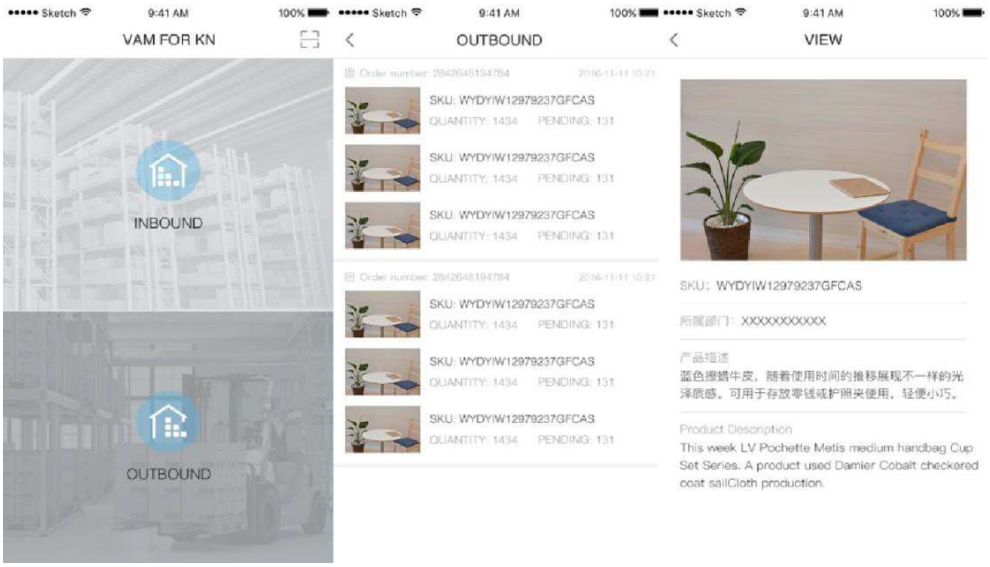


图 6.4.1 德讯物流解决方案展示

在计划后期，我们将与更多合作伙伴、服务提供商和监管机构建立联系。

6.4.2 与恪保科技（LogSafer）一道进行供应链风险管理

唯链和恪保科技（LogSafer ）正在合作开发物流保险区块链解决方案。跨境物流管理是一个复杂的商业模式。一个产品从 A 点运输到 B 点，会涉及不同企业的许多层面。若需要跨国运输，难度更是会大幅增加。商业活动中的诸多变数会引发承销风险，而恪保科技正是提供此类风险管理服务的专家。

为了向客户提供更好的保险服务，恪保科技要求尽快提供未经篡改的真实数据，以便准确进行理赔支付，同时通过审查改善客户的整个风险管理体系，为客户提供更有价值的建议。唯链解决方案可以帮助恪保科技更好地识别跨境供应链中每个环节面临的各种风险，继而采取适当的预防措施降低风险发生概率，提供适当的保险产品转移风险，并在风险过后实施有效的代位索赔。

区块链技术允许多方参与数据的记录，且记录不可篡改。依托唯链雷神区块链和物联网技术，企业可以更好地追踪风险并记录验证数据。通过该解决方案，公司将能够掌握供应链中的最新风险动态，同时利用验证数据研究和探索更佳的替代方案。有了这一优势，便无需再创建支付环节中与数据收集和验证相关的数百万文件，从而大大减少付款审核时间。一旦智能合约在该行业得以实现，公司将可真正获得“即时赔付”，这就产生了一种大为有利的商业模式。这种模式对于被保险人而言是一种终极体验，同时也有利于实现各方共赢。

举例来讲，一位渔民从日本向加利福尼亚发运了一批鱼，并从我们的合作伙伴恪保科技处购买了一份保险。运送途中发生了一些状况，放在货物当中的唯链传感器获取的数据表明，货物的储存温度较高，且暴露期较长，也就是说，鱼无法保鲜。唯链传感器将会取回这些数据，并上传到区块链上。这种数据状态会触发智能合约的执行，然后自动为客户提交索赔请求，并从保险公司获得理赔。

6.5 农业

中国的农业市场面临诸多严峻问题，包括农业规模过小且分散、农产品质量参差不齐、产品安全性欠佳、生产力低下、环境污染等。仅靠互联网技术或官方制订的法律法规很难解决问题。我们认为，通过我们的区块链云项目来验证农业是否绿色有机，将有助于改变现有思维。

中国正在利用物联网技术、农业种植过程管理、区块链技术、大数据和人工智能推进农业种植管理计划，从而完成农业生产前、中、后的全流程管理。通过这种方式，良币可以驱除劣币，规范农业市场。

有鉴于此，唯链正与普华永道、中国联通和辽宁省农业科学院合作开展一项专门用于验证绿色有机农业的区块链云项目。

在该项目中，唯链利用区块链技术对每个农场的绿色大棚进行了注册，并建立一个数据模型来记录每个大棚的功能数据。数据有两个主要来源：一是农户直接记录的生产作业数据；二是来自温室中的物联网传感器。依托普华永道的数据和风险保证服务，为农业科学院的绿色农业认证工作奠定了可信数据基础。此外，在物联网设备的帮助下，务农效率提高了约 9 倍。

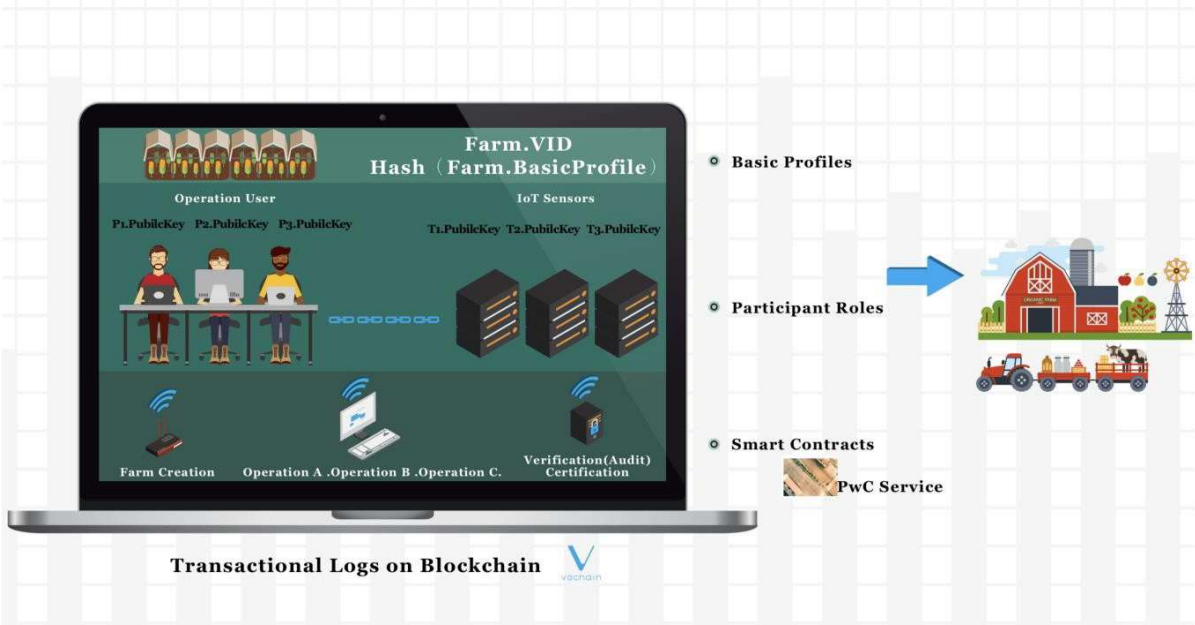


图 6.5 农业应用与物联网技术相结合

6.6 政府事务

全球各地的政府部门都对区块链技术表现出了浓厚的兴趣。中国工信部发布了《中国区块链技术和应用发展白皮书》。国务院强调，区块链有利于营造一个互信的世界。

英国政府科学办公室在《分布式账本技术：超越区块链》的报告中指出了区块链技术的潜在特质和优势：“分布式账本技术有可能改变公共和私人服务的交付方式，有望在数据共享、透明度和互信等方面重新界定政府与公民之间的关系，并为政府的数字化转型计划做出重大贡献。”

唯链与中国贵安新区行政审批局合作，为其提供基于区块链的信息系统，用于收集和分析行政数据，保护保密数据，并采用区块链技术改变企业注册流程，简化繁琐手续。

1)贵安新区行政审批局可以使用唯链雷神区块链技术支持的电子政务系统存储企业注册的相关文件，如经营许可证、银行账号证书、税务登记证、组织机构代码、外贸登记、审计报告等。

2)项目第二阶段，电子政务系统将能够进行远程企业注册、文件上传、文件审查和证书签发。有了这个新的系统，公司不需要浪费时间和精力从不同的政府部门获得实体审批印章。这个流程彻底改变了政府处理行政请求的方式，协作性更佳，同时又降低了费用和时间。

3)电子政务系统的最终结果将对贵安新区的所有政府流程和未来项目提供强有力的审计支持。

例如，由于缺乏协作数据，当前委托方无法查询海关要求的文件。

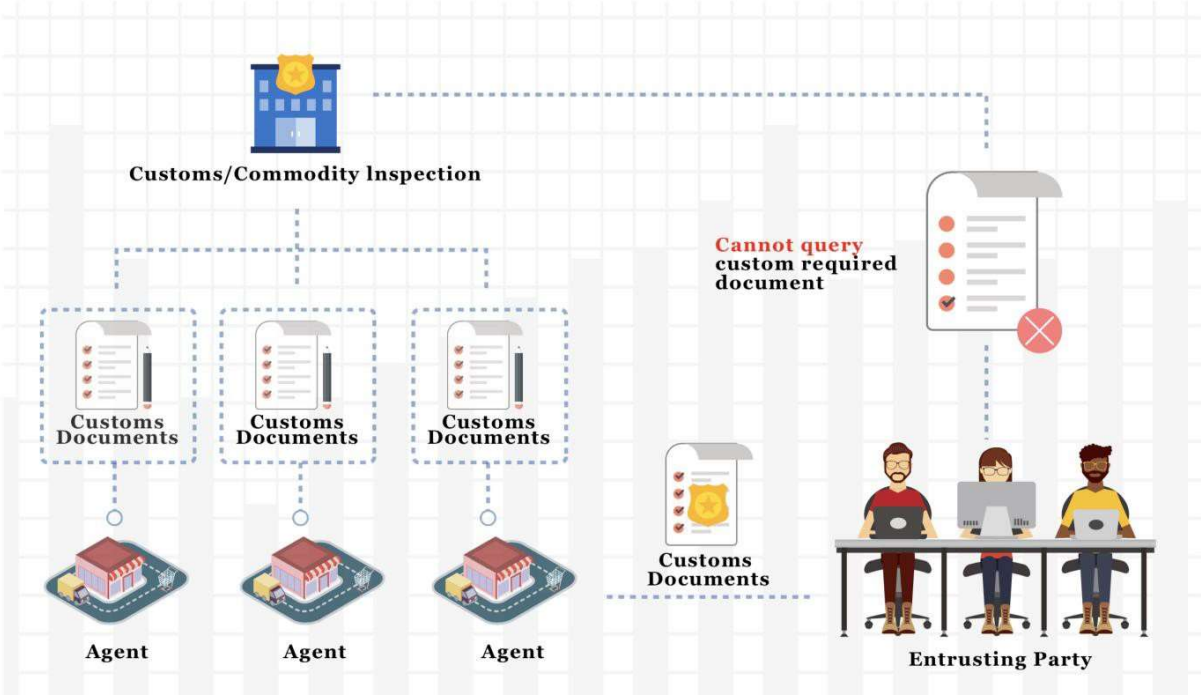


图 6.6.1 海关/商检机构当前的系统流程

唯链雷神区块链提供了一种新型协作式政府系统，可以连接多个不同的职能部门进行数据共享和认证。海关文件可以用统一的 ID 登记到唯链雷神区块链上。因此，不同的部门可以通过适当的授权和信任访问、查询和更新同一文件。该系统流程有助于提高运营效率、节省成本。

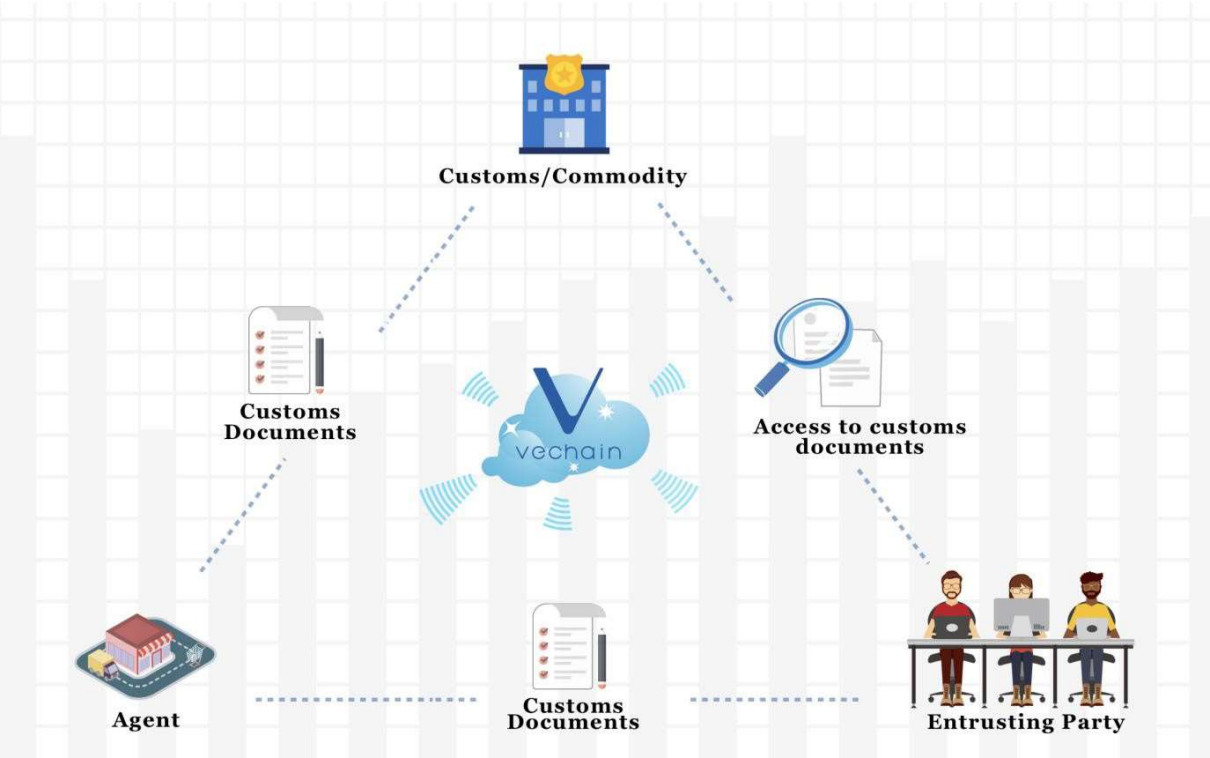


图 6.6.2 未来的区块链在政府的应用

区块链技术对政府具有重要意义。它意味着政府信息和运行状况会更加公开透明。此外，作为整个商业环境的“协调者”，政府可以更多地关注区块链技术如何提高资源分配、调拨和优化的效率，包括跨行业的资源优化配置。

6.7 这仅仅是开始

近两年来，唯链团队在应用案例开发和实施过程中面临的最大挑战不是技术问题，而是如何就新业务模式达成商业共识。不过，我们已经度过了最艰难的时期。非常感谢所有怀抱创新热情的业务及技术合作伙伴，同我们一道开拓和验证了区块链技术的实际应用。

尽管我们已经积累了丰富的经验和解决方案，但若要有所作为，仍然有很长的路要走。一路走来，我们非常感激能够拥有一个强大的唯链社区。在我们筹备的项目和应用中，一半以上来自社区。我们期待更多先行者的加入，同我们一道开发更多应用案例和应用场景，促进唯链雷神区块链上可信任生态系统的蓬勃发展。

7 唯链基金会的经济

唯链基金会在建立生态系统时始终践行并坚持以下原则：

1) 唯链基金会将始终坚持非盈利的初衷
2) 高效且可持续的发展
3) 开源与共享

财务方面，唯链基金会将在可持续运营和社区的发展与推广之间寻求财务平衡。除了通证发售期间募集的初始资金外，基金会还会通过生态系统内的各种运营活动获取数字资产。基金会也将在值得信赖的第三方机构的审计和监督下，将全部净利润以公开透明的方式返还给社区。

唯链基金会设置了专职财务管理团队管理其财务和数字资产。财务管理团队直接向基金会战略决策委员会报告，并定期（通常按季度计）起草基金会的财务报告并完成信息披露。

7.1 资金来源

基金会的收入主要来自两个方面：

1) 非经营性收入，包括首次通证发售募集的资金及数字资产的收益。
2) 经营性收入，包括研发收益、产品销售收入、专利转让费或授权费收入、学术交流及贡献收入等。

下述内容为主要收入来源的具体描述：

7.1.1 初始基金和通证发行

唯链总计发行了 10 亿枚唯链通证（ERC20 VEN）。

其中 132, 837, 366.56 枚 ERC20 VEN 已在值得信赖的第三方机构审计监督下退回并销毁。上述操作已向公众披露，当前 ERC20 VEN 的相关信息可在以太坊的区块链浏览器上查询确认。

当前 ERC20 VEN 总供应量为 867, 126,334.66 枚，在 1:100 通证拆分后，VET 总供应量将为为 86,712,634,466 枚。

唯链通证分配方案如下：

比例	分配方案	明细
41%	公开发售	开发售获取的收入将用于唯链基金会的运营，包括开发、营销、财务和法律咨询等。
9%	私募投资人	私募投资人在社区及行业内有广泛的影响力，其将为技术开发及商业拓展提供帮助。
23%	企业投资人	“企业投资人”指唯链分布式商业生态系统内的企业及为上述企业客户或终端用户提供服务的企业；此类企业投资人将使用 VET 作为其商业活动的关键发展目标。
5%	创始团队、开发团队	以此作为对创始团队及开发团队在唯链的发展过程中所做贡献的回报。
12%	持续经营及技术开发	作为储备金，用于唯链运营及开发所需的费用。

10%	商业落地推广	筛选合适的行业，将唯链技术用于相关行业的战略部署、项目支持及通证置换。

7.1.2 数字资产投资

在运营过程中，唯链基金会划拨 5%至 10%的资金或数字资产，用于设立唯链孵化计划，并与分布式资本（Fenbushi Capital）、明势资本（Future Capital）等风投基金及其他享有盛誉的加密货币基金一道，不断为基于唯链开发商业应用，或未来有望成为技术和商业合作伙伴的区块链项目提供资金支持。

7.1.3 专业服务

在建立生态系统的过程中，唯链基金会将扮演唯链雷神区块链公共服务提供者的角色，并收取一定数额的数字资产或资金。例如，唯链基金会可以为传统企业提供专业服务，通过唯链雷神区块链协助他们轻松简捷的完成业务开发、拓展、维护以及转型的过程。作为回报，唯链基金会将以数字资产（如 VET）的形式收取一定服务费。

7.2 资金使用预算

如前所述，唯链基金会的预算主要用于日常运营、技术研发、商业拓展以及投资等。主要分类如下表所示：

分类	占比	内容
技术开发	50%	主要包括技术团队的薪水、专家及开发人员的招募费用、技术专利及知识产权保护的费用等。
商业开发	35%	唯链商业推广、技术交流与分享、监管与合规、联盟创建或参与等方面的费用。
投资	10%	唯链孵化项目，用于扶持其他初创企业在唯链雷神区块链上开发商业应用，或开展合作。
日常运营	5%	基金会日常的行政和运营工作，包括办公室租赁、后勤管理、交通、财务及报告等。

下图为基金会对未来四年预算方案的预测：

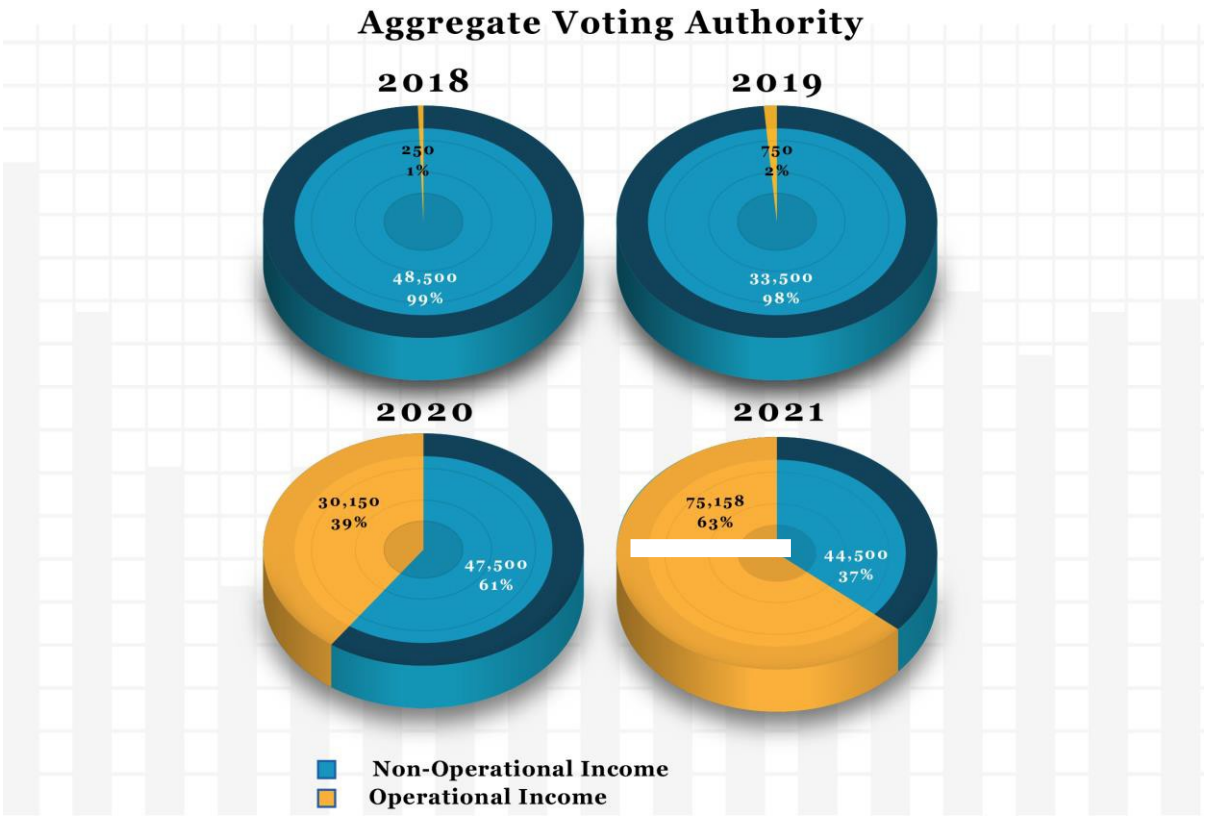


图 7.2.1 唯链基金会 4 年收益预测（单位：千美金）

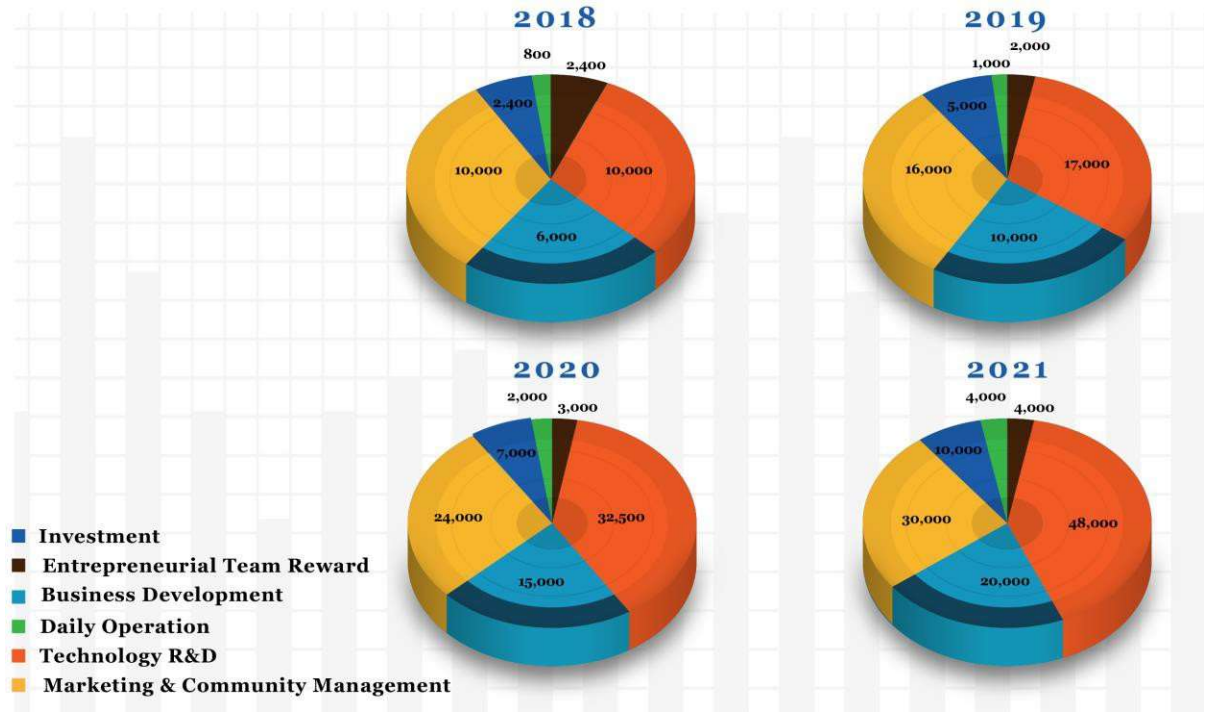


图 7.2.2 唯链基金会 4 年开支预测（单位：千美金）

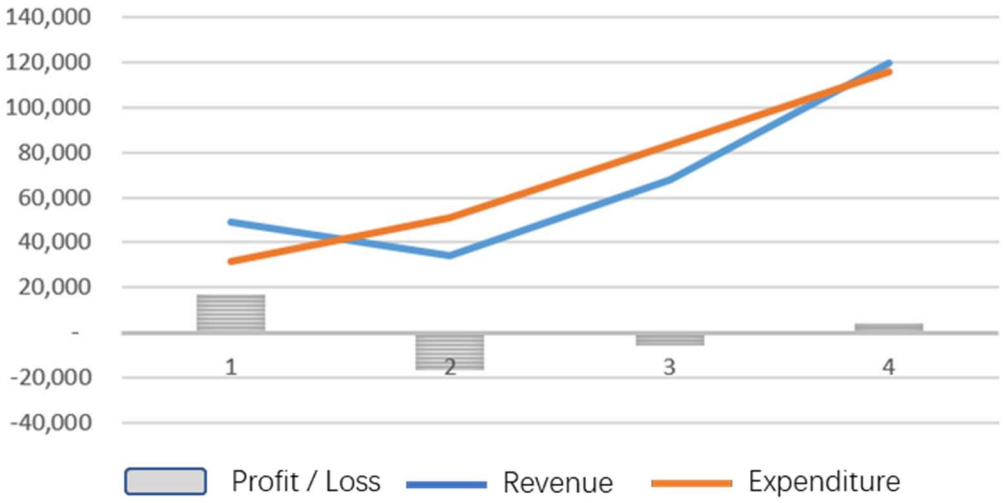


图 7.2.3 唯链基金会 4 年留存收益预测（单位：千美金）

综上所述，唯链基金会已通过通证发行获取启动资金，历时约 3-4 年时间将实现：

唯链基金会的成长：包括：基金会技术及商业开发人员增加至 100—150 人左右；唯链雷神区块链上的“唯链 GDP”实现 200 亿美金的商业增长。

聚焦研发和商业开发：预算中的很大一部分将用于技术开发和商业开发，推进唯链生态系统的发展。

驱动价值：基金会不仅通过通证发行启动资金来建立生态系统并为社区创造商业价值，而且已经并将继续通过在系统内提供各种区块链服务来获取收入。唯链基金会致力于确保收入与持续运营开支的平衡。

坚持非盈利原则：基金会承诺不向创始人团队、基金会的管理者或利益相关者发放利润或分红。基金会运营所得收益，除用于基金会的基本开支外，将全部投入到社区和生态系统的建设中。

7.3 资金使用限制条款

资金的使用本着公开透明的原则。唯链将根据分配原则和预算，设置一系列的独立账户和数字资 产钱包，以实现对数字资产使用的监管。资金将用于唯链生态的建设、区块链技术的开发和应用。相关信息将定期向社区披露。

7.4 财务计划和执行报告

每季度，财务团队将起草一份财务报告，该报告包括财务计划及对上季度的财务执行情况的总结。经运营委员会财务部门负责人审批后，该报告将对公众披露。形成财务报告须提交至战略决策委 员会审核。

7.5 数字资产管理

唯链基金会的数字资产由战略决策委员会监管，并由专职财务团队负责管理，该财务团队受战略决策委员会指派的运营委员会领导。

为规范数字资产的运营，财务团队制定了一套数字资产管理政策和程序。以下为主要管理原则：

1) 专职团队。数字资产由团队而非个人，进行运营、记录和监控。数字资产属于唯链基金会，因此包括战略决策委员会成员在内的任何个人均无权访问数字资产。数字资产钱包的私钥存储在加密令牌中。令牌的密码由经授权的战略决策委员会成员设置，令牌的物理载体保存在银行保险箱内。保险箱须在三名被授权人员同时操作时方可打开，且被授权人没有令牌的密码。
2) 职责划分。职责划分包括两层含义：
    a. 审批和执行的职责分开，负责审批的人员不能操作数字资产钱包。
    b. 会计和操作的职责分开，会计和数字资产操作的工作分由不同人员承担。
    每笔交易均需协调一致。会计账簿必须定期与数字资产分类账本进行核对。
3) 提升资产安全性。安全性也包括两层含义：
    a. 指定资产钱包。基金会将数字资产分配至不同钱包。热钱包用于日常运营。冷钱包存放在安全的保险箱内，用于储存大额资金
    b. 平衡各种数字资产所占份额。基金会会对各种数字资产，如比特币（BTC）、以太币（ETH）或其他通证的价值进行评估，并定期调整各数字资产所占份额，从而平衡通证的流动性，并稳定数字资产的价值。
4) 持续监控。建立监控机制是为了监控数字资产的使用情况。任何异常的资产使用行为均会触发警报，然后由独立团队决定是否进行进一步调查。
5) 业务连续性计划（BCP）和灾难恢复计划（DRP）。基于正式数字资产的 BCP 和 DRP（Crypto DRP，CDRP）已由战略决策委员会制定并批准。相关计划包括在不同紧急情况下恢复数字资产或恢复数字资产钱包的各种措施。紧急情况包括热钱包损毁、设备故障或钱包遭到黑客攻击等。CDRP 演习每季度进行一次。

遵循风险管理和财务内控的最佳实践，基金会在对多重签名技术进行充分测试后，决定采用该技术以确保资产的安全性和准确性。基于独立性原则，唯链基金会的钱包采用 4/7 多重签名。若增加签名，须经过战略决策委员会授权。

考虑到数字资产相关技术在不断进步，上述数字资产管理政策和程序将定期进行审查和改进。改进措施将由战略决策委员会负责审批，审批通过后将向公众披露。

7.6 披露事项

每年，唯链基金会将向社区披露其在商业拓展、技术开发、运营等方面的进展和状况以及未来计划。财务方面，将按季度起草并发布财务报告，年度报告审计工作的情况也将向公众披露。

唯链基金会设立公共关系委员会，作为对外窗口，定期及不定期召开发布会议，向公众发布基金会的重要消息。

7.7 法律事务

唯链基金会已委托具有公信力的第三方机构，在新加坡成立法人实体。所有的运营活动均遵循当地的法律法规及监管要求。若出现需要寻求法律意见的事项，如商业协议、合同、争议等，需通过当地律师予以确认。

7.8 免责条款

唯链基金会坚持唯链生态体系运营及发展的非盈利性质。唯链社区的用户，无论是否已获取唯链代币，均有权持有或放弃唯链通证。对持有者而言，持有唯链通证确保其有权在唯链雷神区块链平台执行通证交易及智能合约。投资者及通证持有者应清楚，在法律范围内，唯链基金会不会以明示或暗示的方式做出保证和/或担保获利。此外，购买者应清楚，通证发行/交易后，唯链基金会不负责退还。

7.9 争议解决条款

一旦出现争议，有关方面应依据协议协商解决。协商无果的，可通过法律解决，相关争议的司法管辖权归属唯链基金会注册所在地，即新加坡。

8 团队成员介绍

唯链团队成员来自不同的国家，不同的行业，拥有各不相同的经历、专长和背景，但是都秉承着一个共同的理想。团队人员构成非常均衡，汇集了业务、技术、运营、支持等多方面的人才，是成功不可或缺的要素。

斯科特·布雷宾（Scott Brisbin），首席法律顾问

布雷宾先生是来自美国的知名律师。他服务过的客户包括滚石乐队及主唱 Mick Jagger、迪斯尼、米高梅等。

1978 年从加州大学洛杉矶分校毕业后，他即加入 MSK 律所，并从 1989 年开始担任律所合伙人。在公司法律事务及专利维护上有着绝对的权威经验。

2016 年加入唯链后负责唯链的法律安全、组织架构、知识产权等事务。

陈琛, 人力及行政总监

陈琛女士拥有超过 7 年的人力资源工作经验，曾在百加得、联合利华负责相关工作。

2015 年加入唯链后，负责人力资源管理、招聘、培训、薪酬、员工福利等政策的制定。

冯艺凯，首席运营官

冯艺凯先生曾在普华永道上海和纽约分所工作超过 12 年，期间负责网络安全和隐私保护相关咨询服务。同时，他也是普华永道中国区块链服务的推动者。

2018 年加入唯链后担任首席运营官，负责运营、安全和隐私保护等。

他还是认证信息系统安全专家（CISSP）和认证云安全专家（CCSP）。

杰罗姆·格雷勒雷斯（Jerome Grilleres），唯链欧洲区总经理

格雷勒雷斯先生毕业于伦敦商学院，拥有工商管理硕士和计算机科学硕士学位。来自于巴克莱银行法国总部，拥有 9 年的零售银行商业战略和制定经验，以及 7 年投资银行实时交易应用开发经验。

2017 年加入唯链后担任欧洲区总经理。

顾建良，首席技术官

顾建良先生毕业于上海大学，并获得控制理论与控制工程硕士学位。曾就职于 TCL 通讯，担任技术总监。在嵌入式软硬件开发及管理具有超过 17 年的经验。

2017 年加入唯链后负责技术开发与管理，致力于推动物联网与区块链技术的结合与发展。

李波，区块链开发经理

李波先生大学主修信息安全技术。拥有 6 年的编程及项目管理经验，在诸多行业中参与过多个大型开发项目，包括金融行业、保险行业、奢侈品行业、汽车行业等。

2014 年开始关注比特币及区块链技术，拥有 3 年的区块链产品开发经验。

李凌波, 风控总监

李凌波女士拥有中国科学院金融工程硕士学位，同时有超过 12 年的信用风险管理及资产投资经验。

2016 年加入唯链，负责数字资产管理及风险管理。

林素君，唯链新加坡总经理

林素君女士毕业于新加坡南洋理工大学电气与电子工程专业。2017 年加入唯链前，主要从事商业开发工作。在从事了 3 年的自营交易后，她出售了自己的电子商务业务，并开始为创业公司和中小企业提供数字战略和转型方面的咨询服务。

2017 年加入唯链后担任新加坡总经理。

陆扬，联合创始人兼首席执行官

陆扬先生毕业于上海交通大学电子与通信工程专业，拥有超过 13 年的 500 强跨国企业IT 高管经验，曾任路易威登中国区首席信息官。

2015 年创办唯链，致力于区块链技术推广及商业落地。

钱斌，区块链研发总监

钱斌先生在移动应用开发领域尤其是网络即时通信系统开发有超过 11 年的工作经验，搭建过千万级用户的即时通信系统，他也是 P2P 网络技术专家。

2016 年加入唯链，负责区块链开发工作。

钱诚诚，渠道及销售副总裁

钱诚诚先生于 2004 至 2016 年期间供职于惠普中国，有丰富的市场和项目管理经验。

2017 年加入 VeChain 后担任负责商业合作伙伴招募和管理的副总裁。

盛云斐 · 财务总监

盛云斐女士曾在普华永道担任经理超过 7 年，期间主要负责内部审计和网络安全评估。

2016 年起涉足区块链行业，并设计了通证发行项目评估系统和数字资产管理系统。2018 年加入唯链后，担任财务总监。

吴少淮, 产品及项目经理

吴少淮先生毕业于纽约圣约翰大学，有超过 4 年的 iOS 开发及项目管理经验。参与过多个项目的开发及管理，项目涉及奢侈品行业、政府机关、汽车行业等。

2016 年加入唯链，负责区块链项目管理。

张杰，联合创始人兼首席财务官

张杰先生曾在四大会计师事务所工作超过 14 年，曾任普华永道中国和德勤英国两所高级经理。

2015 年加入唯链后负责区块链治理架构的设计和数字资产管理框架的搭建工作。

张洋 · 产品总监

张洋先生毕业于华东师范大学，拥有硕士学位，主修软件工程。

他在产品设计和运营方面拥有超过 7 年的工作经验，并领导团队在移动互联网、物联网和金融科技等领域推出过多款成功产品。他参与创办了 2 家公司，拥有 3 年以上的商业管理经验。

2017 年加入唯链后担任产品总监。

周子衡, 首席科学家

周子衡先生于英国南安普顿大学获得计算机博士学位。先后以研究员和资深研究员的身份任职于英国肯特大学和芬兰奥卢大学，参与了欧盟委员会和芬兰科学院多个重要科研项目。

拥有超过十年的科研经验，且在国际一流学术杂志和会议上发表过科研论文。

附录 A：独立性（与利益相关方无关联）

本标准适用于战略决策委员会和顾问委员会的独立成员。

满足相关入选标准的独立性要求且符合下列所有分类标准的成员应视为“独立成员”：

1) 成员本人及直系亲属均不担任基金会的合伙人、重要利益相关者，或任何利益相关者的高管。
2) 成员本人及直系亲属均不大量持有 VET。本标准下所称的 VET 持有者应为重要的 VET 持有者。
3) 成员本人及直系亲属均不担任基金会的高管。
4) 上述标准所称的“直系亲属”包括：配偶、父母、子女、兄弟姐妹、配偶的父母、子女的配偶、养子养女、配偶的兄弟姐妹及任何共同居住人（家政服务人员除外）。

此外，在评估独立性时，战略决策委员会还会考虑其他相关事实和情况。

附录 B：第一届战略决策委员会和顾问委员会成员

战略决策委员会成员及利益相关方：

监督管理委员会负责人 – 张俊贤 （普华永道网络安全和金融科技服务合伙人）

张俊贤先生作为普华永道中国风险及控制服务合伙人，常驻于普华永道上海分所，已在普华永道工作超过 14 年。

张俊贤先生是信息安全方面的专家，熟悉中国内地和香港地区金融服务行业公司的安全评估与法规遵守咨询服务，在上述领域拥有丰富经验。

张俊贤先生毕业于于香港科技大学，拥有信息技术工商管理学士学位（B.B.A.）。_

公共关系委员会负责人 – 康文煜（DNV GL 管理服务 集团大中华区首席执行官）

康文煜先生于 1999 年加入 DNV GL 集团，此前他任职于国有汽车设计和制造巨头之一上汽集团。

康文煜先生在供应链管理和产品认证方面积累了丰富经验，尤其对食品、医疗、汽车和航空行业有深刻认识和卓越见解。

康文煜先生拥有上海交通大学工程学学士学位，以及厦门大学高级工商管理硕士学位。

日常运营委员会负责人 – 张杰（唯链首席财务官、联合创始人）

张杰先生在四大会计师事务所中的两家就职过，曾任普华永道和德勤高级经理。加入唯链后负责区块链治理架构的设计和数字资产管理框架的搭建工作。

张杰先生在信息科技保障和咨询服务行业拥有14 年的经验。专长领域包括IT 一般控制、IT 安全、IT 治理与风险管理以及信息系统程序控制等。

张杰先生毕业于上海交通大学电气与电子工程专业。

薪酬与提名委员会负责人 – 朱睿（香港城市大学助理教授）

朱睿教授拥有复旦大学学士学位、美国印第安纳大学经济学硕士学位和美国德克萨斯大学奥斯汀分校金融博士学位。朱睿教授现致力于研究公司金融、公司风险管理、资本市场与产品市场的交互等。

技术委员会负责人 – 周子衡，（唯链首席科学家/合伙人）

周子衡先生于英国南安普顿大学获得计算机科学博士学位，现为唯链研发负责人。他曾以博士后研究员的身份任职于英国肯特大学，并参与了欧盟委员会和芬兰科学院的多个重要科研项目，在国际一流学术期刊上发表过多篇科研论文。

唯链商业开发事务负责人 – Renato Grottola（雷纳托 • 格罗托拉）（DNV GL 管理服务集团全球数字化转型负责人）

作为资深的全球咨询服务负责人，雷纳托先生在咨询行业拥有良好的工作记录，对战略规划、兼并与收购、商业发展和复杂国际运营管理有着丰富的经验。现负责将私有区块链用于船舶认证的区块链支持项目。

基金会秘书长 – 陆扬（唯链首席执行官、联合创始人）

作为唯链项目的创始人，陆扬先生在奢侈品行业的信息技术和信息安全方面拥有丰富经验，在创办唯链前，他曾担任路易威登中国首席信息官、IS&T 总监等职。

LVMH 集团旗下的其他知名品牌包括奢侈时装品牌纪梵希、迪奥以及香槟品牌 Moet et Chandon、Veuve Clicquot、Dom Perignon 等。

陆扬先生曾就读于上海交通大学电子与通信工程专业。

顾问委员会成员及相关实体：

Jim Breyer（吉姆·布雷耶）- Breyer Capital 创始人兼首席执行官

布雷耶先生是 40 多家已上市或完成并购公司的投资人，包括 Facebook 在内的一些投资项目获益超过 100 倍，另有许多投资收益超过 25 倍。

沈波 – 分布式资本普通合伙人

沈波先生是 Bitshares 的联合创始人，还是 Zcash 及其它一些区块链项目的早期投资人。在传统金融行业经验丰富，在经纪人业务、对冲基金和投资银行等领域有 12 年的高级管理工作经验。

Daniel Kelman（丹尼尔·凯尔曼） – GSR、Bitcoin.com 法律事务总顾问

凯尔曼先生曾在 Mt Gox 洗钱丑闻中担任债权人利益辩护律师。他也是已获得日本监管机构金融事务管理局（FSA）批准的数字货币交易所比特海洋的联合创始人。

龚鸣 – 区块链铅笔首席执行官

区块链铅笔是中国最具影响力的专业性区块链和数字货币媒体。

孙铭 – 世泽律师事务所合伙人

孙铭先生拥有丰富的法律咨询服务，擅长领域包括数字货币、区块链、银行事务和信托等。

南宁 – 比特海洋首席执行官

比特海洋是一家数字货币交易服务提供商，于 2017 年 12 月获得日本监管机构金融事务管理局发放的牌照。

附录 C：参考文献

[1] V. Buterin. A next generation smart contract & decentralized application platform (Ethereum white paper), 2014.

[2] G Wood. Ethereum: A secure decentralised generalised transaction ledger (Ethereum yellow paper), 2014.

[3] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2008.

[4] POA Network. Proof of Authority: consensus model with identity at stake, Medium (https://medium.com/), 2017.

[5] M. Castro and B. Liskov. Practical Byzantine fault tolerance, in the Proceedings of the Third Symposium on Operating Systems and Implementation, 1999.