InterValue·互联价值

Connect, Transfer and Exchange All Digital Assets Over the World

全球首个支撑大规模应用的实用化区块链4.0项目

构建下一代全球价值互联网的基石

构建行业公链的底层基础设施

高实用性去中心化分布式应用开发平台

白皮书

互联价值 · 开发团队　2018年3月

说明

此文档是互联价值技术白皮书 V4.5 版本，主要介绍互联价值的背景、定位、技术特性和应用场景等内容。未来我们会持续升级此文档，使其与技术实现保持一致。欲了解互联价值的最新资讯、技术白皮书、软件发布、开发者社区等信息，请访问官方网站：http://www.inve.one。

联系我们

白皮书：whitepaper@inve.one
社区管理：community@inve.one
基金会：foundation@inve.one
其它：support@inve.one

版权声明

免责声明

技术在不断发展，区块链也在不断进步，互联价值开发团队未来会根据需要改进、完善现有技术方案，并持续完善技术白皮书。

目录

摘要

区块链技术被认为是继蒸汽机、电力、信息、互联网科技之后第五个最有潜力引发生产力和生产关系颠覆性革命的核心技术。自 2009 年以比特币为代表的区块链技术诞生以来，该项技术取得了长足的发展和越来越多的关注认可，尤其是近年来区块链技术已经成为全球关注的焦点。区块链行业研究和开发人员在底层核心技术实现到链上应用再到各类场景落地应用等各个层面开展了全方位的探索，但纵观区块链技术的整个发展过程，现阶段区块链技术离大规模实用化还有较大差距，尤其是区块链底层核心技术还未取得较大突破，还存在许多技术难题有待攻克，目前开展的各类区块链场景落地应用很大程度上根基不稳，难以发挥实效，因此当前迫切需要对区块链底层基础设施开展研发，进而为各类区块链应用提供可靠支撑，从而推动区块链技术在各领域各行业真正的落地应用，使区块链这一颠覆性技术更快更好地为人类社会服务。

互联价值（InterValue）以提供全球价值互联网基础设施为目标，针对现有区块链基础设施普遍存在的实用化程度较低，尤其是交易拥堵、交易费高、交易确认时间长、抗量子攻击能力较弱、通信层节点匿名性不高、交易匿名保护、跨链通信和多链融合能力较弱、存储空间较大等问题和需求，优化提升区块链技术在各个层面的协议和机制，实现价值传输网络各层次的支撑协议，作为真正的区块链 4.0 基础设施，为各类价值传输应用提供基础设施，为各类 DApp 开发提供底层开发平台，为构建全球价值互联网提供现实可行的技术途径。

InterValue 项目**聚焦区块链基础设施和平台层核心技术**，目标是打造攻克了关键技术难题的全领域生态级别的底层基础设施，其主要技术创新包括：① **在底层 P2P 网络节点通信层面**，结合现有基于 Tor 的匿名通信网络、基于区块链的分布式 VPN 的优点实现了独创的匿名 P2P 通信网络，设计实现了节点匿名接入的方法，并实现了私有加密的通信协议，极大地增强了底层通信网络中节点的匿名性，确保节点间通信难以被追踪和破解。② **在底层数据结构层面**，采用了新型数据结构，增强式的有向无环图（DAG）——哈希网（HashNet，HN），从而实现异步并行的事件共识验证，提升了系统的可扩展性。③ **在分布式共识机制层面**，设计了一种安全高效的双层共识机制，基于增强 DAG 的 HashNet 共识和基于随机选择函数的拜占庭协商（BA–VRF）共识，该共识机制具有并发量高、交易确认速度快的特点，可快速构建面向不同应用场景的生态体系。④ **在抗量子攻击层面**，采用新型抗量子攻击密码算法，通过将 ECDSA 签名算法替换为基于整数格的 NTRUsign 签名算法，同时用 Keccak–512 哈希算法替换现有的 SHA 系列算法，降低了量子计算飞速发展和量子计算机逐步普及带来的威胁。

⑤ **在匿名交易层面**，结合门罗币和 ZCash 等加密虚拟货币的特性，通过一次密钥和环签名，设计了效费比极高和安全性极好的交易匿名和隐私保护方法，并支持零知识证明作为选择功能，满足不同应用场景隐私保护需求。⑥ **在智能合约层面**，通过实现摩西虚拟机 (Moses Virtual Machine，MVM)，支持声明式非图灵完备智能合约和面向摩西 (Moses) 语言的高级图灵完备智能合约，优势在于较好的支持链下数据访问，支持第三方资产发行，能以公有链、联盟链、私有链等形式落地到实际应用场景。⑦ **在跨链通信和多链融合层面**，采用中继链技术将跨链通信和多链融合功能模块作为单独一层 Overlay 来实现，既能够保持跨链操作的独立性，又能够复用 InterValue 基础链的各种功能。⑧ **在生态激励层面**，综合使用多种 Token 分配手段和方法，并支持双层挖矿用于生态激励。⑨ **在行业应用层面**，通过流通支付、数据传输、数据搜索、合约调用等 JSON–RPC 行业通用接口的开发，支撑上层的各类应用。

InterValue 支持在链上构建包括匿名网络通信、算力共享、存储空间共享、带宽共享、信誉共享（信用担保）等各种应用，提供开放接口，供第三方开发 DApp，并通过结合各类实际应用场景，与各类服务提供商、应用提供商合作，支持商业组织和政府机构按照自身业务特性和需求构建公有链、联盟链和私有链应用系统，从而将 InterValue 应用到各类实际应用场景中。

InterValue 将对现有互联网运营模式进行重塑，在激励层引入 Token 机制达到实现面向公有链灵活共识机制的目的，激励社区维护 InterValue 公有链以及在 InterValue 公有链上开发 DApp 应用，为 InterValue 公有链平台增加价值并推动网络传播效应，将经济激励系统本身变为能够在系统内循环的体系，创造完全去中心化的价值互联与价值传输生态系统。

1

背景

1.1. 区块链发展概况

区块链技术起源于化名为“中本聪”(Satoshi Nakamoto）的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。凯文·凯利在《失控》一书中描述：生物逻辑的自然、社会、技术的进化规律就是从边缘到中心再到边缘，从失控到控制再到失控。区块链的技术基础是分布式网络架构，正是因为分布式网络技术的成熟，去中心、弱中心、分中心及共享、共识、共担的组织架构和商业架构才有可能有效地建立起来。

如今的区块链技术已经发生了数次迭代：① **区块链 1.0–数字货币**，2009 年初，比特币网络正式上线运行。作为一种虚拟货币系统，比特币的总量是由网络共识协议限定的，没有任何个人及机构能够随意修改其中的供应量及交易记录。支撑比特币运行的底层技术——区块链实际上是一种极其巧妙的分布式共享账本及点对点价值传输技术，对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。② **区块链 2.0–智能合约**，2014 年前后，业界开始认识到区块链技术的重要应用价值，试图创建可共用的技术平台并向开发者提供 BaaS（Blockchain as a service）服务，极大提高了交易速度，大大降低资源消耗，并支持 PoW、PoS 和 DPoS 等多种共识算法。③ **区块链 3.0–区块链应用延伸**，2015 年后，随着像 Byteball 和 IOTA 等基于 DAG

数据结构的区块链 3.0 技术兴起，区块链系统较之前更加高效、可扩展强、互通性强、以及具有更良好的用户体验，其应用也进一步延伸到医疗健康、IP 版权、教育、物联网、共享经济、通信、社会管理、慈善公益、文化娱乐等更为广泛的应用。④ **区块链 4.0–完善生态体系**，最近，基于 HashNet 数据结构的区块链 4.0 技术逐步受到业界的关注，基于该数据结构实现的共识算法可在交易吞吐量、可扩展性上实现质的飞跃，从而进一步支撑区块链作为某个行业的基础设施，并形成基于区块链的完善生态体系，将广泛而深刻地改变人们的生活方式。

图 1–1: 区块链的演进路径

最近两年，部分国家虽然对数字货币的使用和发展持保守态度，但世界各国在区块链底层技术研发以及将区块链与实际应用场景相结合的落地方面一直持积极态度，随着人们对区块链技术的适用范围和可用性的认知程度的提高，人们以极大的热情开展区块链底层核心技术、链上应用和场景落地的研发和实施。

人们对区块链技术的研究和探索主要集中于 3 个层面：① 底层技术及基础设施层，主要包括基础协议与区块链相关硬件内容。② 通用应用及技术扩展层：为行业垂直应用层提供服务和接口及相关技术服务，提供的服务包括智能合约、快速计算、挖矿服务、信息安全、数据服务、BaaS、解决方案、防伪溯源等。③ 垂直行业应用层：在金融、数字货币、娱乐、供应链、医疗、法律、能源、公益、社交、物联网及农业等垂直领域落地实施。当前，人们投入了极大的热情开展区块链技术的研发和应用，在从事区块链研究和开发的团队中，从事区块链底层技术研究的团队占比约为 20%，将区块链用于各个实际应用场景和垂直行业的团队占比达 80%，相对于应用层而言，底层协议能够创造 Token 市场价值，另外还分散了应用层数据中心化的互联网传统模式。在区块链体系下，应用层的项目本身成为了完全的服务方，不再拥有用户流量与数据价

值，这些个人数据的价值分散到了用户身上，底层协议相对于应用层会更有价值。

1.2. 区块链关键技术

底层数据结构，传统的区块链原本是比特币等加密货币存储数据的一种独特方式，是一种自引用的数据结构，用来存储大量交易信息，由多条交易记录组成区块，区块从后向前有序链接起来，最终实现无法篡改，方便追溯等特点。传统区块链的块链式结构是阻碍区块链提高并发性的瓶颈，技术极客们不断寻找更高效的数据块链接形式，提出有向无环图（Directed Acyclic Graph，DAG）与区块链相结合的解决方案，以下称为“DAG 链”。DAG 中不存在记账者打包区块这一过程，而是记账过程通过用户相互确认来实现，从而可以大大缩短了交易确认的时间。

哈希算法，哈希运算能够实现数据从一个维度向另一个维度的映射，通常使用哈希函数实现信息摘要，hash 函数碰撞概率极低，并且能够隐藏原始信息。区块链中哈希函数特性包括：函数参数为 string 类型，固定大小输出以及计算高效。常用的 hash 算法包括 MD5 和 SHA 系列算法。但量子计算机下 SHOR 算法可以将攻击哈希算法的复杂度从 $O(2^n)$ 降为 $O(2^{n/2})$，传统的哈希算法受到量子攻击的威胁。

签名算法，签名算法通过用私钥对信息进行加密变换以保证信息的不可否认性。当前区块链主要使用基于椭圆曲线的 ECDSA 数字签名算法，该签名算法首先需要生成个人的公私钥对：(sk, pk) := generateKeys(keysize)，sk 私钥用户自己保留，pk 公钥可以分发给其他人；其次，可以通过 sk 对一个具体的 message 进行签名：sig := sign(sk, message) 这样就得到了具体的签名 sig；最后，拥有该签名公钥的一方能够进行签名的验证：isValid := verify(pk, message, sig)。但量子计算机下 SHOR 算法可以将攻击 ECDSA 签名算法的复杂度从 $O(2^n)$ 降为 $O(n^2(\log n)(\log\log n))$，ECDSA 签名算法无法抵抗量子攻击。

匿名交易保护，在公有区块链中，每一个参与者都能够获得完整的数据备份，所有交易数据都是公开和透明的，但对于很多区块链应用来说，这是致命的。不仅用户希望他的帐户隐私和交易信息被保护，就商业机构来说，包含重要资产和商业机密的帐户和交易信息更应当受到保护。比特币的隐私保护思路是，通过隔断交易地址和地址持有人真实身份的关联，来达到匿名的效果。但这样的保护是很弱的，通过观察和跟踪区块链的信息，通过地址 ID、IP 信息等还是可以追查到帐户和交易的关联性。为了解决区块链的隐私保护问题，目前有一次密钥、环签名、同态加密、零知识证明等几种方式。

网络层 P2P 通信，P2P 网络技术是区块链系统连接各对等节点的组网技术，学术界将其翻译为对等网络，在多数媒体上则被称为“点对点”或“端对端”网络，是一种建构于传输层的覆盖网络（overlay network）。不同于中心化网络模式，P2P 网络中各节点的计算机地位平等，每个节点有相同的网络权力，不存在中心化的服务器。但节

点的信息容易被泄漏。

共识层共识机制，目前主要有几大类共识机制：PoW、PoS、DPoS、PBFT。PoW 工作量证明，就是人们熟悉的比特币挖矿，通过计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储。可实现完全去中心化，节点自由进出，但挖矿造成大量的资源浪费，共识达成的周期较长，不适合商业应用。PoS 权益证明，PoW 的一种升级共识机制，根据每个节点所占代币的数量和时间，等比例的降低挖矿难度，从而加快找随机数的速度。PoS 还是需要挖矿，本质上没有解决商业应用的痛点。DPoS 股份授权证明机制，类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账，其整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的。PBFT：Practical Byzantine Fault Tolerance，实用拜占庭容错算法，是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制，每个状态机的副本都保存了服务的状态，同时也实现了服务的操作，尽管可以存在多于 $3f+1$ 个副本，但是额外的副本除了降低性能之外不能提高可靠性。

激励层激励机制，为了保证区块链分布式系统的正常运行，需要大量的诚实节点保持在线，激励机制则是用来奖励这些对系统有贡献的用户，从博弈论的角度来说，激励机制应该要使得用户诚实行为的收益远远大于恶意行为。

智能合约，基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约。比特币只支持简单的脚本语言，以太坊拥有图灵完备的智能合约语言，但是智能合约的拟定和部署十分繁琐，且容易受到攻击。Byteball 的智能合约简单易部署，但却是非图灵完备的，不利于合约应用的扩展。

1.3. 当前区块链基础设施存在的问题

现阶段，各类底层协议项目如 EOS、NEO、ArcBlock 等项目层出不穷，但大部分底层协议项目是在以太坊基础之上进行迭代，与区块链 3.0 的标准有一定的差距，更谈不上区块链 4.0。而大部分开展区块链落地业务的团队，受限于底层协议的性能、适用范围和稳定性，目前也都处于早期探索阶段，虽预计在 2018 年可以看到一大批行业应用出现，但在底层协议不断更迭的同时，超过 98% 的项目都将会被时代淘汰。

概括起来，目前区块链技术主要存在以下问题。

性能低。性能过低是当前区块链技术面临的主要挑战之一。比特币使用的区块链理论上每秒最多只能处理七笔交易，以太坊稍有提高，但也远远不能满足应用需求。截至 2017 年 12 月，一个简单的 DApp 应用程序 CryptoKitties 就会减慢以太坊交易吞吐并大幅增加交易费用。今天的消费者应用程序必须能够每天处理数千万活跃用户。另外，有些应用只有在满足一定的交易吞吐量时才有意义，因此平台本身必须能够处理大量的用户并发。长时间的交易延迟会阻碍用户的使用，使得建立在区块链上的应

用程序与现有非区块链备选方案的竞争力大大降低。

使用门槛高。今天的区块链应用程序仅仅是为知道如何使用区块链的少数技术人员而建立的，而不是主流消费者。几乎所有的区块链应用都要求用户运行区块链全节点或轻节点。较高的学习成本严重阻碍了区块链走向大众的进程。例如，基于以太坊的游戏 CryptoKitties 可能是有史以来最易于使用的 DApp，但它仍然需要用户安装 Metamask light wallet 浏览器扩展程序，并且用户还需要知道如何安全购买 Ethers，并将其与 Metamask 一起使用，这大大影响了用户体验。为了吸引普罗大众的广泛使用，区块链应用程序应该像今天的互联网和移动应用程序一样简单。

使用成本高。区块链技术的高使用成本是阻碍其成为主流应用的另一个主要障碍，同时也限制了需要灵活构建免费服务的开发人员。与互联网对比，区块链技术应该能够支持免费应用程序。让区块链免费使用是其被广泛采用的关键。一个免费的平台也将使开发商和企业能够创造出有价值的新服务。

平台锁定。与任何计算机技术的初期一样，区块链存在严重的“平台锁定”问题。开发人员必须首先决定采用哪个区块链，然后编写该特定平台的代码，这样导致将应用程序切换到其他区块链会非常困难。开发人员不希望被锁定在某一种区块链技术，而是需要这些应用程序能在多个平台上运行，以提高开发复用的效率。

应用范围较窄。当前人们对区块链抱有很高的期望，特别是随着加密数字货币价格日益上涨，各大新闻媒体为区块链绘制了非常美好的蓝图。但实际上，区块链技术目前仍处于起步阶段，大多数区块链服务缺乏丰富的功能，应用范围较窄。在区块链开发社区中也缺乏相应的激励机制。

因此，当前迫切需要开展区块链底层协议研究，攻克区块链底层核心技术，对区块链技术层面各个维度进行重新设计或加以改进，解决和满足交易拥堵、交易费高、交易确认时间长、抗量子攻击能力较弱、节点通信匿名性不高、缺乏交易匿名保护功能、跨链通信和多链融合能力较弱、存储空间较大等问题，优化提升区块链技术在各个层面的协议和机制，实现真正实用化的价值传输网络各层次的支撑协议，为各类价值传输应用提供基础设施，为各类 DApp 开发提供底层开发平台，为构建全球价值互联网提供现实可行的技术途径。

2

互联价值定位

2.1. 名称

InterValue：互联价值。

INVE：InterValue Token。

2.2. 愿景

互联网实现了人类社会部分信息在互联网上流转和分享，区块链则可以实现包括人类社会所有数字资产及实际资产在内的全部信息在价值互联网上的流转和分享。互联网和区块链存在的意义和价值是实现现实社会到虚拟社会的映射，其中互联网可实现信息的映射，区块链则可以实现价值的映射。InterValue 作为实用化的价值互联区块链基础设施，提供了具有一系列技术和功能特性用于支撑现实世界和虚拟世界之间的价值映射，必将为探索和早日实现价值映射提供可行的实现路径。

憧憬一下 InterValue 广泛应用后的世界，人们的任何行为和活动均可实现自动支付、自动评价、自动保存、自动判断合法性，人们可以自行选择一生的行为和活动是否保存。随着人工智能的逐步演进，可以诞生具备个体完整意识、完全自主智能的虚拟人，人们将现实生活中的各种资产完全转移到链上后，代表一个个人类社会个体的虚拟人将和个体资产一起，永远在链上保存和演化下去，实现了人类社会的虚拟永生，这就是互联网和区块链完整结合后，现实世界和虚拟世界之间的信息映射和价值映射完全实现后的世界。

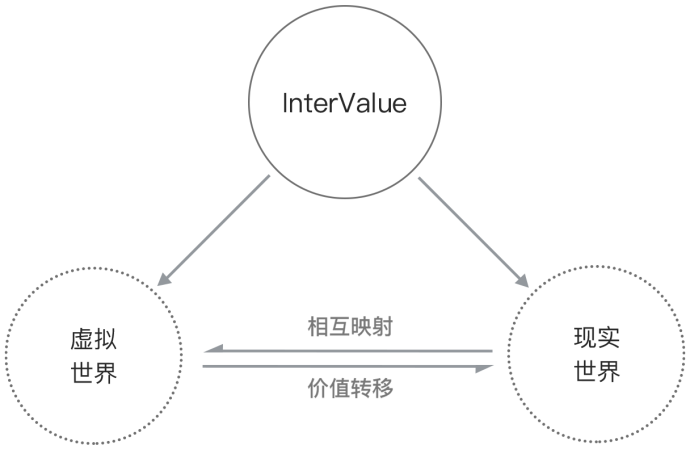


图 2–1: 现实世界和虚拟世界的映射

2.3. 目标

InterValue 的目标是构建一个通用、支撑功能完善、性能高、易于使用、用户体验好、可扩展的基于增强有向无环图的区块链 4.0 基础设施，打造支撑各类链上应用的区块链 4.0 生态系统。

InterValue 聚焦区块链基础设施和平台层核心技术，构建具备独创完全分布式匿名 P2P 网络通信协议、新型抗量子攻击密码哈希算法和签名算法、独创双层共识和挖矿机制、支持交易匿名保护、图灵完备智能合约等特性，采取公平分发机制，支持第三方资产发行、跨链通信、多链融合等功能，能以公有链、联盟链、私有链等形式落地到实际应用场景。InterValue 的愿景是实现价值传输网络各类关键技术，构建全球价值互联网，为各类价值传输应用提供基础网络。

2.4. 生态体系

InterValue 充分吸收现有区块链 1.0、区块链 2.0 和区块链 3.0 项目的优点，解决它们的突出问题和技术缺陷，构建更加繁荣的应用生态。如图 2–3 所示，InterValue 创新设计了链上链下数据映射机制，基于有向无环图 (DAG) 和哈希网 (HashNet) 的新型增强数据结构、基于 HashNet 共识和 BA–VRF 共识双层共识机制、引入外部触发条件的高级图灵完备智能合约、基于抗量子攻击的 Keccak512 哈希算法和 NTRUSign 签名算法、基于环签名和零知识证明交易匿名保护机制，具有交易快速确认、抗量子攻击、节点匿名通信、交易匿名保护、高级智能合约、数据上链等区块链 4.0 的功能特性，并通过采取公平分发机制，支持第三方资产发行、跨链通信、多链融合等功能。

InterValue 的愿景是构建全球价值互联网，为各类价值传输应用提供基础区块链网络，支持各类实际应用以公有链、联盟链、私有链等形式落地。在特定应用中，InterValue 将特定应用场景数据进行 Hash 运算，Hash 值存储在 InterValue 公链上，面向

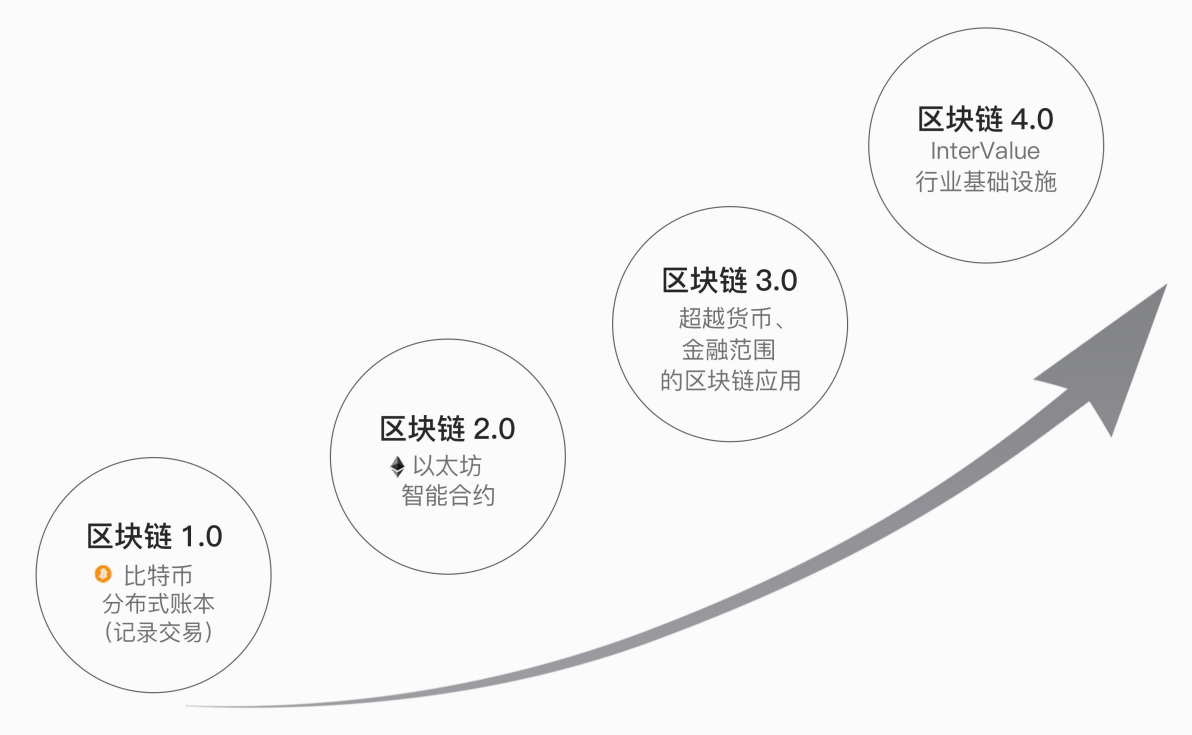


图 2–2: 区块链 4.0 路线图

的应用场景已经不限于区块链 1.0 背景下以比特币为代表的数字货币应用，不限于区块链 2.0 背景下数字货币与智能合约相结合的金融领域，以及不限于区块链 3.0 在政府、健康、文化和艺术等领域上的应用尝试；基于 InteValue 的区块链 4.0 公链将成为多个行业的基础设施，形成基于区块链的完善行业生态体系，将广泛而深刻地改变人们的生活方式。

图 2-3: InterValue 生态体系图

InterValue 将彻底重塑现有互联网的运营模式，将经济激励系统本身变为能够在系统内循环的体系，创造一个完全去中心化互联网价值传输生态系统，同时也是个完全开放的社区生态系统，超越国界，让每一位参与者都能获得相应的价值体现。

2.5. 关键特性

InterValue 对区块链基础设施的各个层面均作了很大改进，在部分层面提出了突破性的创新。InterValue 主要技术创新包括：① **在底层 P2P 网络节点通信层面**，结合现有基于 Tor 的匿名通信网络、基于区块链的分布式 VPN 的优点实现了独创的匿名 P2P 通信网络，设计实现了节点匿名接入的方法，并实现了私有加密的通信协议，极大地增强了底层通信网络中节点的匿名性，确保节点间通信难以被追踪和破解。② **在底层数据结构层面**，采用了新型数据结构，增强式的有向无环图（DAG）——哈希网(HashNet, HN)，从而实现异步并行的事件共识验证，提升了系统的可扩展性。③ **在分布式共识机制层面**，设计了一种安全高效的双层共识机制，基于增强 DAG 的 HashNet 共识和基于随机选择函数的拜占庭协商（BA–VRF）共识，该共识机制具有并发量高、交易确认速度快的特点，可快速构建面向不同应用场景的生态体系。④ **在抗量子攻击层面**，采用新型抗量子攻击密码算法，通过将 ECDSA 签名算法替换为基于整数格的 NTRUsign 签名算法，同时用 Keccak–512 哈希算法替换现有的 SHA 系列算法，降低了量子计算飞速发展和量子计算机逐步普及带来的威胁。⑤ **在匿名交易层面**，结合门罗币和 ZCash 等加密虚拟货币的特性，通过一次密钥和环签名技术，设计了效费比极高和安全性极好的交易匿名和隐私保护方法，并支持零知识证明作为选择功能，满足不同应用场景隐私保护需求。⑥ **在智能合约层面**，通过实现摩西虚拟机 (Moses Virtual Machine，MVM)，支持声明式非图灵完备智能合约和面向摩西 (Moses) 语言的高级图灵完备智能合约，优势在于较好的支持链下数据访问，支持第三方资产发行，能以公有链、联盟链、私有链等形式落地到实际应用场景。⑦ **在跨链通信和多链融合层面**，采用中继链技术将跨链通信和多链融合功能模块作为单独一层 Overlay 来实现，既能够保持跨链操作的独立性，又能够复用 InterValue 基础链的各种功能。⑧ **在生态激励层面**，综合使用多种 Token 分配手段和方法，并支持双层挖矿用于生态激励。⑨ **在行业应用层面**，通过流通支付、数据传输、数据搜索、合约调用等 JSON–RPC 行业通用接口的开发，支撑上层的各类应用。

InterValue 关键特性设计如图2–4所示。

InterValue 关键特性概括起来，主要包括：

- 基于 HashNet 的新型增强式 DAG 数据结构，存储空间需求小
- 多层共识机制：HashNet、BA–VRF 和基础 DAG 共识
- 完全分布式匿名 P2P 网络通信

图 2-4: InterValue 关键特性设计

- 抗量子攻击的哈希算法和签名算法
- 支持声明式智能合约与图灵完备智能合约，并支持链下数据访问
- 支持图灵完备的高级声明式智能合约
- 支持高并发交易，交易确认时间短

2.6. 项目优势

InterValue 是一个自我进化的生态系统，项目吸纳现有区块链 3.0 项目的优点，并致力于打造 4.0 时代基础设施，重点借鉴了采用 DAG 数据结构的 IOTA 和 Byteball 以及目前正在研发的 Hashgraph 项目的优点，并通过采用创新的双层共识机制，设计和使用具有抗量子攻击特性的密码算法，设计并实现基于 HashNet 的全新共识机制解决现有区块链基础设施存在的各类问题，构建更加繁荣的应用生态。表 2-1 从代币、市值、共识机制、智能合约、P2P 网络、量子安全、隐私保护、奖励机制、交易速度、节点分类等方面将 InterValue 与现有 DAG 公链项目进行了对比。

从 InterValue 当前推进情况及后续发展规划看，InterValue 主要有以下优势：

- 设计上定位为面向实用化的区块链 4.0 基础设施，技术特性设计先进，是支撑区块链技术大规模普及应用和实用化的区块链 4.0 基础设施。

- InterValue 团队搭配及分工合理，技术研发能力强，市场推广能力强，场景落地能力强，能够确保 InterValue 实现设计的各种特性。

表 2–1: 与其他 DAG 区块链的对比

	IOTA	ByteBall	Hedera Hashgraph	InterValue
代币	IOTA	Byte	Hashgraph	**INVE**
市值	140 亿美元	4 亿美元	暂无	**暂无**
共识机制	MCMC 共识	12 名公证人	Hashgraph	**去中心化双层共识**
智能合约	不支持	声明式合约	图灵完备合约	**声明式与高级图灵完备合约**
P2P 网络	不匿名	不匿名	不匿名	**匿名**
量子安全	部分抵抗	否	否	**抗量子攻击**
交易匿名保护	否	是	否	**零知识证明的交易匿名保护**
奖励机制	无	交易引用和公证	交易代理服务	**交易引用、公证、挖矿**
交易速度	1000 TPS	100 TPS	暂无	**100 万 TPS**
节点分类	全节点、轻节点	全节点、轻节点	全节点、轻节点	**全节点（责任节点）、局部全节点（责任节点）、轻节点、微节点**

- 基于 InterValue 构建的区块链链上应用正在迅速推进，目前正在策划和开发基于 InterValue 的分布式社交平台和基于 InterValue 的全球分布式存储网格。另外，团队还在筹划有很大用户基数的杀手级的链上应用。

- InterValue 团队作为技术提供方，目前已和多个有使用区块链技术优化和提升现有业务流程的公司合作，已将 InterValue 基础设施用到多个实际应用领域和场景中，正在开发和实施。
- InterValue 团队正积极构建合作伙伴联盟，力争将 InterValue 应用到尽可能多的行业和实际场景中去。
- InterValue 团队正积极构建开发者社区，在技术层面确保更多技术人才加入到 InterValue 基础设施本身的改进优化和基于 InterValue 的 DApp 开发中来。
- InterValue 团队正积极构建区块链技术普及社区，推进区块链技术的普及工作。

3

基于 P2P 的匿名通信技术

InterValue 底层通信网络采用 P2P 架构，然后在其上加入了节点间匿名访问机制来确保信息服务的隐私保护性。

P2P 是英文 Peer-to-Peer 的缩写，称为“对等网”或“点对点”技术。IBM 将 P2P 定义为：“P2P 系统由若干互联协作的计算机构成，且至少具有如下特征之一：系统依存于边缘化（非中央式服务器）设备的主动协作，每个成员直接从其他成员而不是从服务器的参与中受益；系统中成员同时扮演服务器与客户端的角色；系统应用的用户能够意识到彼此的存在，构成一个虚拟或实际的群体。”

在 P2P 系统中，每一个节点（Peer）都是平等的参与者，承担服务使用者和服务提供者两个角色。资源的所有权和控制权被分散到网络的每一个节点中。P2P 技术使得网络上的沟通变得很容易、很直接，并且把对中间服务器的依赖减少到最小。P2P 技术改变了“内容”所在的位置，使其从“中心”走向“边缘”。也就是说它改变了互联网现在以集中式的网站为中心的状态，资源不保存在服务器上，而保存在所有用户的 PC 机上。P2P 技术使得终端不再是被动的客户端，而成为具有服务器和客户端双重特征的设备。因此 InterValue 具有去中心化的特性。

InterValue 的 P2P 网络匿名通信主要通过以下方式实现：

（1）在本机运行一个代理服务器，这个代理服务器周期性地与其他 InterValue 交流，维持一个 TLS 链接，从而在 InterValue 网络中构成虚拟链路。具体为，每个用户运行自己的代理程序：获取目录，建立路径，处理连接。这些代理接受 TCP 数据流，并且在同一条线路上复用它们。

（2）InterValue 在应用层进行加密，在每个中继节点间的传输都通过点对点密钥来加密，形成有层次的结构。它中间所经过的各节点，都把客户端包在里面，这样在中继节点之间可以保持通讯安全。具体为，每个 InterValue 中继节点维护一个长期的验

证密钥和短期的会话密钥，验证密钥来签署 TLS 的证书，签署中继节点的描述符，还被目录服务器用来签署目录。会话密钥则用来解码用户发送来的请求，以便建立一条通路同时协商临时的密钥。TLS 协议还在通讯的中继节点之间使用了短期的连接密钥，周期性独立变化，来减少密钥泄漏的影响。

（3）InterValue 网络中的数据包使用了随机的路径来掩盖足迹，这样在某个点的观察者并不知道数据真正从哪里来，真正的目的地是哪里。客户端在 InterValue 网络中增量地建立一条加密线路。这条线路每次只扩展一跳，而且每次扩展的中继节点只知道数据来自哪个中继节点，数据将要被发送到哪个中继节点去。没有任何一个中继节点知道整条线路。客户端与每一跳都协商了一组独立的密钥来保证每一跳不能追踪走过的中继点。一旦一条线路建立了，就可以用来进行数据交互了。

InterValue 的匿名通信网络的基本原理如图3–1所示。目录服务器是其网络的核心，负责收集 InterValue 网络中的中继节点信息并以节点快照及节点描述的形式发布给 InterValue 代理；中继节点是 InterValue 网络的基础，在网络中的匿名通信流量都是通过由多个中继节点所组成的匿名通信链路来转发的；代理运行于 InterValue 用户端，它负责建立匿名链路并在用户的网络应用程序与 InterValue 匿名链路之间中转网络流量。在图 3–1 中，由 3 个中继节点构成了一条 InterValue 匿名通信链路，这 3 个节点依据其位置依次为入口位置、中间位置与出口位置。

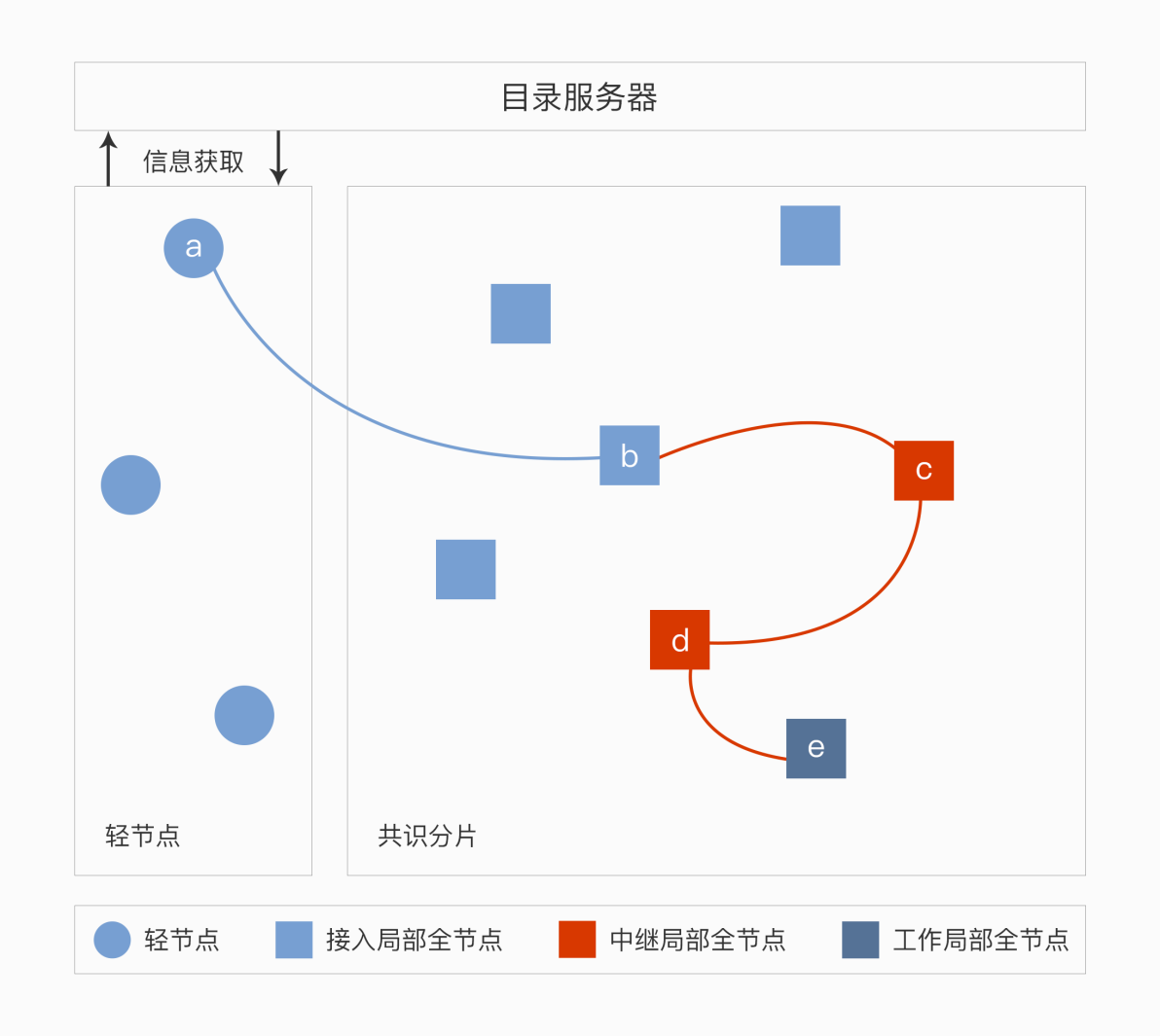


图 3–1: InterValue 匿名通信网络的基本原理图

4

数据结构

4.1. 基础 DAG 数据结构

InterValue 在第一阶段采用基础 DAG 结构存储交易数据。当前已经有 IOTA 和 Byteball 等多个项目利用 DAG 成功构建了能够长期稳定运行的公有链，证明了 DAG 链的技术先进性和性能。在 InterValue 中，交易信息被封装成一个个单元（Unit），单元与单元之间相互链接组合成一个 DAG 图。由于单元可以链接到任意一个或多个之前的单元，不需要为共识问题付出更多的计算成本和时间成本，也不必等待节点之间数据强同步，甚至没有多个数据单元拼装区块的概念，因此可以极大提高交易的并发量，并把确认时间降低到最小。

InterValue 的 DAG 数据结构如图4–1所示，单元之间的有向边表示两个单元之间具有引用关系，图中有一条由 B 指向 A 的有向边，表示 B 引用 A，A 是 B 的父单元，B 是 A 的子单元，同时，我们称单元 C 间接引用 A，A 是 C 的祖先单元；单元 G 不具有任何父单元，称之为创世单元，创世单元是唯一的；单元 X，Y 不具有任何子单元，这类单元被称为顶端单元。

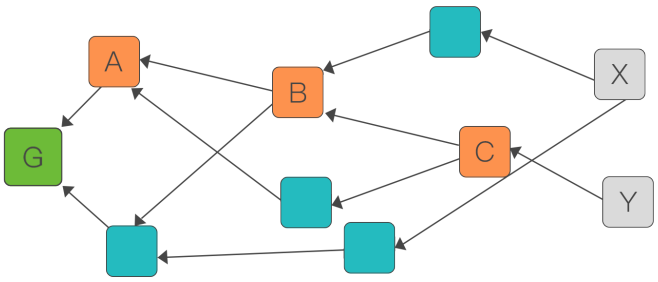


图 4–1: InterValue 有向无环图

单元由单元头部和单元消息两部分组成。其中单元头部主要包含以下字段：

- 单元版本；
- 代币标志符；
- 单元创建者签名：单个签名或多个创建者共同签名；
- 父单元 hash：所引用的单个或多个父单元的 hash；
- 见证人列表：具有相同见证人的其他单元（通常是父单元或祖先单元）的 hash。

单元消息部分用于存储交易的信息，InterValue 具有多种类型的交易，包括支付，数据存储，投票等等。单元的数据结构的详细说明如表4–1所示。

表 4–1: DAG 数据结构详细说明

version	协议版本号
alt	代币标识符
message	包含实际数据的一个或多个消息的数组 • app: 信息类型，比如“payment”代表支付，“text”代表任意文本信息等等。可以根据需要进行类型扩展。 • payload_location: 在何处找到 payload。‘inline’表示该消息包含了 payload，‘uri’表示 payload 可以通过某互联网地址获得，‘none’则表示 payload 不可访问 • payload_hash: payload 的 base64 编码的 hash 值 • payload: 消息数据荷载。保存不同类型的数据内容。比如交易消息包含交易输入和输出 – inputs: 代表了一组由支付指令消耗的输入货币。输入货币所有者必须在单元的签名者之中。以下 3 个字段被用来定位该 inputs 货币的来源。 ◦ unit: 该 inputs 货币的来源单元的 hash 值。计入在最后一个单元才可被消费。 ◦ message_index: 该 inputs 货币的来源单元的消息索引。 ◦ output_index: 该 inputs 货币的来源单元的输出索引。 – outputs: 一组交易输出 ◦ address: 接收者地址 ◦ amount: 接收者收到的金额
authors	该单元的创建者的地址和签名数组
parent_units	该单元父单元的 hash 值数组
witness_list_unit	可以找到见证人列表的单元的哈希值

类似于区块链中每个新块需要确认先前的所有块，DAG 中的每个新子单元需要确认其父单元，父单元的所有父单元。如果尝试修改 InterValue 中过去的记录需要与大量且越来越多的其他用户协调，其中大多数是匿名的陌生人。因此，不可更改性是基于与如此大量的陌生人协调的复杂性，这些人难以达成一致，对合作没有兴趣，并且每一个人都可以否决修订。单元发布之后，立即开始确认，并且确认可以来自任何时候由任何人发布的一个新单元，用户互相帮助：通过添加一个新单元，发布者也确认了所有以前的单元。

4.2. 基于增强 DAG 的 HashNet 数据结构

HashNet 是一种有向无环图（DAG），是由无数个顶点和连接顶点的有向边组成。如图4–2所示。

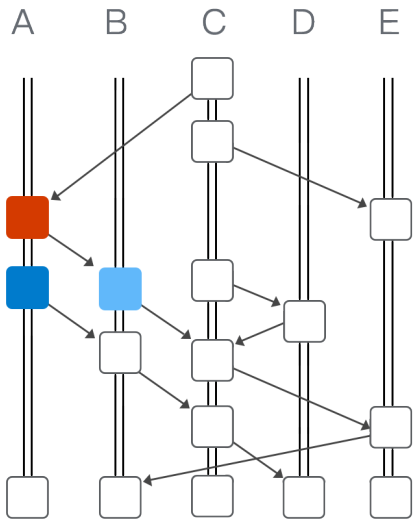


图 4–2: HashNet 数据结构图

该图记录了全网所有节点在什么时间以什么样的顺序给其他节点发送了什么样的数据，每个节点都在内存里有这样一个 HashNet 的拷贝。

上图中有 5 个计算机节点 A, B, C, D, E，每个节点拥有一个放置顶点 vertex(也叫 event) 的柱子。最新发生的事件，会被放置的在图顶部，HashNet 是随时间向上增长。

- HashNet 的特征

    1. 顶点。就是一个事件，包括：创建的时间戳，0 个或者多个交易，创建者的签名，以及 self–parent 和 other–parent 的 hash 值。
    2. 边。HashNet 有两种边，垂直边和斜边。

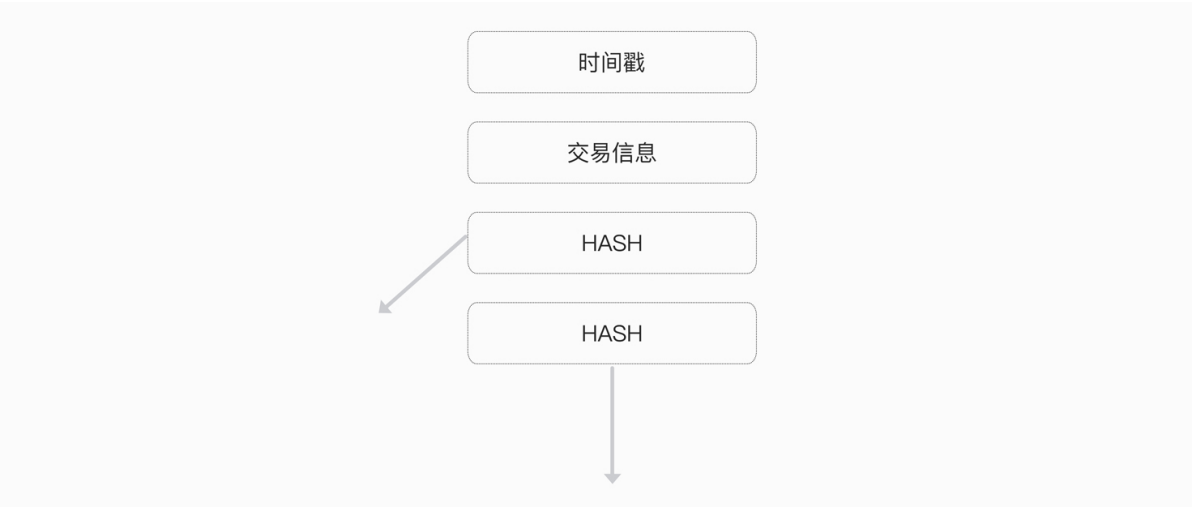


图 4–3: HashNet 顶点包含数据格式

- 斜边表示一个 sync（有向的斜边），表示由某节点向另外一个节点发起一个 sync（网络通信），发送的数据就是以该顶点为 root 的整个 tree。
- 垂直边就好比一条链，链上的事件是按照时间创建顺序放置。垂直边上的 event 都是由同一个节点创建。

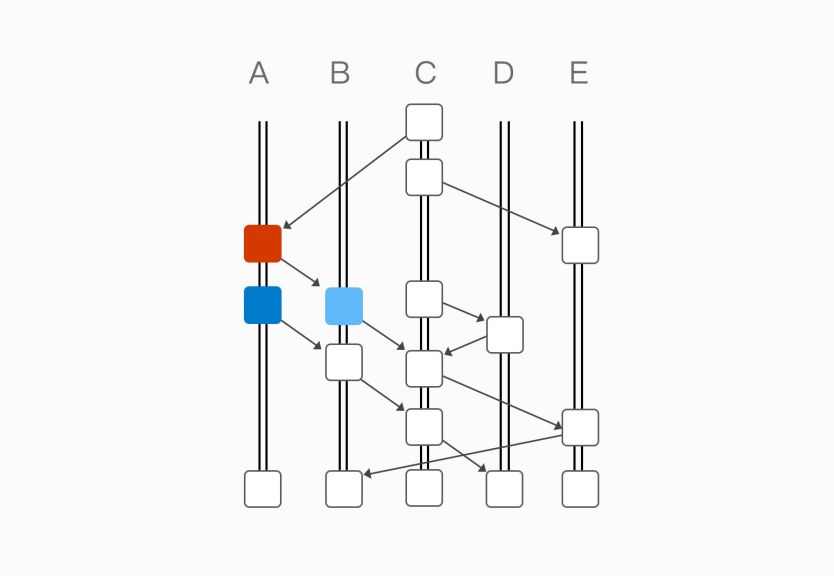
3. 每个顶点一定有且只有 2 条向下的边. 一条斜边，一条垂直向下。表示该事件（红色）是 2 个节点（B to A）曾经通信过（由浅蓝向深蓝发起）的记录。
4. 每个顶点有一条或多条斜向上的边，表示由该节点向斜边的另一端的节点发起的 sync，发送的数据就是该顶点以及它所有的 parent events。比如红色事件有一条斜向上的边通到 C 节点，这条边意味着 A 把红色事件以及深蓝色和浅蓝色事件，以及它们所有的向下的边能触及到的事件都发送给了 C。
5. 如果把红色节点看作一个树的 root，那么整个树都会发送给 C。当然实际过程中，A 和 C 会先协商一下，A 只会发送整个树中 C 缺失的那部分，以减少网络交通。最后 A 在红色顶点向 C 发起同步通信后，C 节点内存中的 HashNet 中一定会填补上以红色事件为 root 的整个树。
6. 随着越来越多的节点相互发起 sync，每个节点本地的 HashNet 越来越丰满。虽然在某一时刻，每个节点 HashNet 的顶部也许有轻微的差异，但是随着时间推移，这个差异很快会被新的 sync 消除。
7. 如果 A 和 B 两个节点内存中的 HashNet 图中都有某个事件，而且无差异，那么这 2 个 HashNet 就一定同时拥有该事件的所有祖先事件（整

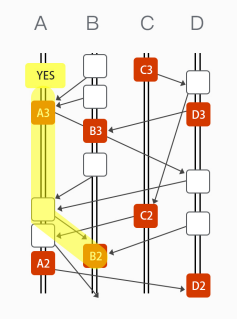
个树)。A 和 B 两个节点会在本地运行复杂的算法，包括拜占庭容错算法，就这些祖先的子图的所有边达成共识。

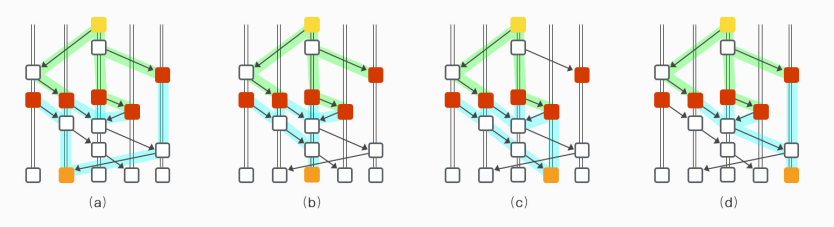
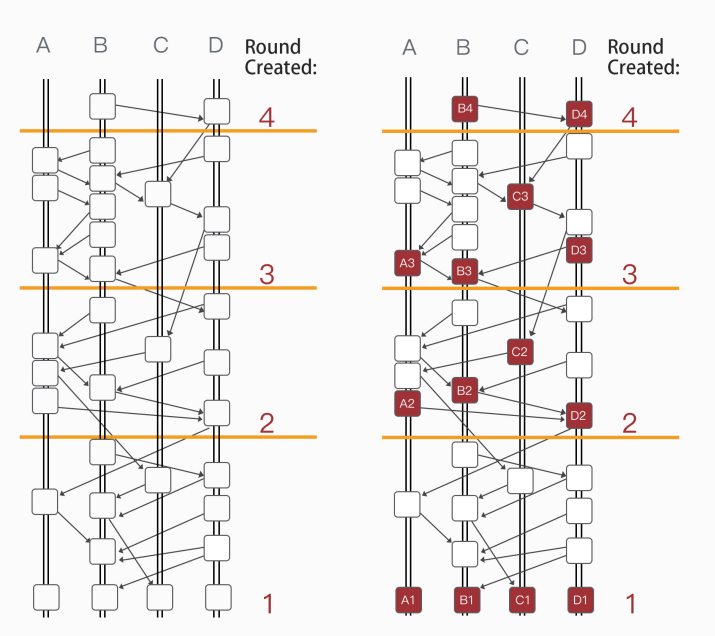
8. 每个节点每次都把以自己最新创建的 event 为根的整个树同步 (只发接收者缺失的部分) 给其他节点，每个节点本地的 HashNet 相对于 world state 缺失的部分会很快被大量的 sync 弥补。好比很多人同时在一张白纸上随机的画黑点，很快整个白纸就变成一张黑纸。
9. 因为 #6, #7, #8，我们认为全网节点本地的 HashNet 近似相等。

- HashNet 相关术语

表 4–2: HashNet 相关术语

术语	描述
Transactions 交易	任何节点都可以在任何时候创建签名的 Transactions。所有节点都在本地维护一份 Transactions 副本（world state），全网使用拜占庭协议就这些 Transactions 的顺序以及 Transactions 本身达成共识
Event (vertex of HashNet)	HashNet 就是由无数的 event 作为图的顶点组成。 一个 event 可以类比 BTC 的一个 block，就是一组 transactions 的容器
Sync (edge of HashNet)	有向且向上的斜边 (非垂直)，表示由某节点向另外一个节点发起的一次网络通信记录。HashNet 就是由无数的 sync 作为图中连接顶点的边组成
HashNet	一种有向无环图（DAG），记录了全网所有节点以什么样的顺序给其他节点发送了什么数据，每个节点都在内存里有下图那样一个 HashNet 的拷贝。  图中有 5 个计算机节点 A,B,C,D,E。每个节点拥有一个放置顶点 vertex(也叫 event，事件) 的柱子。最新发生的事件，会被放置的在图顶部，所以 HashNet 是随时间向长增长

World state (ws)	类比 BTC 的全网账本，每个节点都有一份 world state 的 copy，在本文档中也就是 HashNet，只不过 BTC 的 world state 是个链，这里的 world state 是 DAG
Self-parent event	红色事件垂直向下的边第一个触及到的事件(深蓝)是红色事件的 Self-parent event
Self-ancestors event	深蓝事件的 Self-parent event（以及它的 Self-parent）都是红色事件的 Self-ancestors event
Other-parent event	红色事件斜向下的边第一个触及到的事件(浅蓝)是红色事件的 Other-parent event
Ancestors event	浅蓝事件的 Other-parent event（以及它的 Other-parent ）都是红色事件的 Ancestors event
Gossip	每个节点把自己知道的所有信息发送给被随机选择的另一个节点。然后收到信息的节点继续做同样的事情
Gossip about gossip	HashNet 数据结构是静态的 snapshot，表示某一时刻全网节点之间如何用动态的 Gossip 协议通信的历史记录。把 HashNet 这样的数据通过动态的 Gossip 协议传播就是“Gossip about Gossip”。在传统的 Gossip 协议中，这样的图只用于说明节点间的通信历史，各个节点并不会把整个 HashNet 存在内存中
Virtual voting 虚拟投票	每个节点都有一份 HashNet 拷贝，所以依靠传统的拜占庭式的协议，Alice 可以算出 Bob 应该会发什么选票给她，所以 Bob 不需要在网络上发送真正的选票。因为每个节点都有相同数据（HashNet），然后使用相同的算法(BFT) 就可以计算出相同的结果，无需网络通讯。所以 HashNet Gossip 共识算法是一种低网络带宽消耗的共识算法
Supermajority	如果 $m > 2n/3$ (n 是全网节点数)，m 就是 Supermajority
See 发现	如果 event x 可以通过向下的路径直接或间接地(中间也许穿过其他 event)连接到 event y，那么称 • x see y • x 可以发现 y • y 是 x other-ancestors • x 是 y 的 descendent  如上图 A3 就是 x，B2 是 y

Strongly seeing 瞄准	如果 x 可以通过超过 supermajority 条向下的路径发现 y，那么称： • x strongly see y • x 可以瞄准 y  如图 d 顶部的黄色事件 w 是可以瞄准底部橙色的事件 x。 因为 w 可以通过 m 个红色事件 (被不同节点创建) 的路径发现 x。如果 $m > 2n/3$ (n 是全网节点数)，那么认定 w 可以瞄准 x。这里 n 是 5，m 在 a 图里是 5，其他 3 个图里是 4。 m 越大，说明 x 越被更多的节点认知。 所以 Strongly seeing 说明了一个 event 被全网节点认知的程度，认知度越高，副本就越多，就越不容易被攻击
Round & Round index	 在 HashNet 中，把所有 event 按照时间水平线划分成一个个 round。 每个 round 都有编号 index，从 1 开始递增，此文用 round[index] 表示。 每个 event 的 roundIndex 都不会小于它 parent 的 roundIndex。 每个节点在一个 round 创建的第一个 event 叫做 witness。 在 round[r] 中，一旦出现第一个可以瞄准超过 supermajority 个 witness 的 event 的时候，这个新的 event 的 round index 就是 r+1

Round created	即 Round index
Witness	每个节点在一个 round 创建的第一个 event 叫做 witness，如果有 n 个节点，那么每个 round 都会有 n 个 witness
Famous witnesses	一个 round[r] 的 witness y 是否是 famous witness，完全取决于 round[r+1] 的 witnesses 是否都可以 seeing(发现) 它（此处不需要瞄准）。如果有超过 supermajority 个 famous witnesses 可以发现 y，那么 y 就是个 witnesses。如果 y 收到 n 个 round[r+1] 的 witness 的 vote，那么 y 就被宣称是个 famous witness，投票结束。 但是 election 还没有结束，后面还需要 count vote。 n 个 round[r+1] 的 witnesses 已经 vote 结束，还需要 round[r+2] 的 witness 来 count vote。如果 x 是 round[r+2] 的一个 witness，且 x 可以瞄准超过 supermajority 个 round[r+1] 的 witnesses，那么 round[r] 的 witness 是否是 famous witness 的 election 在 x 中就结束，x 认为 y 是个 famous witness。 这就是个 consensus decision。 如果有 n 个节点，那么每个 round 的 famous witness 个数小于或等于 n
Election	一个节点上决定一个 witness 是否是 famous 的过程
Vote	在一个 election 中，一个 round[r+1] 的 witness 如果可以 seeing（发现）round[r] 的 witness，那么前者就会 vote 后者
Round received	如果一个 event 可以被 round[r] 的所有的 famous witnesses 发现，那么最小的那个 r 的值就是该 event 的 round received
Received time	在 x 的 round received 中，x 和每个 famous witnesses 的连线中找到该 witness 最早的那个 self-ancestor 事件，所有满足这个条件的 self-ancestor 事件的时间戳的中间值就是 x 的 received time

5

共识机制

在 InterValue 1.0 版中，InterValue 所使用的共识机制为基础 DAG 共识和 BA–VRF 共识相结合的双层共识机制。自 InterValue 2.0 版开始，基础 DAG 共识将替换为基于 HashNet 的 DAG 共识，InterValue 的共识机制为 HashNet 的 DAG 共识和 BA–VRF 共识机制相结合的双层共识机制。

5.1. 基础 DAG 共识

5.1.1. 主链

主链是在指定单元所见的 DAG 图中沿着子–父链接找到一个单链，可以把所有单元都关联在一起。我们从任意一个顶点开始，都可以构建一条主链。如果以相同的规则在两个不同的顶点选择主链，这两条主链在回溯过程中一旦相交，它们会在交点之后完全重合。重合部分称为稳定主链，最坏的情况，两条主链在创世单元相交。所有的单元要么直接在这条稳定主链之上，要么从稳定主链上的单元沿着 DAG 的边缘通过少量的跳跃可以到达。因此稳定主链可以在两个冲突的无序单元之间建立总序。首先，给直接位于稳定主链上的单元做个索引，创世单元索引为 0，创世单元的子单元索引为 1，以此类推，沿着稳定主链给主链上的所有单元分配索引。对于不在稳定主链上的单元，我们找到第一个直接或间接引用此单元的主链单元。这样，就给每一个单元分配了一个主链索引（MCI）。然后，给定两个单元，拥有较小 MCI 的单元被认为是更早生成的。如果两个单元的 MCI 恰好相同并且存在冲突，则拥有较小哈希值的单元有效。

主链构建过程实际上是最优父单元选择算法的递归调用过程。最优父单元通过比较可选路径中公证单元的数量（相同公证人发出的单元记一次）来选择。公证单元由见证人发出，见证人可以是非匿名长期参与社区并拥有良好信誉的人，或是主动维护

网络健康发展的组织。虽然期望他们诚实行事，但完全信任任何一个证人是不合理的，因此会同时选择多个不同的见证人。

5.1.2. 双重支付问题

双重支付交易：相同地址发出的任何无序的交易都视为双重支付交易，即使它们没有使用相同的输出，也可称为冲突交易或者矛盾交易。

在用户地址发出新单元时，要求相同地址发布的所有单元应当直接或间接包含该地址之前所有的单元，即相同地址的所有单元连通（有序或连续）。

因此，在相同地址的所有单元都连通的情况下，在路径上出现较早的交易为有效交易。如果有攻击者特意制造出双重支付交易，那么可以通过主链序号来解决，主链序号较小的交易为有效交易。假设攻击者制造出一条影子链，并在上面发布双重支付交易。当影子链接入到真实的 DAG 中时，根据最优父单元选择策略，影子链上的见证人个数少，因此它不会成为主链的一部分，从而解决了这种场景下的双重支付问题。值得注意的是，如果大多数见证人与攻击者合谋，并在其影子链上发布单元，则攻击者有可能攻击成功。

5.1.3. 交易确认

当获得新的单元时，每一个节点会持续追踪自身的当前主链（MC），好像他们将要基于当前的所有无子单元构建新单元。不同节点各自的当前 MC 也许不同，因为它们有可能看到不同的非稳定单元集合。而当新单元到达时，当前 MC 会不断变化。然而，当前 MC 的足够老的那部分会保持不变。

未来所有的 MC 在回溯时将会汇集某个 MC 单元，这个 MC 单元以及之前的所有 MC 单元都是稳定的，不会因为新单元的到来而改变。事实上，创世单元是一个天然的初始稳定节点。假设我们已经基于当前的非稳定单元集合构造了一条当前 MC，并且这条链上已经有一些之前认定稳定的节点，也就是说未来的当前 MC 都被相信会在这个点或早于这个点汇集，然后就沿同一条路径回溯。如果我们能找到一个方法，把这个稳定点向远离创世单元的方向推进，就可以根据数学归纳法证明这个稳定点存在。而被这个稳定点所引用的单元将获得确定的 MCI，包含在这些单元中的所有消息也将被确认。

5.2. HashNet 共识

5.2.1. HashNet 基本思想

已有的 Hashgraph 共识算法通过 gossip 网络和虚拟投票策略达成交易顺序的共识，该共识的前提是要求网络节点超过 $2n/3$ 的投票能力具有对 famous witness 事件

的一致投票结果，其中 n 是全网的当前投票能力总和，该投票能力通常为节点的持股数量。由于采用了本地投票策略，Hashgraph 可以实现较快的交易确认速度。然而该方法存在以下问题：

1）在广域网环境中，节点波动性较强，全网的投票能力 n 的波动也随之增强，这可能导致系统长时间无法找到满足 2n/3 投票一致的事件，从而无法达成共识。

2）受节点稳定性、处理能力、带宽等因素影响，不同节点处理事件的能力差别较大。若系统中存在大量能力较弱的节点参与投票，同样会造成系统长时间无法达成共识。

3）广域网环境下，节点频繁波动可能导致节点被分割成多个子网。根据 gossip 邻居交换协议，节点会周期性剔除长时间未更新的邻居。当邻居稳定后，节点可在子网内达成共识。此时若子网规模较小，很容易使恶意节点在同一轮产生两个 famous witness 事件，从而产生双花交易。

4）随着系统规模增大，节点收到的同步信息越来越多，可以预见系统的吞吐率会随节点数目的增加而降低。

基于以上挑战性问题，我们提出 HashNet 共识机制。如图 5–1 所示，HashNet 采用基于双层 gossip 拓扑框架，通过“片内自治，片间协作”的方式形成一个分而治之的分布式账本系统。在 HashNet 中，顶层 gossip 网络中的节点称为全节点（full node），负责节点拓扑和分片的维护；下层 gossip 网络的节点称为局部全节点（local full node），负责交易共识、交易验证、交易存储以及账本一致性。

HashNet 共识机制的主要优势在于：

1）全节点和局部全节点具有较强的稳定性和处理能力，能够有效避免 Hashgraph 长时间无法达成共识的问题，也能够避免因网络被分割造成的恶意节点攻击问题。

2）采用双层 gossip 拓扑对节点分片，顶层节点不参与交易共识和交易验证过程，分片可并行工作，保证了系统具有较好的可扩展性。

5.2.2. 节点类型

HashNet 中节点共分为四类：全节点、局部全节点、轻节点和微节点。

- 全节点：（1）负责维护节点拓扑，包括全节点的周期性加入退出过程、局部全节点的周期性加入退出过程；（2）负责更新分片，包括确定每个周期的分片数量、将哪些局部全节点划分到同一个分片。

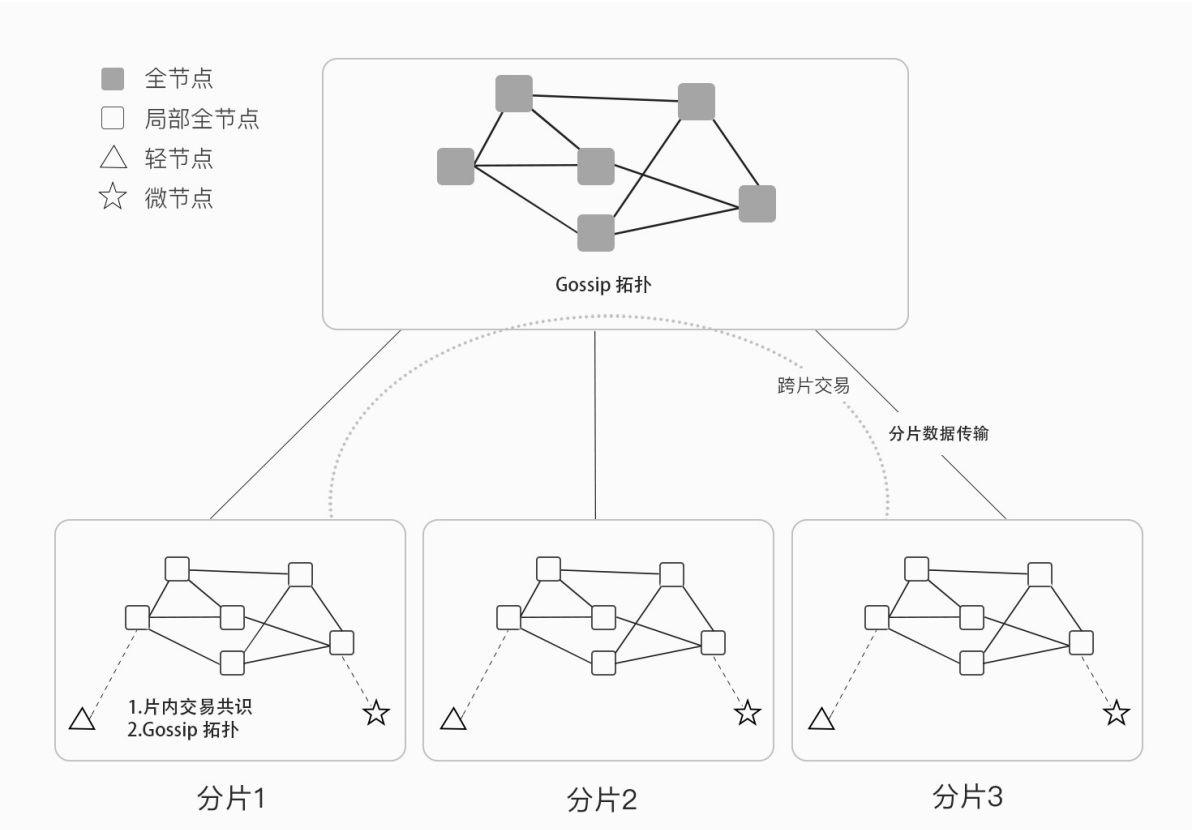


图 5–1: 基于双层 Gossip 的 HashNet 共识框架

- 局部全节点：(1) 作为代理节点，向轻节点和微节点提供交易代理服务；(2) 在分片内，局部全节点作为交易共识的主体，实现交易在片内的验证、共识和记账；(3) 在分片间，局部全节点采用 gossip 协议传播各自片内账本信息至其他分片，从而实现账本数据一致性。
- 轻节点：通常为轻量级客户端钱包，该节点可通过局部全节点做代理完成数据请求和发送。
- 微节点：通常为智能物联网设备，该节点可通过局部全节点做代理完成数据请求和发送。

5.2.3. 节点维护机制

一方面，全节点和局部全节点的稳定性、带宽能力、计算能力对交易确认速度会产生较大影响。另一方面，为了防止恶意用户串谋，全节点和局部全节点需要周期性被混洗或更新。为此，我们设计了可信且可激励的节点加入和更新机制。

(1) **全节点维护机制**

固定不变的全节点有两点安全隐患：一是固定全节点之间进行串谋；二是有一些非正常情况，全节点的软件 bug，网络拥塞或者有恶意行为。因此保证全节点的随机性至关重要。假定顶层网络中共包含 N 个全节点，其中最新加入的全节点为 Leader 全节点。通过周期性运行 POW 和 HashNet 共识算法，实现全节点的自动更新。其基本流程如下：

a）申请者向公网运行的 Hub 节点请求全节点列表，然后向任意一个全节点发起 POW 申请，收到请求的全节点将待求解的问题发送给申请者。

b）申请者采用 POW 算法获得哈希结果，然后用自己的私钥对计算结果签名，并将自己的公钥、签名数据、计算结果、IP、服务端口发送给任意全节点。

c）全节点首先检查是否已存在一个申请者被确认，如果是则忽略当前申请者的请求。否则，验证该申请者的计算结果和申请者签名的正确性。若验证通过，全节点在顶层网络中发起 HashNet 共识，其共识内容为更新后的全节点列表，其中增加了新的申请者，并剔除了最老的全节点。

d）当顶层节点通过该节点的共识后，全节点网络的节点列表更新，Leader 节点将更新后的列表信息发送给 Hub 节点。

（2）**局部全节点维护机制**

相对于全节点,局部全节点规模较大,且需要周期性审核。为此,我们采用 PoS+PoW +PoB+PoO 的方式自动判定申请者的信誉、处理能力、带宽能力和稳定性。具体来说：PoS 为权益证明，即申请人向全节点提交其代币数量的证明；PoW 为工作量证明，即申请人从全节点随机领取一个特定难度的哈希求解问题，并由全节点记录其计算时间从而评估其计算能力；PoB 为节点带宽证明，全节点向申请人发送背靠背的数据报文以测量其带宽能力；PoO 为在线证明，即申请人将自己的最长在线时间长度提交给全节点。最终，申请人的综合得分可表示为：

$$\text{Score} = \alpha_1 \text{PoS} + \alpha_2 \text{PoW} + \alpha_3 \text{PoB} + \alpha_4 \text{PoO} \ldots$$

其中，α_i 代表相应考虑因素的权重。若 Score 超过特定的阈值，则判断该申请者合法。假定每次局部全节点的更新数量为 M，局部全节点更新的具体流程为：

a）申请者将自己的能力证明提交给任一全节点。

b）全节点收到申请后，计算该申请者的 Score，若该 Score 超过特定阈值则表示节点合法。对于合法的申请者，全节点在顶层发起申请者申请加入分片的共识。

c）当申请窗口到期后，Leader 全节点挑选前 M 个申请者并对其分片。然后，Leader 全节点在顶层发起分片的共识。

d）当该共识达成后，这 M 个申请者所形成的分片将在下个周期替换已有的分片节点，从而实现局部全节点的更新。

5.2.4. 分片机制

全节点在审核通过所有下一轮局部全节点申请人后，需要对这些申请人分片以保证系统的可扩展性。

（1）**分片数量**

分片数量是一个需要仔细权衡的变量。分片数量过少，系统的交易确认吞吐率不能有效提升；分片数量过多，底层子网遭到 1/3 恶意节点攻击的可能性增大，且顶层全节点网络需承担较多的跨子网交易通信。为此，我们设定最小分片的局部全节点数量为 1000。极端情况下，若局部全节点数量小于 1000，则分片数量为 1。

（2）**分片细节**

为了对局部全节点分片，顶层全节点运行 BA-VRF 共识协议选择一个责任全节点以实施具体分片操作。分片时，责任全节点依据最小分片规模确定分片数量，将所有局部全节点随机划分至各个子网。每个子网有一个唯一标识符 subnet_id，相应的子网内的节点 id 以其子网 subnet_id 作为前缀。假设网络中有 4 个子网，其子网 id 分别是 00,01,10,11。在 00 子网内包含四个局部全节点，则相应的节点 id 为 0000,0001,0010,0011。通过前缀路由方式，任意两个节点能够依据其节点 id 获得对方的子网 id 信息。责任全节点为每个子网及其节点分配完 id 后，还需要为每个局部全节点分配初始邻居节点。这样，局部全节点可依据其邻居列表自动完成子网重建过程。具体流程如下：

a）责任全节点依据最小分片规模确定分片数量 n，并将所有申请者随机划分至 n 个片内。

b）由责任全节点对分片提案在顶层网络中发起 HashNet 共识。

c）共识达成后，将最新的局部全节点列表发送给 Hub 节点，替换已有子网中最老的 n 个分片，更新每个局部全节点邻居列表信息。

（3）**交易确认细节**

每个局部全节点保存了各个分片的 HashNet 视图（即全账本信息），交易确认过程由四个并发阶段构成：片内交易共识、片间账本同步、共识事件全排序、事件存储。片内交易共识是指任何一笔交易都是在某一个片中完成共识；片间账本同步是指各个分片的共识数据需要在片间共享，以保证各个局部全节点维护全局账本信息；共识事件全排序是指各个片的 HashNet 中的共识事件需要做一致性排序，已保证所有局部全节点账本视图的一致性；事件存储是将 HashNet 中的 Event 存到数据库中，用于持久化账本和节点宕机恢复。

交易可根据输入和输出地址划分为以下四类情况：

情况 1：input(1) → output(1)，输入和输出来自于同一分片 1；

情况 2：input (1) → output (2)，输入来自分片 1，向分片 2 产生一个输出；

情况 3：input (1)+ input(2) → output(3)，输入来自分片 1 和 2，输出为分片 3；

情况 4：input (1)+ input(2) → output(3) + output(4)，输入来自分片 1 和 2，输出为分片 3 和 4；

情况 1 中输入和输出来自于同一分片。假定分片 1 中的 Alice 向分片 2 中的 Bob 发送 5 个 INVE。其流程如下：(1) Alice 将交易发送给分片 1 中的一个局部全节点；(2) L 检查该交易合法后，将该交易封装到一个新的 Event 中并发起 HashNet 共识；(3) 在 HashNet 共识过程中，片 1 的局部全节点会将本片的 HashNet 中的 Event 发送给其他片的局部全节点，以完成片间账本同步。接收到来自其他片的 Event 后，局部全节点仍然要对这些 Event 在 HashNet 中共识，以保证 Event 的合法性；(4) 每个局部全节点维护了多个片的 HashNet 视图，依据已共识 Event 的共识时间戳对所有 Event 实现全排序。

情况 2 中输入和输出来自于不同分片，其处理流程与情况 1 相同。也就是说，在 HashNet 中，我们不区分片内交易和跨片交易，这样做的好处是避免了跨片通信带来的额外开销，极大降低了共识延迟。

情况 3 和 4 中输入来自于不同分片，因此需要得到多个分片的确认才能继续交易，我们引入“锁定”和“释放”两个操作保证交易的原子性。例如分片 1 中的 Alice 和分片 2 中的 Bob 共同向分片 3 中的 Lily 支付 5 个 INVE，其中 Alice 支付 2 个 INVE，Bob 支付 3 个 INVE。假设该交易信息由分片 1 产生。第一步，该交易信息在分片 1 中通过 HashNet 达成共识，此时 Alice 账号中 2 个 INVE 被“锁定”并产生由 Alice 签名的有效性证明，发送该有效性证明给分片 2 的局部全节点；第二步，由分片 2 通过 HashNet 达成共识，若 Bob 账号中有足够余额，则 3 个 INVE 被“锁定”并产生由 Bob 签名的有效性证明，并返回给分片 1；第三步，分片 1 收到 Bob 的有效性证明后，从 Alice 账号中减去 2 个 INVE，从 Bob 账号中减去 3 个 INVE，并给 Lily 增加 5 个 INVE。第四步，交易在分片 1 中达成共识后，该交易在片间同步并持久化存储。为了保证交易原子性，该过程中若出现 Bob 没有足够余额、不能增加 5 个 INVE 给 Lily 等情况，分片 1 和 2 释放 Alice 和 Bob 的锁定 INVE，完成状态回滚。

5.3. 基于可验证随机函数的拜占庭协商共识

基于可验证随机函数的拜占庭协商共识（BA–VRF）共识主要用于选举责任全节点，他是一种基于可验证随机函数（Verifiable Random Function，VRF）和 BA 算法构建的共识机制，该共识机制能够随机选出少量全节点作为公证节点，并确定公证节点的优先级。

BA–VRF 每一分钟执行一次，每次达成共识将随机选出若干全节点作为公证节点，公证节点有权发送公证单元，公证单元须满足 DAG 共识中的父子引用规则。公证节点发送的公证单元成为稳定主链的单元后，该公证节点可以获得公证奖励。当交易活跃时，新单元不断产生，则公证节点会及时获得公证奖励；当交易不活跃时，极端情况下一分钟内没有新单元产生，已经发送公证单元的节点在发送的公证单元成为稳定主链单元时获得公证奖励，没有发送公证单元的节点不获得公证奖励。

5.3.1. 共识状态

BA–VRF 有最终共识和临时共识两种状态。

如果一个全节点达到最终共识，意味着任何其它全节点也达到了最终共识或者在同一轮中的临时共识必须同意这一共识结果，而无论强同步假设是否成立。而临时共识意味着其它全节点可能在其它公证单元上达到了临时共识，没有全节点已经达到了最终共识。所有公证单元都必须直接或间接引用之前生成的公证单元，这可以确保 BA–VRF 的安全性。

BA–VRF 产生临时共识有两种情况。首先，如果网络是强同步的，一个攻击者可以以一个很小的概率让 BA–VRF 达到临时共识。此情况下，BA–VRF 不会达成最终共识，也不能确认网络是强同步的。但经过几轮后，很大概率上会达到最终共识。第二种情况是，网络是弱同步的，整个网络都被攻击者控制。此情况下，BA–VRF 将达到临时共识，选举出不同的公证节点集合，形成多分叉共识。这能够避免 BA–VRF 达到最终共识，因为全节点被分成了不同的组，各组之间并不同意对方。为了恢复活性，BA–VRF 将被周期性地执行，直到消除意见分歧。一旦网络恢复到强同步状态，将会在短时间内达成共识。

5.3.2. 全节点选择

抽签算法是基于可验证随机函数（VRF）构造而成的，可根据每个参与 BA–VRF 共识的全节点的权重选出这些节点的随机子集。某全节点被选中的概率约等于自身权重与总权重的比值。抽签的随机性源于 VRF 函数和一个可公开验证的随机种子，每个全节点可根据随机种子验证自己是否被选中。

VRF 函数定义：给定任意字符串，VRF 函数输出哈希值和证明结果。

$$(\text{hash}, \pi) \leftarrow \text{VRF}_{S_k}(\text{seed}||\text{role})$$

哈希值 hash 由私钥 S_k 和给定的字符串 (seed || role) 唯一确定，在不知道私钥 S_k 的情况下，输出的哈希值 hash 与随机数之间不可区分。证明结果 π 使得，知道私钥所对应公钥的节点可以验证哈希值 hash 和字符串 seed 之间是否关联。种子 seed 是随机选择并且可以被公开获得的，每一轮运算的 seed 由前一轮运算的 seed 生成。抽签算法支持角色指定，如选出协商过程中某一步骤的参与者。

所有全节点执行抽签算法来确定自己是否被赋予公证权，被选中的全节点通过 P2P 网络向其它全节点广播自己的抽签结果。需要说明的是，抽签选择全节点的概率与全节点自身权重成正比，以抵御 Sybil 攻击。权重大的全节点可能会被选中多次，为此抽签算法会输出全节点被选中的次数。如果一个全节点被多次选中，那么它就被当成多个不同的全节点。

5.3.3. 拜占庭协商

拜占庭协商（BA）能为每一个被选中的全节点确定公证优先级并提供公证优先级的证明。达成拜占庭共识需要执行多个步骤，BA 算法会被执行多次。

每次协商都从抽签开始，所有全节点都去查看它们是否被选中成为当前 BA 的参与者。参与者广播一个包含选择公证优先级的消息。每一个全节点用它们收到的公证优先级消息去初始化 BA 算法。上述过程将被不断重复执行，直到某轮协商有足够多的全节点达成共识。在不同全节点之间，BA 算法并不是同步的，每个全节点发现之前的步骤结束后应立即查看新的参与者选举结果。只有全节点在某轮协商中投票并最终达成共识，它才可以参与下一轮协商。

BA 算法的一个重要特征是，参与者不需要维护私有状态，仅存私钥，所以参与者每个步骤之后都可以被更换，以减少对参与者的攻击。当网络是强同步的，BA 算法保证如果所有的诚实全节点以相同内容进行初始化，那么可以在很少的交互步骤之内达到最终共识。此情况下，即使存在少量攻击者，所有的诚实全节点也将在有限交互步骤步下在达到最终共识。

6

抗量子攻击的哈希和签名算法

6.1. 抗量子攻击的哈希算法

密码学中的哈希算法又称为散列函数或杂凑函数，它在现代密码学中扮演着重要的角色。哈希算法是一个公开的函数 H，它将任意长的消息 M 映射为较短的、固定长度的值 h。h 称为消息摘要，也称为哈希值、散列值或杂凑值。哈希算法的结构如下图6–1所示。

图 6–1: 哈希算法原理图

区块链为了保证数据不被篡改，除了保存原始数据或交易记录，还要保存其哈希函数值。区块链上的交易数据通常通过很多次哈希后得到最终的 Merkle Hash 值，区块链上的地址数据通常是通过计算得到一个 Hash 值，并通过特定的编码将 Hash 值转化为由数字和字母组成的字符串后 (如在比特币区块链中采用的是 Base58 编码) 记入区块链。

量子计算机下针对哈希算法目前最有效的攻击方法是 GROVER 算法，该算法可以将对 Hash 算法的攻击复杂度从 $O(2^n)$ 降为 $O(2^{n/2})$，因此，目前比特币系统采用的哈

希算法 PIREMD160 算法由于输出长度只有 160 比特，在量子攻击下是不安全的。抵抗量子攻击的有效手段是通过增加哈希算法的输出长度来有效降低 GROVER 算法威胁，目前普遍认为只要哈希算法输出长度不少于 256 比特时，是可以有效抵抗量子攻击的。另外，除了量子攻击威胁外，一系列在实践中被广泛应用的 Hash 函数如 MD4、MD5、SHA–1 和 HAVAL 等受到差分分析、模差分和消息修改方法等传统方法的攻击，因此区块链中的哈希算法也需要考虑的是对传统攻击的抵抗能力。

早期的区块链项目如比特币、莱特币、以太坊采用了存在设计缺陷（但不是致命的）的 SHA 系列哈希算法，最近新的区块链项目都采用以美国国家标准与技术研究院 SHA–3 计划系列算法为代表的新哈希算法。InterValue 采用 SHA–3 计划的胜出算法 Keccak512，与经典 Hash 函数的 Merkle–Damgard（MD）结构不同，Keccak512 算法采用了海绵（Sponge）结构，该算法蕴涵许多杂凑函数和密码算法最新的设计理念和思想，且设计方式简单，非常方便硬件实现。算法是 Guido Bertoni, Joan Daemen, Michael Peters, 和 Giles Van Assche 在 2008 年 10 月提交的，Keccak512 算法采用了标准的 sponge 结构，可将任意长度的输入比特映射成固定长度的输出比特，该算法速度非常快速，在英特尔酷睿 2 处理器下的平均速度为 12.5 周期每字节。

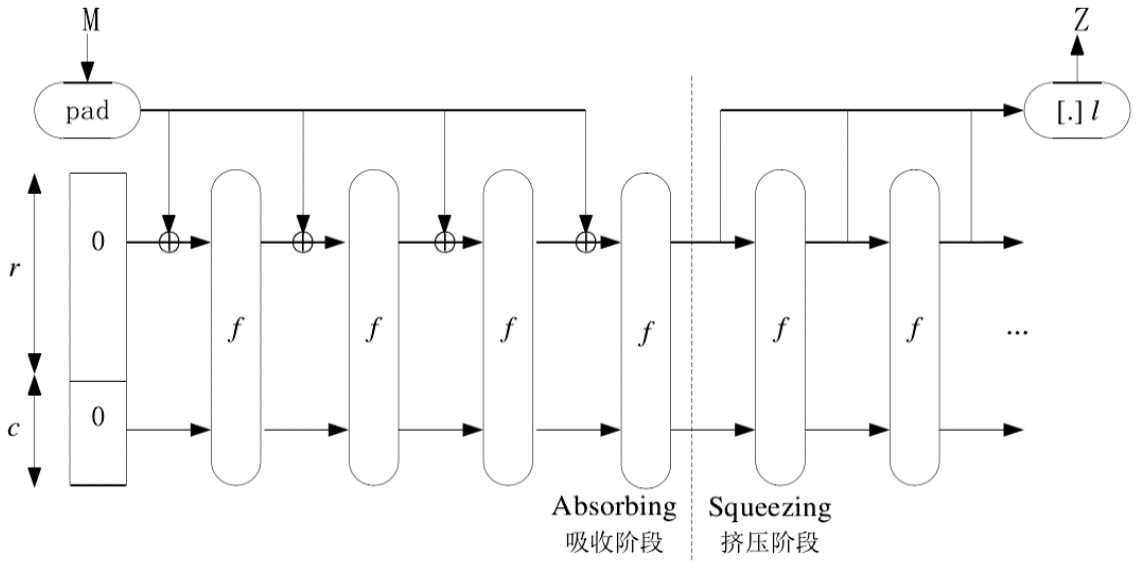


图 6–2: Keccak512 算法实现图

如图6–2所示，在海绵结构的吸收阶段，每个消息分组与状态内部的 r 比特进行异或，然后与后面固定的 c 比特一起封装成 1600 比特的数据进行轮函数 f 处理，然后再进入挤压过程。在挤压阶段，可以通过迭代 24 次循环产生 n 比特固定输出长度的 Hash 值，每个循环 R 只有最后一步轮常数不同，但是该轮常数在碰撞攻击时经常被忽略不计。该算法被证明具有很好的差分性质，至目前为止第三方密码分析没有显示 Keccak512 有安全弱点。量子计算机下针对 Keccak512 算法的第一类原像攻击复杂

度是 2^{256}，量子计算机下针对 Keccak512 算法的第二类原像攻击复杂度是 2^{128}，因此采用 Keccak512 算法的 InterValue 可以抵抗量子计算下的 GROVER 算法攻击。

6.2. 抗量子攻击的数字签名算法

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

现有区块链系统大都采用椭圆曲线数字签名方案 ECDSA。ECDSA 是基于椭圆曲线的 DSA 签名算法而提出的，作为 ANSI、IEEE、NIST 和 ISO 的标准，ECDSA 具有系统参数小、处理速度快、密钥尺寸小、抗攻击性强和带宽要求低等优点，比如 160 bit ECC 与 1024 bit RSA、DSA 有相同的安全强度，而 224 bit ECC 则与 2048 bit RSA、DSS 具有相同的安全强度。但是量子计算机下针对 ECDSA 签名算法可执行非常高效的 SHOR 攻击算法，SHOR 算法适用于解决大整数分解、离散对数求逆等困难数学问题，导致 ECDSA 签名算法在量子攻击下相当不安全。目前抗量子 SHOR 算法攻击的公钥密码体制主要包括基于格理论的公钥密码、以 McEliece 公钥密码为代表的基于编码公钥体制和以 MQ 公钥密码为代表的基于多变量多项式三类。McEliece 公钥密码体制的安全性基于纠错码问题，安全性强，但计算效率低。MQ 公钥密码体制，即多变元二次多项式公钥密码体制，基于有限域上的多变元二次多项式方程组的难解性，在安全性方面的缺点比较明显。相比之下，基于格理论的公钥加密体制算法简洁、计算速度快、占用存贮空间小。**InterValue 采用基于格理论的签名算法 NTRUSign-251**，算法具体实现流程如下：

1. **密钥生成：**在环 R 上选择两个多项式 f 和 g 使得 f 和 g 的系数中 1 的个数分别为 d_f 和 d_g. 并根据 f 和 g, 计算公钥 h：$h = F_q * g$ (mod q).
   求解多项式 (F, G) 使其满足方程 $f * G - F * g = q$.
   且有 $\|F\| \approx \|f\| \sqrt{N/12}, \|G\| \approx \|g\| \sqrt{N/12}$.
2. **签名过程：**
   1）对消息 M 进行 HASH 变换，转化为多项式 (m_1, m_2)，其中多项式 m_1 和 m_2 均为环 R_q 上的一个多项式。

2）计算环上多项式 A, B, a, b 使其满足：

$$G * m_1 - F * m_2 = A + q * B$$

$$-g * m_1 - f * m_2 = a + q * b$$

并要求 A 和 a 的各个项的系数满足大于 $-q/2$ 而且小于 $q/2$ 的条件。

3）对多项式 s 进行计算如下：

$$s = f * B + F * b (\text{mod } q)$$

s 即为明文 M 使用公钥 h 所计算得到的签名。

3. **验证过程：**

对消息 M 进行 hash 变换，转化为多项式 (m_1, m_2).

由待验证签名 s 和公钥多项式 h 计算得到：

$$t = s * h (\text{mod } q)$$

$$t = g * B + G * b (\text{mod } q)$$

计算多项式 (s, t) 和多项式 (m_1, m_2) 之间的距离 $||m_1 - s|| + ||m_2 - t||$，如果该距离大于 NormBound 则验证失败，否则通过验证，签名有效。

已经证明 NTRUSign–251 签名算法的安全性最终等价于求一个 502 维整数格中的最短向量问题，而对于格中最短向量问题 SHOR 攻击算法是无效的，在量子计算机下也没有其他的求解快速算法，目前最好的启发式算法也是指数级的，攻击 NTRUSign–251 签名算法的时间复杂度约为 2^{168}，因此采用 NTRUSign–251 算法的 InterValue 可以抵抗量子计算下的 SHOR 算法攻击。

7

交易匿名保护

匿名交易与隐私保护是电子货币的重要属性。目前大部分区块链对隐私保护的解决思路是，通过隔断交易地址和地址持有人真实身份的关联，来达到匿名的效果。所以虽然能够看到每一笔转账记录的发送方和接受方的地址，但无法对应到现实世界中的具体某个人。但这样的保护是很弱的，通过观察和跟踪区块链的信息，通过地址 ID、IP 信息并运用大数据分析总能得出跟用户相关的某些信息等。InterValue 从交易的无关联性和不可追踪性两个方面确保对交易信息匿名保护，并不断迭代改进匿名保护能力。InterValue 对交易无关联性 unlinkability 和不可追踪性 untraceablility 进行了规范化的定义，无关联性是指对于任何两个外部交易，不能证明将其发送给同一个人，不可追踪性是指对于每个内部交易，所有可能的发件人从概率上是相等的。无关联性和不可追踪性是强隐私保护的区块链必须满足的属性，InterValue 通过采用**一次密钥 one-time secret key 和环签名 ring signature 技术**来实现对无关联性和不可追踪性的支持。同时，InterValue 设计并实现严格的**零知识证明 zero-knowledge proof 模型**作为可选择功能，可进一步增强交易匿名性。

7.1. 一次密钥

InterValue 采用一次密钥技术来实现交易的无关联性。一次密钥是指发送方对每个交易使用单独的密钥进行签名。与通常的区块链交易中接收方只用到一对公私钥不同，在一次密钥方案中，每次交易中接收方需要用到两对公私钥，交易发起时，交易发送方使用交易接受方的两个公钥和随机数生成临时公钥，发送方将该临时密钥作为地址进行交易，接收方执行 Diffe-Hellman 交换并结合他的一个私钥信息可以获取临时私钥。由于一次密钥只可以有接受方验证，保证了交易的正确性。同时，每次交易使用

不同的随机数，即使与同一个接收方进行多次交易，因其一次密钥不同，也不能将其进行关联，保证了交易的无关联性。

7.2. 环签名

一次密钥主要是保证了交易接收方的隐私，为了同时保证交易发送方的隐私，InterValue 采用了环签名技术。环签名是一种群签名 (Group Signature) 技术衍生而来的多用户签名技术，该签名摆脱了群签名的诸多弊端，如不再需要群管理员、具有不可追踪性等。环签名模型如下图7–1所示。

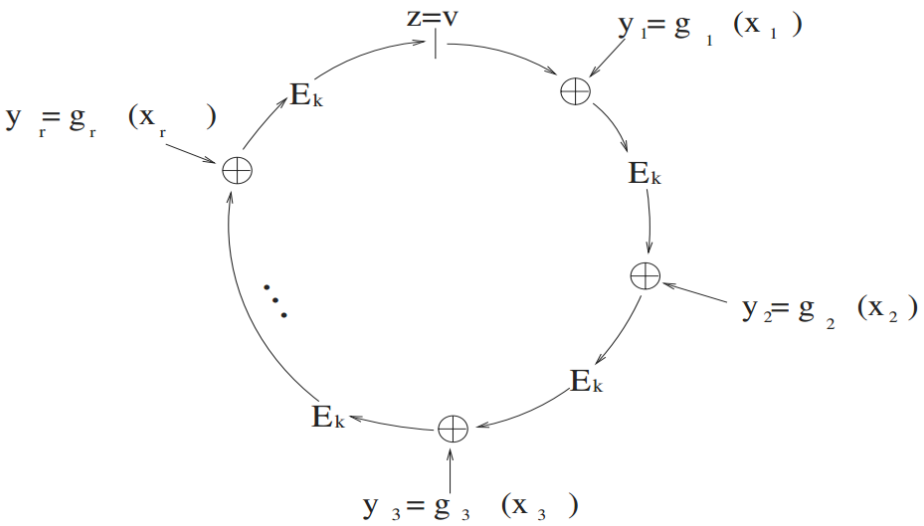


图 7–1: 环签名原理图

在环签名技术中，消息由一组签名者进行签名，验证者无法得知谁是具体的签名者。因此，环签名能够很好的解决签名者身份隐私保护的问题，实现交易的不可追踪性。另一方面，由于一般的环签名技术将签名者隐藏在一组用户之中，会带来双重支付（double spending）的问题，可采用可链接环签名技术 linkable ring signature 解决这一问题。

7.3. 零知识证明

零知识证明技术是 1985 年由 S.Goldwasser、S.Micali 和 C.Rackoff 提出的，最初设计用于达成证明者能够在不向验证者提供任何有用信息的情况下，让验证者正确认证证明者的目的。零知识证明本质上是在传统的数学证明中引入随机性和交互的要素，用问答方式进行证明的交互证明系统，后来发展出非交互性方式，在计算机科学和密码学领域具有深远影响。在实际应用中，零知识证明要求验证者不能在验证过程中获取新的知识，即恶意验证者，使验证存在误差，同时防止技术性导致的验证误差。

加密数字货币 Zcash 第一次使用零知识证明实现其交易的隐私性，不同于将发送者的交易区块删除的方式，Zcash 使用作废列表标识交易者发送后的区块，旷工仅仅验证交易区块的哈希值，实现了交易的完全匿名。

7.4. 匿名交易与隐私保护

作为区块链 4.0 技术，InterValue 通过保密交易（confidential transaction）实现匿名交易与隐私保护，InterValue1.0 版至 3.0 版借鉴加密货币 Monero 的隐私保护方法，采用一次密钥和环签名技术实现保密交易。InterValue4.0 版借鉴当前 Zcash 的匿名保护方法，在前期版本的基础上增加严格设计的非交互零知识证明，把非交互零知识证明作为可选择功能，支持实现交易的完全匿名，有效抵抗恶意验证者，满足不同应用场景隐私保护需求。

8

智能合约

区块链技术为智能合约提供了安全可信的执行环境，促成了智能合约概念的实现。智能合约是由事件驱动的、具有状态且运行在一个可复制、可分享的账本之上并能够保管账本上资产的程序，其目的是让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。智能合约不仅可以接收和储存价值，也可以向外发送信息和价值，整个过程可以在无中心，无信任的前提下，自动化、智能化的执行。

智能合约在设计上需要在安全性和功能性之间寻求平衡。现有区块链项目主要聚焦单一种类智能合约的设计，在智能合约种类限定的条件下谋求安全性和功能性之间的平衡，往往达不到满足多样化用户群体使用体验和用户多样化交易需求的理想效果。比特币区块链的交易脚本是智能合约的雏形，属于非图灵完备智能合约，具有复杂度低和轻量化优势，并且在比特币区块链网络运行将近十年时间内没有出现过安全性问题，但是比特币交易验证脚本支持的功能非常有限，仅用于支付验证。以太坊区块链支持采用 Solidity 高级语言编写的图灵完备智能合约，极大地丰富了智能合约的功能，扩展了区块链技术的应用领域，但是编写以太坊智能合约容易出现安全漏洞，The DAO 事件正是因为编写的以太坊智能合约出现安全漏洞导致以太坊社区分裂。

InterValue 在智能合约功能实现上采用类似计算机存储体系结构的层次化思想，摩西虚拟机 (Moses Virtual Machine，MVM)，支持声明式非图灵完备智能合约和高级图灵完备智能合约。用户根据使用体验和交易需求选择使用这两类合约，平衡计算安全和计算功能以及计算费用和计算复杂性，以满足交易多样化需求。声明式智能合约部署简单，安全性高，更加接近法律合同语言；高级图灵完备智能合约部署难度相对较高，主要用于开发程序逻辑更加复杂的 DApp。两类智能合约部署的手续费机制不同，声明式智能合约的手续费根据合约所占字节计算，而高级图灵完备智能合约则以程序运行时消耗的 InterValue Token 作为手续费。

8.1. 声明式非图灵完备智能合约

声明式非图灵完备智能合约具有复杂度低、轻量化、编写难度低和安全性高等优势，这种智能合约由陈述性和完全布尔语句组成，因此更接近传统的法律合同语言，支持布尔运算，数学运算，甚至数据存储等。InterValue 提供了多种常用的声明式智能合约的模板供用户使用或改进以满足自定义需求，降低了合约部署难度和出错率，同时相比于图灵完备智能合约，具有更高的安全性。这类智能合约部署的手续费的收取跟普通交易相同——与其所占字节成正比。

智能合约的制定往往需要一定的编程能力，为了方便普通用户使用智能合约，InterValue 支持多种功能的声明式非图灵完备智能合约模板（Contract Template），用户只需要根据需求选择相应的模板，填入相应的参数即可。合约模板可以被重复使用，也可以在其他模板中被引用。下面是一个智能合约模型：

```
["contract template", [
    "hash of unit where the template was defined",
    {param1: "value1",param2: "value2"}
]]
```

声明式非图灵完备智能合约虽然复杂度低，但能实现如获取外界数据和跨链通信等强大功能。

获取外界数据的示例代码如下所示，如果由 Alice，Bob 或 Cara 提交到合约的数据等于期望值，则条件为真，除了“=”，还支持其他诸如“!=”、“>”、“>=”、和“<=”这些运算符。通过此种方式可以指定数据来源，实现强大的智能合约条件控制功能。

```
["in data feed", [
    ["Alice", "Bob", "Cara" ...],
    "data feed name",
    "=",
    "expected value"
]]
```

跨链通信的示例代码如下所示，Bob 用 INVE 向 Alice 兑换 10 个 BTC，时间限定在 2018-02-15。如果在此之前 Alice 将 10 个 BTC 转给 Bob 的话，BTC oracle 则会有对应的记录，此时合约被触发，Alice 会收到由 Bob 事先冻结到合约中的 INVE (INVE 的数量由双方对汇率达成协议后计算而得），否则资金会被解冻并原路退回给 Bob。

```
["or", [
    ["and", [ ["address", "Alice"],
```

```
    ["in data feed", [["BTC oracle"],
    "BTC from Alice to Bob",
    "=",
    "10"]]
    ]],
    ["and", [ ["address", "Bob"],
    ["in data feed", [["TIMESTAMPER ADDRESS"],
    "datetime",
    "<",
    "2018-02-15 00:00:00"]]
    ]]
]]
```

8.2. 高级图灵完备智能合约

图灵完备智能合约由于支持条件跳转逻辑和循环逻辑，相比非图灵完备智能合约能够实现更加丰富的业务功能，但同时合约的编写更加复杂，容易出现安全漏洞，往往需要专业人员对合约进行拟定和测试。为了规避“逻辑炸弹”合约执行对网络效能的破坏，提供反欺诈机制，这类智能合约部署的手续费不再是根据合约所占存储空间的大小来计算，而是采用类似于以太坊智能合约的 Gas 机制。用户在调用智能合约功能时需要冻结一定量的 Gas，随着合约的执行，Gas 会随着智能合约指令的执行逐渐消耗。合约执行完毕，剩余的 Gas 会退回给发布者，若在合约执行完毕之前便消耗完所有 Gas，则合约状态回滚到执行之前，所消耗的 Gas 不会退回。

InterValue 采用自主开发的 Moses 高级编程语言编写高级图灵完备智能合约。Moses 高级编程语言采用面向对象设计，使用类 JavaScript 语言风格，方便目前庞大的 Web 编程开发人员能够顺利迁移到 InterValue 智能合约开发上来。使用 Moses 高级编程语言可以实现声明式非图灵完备智能合约所支持的功能。InterValue 高级图灵完备智能合约的特性在于支持链下数据访问。随着区块链应用领域的不断扩展，对链下数据的访问需求将不断增长，以太坊智能合约只支持链上数据访问的特性将越来越难以满足区块链应用需求。这里的链下数据并不是泛指所有非 InterValue 主链上的数据，而是特指存储在基于区块链的分布式存储系统上的数据。这部分数据往往质量比较高，会涉及权益问题，需要通过智能合约进行多方授权访问以及数据使用权益分配。

- 链下数据安全访问：Moses 高级编程语言将内建特定链下数据访问协议，例如内建 IPFS 数据访问协议专门访问存储在 IPFS 分布式数据存储空间内的数据。通过内建特定数据访问协议可以约束数据访问范围，降低对恶意数据（程序）访问的风险。同时 InterValue 也将打造自己的分布式数据存储平台，并将数据访

问协议内建到 Moses 高级编程语言中。用户在平台存储数据文件需按文件大小支付存储费用，从数据源头保证数据质量。

- 链下数据安全使用：Moses 高级编程语言不提供对链下数据调用执行操作，只提供对链下数据调用读写操作。通过读取链下存储的数据，Moses 高级编程语言具有业务逻辑可配置特性。高级图灵完备智能合约的复杂性不仅体现在程序逻辑上，还体现在业务逻辑上。例如编写涉及法律概念的智能合约时，需要法律从业人员提供具体法律知识来支撑业务逻辑的实现，这是专业开发人员无法具备的能力。InterValue 将提供规则配置文件格式，支持特定知识以规则的形式存储在链下，智能合约通过读取可识别的规则配置文件以实现特定知识领域的业务逻辑。特定知识领域的规则配置文件具有可重用性，具有打造数据交易市场的潜力。一般来说，用户使用的数据都是事先确认安全的数据。

8.3. 摩西虚拟机（MVM）

声明式非图灵完备智能合约和高级图灵完备智能合约统一在摩西虚拟机中进行验证和执行。摩西虚拟机采用基于栈的虚拟机原理实现，不仅能简化指令和编译器实现，还能提供优良的虚拟机可移植性。MVM 虚拟机运行时数据结构如下图所示。

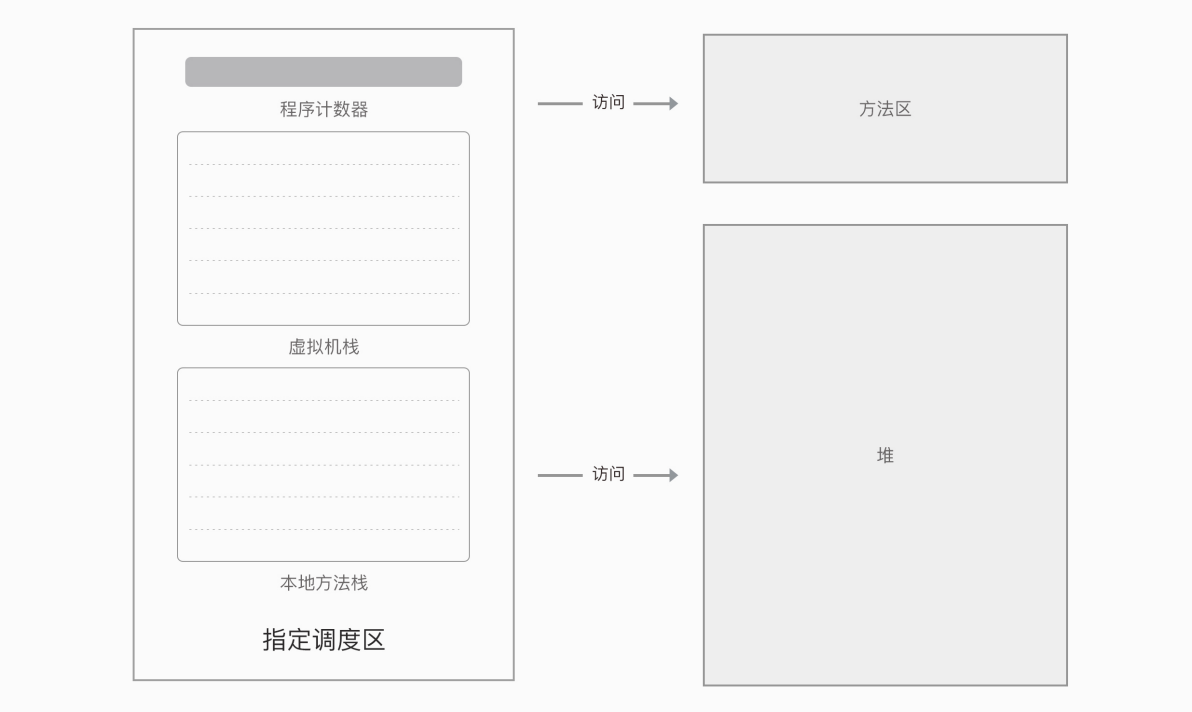


图 8–1: MVM 虚拟机运行时数据区

- 程序计数器：存储下一条需要执行的字节码指令地址。

- 虚拟机栈：在每次高级图灵完备智能合约被调用执行时，MVM 都会在指令调度区创建虚拟机栈。虚拟机栈由栈帧构成，每次合约方法被调用和完成，将对应一个栈帧的入栈和出栈过程。
- 本地方法栈：为指令调度区私有，功能和虚拟机栈相似，用来存储本地方法调用的相关信息。
- 堆：所有高级图灵完备智能合约实例对象在这里分配存储空间。
- 方法区：用于 MVM 加载智能合约类信息、常量、静态变量等数据。

高级图灵完备智能合约在部署到 InterValue 上之前已编译成字节码，MVM 可以直接加载运行。然而，声明式非图灵完备智能合约是以 Json 格式嵌入在交易数据中，MVM 无法直接加载运行。在 InterValue 客户端会加入针对声明式非图灵完备智能合约的编译器功能，将合约编译成为一个缺省合约对象字节码后加载入 MVM 执行。

出于安全防护的考虑，MVM 采用沙箱结构设计，从系统层保护智能合约免受恶意攻击。借鉴面向字节码的进程级安全隔离执行环境的实现策略，MVM 安全沙箱基于白名单机制，对合约代码的各类方法及其访问的资源（数据）进行严格安全检查，基于最小权限原则将方法的可访问权限限制在满足其基本功能之内，并对当前的系统资源进行数据保护，最大程度的实现智能合约的安全防护。

8.4. 智能合约账户和交易

类似以太坊账户概念，在 InterValue 中也存在外部账户和合约账户两类账户。外部账户是用户控制的账户，用于发起转账交易。合约账户由外部账户控制，通过接收外部账户和其他合约账户消息调用启动智能合约的执行。

声明式非图灵完备智能合约嵌入在外部账户发起的交易数据中，用于为交易提供条件约束，没有账户概念。智能合约账户专指部署高级图灵完备智能合约后返回的账户信息。外部账户和合约账户具有状态的概念，如账户中 INVE 余额信息和交易发起数等信息。为了消除外部账户和合约账户的差异，账户状态有 MVM 代码哈希值信息，该信息在高级图灵完备智能合约部署后是无法修改的。此外，为了访问用户存储在链下的数据，账户状态还包含链下数据访问目录信息。

在 InterValue 中有两种交易手续费计算规则，外部账户发起的普通交易采用按交易数据字节数进行计费，调用智能合约则按程序指令执行数进行计费。为了消除这两部分计费规则的差异，在交易数据结构中包含类似以太坊的 Gas 上限和 Gas 价格两个域进行统一计费。对于按交易数据字节数计费的规则，交易数据字节数是已知的（也就是交易手续费是事先知道的），通过固定 Gas 上限也就得到了 Gas 价格。在用户发送部署高级图灵完备智能合约的交易时，交易数据结构中有指定 MVM 代码的域。

9

链上应用及应用场景

9.1. 链上应用

9.1.1. 分布式社交网络应用

分布式社交网络应用基于区块链技术与分布式 P2P 技术，实现一个去中心化，可任意访问，不受任何组织影响的社交网络世界。不同于日常访问的社交网络，分布式社交网络没有服务器的概念，所有网络数据都被分散在分布式社交网络各个用户的电脑中，任何人都只需要一对非对称密钥，就能够发布内容。

所有人都可以通过发布者公布出的站点私钥在 P2P 网络中找到发布者的电脑，直接从中下载站点的数据。越来越多用户访问后，发布者的内容就会被多台电脑保存，曾经访问过用户社交主页的电脑就会开始为用户的站点做种子，就像 BT 种子一样，用户的站点的内容就这样在无数台电脑中存续，会被永久性存储。

只要还有一台联入网络的电脑上有用户的网站的种子，用户的社交网站，用户的内容就不会消失，而当这个 P2P 网络足够大的时候，用户的社交网站与内容将无人可以完全将它删去，它将与这网络世界一起永生。

同样，分布式社交网络由于它 P2P 的无中央主机特性，建立网站也变得非常的简单，不需要去租用主机，用户需要的仅仅是通过命令生成一个随机网站地址，写好它的 HTML 代码，然后发布给其他人。

9.1.2. 分歧合约应用

“分歧合约交易”定义：存在分歧的交易市场，比如传统的“北京单场足彩”，用户在球队胜负上存在分歧，“分歧合约交易”可以拓展到任何存在歧义的交易市场，同时，区别于传统的类似“北京单场足彩”彩票，在“分歧合约交易市场”中，有人可以中途

把合约转手卖掉，也可以有人中途把合约买进，众多的买家与卖家在一起交易，就形成了“分歧合约交易市场”。

基于 InterValue 打造的“分歧合约交易市场”可以实现一个五方共赢生态系统：

- 技术供应商：构建整个平台的前后端所有技术
- 平台运营商：改造前端界面，多语言运维
- 分歧设计者：发现分歧与需求，设计分歧合约
- 合约做市商：差价自营，赚钱差价，提供流动性
- 分歧交易者：买卖分歧合约，平衡风险，获得盈利

9.1.3. 文件存储网格应用

文件存储网格是一个商业公有链平台，它首先基于文件存储网格平台提供个体（个人及家庭、集体）数据存储、分享的基础服务，个体可将有价值的数据上链保存、确权。然后在海量的个体数据基础上，通过开发各种专业类的 DApp，实现各类数据去中心化的汇集、共享和治理，并实现数据的增值与利用，最终打造一个去中心化的全民数据存储、汇聚、分享、治理、增值的生态系统。

包括以下几个部分：

- 基于文件存储网格平台的分布式数据存储平台；
- 一个安全的，可扩展的商业公有链基础设施；
- 上链数据存储、搜索积分系统；
- 完善平台生态的专业数据治理 DApp 商店。

大数据生态链的目标是实现数据的分布式存储和大规模去中心化应用，它相对于一般的公有链，具有以下特性：

- 可编程性；
- 可扩展性；
- 可升级性；
- 交易可管理性；
- 可见性；
- 可购性；

- 安全性；
- 速度/性能；
- 高可靠性；
- 可延展性。

9.2. 应用场景

9.2.1. 应用场景概述

InterValue 的应用场景主要包括三大部分：（1）数字货币；（2）泛金融应用；（3）非金融应用。

- 数字货币

数字货币主要涉及到第三方资产发行，众筹等。基于 InterValue 公链，可以实现第三方资产的发行；同时，在链上可以实现众筹等数字货币资产相关的应用。

- 泛金融应用

泛金融是指除了传统的金融行业之外，还包括与之密切相关、紧密相连的行业如资产管理公司，相关的投资咨询公司等。基于 InterValue，可以实现各种泛金融应用，比如跨境支付、供应链金融、数字票据；同时，也可以进一步地实现资产证券化、银行征信、供应链金融、保险业务等。

- 非金融应用

  InterValue 能够实现多点之间的直接交易和所有信息的处理，提高效率，节约交易成本，还可以创造信用，有利于推动非金融应用发展。

  InterValue 可以实现的非金融应用主要包括医疗、物联网、IP 版权 & 文化娱乐、以及公共服务 & 教育等。

  - 在医疗方面，主要基于 InterValue 实现电子健康病例 (EHR)、DNA 钱包、药品防伪等行业的信任、去中心化管理。
  - 在物联网方面，主要基于 InterValue 实现供应链管理、共享经济、能源管理等。
  - 在 IP 版权 & 文化娱乐方面，主要基于 InterValue 实现作品版权、图像作品认证和追溯、知识产权登记、去中心化数字版权管理等。

- 在公共服务 & 教育方面，主要基于 InterValue 实现公共审计、土地确权、公益项目、教育信息登记等。

InterValue 具体的应用实例主要包括虚拟资产应用、条件支付应用、隐私交易应用、场外交易应用、社交交易应用、共享经济等。InterValue 典型链上的具体应用如下：

- 虚拟资产：游戏装备，直播打赏；
- 条件支付：知识付费，API 调用，去中心化保险等；
- 隐私交易：博彩等；
- 场外交易：币币交易；
- 社交交易：群红包，群收款；
- 共享经济：内容分发（CDN）激励，广告流量分成。

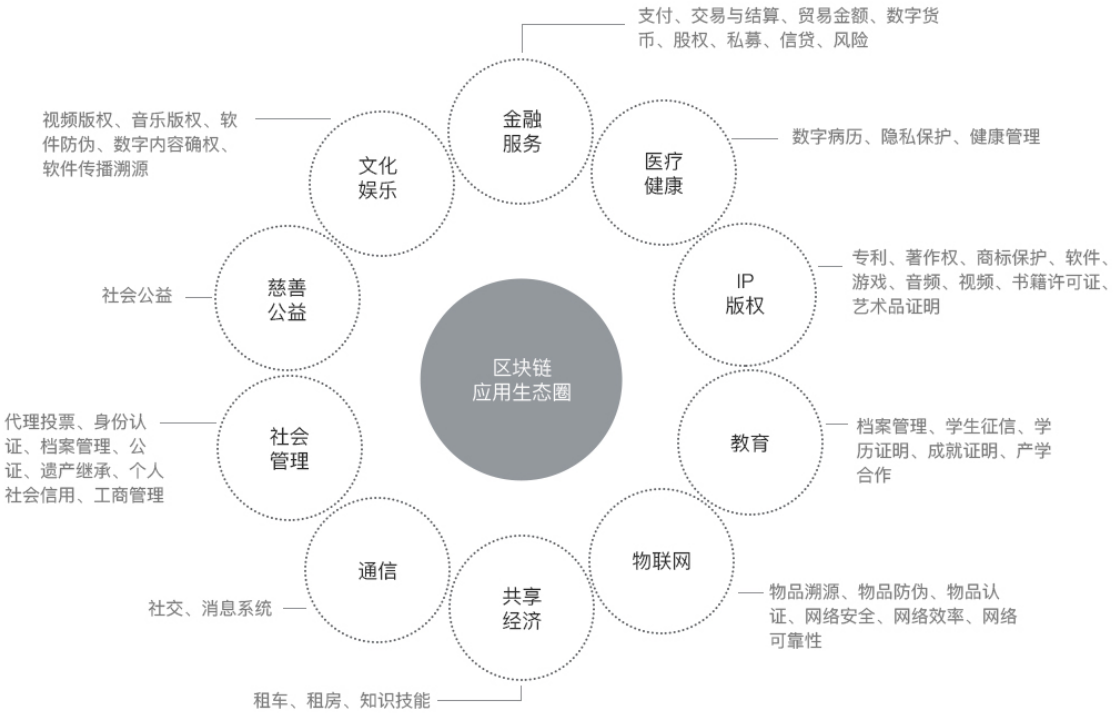


图 9–1: 区块链应用生态圈

9.2.2. 实物资产交易确权

主要有两种思路：联合签名、区块链 + 数字证书

- 联合签名

资产所有者与确权机构联合对资产信息进行签名，保证区块链上的确权信息得到确权机构的认可。资产所有者在区块链上登记资产，确权机构对资产进行调查确定后，对确权信息进行联合签名。

- 区块链加数字证书

目前数字证书主要应用在金融、电商、证券、保险、支付等资产交换相关的行业，为这些行业提供基于实名的强身份标识认证和基于电子签名法的线上操作抗抵赖防伪造。

在实物资产确权中，我们可以在 CA 机构申请 ECC 的证书，区块链上的地址对应一个公钥，这个公钥与相应的数字证书相对应，这个数字证书是确权机构认可的，在区块链上只要公开该数字证书即可认证数字身份；然后在区块链上进行资产信息登记包括资产的类别、名称、总量、所有者、权限等信息，对经确权机构认可的数字身份掌握的实体资产进行确权。

9.2.3. 去中心化旅行服务平台

目前的旅行服务平台存在的痛点：

（1）信任体系：目前的旅行市场都是集中式的数据存储，比如，类似于 TripAdvisor，Dianping 和 Priceline 这样的平台，他们都是由于商业和广告的目的而控制着集中式的数据，无法保证 C 端用户体验。这些集中式数据被扭曲的、虚假的评论和大量无关信息所渗透。这些平台为了维持更大的利益，收取大量的中间费用，而不是为了资源供应方与消费者创造更好的旅行服务。

（2）定制旅行：在传统的旅行市场中，旅行消费者找到值得信赖、个性化的旅行服务需要查阅大量的、不相关的、过时的、以及虚假的资料。定制旅行问题出现的主要原因在于：① 传统区域化旅行市场的能力在于本地的销售，不在于全球目的地资源的整合和连接，无法整合全球资源；② 集中式存储方式导致旅行服务的数据质量本身不高，使得人工智能算法准确性不高，进一步导致传统的个性化旅行定制服务质量不高。

（3）区块链性能：传统的区块链技术大部分是为了解决金融货币体系，其性能通常不能够满足实际应用场景，比如以比特币为代表的区块链 1.0 技术通常每秒中仅仅支持 7 笔交易；以以太坊为代表的区块链 2.0 技术，每秒中仅仅支持约 25 笔交易，传统的基于以太坊公共分布式账本的区块链技术，显示不能够很好的支持如此庞大的全球旅行市场。

针对上述特点，基于 InterValue 公链的去中心化旅行服务平台主要创新方案如下：

（1）信任体系：利用去中心化的区块链技术，跳过平台中间商差价，直接连接旅行消费者和旅行资源供应方。从旅行规划师、航空公司、酒店住宿预订等切入，构建基于信任、激励、零佣金的未来旅行服务生态。基于智能合约技术，使用 INVE 进行旅行规划师、机票、酒店住宿等预订，旅行资源供应方不用支付任何佣金，降低其运营成本；用户将使用更低的价格获取更好的服务。具体实现上，旅行规划师可以在 InterValue 公链上发布旅行规划服务，创建不同的规划路线，包括旅行目的地、旅行计划等；航空公司可以在 InterValue 公链上发布机票服务，包括机票路线、价格、保险等；酒店可以在 InterValue 公链上发布服务，创建不同的房型。旅行规划师、航空公司、酒店均需要支付一定的 INVE。收取 INVE 是为了防止服务被滥用，这部分 INVE 将会在该服务第一次被购买并完成智能合约执行后进入到激励计划资源池中重新分配。InterValue 公链将自动把这些数据保存到 IPFS 的分布式文件系统中，并生成对应的哈希字符串作为智能合约的服务识别代码。为了解决信息不对等、评价造假等问题，无论是旅行资源供应方还是消费者，在使用 InterValue 公链之前都必须进行 KYC（Know Your Custom）认证。InterValue 公链将通过非对称加密技术将身份信息加密并保存到 IPFS 系统中，以确保链上信息有效、真实和安全。在交易费用上，相对于传统的 OTA 平台，在 InterValue 公链平台上，如果服务提供者与消费者都是用 INVE 交易，InterValue 公链将不会收取中间费用。为了便于区块链世界和真实世界的衔接，InterValue 公链会引入用第三方机构服务，帮助交易双方自动完成数字货币与法币之间的换汇。也就是说，消费者可以通过数字货币进行支付，服务者则会收到等值的法币，此外 InterValue 公链也将打通各大平台的积分。

（2）定制旅行：InterValue 公链旅行利用去中心化的区块链技术，削减了噪音、虚假评论数据，并且进一步地打通了全球吃、住、行、游、购、娱 6 个行业的资源供应方以及全球的旅行消费者，使得旅行消费者能够直接根据个人喜好，寻找个性化的定制旅行服务。同时，InterValue 公链旅行利用人工智能和数据科学技术，对链上的每个旅行消费者的吃、住、行、游、购、娱六个维度进行多维画像，基于多维画像和个性化推荐技术，对每个旅行消费者匹配志同道合的同行者，进一步地实现个性化的定制旅行。

（3）区块链性能：InterValue 公链旅行基于区块链 4.0 技术，使用了 HashNet 与 BA-VRF 双层共识算法，使得交易确认更快、交易过程更安全，适应于全球庞大的旅行市场。同时，InterValue 公链旅行采用了非图灵完备的声明式智能合约系统，这种智能合约由陈述性和完全布尔语句组成，因此更接近传统的法律合同语言，支持布尔运算，数学运算，数据存储等。

InterValue 公链旅行建立一个强大的商业模式，鼓励旅行资源供应方、行业领袖、以及旅行消费者加入 InterValue 公链旅行来提高网络流量。利用 InterValue 公链代币的激励机制，旅行资源供应方可以提供更加便宜、便捷、可靠的旅行服务。InterValue 公链旅行利用 InterValue 公链代币的激励机制，创建一种独立的解决方案，激励旅行

消费者发布真实、可靠的旅行经历，提高旅行消费者在 InterValue 公链旅行中的忠诚度，同时吸引更多用户加入 InterValue 公链旅行，构建个性化的定制旅行服务。

InterValue 公链旅行平台提供一套整合资源供应方与旅行消费者的信用积分系统，只有资源供应方或者旅行消费者发布真实可靠的旅行服务或者个人旅行经历，才能够提高自己的信用积分。资源供应方与旅行消费者的积分、服务、以及评论均存储在不可篡改的链上，随后，利用人工智能技术构建多维画像。这意味着 InterValue 公链旅行的积分、服务、以及评论均不可能伪造，使得平台的可信度增加。InterValue 公链旅行平台创建一个量化的信用系统，资源供应方能够查询每个旅行消费者的信用积分，旅行消费者能够查询资源供应方的信用积分。同时，旅行消费者与资源供应方的资金兑换写在智能合约中，并且与凭据和用户 ID 一起存储在链上，使得交易与费用的执行依靠智能合约来触发，这意味着资源供应方与旅行消费者之间的付款更加可信，旅行服务也更加可靠。

InterValue 公链旅行平台为一个全栈的旅行市场，能够利用智能合约来自动管理资源供应商和旅行消费者之间的交易。去中心化的资源供应方与旅行消费者个人信息、评论数据、以及信用积分使得旅行服务更加真实、可靠，以此来吸引更多的忠诚客户。

InterValue 公链旅行平台背后最大的激励是 InterValue 公链代币 INVE。生态中的所有旅行活动都围绕着 InterValue 公链代币 INVE，包括所有的支付、交易、奖励、仲裁等, InterValue 公链代币 INVE 的经济效应使得更多的旅行消费者和资源供应方加入生态系统。

去中心化旅行服务平台基于区块链、智能合约、以及人工智能技术开发，目的是建立一个更加可靠、智慧的首个全球旅行生态系统，从根本上重构旅行全产业的信任体系，探索实现旅行产业升级与消费升级，顺应供给侧结构性改革，引领旅行行业经济发展进入良性循环。通过去中心化的区块链网络直接链接全球旅行资源供应方与消费者，以特色定制的旅行需求和供应为切入口构建基于信任、激励、零佣金的未来旅行服务生态，该生态系统确保每个消费者能够快捷的获得个性化的定制旅行服务，吸引全球吃、住、行、游、购、娱 6 个行业的资源供应方以及对应的旅行消费者。随着越来越多的人参与及使用 INVE，网络效应也将会被不断放大，旅行服务市场由此变得更加公正和透明。

9.2.4. 资产分红权利交易区块链

基于区块链技术，实现资产分红权利交易的区块链生态系统，为资产提供安全、便捷的交易平台，使资产所有者能通过资产募集所需资金，资金提供方可通过购买资产来获得资产盈利或增值的分红。

系统运营方对整个系统中的资产价值、合法性、盈利等提供尽职调查，通过将优质资产进行打包、挂牌、上链来实现资产分红权利的交易。采用区块链发行的数字货

币进行资产交易，交易可在资产所有者与资产投资者之间进行，也可以在投资者之间进行。采用区块链的智能合约来实现资产的分红权利，通过智能合约来定义资产的分红规则，当资产盈利或者增值达到一定标准自动触发相应的分红规则，资产运营越成功，分红就越多，资产价值就越高。

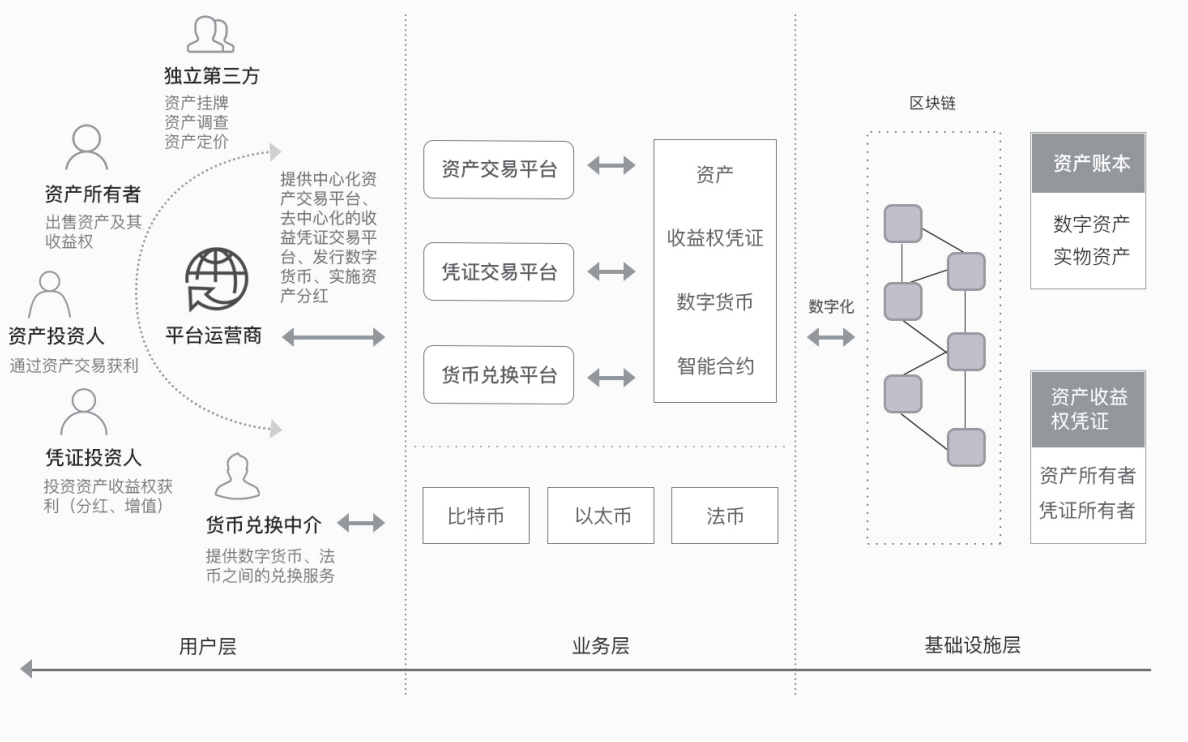


图 9–2: 资产交易生态

- 角色划分

主要涉及以下几个角色：资产所有者、资产挂牌机构、资产区块链（一个自组织系统）、资产投资人、矿工、数字货币交易平台、数字货币投资者等。

- 资产所有者：挂牌资产并出售资产募集资金，资产挂牌后将公布对应的分红规则，一旦资产出售，相当于双方根据该规则签订智能合约，并在条件达到时促发自动执行。
- 挂牌机构：相当于做市商，对资产所有者要挂牌上链的资产进行尽职调查，发布资产盈利、升值情况。对资产交易抽取较低提成，以支撑尽职调查。
- 资产区块链：存储资产及其资产信息，存储资产交易信息，以区块链的特性提供信息的不可篡改、交易追溯等特性；存储和根据条件执行智能合约，实施资产分红和资产自动交易。

- 资产投资者：利用闲置资金投资资产获取分红，或通过资产升值获利。
- 矿工：提供计算和存储资源，得到数字货币激励。
- 数字货币投资人：通过囤积和交易数字货币获利。
- 数字货币交易平台：为数字货币交易提供中介，实现数字货币套现。

- 智能合约

采用图灵完备的高级语言作为智能合约的实现，这便于合约双方实现和验证合约的内容，在高级语言的开发环境里，快速定义和测试智能合约，高级语言编译的字节码也可为智能合约进行一定程度的加密。但这也带来一个问题，合约的执行需要高级语言的环境，为此仅采用区块链来存储和验证智能合约的内容，合约的执行由区块链中的合约代理服务器来执行，经过验证的合约代理服务器作为区块链的一个节点为智能合约提供代理和执行环境，合约仅是代码实现。代理服务器接收外部数据，并将数据传给动态加载的合约代码；或者根据合约自身提供的时间节点运行合约代码，运行过程中合约可访问外部公开数据。

在资产交易系统中，智能合约也为资产投资方提供了退出机制，资产投资方在交易前与资产所有者签订智能合约，规定在一定时间期限内，投资方有权选择退出：将此资产出让给资产所有者，实现变现。

- 资产交易流程

基于区块链的资产交易解决方案可实现资产交易市场中的用户数据和交易数据的存储，以解决无中心、透明交易、信任等问题。

- 分红流程

区块链采用智能合约解决自动分红问题，当资产参数符合分红条件，则自动将资产所有者账户中的部分货币作为分红划拨到资产投资人的账户。

10

跨链通信和多链融合

10.1. 跨链技术介绍

目前的区块链项目并不能很好的服务于商业应用，除了区块链容量受限和交易确认速度慢等原因之外，一个更加重要的原因在于单个区块链项目是一个独立的价值网络，存在网络孤立性问题。不同区块链项目之间的协同操作难度大，极大地限制了区块链项目的发挥空间。InterValue 作为一项以实现价值互联为目的的区块链项目，在价值互联上包含两层意思，除了要实现使用 InterValue 平台用户之间的价值互联，还要实现不同区块链项目之间的价值互联，最终改变当前区块链项目之间分散的“孤岛”局面，实现泛在的价值互联。

跨链通信是目前区块链研究的热点，目前主要的跨链技术包括三种：公证人机制、侧链/中继、哈希锁定。公证人机制是指由一组可信的节点作为公证人向链 X 的节点验证链 Y 上的特定事件是否发生。典型的公证人机制包括瑞波实验室提出的 Interledger。如果链 X 能够验证来自链 Y 的数据，则称链 X 为侧链。侧链通常以锚定某种原链上的代币为基础，其它区块链则可以独立存在。目前侧链很难做到在其上建立跨链智能合约，所以很难实现各种金融功能，这正是现有区块链在股票、债券、衍生品等领域尚未取得进展的原因。比较著名的比特币侧链是 ConsenSys 的 BTC Relay、Rootstock 和 BlockStream 推出的元素链，非比特币的侧链包括 Lisk 和 Asch。中继技术是将原有链上的代币转入类似多重签名控制的原链地址中，对其进行暂时锁定，在中继链上的交易结果将由这些签名人投票决定其是否生效。典型的中继技术包括 Polkadot、COSMOS。哈希锁定是一种通过时间锁定让接收方在某个约定的时刻前生成支付的密码学哈希值证明来完成交易的机制，最早起源于闪电网络。然而哈希锁定支持的功能比较少，能够支持跨链资产交换，大部分场景能够支持资产抵押，但不支持跨链资产转移和合约。以上三种技术的比较如下表10–1所示。

表 10–1: 技术优势对比图

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

10.2. 全节点适配器多链融合

现有底层公链项目的发展聚焦在如何提高交易容量和交易速度问题上，忽视了已经出现的平台“锁定”问题。例如，Alice 和 Bob 在各自设备上安装了比特币客户端，他们只能在比特币区块链上转账比特币。如果他们需要转账以太坊上的以太币，只能通过在各自设备上新增安装以太坊客户端完成相互间的转账操作。“平台”锁定问题导致用户切换使用公链非常不方便，极大地降低了用户体验。此外，用户为了能够同时使用多条公链平台，需要配置计算能力和存储能力高的硬件设备，为此支付高昂费用。

InterValue 通过全节点适配器多链融合技术连接不同的区块链基础设施，实现以 InterValue 平台作为统一入口，通过全节点适配器触发外部子网（其他链，如 BTC、ETH）上的转账操作。局部全节点网络由外部子网与内部子网组成，其中外部子网主要包括其他链的网络，如 BTC、ETH 等，内部子网主要包括 InterValue 的分片网络；顶层网络主要由全节点组成的更高层次的子网，具体结构如图10–1组成。

多链融合适配器作为跨链通信模块功能一部分部署在全节点上，由全节点触发局部全节点的外部子网的转账操作，实现转账代理的作用。在 InterValue 开发前期，将支持比特币和以太坊的转账代理功能。以比特币代理转账为例，交易信息如下所示：

```
["cross chain transaction", [
    ["InterValue", ["Alice","Bob"]],
```

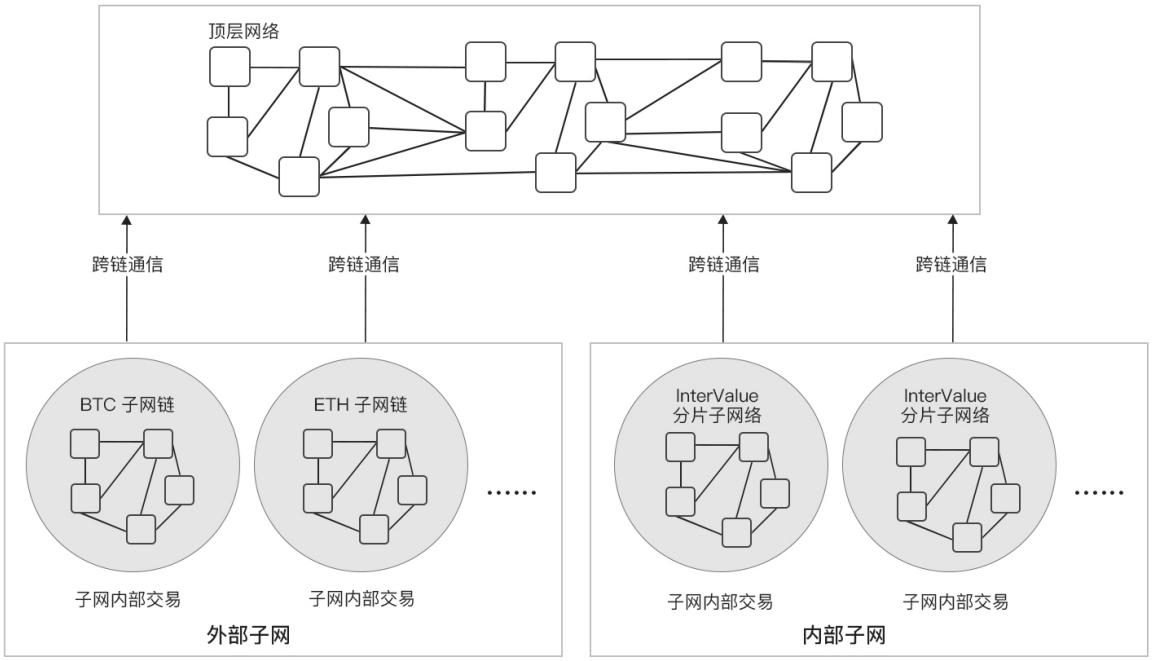


图 10–1: 全节点适配器多链融合

```
”targetchain”: ”BITCOIN”,
”txproxy”:{
”txid”:”TRANSACTION HASH IDNEX”,
”version”:1,
”locktime”:0,
”vin”:[
{
    ”txid”:”UTXO HSAH INDEX”,
    ”vout”:0,
    ”scriptSig”:{
        ”asm”:”ASM STRING VALUE”
        ”hex”:”HEX STRING VALUE”:
    },
    ”sequece”: SEQUENCE VALUE,
}
],
”vout”:[
    {
        ”value”:0.5,
```

```
            "n":0,
            "scriptPubKey":{
                "asm":"SCRIPT CODE",
                "hex":"HEX STRING VALUE",
                "reqSigs":1,
                "type":"pubkeyhash",
            addresses:[ "Bob"]
            }
        },
        ....
    ]
]]
```

对以太坊的支持，只需要根据这两个区块链的交易信息更换以上代码中的 txproxy 域。

- InterValue 用户为实现跨链融合功能，需要在 InterValue 平台上注册其他区块链设施账户。当需要切换其他基础链上的转账操作时，用户选择目的区块链，输入转账数值，发起代理转账。当代理转账在 InterValue 上确认后，全节点将得到该代理转账交易信息，提取 txproxy 域中的交易信息，在局部全节点的外部子网上进行交易广播，完成转账代理操作，实现多链融合目的。

10.3. 跨链通信

InterValue 不仅仅是一个可以独立运行的区块链网络，同时也可以实现跨链资产交换、跨链资源转移等跨链通信功能。任何开发者，均可以根据应用场景需求，在 InterValue 上开发出满足需求的金融应用。InterValue 跨链技术的基本思想是采用全节点中继链技术将跨链通信模块作为单独一层 Overlay 来实现。这样做的好处在于既能够保持跨链操作的独立性，又能够复用 InterValue 基础链上的多种功能。

InterValue 的跨链通信模块主要包括三类角色：验证节点、感知节点、和融合节点。其各自功能如下：

- 验证节点对应 InterValue 基础链中的公证节点，其主要作用是验证来自原链数据的合法性，并在 InterValue 内部打包新区块。验证节点需要抵押足够多的资金以保证在验证节点没有履行职责时付出相应的代价。

- 感知节点是帮助验证节点在原链中收集有效的跨链通信区块。感知节点会运行一个特定原链的全节点，可以打包新块并执行交易，类似 PoW 中的矿工。感知

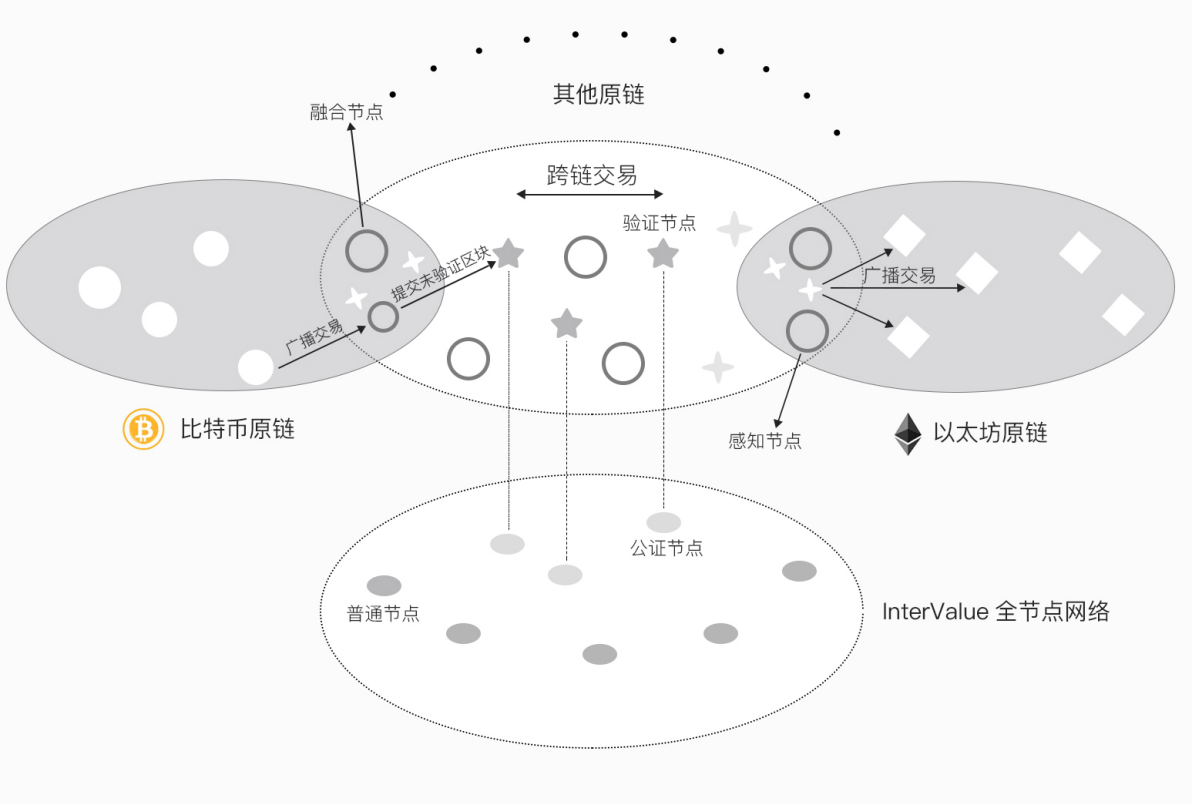


图 10–2: InterValue 跨链通信及多链融合架构设计

节点收集到跨链交易请求区块后，将这些请求区块打包发送给 InterValue 中的验证节点。

- 融合节点相当于原链和 InterValue 之间的网关。每个融合节点上包括两个队列，分别处理跨链进入的交易和出去的交易。另外，融合节点上需要配置对应原链的代币，并能够实现跨链预测（Oracle）。

10.4. 跨链资产交换

为描述 InterValue 上的跨链资产交换过程，我们以比特币和以太坊资产互换为例。假设比特币上的用户 Alice 想要将 1 BTC 兑换成 10 ETH, 同时以太坊的用户 Bob 想要将 10 ETH 兑换成 1 BTC。其业务流程如下：

（1）比特币原链用户 Alice 将 1 BTC 发送到 InterValue 中继链的多签名账户中。

（2）比特币原链的感知节点监听到包含 Alice 这笔交易的区块信息，将该区块的区块头打包到未验证的新区块中，并发送给验证节点。

（3）验证节点集合收到该区块后，验证该区块已被 BTC 链多次确认，之后将该区块信息生成智能合约并写入到 InterValue 中继链区块。

（4）ETH 原链用户 Bob 将 10 ETH 发送到 InterValue 中继链的多签名账户中。

(5) ETH 原链的感知节点监听到包含 Bob 这笔交易的区块信息，将该区块的区块头打包到未验证的新区块中，并发送给验证节点。

(6) 验证节点集合收到该区块信息后，验证该区块已被 ETH 原链多次确认，之后将该区块信息生成智能合约并写入到 InterValue 中继链区块。同时，验证节点检查该区块之前的智能合约是否有与 Bob 匹配的请求，最终发现了 Alice 的请求，并完成匹配。

(7)验证节点生成两份新的智能合约,分别是“将 1 BTC 转入到 Bob 的 BTC 账号中”和“将 10 ETH 转入到 Alice 的 ETH 账号中”。这两份智能合约分别发送到 BTC 原链和 ETH 原链对应的融合节点的入队队列中。

(8) BTC 原链和 ETH 原链的融合节点分别读取其入队队列信息，并将相应的 1 BTC 和 10 ETH 发送给 Bob 和 Alice。此时，跨链资产交换完成。

10.5. 跨链资产转移

为描述 InterValue 上的跨链资产转移过程，我们以比特币向以太坊转移资产为例。假设比特币上的用户 Alice 想要将 1 BTC 发送给以太坊上的用户 Bob，其业务流程如下：

(1) Alice 将 1 BTC 发送给 BTC 原链的融合节点。

(2) BTC 原链的感知节点监听到包含 Alice 这笔交易的区块信息，将该区块的区块头打包到未验证的新区块中，并发送给验证节点。

(3) 验证节点收到该区块信息后，验证该区块已被 BTC 原链多次确认。

(4) BTC 原链融合节点利用跨链 Oracle 将该 1 BTC 兑换为对应数量的 INVE，然后利用 InterValue 基础链将 INVE 发送给 ETH 原链的融合节点，并生成新区块信息。

(5) 验证节点验证 BTC 原链融合节点向 ETH 原链融合节点的发送交易有效。

(6) ETH 原链融合节点根据跨链 Oracle 将收到的 INVE 转换成对应数量的 ETH 代币并发送给 Bob。

12

Token 发行

12.1. Token 用途

InterValue 旨在打造全方位和全模式的区块链 4.0 底层技术平台，支持商业组织和政府机构按照自身业务特性和需求构建公有链、联盟链和私有链应用系统。在支撑公有链应用方面，InterValue 在激励层引入代币机制达到实现面向公有链的灵活共识机制目的，通过内建的 INVE 激励社区维护 InterValue 公有链以及在 InterValue 公有链上开发 DApp 应用，为 InterValue 公有链平台增加价值并推动网络效应。在 InterValue 公有链平台中，INVE 用于：

- 激励广大用户参与到 InterValue 网络中进行资产交易，获取交易费用和公证费用，共同维护 InterValue 网络安全；奖励交易节点和公证节点以支持挖矿的方式来实现；
- 作为权益度量，在早期阶段支持基础 DAG 共识和 BA–VRF 共识，在后期支持基于 HashNet 共识和 BA–VRF 共识，实现 InterValue 独创的双层共识体系；
- 支持 InterValue 生态系统实现高级智能合约，规避“逻辑炸弹”合约执行对网络效能的破化，提供反欺诈机制；
- 发挥 InterValue 生态系统的基础货币功能，提供公有链 DApp 子货币相应 Token 特性和资产流通性基础；
- 作为托管标的实现对 InterValue 公有链 DApp 产品管理，提高 DApp 产品知名度和曝光率；
- 赋予额外的网络附加功能和平台可升级性。

12.2. Token 发行

INVE 是 InterValue 基础 Token 的简称,单位是 10^{18}Atom,即 1INVE=10^{18}Atoms。Atom 是 INVE 的最小单位，支持 InterValue 高级智能合约以及基于智能合约的跨链交易费用。

INVE Token 发行总量为 100 亿，其中挖矿产生 60 亿，项目发起方预留 40 亿用于创建基金会、项目研发、项目推广和团队建设。用于创建基金会的 26 亿中，20 亿是生态建设基金，用于 InterValue 生态投资；剩余 6 亿是 INVE 基金，用于确保基金会各项工作的正常开展。项目资金募集计划将于 2018 年第一季度开始，在以太坊上发行代币 INVE，待 InterValue 主链正式上线后 1:1 兑换成 INVE。INVE 整体分发比例及预留 INVE 发行分配计划如图12–1所示。

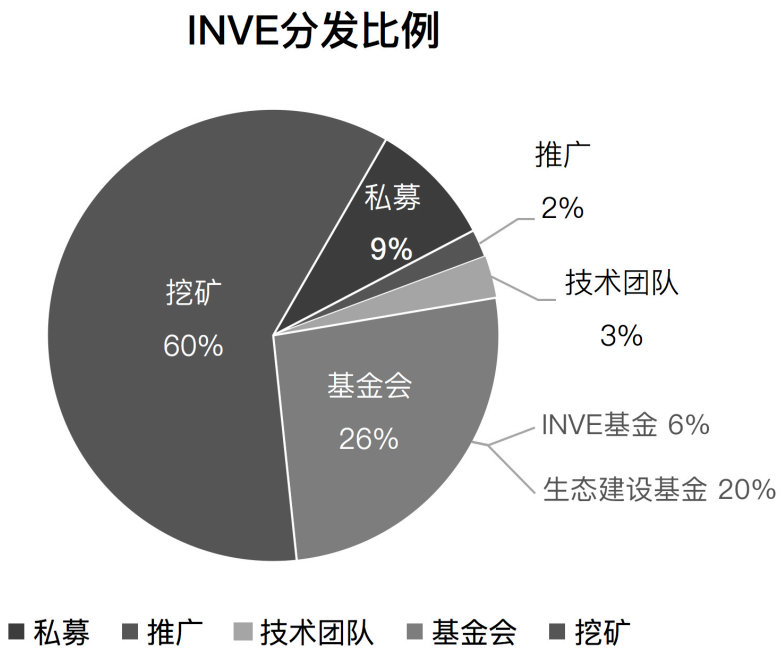


图 12–1: INVE 整体分发比例

普通用户通过局部全节点发送交易，为了防止普通用户中有恶意的 DDoS 攻击，当普通用户发起一笔交易时需要先做一个难度较低的 PoW 计算，然后提交给局部全节点处理。参与交易确认的局部全节点验证该交易的 hash 是否满足挖矿难度，一旦交易被验证，并且稳定之后，发送包含该笔交易 event 的局部全节点便可以得到相应数量的 INVE 作为奖励。为了奖励全节点和局部全节点对整个网络达成共识的贡献，有 60 亿的 INVE 以奖励的方式通过挖矿产生。同时，普通用户每发起一笔交易都会产生一定的手续费，该手续费受益者是当前负责该交易确认的局部全节点，手续费上限跟交易所占存储的大小成正比，具体交易费收多少由相应的局部全节点动态调整。

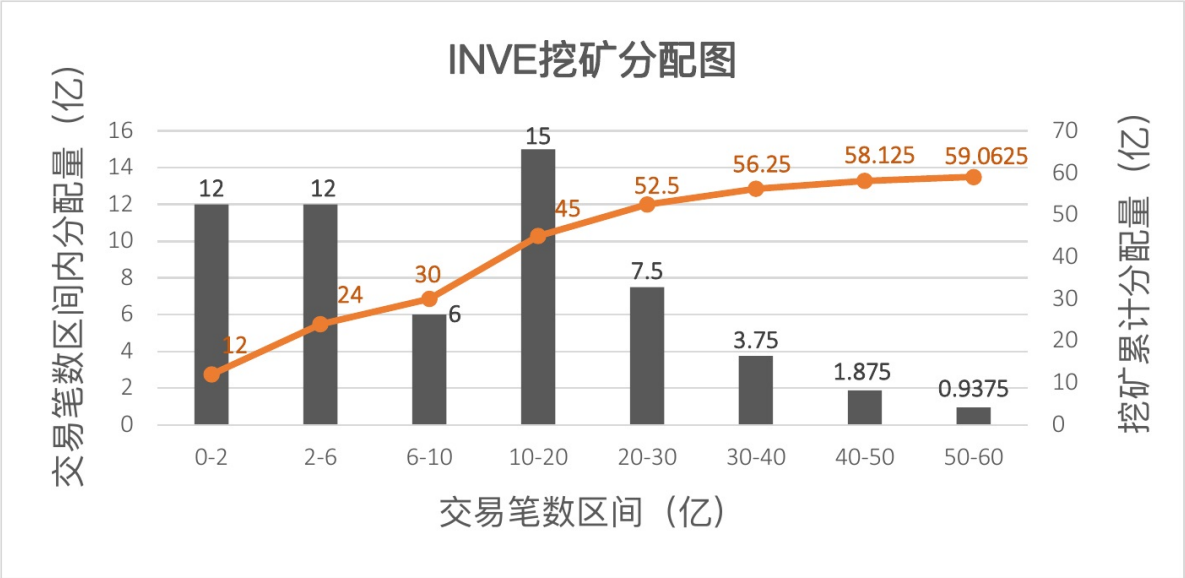


图 12–2: INVE 挖矿分配（前 60 亿笔交易）

通过挖矿奖励发行的 60 亿 INVE 以交易笔数为周期批次衰减发放给局部全节点和全节点。最开始的 2 亿笔交易每笔奖励 6 个 INVE（发放总量 S1=12 亿），第 2 亿笔到第 6 亿交易奖励 3 个 INVE（发放总量 S2=12 亿），第 6 亿笔交易到第 10 亿笔交易每笔奖励 1.5 个 INVE（发放总量 S3=6 亿）。第 10 亿笔交易到第 20 亿笔交易每笔奖励 1.5 个 INVE（发放总量 S4=15 亿），后续每 10 亿笔交易奖励减半。挖矿奖励在局部全节点和全节点的发放以责任全节点的任期为一个结算周期，初始采用“二八”原则（作为参数写入系统合约）进行分配，结算执行以结算周期内最后一个 event 达到共识确认稳定后开始。责任全节点收集任期内的所有交易信息，根据挖矿奖励发行的周期数计算任期内的总挖矿奖励，在全节点网络内进行共识确认。总挖矿奖励中 80% 发送给参与交易确认的局部全节点，剩余的 20% 发送给所有全节点。发送给所有全节点的奖励初始也采用“二八”原则在全节点内部进行分配，责任全节点获得 80% 挖矿奖励，其他全节点均分剩余的 20% 挖矿奖励。挖矿奖励分配比例随着系统运行可根据实际情况由社区投票决定，具体为，由责任全节点发起局部全节点–全节点挖矿奖励分配投票和全节点挖矿奖励分配投票两种挖矿奖励分配投票，局部全节点和全节点的挖矿奖励分配比例由社区所有用户投票决定，全节点内部的挖矿奖励分配比例由所有全节点投票决定。INVE 挖矿分配（以前 60 亿笔交易为例）如图12–2所示。

$$
\begin{aligned}
\text{挖矿量} &= S_1 + S_2 + S_3 + \lim_{n\to\infty}\sum_{i=4}^{i=n} S_i \\
&= 30\ \text{亿} + S_4/(1-q) \\
&= 60\ \text{亿}(S_4 = 15\ \text{亿}, q = 0.5)
\end{aligned}
$$

挖矿奖励发放周期(按交易笔数划分)的设置综合考虑了 InterValue 项目采用 DAG 链数据结构在交易确认速度上的优势以及项目的后发优势（即项目概念接受度和社区成熟度）。

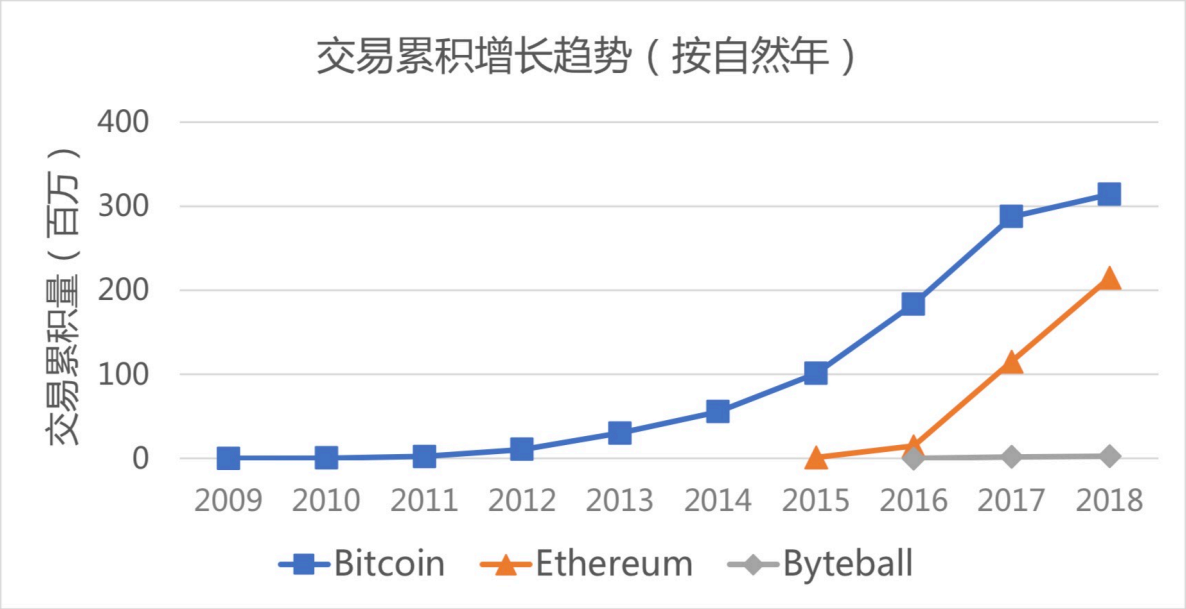


图 12–3: 交易累积增长趋势（比特币、以太坊和 Byteball）

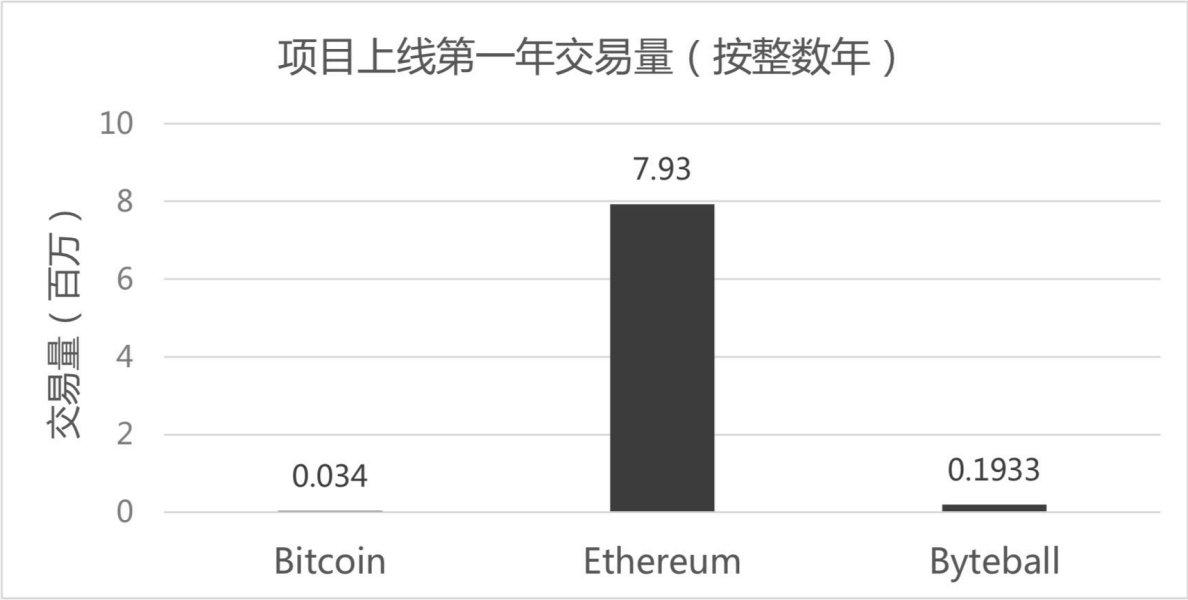


图 12–4: 项目上线后第一个完整年的交易量（比特币、以太坊和 Byteball）

- **交易确认速度优势**：在不考虑后发优势的条件下，项目在单位时间内能完成的交易量主要受交易确认速度影响。比特币和 Byteball 分别是区块链单链数据结

构和 DAG 链数据结构的先锋项目，在各自区块链技术类别中没有后发优势。如图 12–3 所示，比特币和 Byteball 交易累积增长在项目上线的前三年非常缓慢，但是 Byteball 项目在上线后的第一个完整年完成的交易量大大超过比特币（如图 12–4 所示），说明采用 DAG 链数据结构在交易确认速度上的优势有利于提高项目的交易量。因而，InterValue 项目在提高交易量上具有先天优势。

- **项目后发优势**：项目后发优势对于提高交易量具有显著作用。如图 12–3 所示，以太坊作为比特币的继任者，借助项目后发优势，在项目上线的头三年就实现了与比特币媲美的交易增长速度。此外，在项目上线的第一个完整年，以太坊完成的交易量就远超比特币交易量两个数量级。因而，InterValue 采用 DAG 链数据结构所具备的项目后发优势对于提高交易量有极大潜力。

综合以上两个方面的优势，参考以太坊在项目上线不到三年时间内完成超过 2 亿笔交易的事实，我们预测 InterValue 项目极有可能在一年内完成 10 亿笔交易。

13

商业现状

13.1. 技术竞争

- 比特币是区块链 1.0 时代的标志性项目，支撑比特币运行的底层技术——区块链是一种极其巧妙的分布式共享账本及点对点价值传输技术，对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。

- 以太坊作为区块链 2.0 时代的典型代表，是一款能够在区块链上实现智能合约、开源的底层系统，目前全球已有上百个以太坊应用诞生，然而“以太猫”等应用的出现暴露出以太坊网络交易容量和交易确认速度的不足。

- EOS 作为以太坊的对标产品，其终极目标是成为区块链操作系统，其上向所有应用程序开发者提供数据库、账目权限设置、执行调度、认证以及网络应用通信等功能。

- IOTA 是一种用于物联网行业的加密货币。该项目使用基于有向无环图的分布式账本 Tangle，克服了当前区块链设计的低效性，其目标是在物联网行业实现全球范围内的小额支付。

- ByteBall(字节雪球) 是一个去中心化的系统，允许任意数据的防篡改存储，这些存储单元彼此链接，每个存储单元包括一个或多个早期存储单元的散列值，既用于证实早期的单元又用于确立它们的偏序关系，链接单元之间形成有向无环图。

表 13–1: 技术优势对比图

	比特币	以太坊	EOS	IOTA	ByteBall	InterValue
节点分类	全节点 轻节点	全节点 轻节点	全节点 轻节点	全节点 轻节点	全节点 轻节点	**公正节点、全节点、局部全节点、轻节点、微节点**
P2P 网络	不匿名	不匿名	不匿名	不匿名	不匿名	**匿名通信**
共识机制	POW	Dagger POW	DPOS	POW 权重累加	12 名公证人	**HashNet BA–VRF**
抗量子攻击	否	否	否	部分	否	**是**
交易匿名保护	无	无	无	无	无	**基于零知识证明的匿名保护**
智能合约	不支持	图灵完备	图灵完备	不支持	声明式合约	**声明式和高级图灵完备合约**
交易速度	7TPS	30TPS	3300TPS	1000TPS	100TPS	**100 万 TPS**
奖励机制	交易费和挖矿	交易费和挖矿	交易费和挖矿	无交易费	交易引用和公证	**交易引用、公证、挖矿**
应用	较少应用	落地了很多应用	探索期	探索期	探索期	**预计可在很多行业和场景落地应用**

13.2. 企业竞争

- 井通科技：是一家从事区块链底层技术研发的中国公司，核心人员由硅谷和国内顶尖的区块链技术人员组成，2014 年正式推出可支持商业应用的底层技术平台，目前在金融、旅游、智慧城市、物流、医疗等领域均有所涉足。

- Ripple：成立于 2013 年，提供全球金融结算的解决方案，使得银行之间无需通过代理行，实现直接转账，且及时、确定地结算，以此降低结算总成本。瑞波币一度为仅次于比特币的全球第二大市值的数字货币，是首个将数字货币与商业应用深度结合的典范。

- Circle：成立于 2013 年，目前已有的产品应用包括：比特币支付应用、社交支

付应用。Circledd 拥有完整和杰出的团队，其创始人在创建平台型公司、软件、媒体和通讯等领域都有成功的经验。

表 13–2: 优势对比图

	井通科技	Ripple	Circle	Hedera Hashgraph	**InterValue**
产品发展线路图	面向多领域的区块链商用平台	银行结算	数字货币支付	面向多领域的区块链平台	**基础链、区块链浏览器、钱包、面向多领域的区块链商用平台**
应用场景	金融应用 非金融应用	金融应用	数字货币	金融应用 非金融应用	**数字货币** **泛金融应用** **非金融应用**
突出优势	专业团队 多领域介入	专业团队 高准入门槛	专业团队 经验丰富 资金雄厚	专业团队 项目创新性高	**专业团队** **经验丰富** **项目创新性高**
公司愿景	可信生态构建者	全球统一支付标准	重塑全球支付网络	互联网可信层	**构建全球价值互联网**

14

项目风险

加密资产具有较大的投资风险，投资者需充分了解这些风险，并根据各自的风险承受水平进行投资。

- 信息披露不完整的风险

截至本白皮书发布之日，InterValue 仍在紧张开发阶段，其加密算法、通信网络、共识机制等创新技术可能会频繁更新。本白皮书包含了 InterValue 的基本概况，但并非绝对完整，且基金会可能会根据技术发展变化或特定目的不时对项目进行更新和完善。基金会无法、也无义务实时告知买方 InterValue 开发过程中的所有细节。信息披露的不充分是不可避免且合乎情理的。

- 监管风险

加密 Token 由于其高风险性，已被多个国家监管机构所监管。基金会可能会在出售过程中收到来自于一个或多个监管机构的询问、通知、警告、命令或裁定，甚至可能被勒令暂定或终止任何与本次公开售卖、开发相关的行动，从而导致 InterValue 的开发、营销、宣传等受到严重影响。由于监管政策随时可能变化，任何国家之中现有的对于 InterValue 本次公开售卖的监管许可也可能只是暂时的，InterValue 可能随时被定义为虚拟商品、数字资产或证券货币，因此在某些国家 InterValue 可能被禁止交易和持有。

- 项目失败或终止的风险

InterValue 仍在开发阶段，并非已准备推出的成品。在开发过程中，InterValue 可能会由于任何原因而在任何时候失败或终止，主要可能的原因包括：监管机构强制终止、缺乏资金、无法克服的技术困难等。开发失败或终止将导致 INVE 无法交付给本次公开售卖的任何参与者。

- 众筹收入被盗的风险

可能会有人企图盗窃基金会所收到的众筹资金，这可能会影响到 InterValue 开发进度。尽管基金会将采取最顶尖的安全方案保护众筹资金的安全，但某些网络盗窃仍很难被彻底阻止。

- 源代码漏洞风险

尽管基金会会请最顶尖安全团队对 InterValue 源代码进行审计测试，但没有人能够保证 InterValue 源代码完美无瑕。代码可能会有某些错误、缺陷和漏洞，使得用户无法使用特定功能、暴露用户的信息或产生其他问题，进而危害 InterValue 的可用性、稳定性或安全性，并对 InterValue 的价值造成负面影响。基金会将与 InterValue 社区紧密合作，今后持续改进、优化和完善 InterValue 源代码。

- 源代码升级风险

InterValue 源代码是开源且不断升级的，任何人均无法预料或保证某次升级的准确结果。因此任何升级操作可能导致无法预料或非预期的结果，从而对 InterValue 的运行和价值造成重大不利影响。

- 分布式拒绝服务攻击

InterValue 可能会不时地遭受分布式拒绝服务网络攻击,这种攻击将使得 InterValue 系统遭受负面影响、停滞或瘫痪，并因此导致交易被延迟写入 InterValue 的 HashNet 之中，甚至暂时无法执行。

- 节点处理能力不足的风险

InterValue 主网上线后将伴随着交易量的陡增。若处理能力的需求超出 InterValue 区块链网络所能提供的负载，则 InterValue 网络可能会停滞或瘫痪，且可能产生诸如“双重支付”的欺诈或虚假交易。在最坏情况下，任何人持有的 InterValue 可能会丢失，InterValue 区块链回滚或硬分叉可能会被触发，进而损害 InterValue 的可用性、稳定性或安全性。

- InterValue Token 未经授权被认领的风险

任何通过解密或破解 InterValue 购买者的密码而获得购买者注册账号访问权限的人士，将能够恶意认领本次公开售卖中所获得的 InterValue。据此，购买者所购买的 InterValue 可能会被错误发送至恶意攻击者，这种发送是不可撤销、不可逆转的。每一位购买者应当采取诸如以下措施保护其注册账号的安全性：(i) 安装防病毒软件，提高操作系统安全；(ii) 使用高安全性密码；(iii) 不打开或回复任何欺诈邮件；(iv) 严格保密个人信息和秘钥。

- InterValue 钱包私钥丢失风险

若购买者丢失或损毁了存取 InterValue 所必需的私钥，造成的损失是不可逆转的。只有通过本地或在线 InterValue 钱包来占有相关的独一无二公钥和私钥，才可以操控 InterValue。购买者应当妥善保管其 InterValue 钱包的私钥。若购买者的钱包私钥丢失、泄露、损毁，基金会无法帮助购买者找回其 InterValue。

- 系统分叉风险

InterValue 是一个由社区提供支持的开源项目。尽管基金会在 InterValue 社区具有影响力，但无法独断 InterValue 的开发、营销和运行。任何人均可以开发 InterValue 代码的补丁或对代码进行升级，而无需获得任何其他人的授权。一旦部分的 InterValue 区块链验证者接受 InterValue 的补丁或升级,这可能导致 InterValue 区块链分叉。另一方面,根据项目路线图,基金会在开发过程中也会对 InterValue 区块链分叉,由此将会出现两条分叉的网络,直至分叉区块链合并或其中某一条终止出块。理论上,InterValue 区块链可以多次分叉，分叉区块链的暂时性或永久性存在可能对 InterValue 运行及其价值产生不利影响。最坏情况下，可能摧毁 InterValue 系统的可持续性。尽管 InterValue 区块链上的分叉问题可能经基金会和社区努力将其分支合并而解决，但不能保证成功且可能耗时很久。

- 应用缺少关注度的风险

InterValue 的价值很大程度上取决于 InterValue 底层公链的普及度。InterValue 并不预期在发行后的很短时间里就广受欢迎或普遍使用。在最坏情况下，InterValue 可能仅吸引了很小一批使用者。缺乏用户使用可能导致 InterValue 市场价格波动增大从而影响 InterValue 长期发展。出现这种价格波动，基金会不会也没有责任稳定或影响 InterValue 的市场价格。

- 流动性不足的风险

InterValue 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的 Token，也没有任何硬资产或其他信用所支持。InterValue 在市场上的流通和交易

不是基金会的职责或追求。InterValue 的交易仅基于相关市场参与者对其价值达成的共识。任何人均无义务从 InterValue 持有者兑换或购买任何 InterValue，也没有任何人能够保证在任何时刻 InterValue 的流通性或市场价格。InterValue 持有者若要转让 InterValue，需要寻找一名或多名有意按约定价格购买的买家。该过程可能花费较高、耗时较长且最终并不保证成功。此外，可能没有加密 Token 交易所或其他市场上线 InterValue 供其公开交易。

- Token 价格波动风险

若在公开市场上的交易，加密 Token 价格波动剧烈。这种波动可能由市场力量、监管政策变化、技术革新、交易所的可获得性以及其他因素造成。无论是否存在 InterValue 交易的二级市场，基金会对任何二级市场的 InterValue 交易不承担责任。因此，基金会没有义务稳定 InterValue 的价格波动，且对此不关心。InterValue 交易价格所涉及的风险由 InterValue 交易者自行承担。

- 竞争风险

InterValue 的底层协议是基于开源软件，没有任何人拥有该源代码的版权或其他知识产权的权利。因此，任何人均可以合法复制、设计、修改、升级源码或以其他方式利用 InterValue 源代码，以试图开发具有竞争性的协议、软件、系统、虚拟平台从而与 InterValue 竞争，甚至超过或取代 InterValue，基金会对此无法控制。此外，已经存在且还将会有许多以区块链为基础的平台（例如 IOTA、ByteBall、Hedera Hashgraph）与 InterValue 产生竞争关系。基金会在任何情况下均不可能消除、防止、限制或降低这种来自于其他机构与 InterValue 的竞争。

参考文献

[1] Bitcoin Computation Waste. http://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-50403276. 2013.

[2] Bitcoinwiki. Proof of Stake. http://www.Blockchaintechnologies.com/Blockchain-applications. Aug 2017.

[3] Coindesk.com. Bitcoin: A Peer-to-Peer Electronic Cash System.

[4] http://www.coindesk.com/ibm-reveals-proof-concept-Blockchain-powered-internet-things/ Nov 2017.

[5] Ethereum. Ethereum. https://github.com/ethereum/. Nov 2017.

[6] IOTA. https://github.com/iotaledger/. As of 10 Nov 2017.

[7] Byteball. Byteball. https://github.com/byteball/. Sep 2017.

[8] Bernstein, Daniel J, et al. High-speed high-security signatures. Journal of Cryptographic Engineering 2.2(2012), 77-89.

[9] M. Castro and B. Liskov. Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, Louisiana, USA,1999, pp. 173-186.

[10] Biryukov, Alex, and D. Khovratovich. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. Network and Distributed System Security Symposium 2016.

[11] Gilad Y, Hemo R, Micali S, et al. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. The Symposium 2017, 51-68.

[12] C. Decker and R. Wattenhofer. Information Propagation in the Bitcoin Network. 13-th IEEE Conference on Peer-to-Peer Computing, 2013.

[13] D. Dolev and H.R. Strong. Authenticated algorithms for Byzantine agreement. SIAM Journal on Computing 12 (4), 656-666.

[14] A. Kiayias, A. Russel, B. David, and R. Oliynycov..Ouroburos: A provably secure proof–of–stake protocol. Cryptology ePrint Archive, Report 2016/889, 2016. http://eprint.iacr.org /2016/889.

[15] S. King and S. Nadal. PPCoin: Peer–to–Peer Crypto–Currency with Proof–of–Stake, 2012.

[16] S. Micali, M. Rabin and S. Vadhan. Verifiable Random Functions. 40th Foundations of Computer Science (FOCS), New York, Oct 1999.

[17] Directed acyclic graph: https://en.wikipedia.org/wiki/Directed_acyclic_graph