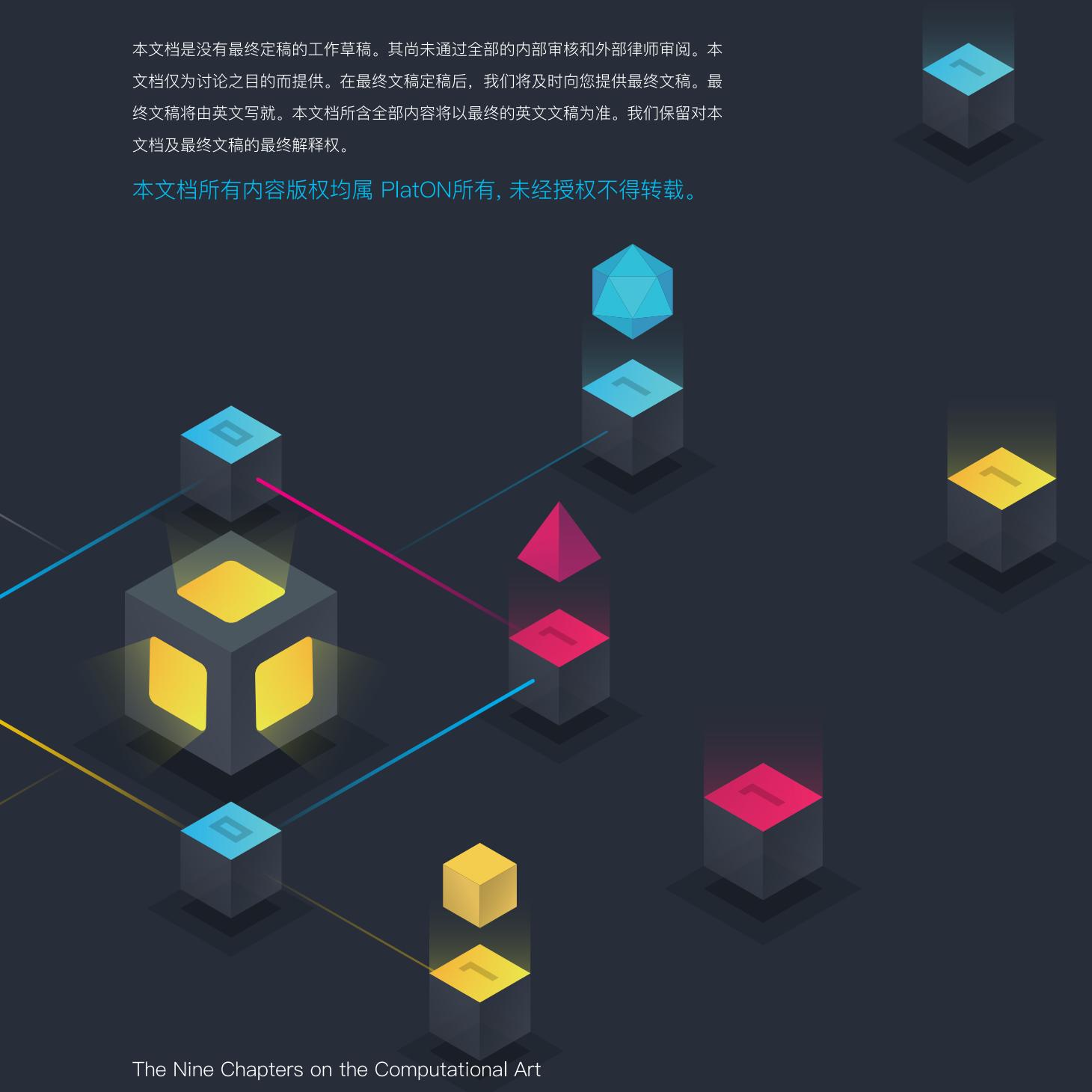


一切皆可计算—PlatON

/下一代计算架构技术白皮书/

本文档是没有最终定稿的工作草稿。其尚未通过全部的内部审核和外部律师审阅。本文档仅为讨论之目的而提供。在最终文稿定稿后，我们将及时向您提供最终文稿。最终文稿将由英文写就。本文档所含全部内容将以最终的英文文稿为准。我们保留对本文档及最终文稿的最终解释权。

本文档所有内容版权均属 PlatON所有, 未经授权不得转载。

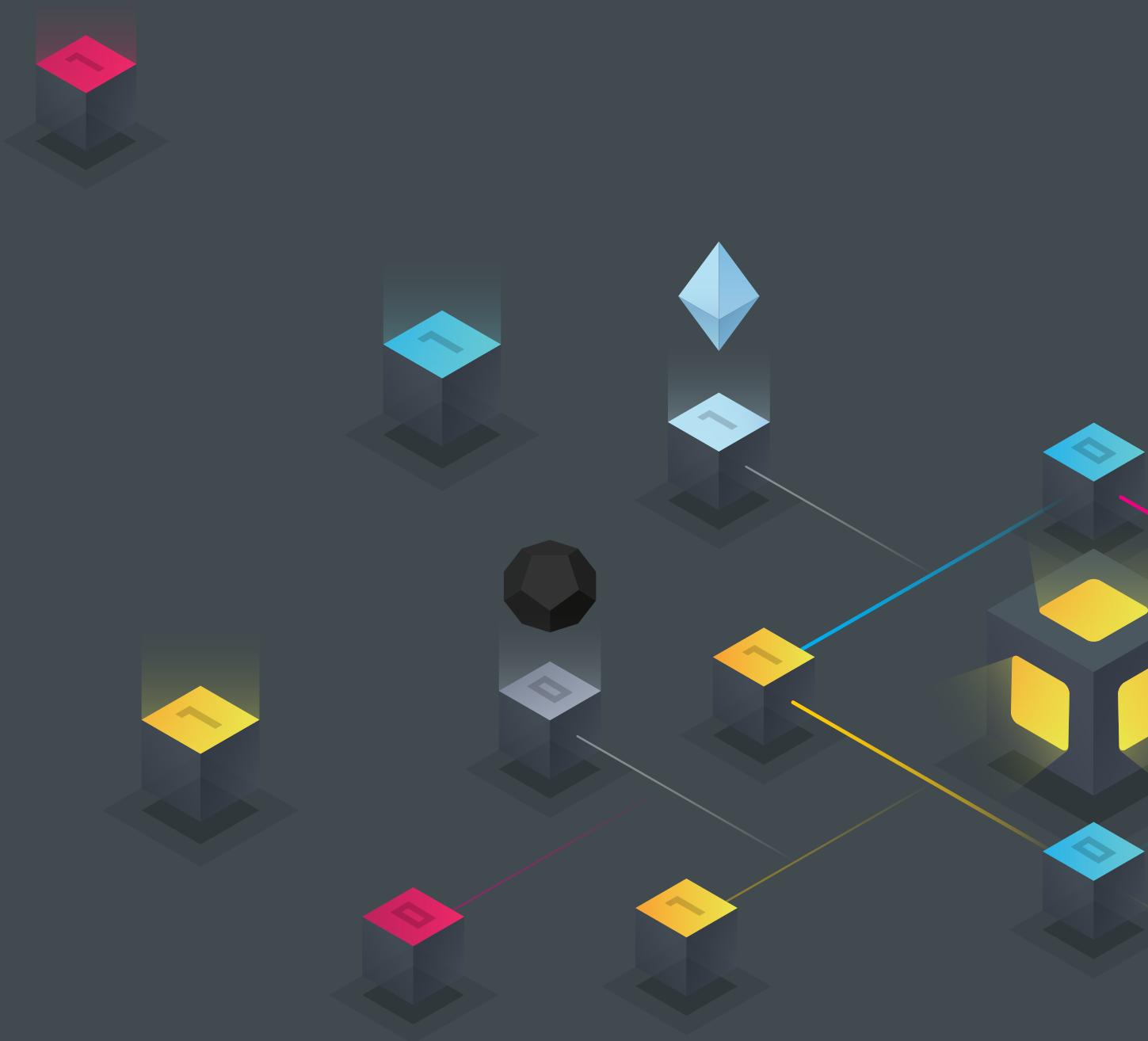




“世界不仅是一台最值得称道的机器，而且就其心灵组成而言，它也是一个最好的共和国。”

Gottfried Wilhelm Leibniz

—《论万物的终极起源》



序章一云图

我们身处于一个由**复杂性**构筑的时代。

人与人、人与物、物与物之间的关系，“涌现”般的从单向性、单线性的关系进化到多维度的复杂拓扑结构。

从当下开始，直到可见的未来，数以百亿乃至万亿计的智能节点逐步加入并组成全球计算网络。“**节点**”们不同程度上掌握了充分甚至冗余的算力与存储，期待着与世界的链接与共识。

在农业社会，人类以“观察”获取数据；在工业社会，人类以“测量”获取数据；在信息社会，海量数据遗留在互联网上，人类以“一键记录”的方式获取数据。但数据的主权何属？隐私何归？价值何如？

节点之间正在产生难以计量的多维度的链接，多层次的定义了万事万物的价值、“**链接**”产生了意义，决定了某一“节点”的特定状态对其他“节点”的影响或改变，产生了新的**度量衡**。

这一切正在并将逐步建构真正意义上的复杂网络，呈现为高度自组织的分布式体系。这一基本事实亦将逐步解构乃至瓦解传统计算架构对于治理结构、算法、算力与数据的垄断，直至新一代的全数字化基础设施横空出世。

结构决定功能。目前几乎所有的区块链技术体系都仍局限于节点之间的“信任”与性能问题。但如果继续沿袭这样的思路，我们将仍然无法摆脱今天这个离散、孤立、无隐私保护的互联网架构，我们也将仍然无法处理各类复杂问题。

将复杂性还原为根本问题之后，全数字化世界的公共基础设施可以展开为：数据的流动性、多源异构网络的自组织与可装配的隐私保护。要实现充分的数据交换与协同计算，这一切都源于无所不在的计算。也只有依赖这一不断进化中的基础设施，我们才可以真正展望人工智能可计算的未来。

自莱布尼茨始，计算日益成为科学与哲学的基础方法论，并已经在从原子世界到比特世界中呈现出统一的威力。计算是对数据和信息的处理过程、计算是宇宙与生命存在和进化的基本方式、计算是人类认知和行为的基础范式。

PlatON是面向未来的下一代计算架构，她的发展与完善是一次软硬件的**协同进化过程**。

从生态治理、业务重构、网络运营到应用分发，无不涉及到计算复杂性与通讯复杂性的平衡与突破，承载了计算体系架构的新变革。

PlatON是一次根植于基本哲学理念的践行，从技术层面展开为计算复杂性领域中各个分支的理论突破、算法进化及工程实践；从业务层面展开为全数字化世界的超级基础设施，是对各个行业传统业务治理和网络的拓扑重构；从社区生态层面将会是人类集体的科学探索与智慧融合；从网络层面PlatON将会逐步覆盖空天地一体，面向广域的计算节点组网，先脚踏实地，尔后仰望星空。

基于我们的信念与积累，在历经了两年之久的酝酿与反复验证之后正式推出PlatON，我们将根据路线图逐一实现和打磨每一个细节。PlatON是一次对于未来计算架构的展望与实践，是一次对于区块链技术和计算复杂性领域的致敬与超越，致力于为下一个时代的分布式密码经济体提供共享的、运营商级的服务，更是对人类全数字化时代公共基础设施治理服务的全面阐释，以此拥抱扑面而来的新时代。

本文聚焦于PlatON在第一个历史阶段的技术架构、网络架构、计算框架等，给出了相关服务和应用的实现。

以此九章“算”术，进入一个未来。

在未来，**一切皆可计算**。

目录

▪序章	01	2.6. 可验证计算	16
▪第一章 计算的进化	05	2.6.1. 基本概念	
1.1. 计算需求的多样化	05	2.6.2. VC在PlatON中的应用	
1.1.1. 计算密集化		2.7. 同态加密	17
1.1.2. 计算协同化		2.7.1. 基本概念	
1.1.3. 计算边缘化		2.7.2. HE在PlatON中的应用	
1.1.4. 计算隐私化		▪第三章 关于PlatON	19
1.2. 计算架构的去中心化	06	3.1. 什么是PlatON	19
1.2.1. 云+网+端的动态平衡		3.2. 核心技术特征	20
1.2.2. 现有云计算架构的挑战		3.2.1. 计算合约化	
1.2.3. 现有区块链的缺陷与挑战		3.2.2. 合约计算化	
1.3. 计算硬件的专用化	08	3.2.3. 元智能合约	
1.3.1. GPU		3.2.4. 可验证计算证明共识Giskard	
1.3.2. DSP		3.2.5. 专用计算硬件	
1.3.3. FPGA		3.2.6. 同构多链架构	
1.3.4. ASIC		3.3. 应用生态	24
1.3.5. SoC		3.3.1. 应用体系	
1.3.6. 软硬件协同进化		3.3.2. PlatON联合体	
▪第二章 算法世界Aladdin	10	3.3.3. 开放的生态建设	
2.1. 新时代的密码学	10	3.4. 隐私保护与合规性	25
2.1.1. 密码学的崛起		3.4.1. 数据保护监管	
2.1.2. 区块链与密码学		3.4.2. PlatON的合规性	
2.1.3. 对于密码学的误读		▪第四章 技术架构	27
2.2. PlatON中的密码学	12	4.1. PlatON网络协议	27
2.3. 关于电路	12	4.1.1. 网络协议栈	
2.4. 安全多方计算	13	4.1.2. 服务发现	
2.4.1. 基本概念		4.1.3. TURN服务	
2.4.2. MPC在PlatON中的应用		4.1.4. SIP服务	
2.5. 零知识证明	14	4.1.5. 计算服务	
2.5.1. 基本概念		4.1.6. 区块链服务	
2.5.2. ZKP在PlatON中的应用		4.2. PlatON网络结构	33

4.2.1. PlatON节点	58
4.2.2. 多链路由机制	
4.3. 共识与计算解耦	35
4.4. 元计算框架Monad	37
4.4.1. 元计算定义	
4.4.2. 元计算参与方	
4.4.3. 元计算任务	
4.4.4. 计算通道	
4.4.5. 计算任务执行	
4.4.6. 专用计算硬件	
4.5. 可验证计算证明共识Giskard	43
4.5.1. 计算贡献值	
4.5.2. 可验证计算证明共识	
4.6. 元智能合约Sophia	44
4.6.1. 元智能合约分类	
4.6.2. 元智能合约虚拟机	
■ 第五章 能量块Energon	47
5.1. 能量块 (Energon)	47
5.2. 能量块交换合约	47
5.3. 去中心化交易所	47
■ 第六章 用户客户端Edge	49
6.1. 数字钱包	49
6.2. 即时通讯 (IM)	49
6.3. Dapp 门户	49
6.4. 前端应用运行环境ERE	50
6.5. Energon转移	50
■ 第七章 应用与生态	51
7.1. 数据交易	51
7.2. 科学计算	52
7.3. 身份认证	52
7.4. 医疗健康	53
7.5. 征信体系	54
7.6. 社交网络	55
7.7. 物联网及工业互联网	56
■ 第八章 技术路线图	58
■ 第九章 社群的进化	59
9.1. 技术的进化	59
9.2. 组织的进化	59
9.3. 网络的进化	60
■ 术语表	61
■ 参考文档	67

第一章/计算的进化

1.1. 计算需求的多样化

1.1.1. 计算密集化

随着互联网、移动互联网、智能物联网的快速更迭，使得数据的采集生产、分发交换的速度和规模达到空前水准，促进了大数据时代的到来，机器学习和Web服务的规模呈指数级增长，计算复杂度与通讯复杂度急剧提升，计算任务也趋向于计算密集型任务和通讯密集型任务，对计算性能提出了全新挑战。

1.1.2. 计算协同化

全数字化世界中每天都会产生大量的数据，但任何单一实体永远都只能掌握数据集合的局部，而没有任意实体可以实时获取所有的全局数据。这是数字化世界面临的基本挑战——“**盲人摸象**”。

每个数字化世界的参与者都是“盲人”，其拥有的数据不足以反映全量数据——“大象”的特征。参与者只有通过数据交换或者协同计算才能获取所需之计算结果，从而加速数据的流动性。

1.1.3. 计算边缘化

在可见的10年左右，全球将有接近万亿级终端与设备联入网络，超过40%的数据将需要在网络边缘侧进行分析、处理与存储。由此产生的天量级数据在当前模式下对传输中的网络带宽、存储和安全都带来了巨大挑战。

01

因此边缘计算势在必行，物联网的核心在于物与物、人与物的强关联，而多数时候的彼此联系会发生在本地。也就是说，计算、存储、分析等需求响应通常在距离物理位置较近的地方完成，而不是传输到千里之外的数据中心。这种就近处理的方式耗时更短，而且足以应付本地业务交互的轻量化需求。

边缘计算
(Edge computing)
是一种在物理上靠近数据生成的位置处理数据的方法。

就近提供智能互联服务，满足行业在数字化变革过程中对业务实时、业务智能、数据聚合与互操作、安全与隐私保护等方面的关键需求。而本质上边缘计算是去中心化的。

1.1.4. 计算隐私化

Facebook、Google、及数家中国互联网企业掌握了大量用户个人数据，并以处理、使用、传播这些数据而牟利。然而近两年全球对于数据隐私保护的关注程度越来越高，频繁爆发的数据泄露丑闻使得公众感觉自己的隐私被侵犯，一些大公司因此遭到公众的抵制和声讨，并受到政府的调查和处罚。而这只揭露了整个问题的冰山一角。

数据作为核心资产迄今为止尚不能完全明确其主权方，但个人、机构、企业、政府等不同实体都已经日益认识到数据主权的重要性、数据安全以及数据交换当中的定价和隐私保护问题。在数据与算法进入计算过程的前后，相关的伦理及法律问题日渐突出。

2018年5月25日起，欧盟率先开始实施《一般数据保护条例》（General Data Protection Regulation，缩写为GDPR），赋予欧盟居民对个人数据的更多控制权，并明确在线服务商在收集、利用欧洲用户个人数据的规则和责任。可以预见，其他国家相关的法律法规也将随后出台，以弥补数字化时代的法律空白。

有趣的是，PlatON恰好完全支持了GDPR理念，其中约定的“数据控制方”、“数据处理方”和“第三方”，都在PlatON当中有所体现。

基于前述“盲人摸象”命题带来的挑战和客观事实，以及数据保护问题的刻不容缓，数据共享过程中应该明确区分数所有方、数据处理方和数据使用方这三个基本角色，达到三权分立状态下的平衡。下一代计算架构将必须提供一个数据隐私保护前提下的安全共享服务平台，以使得数据所有方的数据主权不受侵犯、数据隐私不被暴露，而数据使用方仍能基于授权对数据进行处理，并得到预想的结果。当前的互联网以及区块链技术体系还不能完备的提供这种能力，需要在安全多方计算、全同态加密、零知识证明、可验证计算等多个领域的理论突破及工程实践。

1.2. 计算架构的去中心化

1.2.1. 云+网+端的动态平衡

人类整个计算进化史在最近几十年得以全面加速，贯穿始终的核心是为来自应用需求的服务提供全面支撑、高性价比、数据安全、稳定运行。计算技术的发展从云、网、端三个不同视角也呈现出此起彼伏的波浪式前进、螺旋式上升的特点。依次经历中心化（大型主机）、去中心化（桌面计算）以及再次中心化（云计算）几个发展阶段。今天，去中心化（区块链）再次引发全球关注。

当下，5G、云计算、边缘计算、雾计算、区块链等各种概念层出不穷⁰²，其本质都是围绕着计算在云、网、端三侧保持迭代演进。虽然人类社会整体始终保持集体理性来看待新兴技术，但其中一部分超卓的冒险家在区块链时代又一次先行启航。

1.2.2. 现有云计算架构的挑战

目前全球云计算架构的基本模式是将计算任务分布在大量计算机构成的资源池上，使各种应用系统能够根据需要获取算力、存储空间和各种软件服务。这一模式刚刚兴起，但同时又面临巨大挑战。

雾计算

雾计算（Fog Computing）是云计算（Cloud Computing）的延伸概念，由思科（Cisco）提出，在该模式中数据、数据处理和应用程序集中在网络边缘的设备中，而不是几乎全部保存在云中。

现有云计算架构的高度集中化使其远离终端设备和用户。对于实时性要求较高的计算服务，当需要远端的云计算中心的反馈时，通常会引起长距离往返延时、网络拥塞、服务质量下降等问题。

现有云计算架构并不能真正提供数据隐私保护。大量云计算平台提出的“云端安全屋”概念，本质上是一个系统安全产品，需要将数据保存到云端，涉密数据的集中本身就是新的风险。理论上云计算厂商仍然可以拥有对客户数据的所有权限。同时由于硬件基础设施是在云提供商的控制之下，如果云提供商内部人员恶意控制了可信硬件（CPU、TPM）⁰³，就无法保证计算的机密性。

在共享计算体系中才有可能真正解决以上问题。基于全新的治理架构，不让网络中个别节点掌握过多的资源，构建更加“对等”的网络生态。这将会成为比桌面计算和云计算影响更加深远的技术革命，在这场革命中大型技术公司的势力将会被极大削弱，而用户将成为自己的主人。

TPM
TPM (Trusted Platform Module) 安全芯片是指符合TPM (可信赖平台模块) 标准的安全芯片，它能有效地保护PC、防止非法用户访问。

1.2.3. 现有区块链的缺陷与挑战

现有以PoW为共识机制的区块链架构造成了巨大的算力与资源浪费。虽然新兴的区块链技术正在以去中心化架构为全球集中算力提供了强大的想象力，但是公链为保证安全，普遍采用PoW工作量证明共识和重复的交易执行验证，需要消耗大量的算力，造成大量的资源浪费。同时也带来交易性能效率低下的问题，以至于无法支撑大规模应用。

现有的智能合约体系也未能真正实现“智能”。当下以以太坊为代表的智能合约也可被认为是一种Serverless架构⁰⁴，智能合约在虚拟机（VM）中执行计算，但智能合约并不“智能”，目前智能合约实际只有单线程运行性能，增加计算资源实际上并不能提高智能合约执行性能。目前包括以太坊在内的业界也都在探讨分片、状态通道、多链架构等性能扩展方案，但尚未出现成熟应用。

Serverless架构
Serverless是一种无服务的架构，跟传统架构不同，由开发者实现的服务端逻辑运行在无状态的计算容器中，它是通过事件触发，短暂的（可能只存在于一次请求过程中），完全被第三方管理。

现有区块链技术体系并不能提供真正的隐私保护。绝大多数区块链项目都声称自己可以提供完美的隐私保护方案，但事实上传统的区块链技术本身并不能做到这一点。以太坊给出了四种适用于以太坊区块链的兼顾隐私性和安全性的解决方案：通道（Channels）、混合器（Mixers）、环签名（Ring Signature）及零知识证明（Zero knowledge proofs）。但是这些解决方案在以太坊区块链中也都尚未得到真正意义上的部署和实施，即便是有，也基本局限于传统的数字资产交易。

1.3. 计算硬件的专用化

"People who are really serious about software should make their own hardware. "

——Alan Kay

由于接近物理极限，半导体行业的摩尔定律已开始步入暮年，制程工艺迭代速度开始减缓，通用处理器（CPU）计算能力发展开始减缓，随着人工智能等应用大规模的部署，我们需要寻求一种更加高效的计算资源，除通用处理器以外，被广泛使用的芯片还有GPU、DSP、FPGA、ASIC/ASSP、以及SoC等。

1.3.1. GPU

随着近年来机器学习等领域的突飞猛进，GPU也早已经不再局限于3D图形处理，其在浮点运算、并行计算等部分计算方面的特性已经引起业界越来越多的关注。但GPU和CPU一样，都同属冯·诺依曼结构，指令译码执行、共享内存，计算速度和并行计算受到限制。

1.3.2. DSP

是一种哈佛架构的处理器，哈佛结构是一种将程序指令存储和数据存储分开的存储器结构。哈佛结构是为了高速数据处理而采用的，因为可以同时读取指令和数据（分开存储的）。大大提高了数据吞吐率，缺点是结构复杂。通用微机指令和数据是混合存储的，结构上简单，成本低。DSP一般被用来进行信号处理，譬如无线基站、影音多媒体转码等。

1.3.3. FPGA

现场可编程逻辑阵列（Field Programmable Gate Array，缩写为FPGA），是作为专用集成电路（ASIC）领域中的一种半定制电路而出现的。既解决了定制电路的不足，又在性能与应用广度上显示出优势。

1.3.4. ASIC

专用集成电路（Application Specific Integrated Circuit，缩写为ASIC），也可以叫做ASSP（Application Specific Standard Parts）。一种专门为特定目的而设计的集成电路，是按照特定用户要求和特定电子系统的需求而设计、制造的集成电路。因为它面向特定用户的特点，ASIC在批量生产时与通用电路比具有体积更小、功耗更低、可靠性提高、性能提高、保密性增强、成本降低等优点。但是设计周期长和设计成本高、应用范围窄的通病，使得ASIC/ASSP仅适合于大批量部署的应用场景。

1.3.5. SoC

芯片级系统 (System on Chip, 缩写为SoC) , 也称为片上系统, 意指它是一个产品, 是一个有专用目标的集成电路, 其中包含完整系统并有嵌入软件的全部内容。

1.3.6. 软硬件协同进化

在去中心化的环境中, 计算主体不再是单个数据中心或云计算中心的基础设施, 而是遍布全球的PC、手机、电视盒子, 也可能是摄像头, 也可能是计算、网络和存储的复合处理。这种新兴的应用场景也对计算硬件提出了更高的要求: 高性能 (并行计算) 、高安全 (机密性)⁰⁵、绿色环保 (低功耗、低成本) 和网络高吞吐量, 要满足这些需求, 从软件定义所有 (SDx, Software-Define-Everything) 到针对目标应用提供最优的软硬件一体的方案, 从通用的CPU走向 FPGA/ASIC 是一个必然的过程。

软件定义所有

软件定义所有, 就是通过虚拟化将软件和硬件分离出来, 将服务器、存储和网络三大计算资源池化, 最终实现将这些池化的虚拟化资源进行按需分割和重新组合。软件定义所有的概念广泛, 包含了软件定义网络 (SDN) 、软件定义存储 (SDS) 、软件定义数据中心等不同领域。

第二章/算法世界Aladdin

算法与计算的关系密不可分。算法包罗万象，万事万物皆可用算法来描述和展开。我们已经并且终将全面沉浸于算法世界之中。

PlatON作为下一代计算架构，尤为彰显和注重密码学算法的价值和作用。在本章节中，我们将主要目光投注于密码学理论基础及其在PlatON当中的延伸。

2.1. 新时代的密码学

2.1.1. 密码学的崛起

密码学最早起源于军事，例如凯撒密码，用于军队之间传递消息。密码学（或者称密码术）一直被认为是一门艺术而非科学。真正跨时代的事件是1976年密码学家Whitfield Diffie, Martin Hellman发表的《New Directions in Cryptography》真正拉开了现代密码学的序幕。在该文中提出了公钥密码学的基本思想，为后续的可证明密码学的发展奠定了基础。同时密码学家Ralph Merkle和James Ellis也独立提出过类似的思想。

采用密码学提供更强大的隐私保护，恰恰是为了让数据更加开放。密码学的崛起伴随着整个全数字化世界的演进过程。在每一个复杂网络中，数据的流动性与节点的泛智能化都将隐私问题的极端重要性摆在了机构和个人面前。数据的所有权归属本质上是对数据隐私的保护，这将构成下一代互联网的基础，也是人类数字化生存和技术的“栖居”的基本模式。这一看似矛盾的历史使命毫无疑问将由密码学来承担。

但必须说明的是密码学并不能孤立的解决全部问题，也不是密码算法越多越好。需要跨学科的理论突破、恰当的数据治理结构与大量的工程实践，才能够真正解决数据隐私性与可用性之间的根本“矛盾”，也是唯一能够解决现实场景中看似“不可能”问题的工具。

2.1.2. 区块链与密码学

传统的区块链在技术层面只是用到了最为简单的密码学工具，其本身也并未提供隐私保护的功能。

与之相反，区块链这种新的分布式架构，对于隐私保护的需求远远高于传统架构，这也是为何不断有高级的密码学工具不断叠加于区块链之上以提供隐私保护的根本源动力。合适的密码学工具遇到合适的场景，进而推动了密码学的崛起。

密码学是一门真正的交叉学科，从数学到计算机科学，再到底层的量子力学甚至到生物学，都显示了密码学的强大的生命力。密码学吸收各个学科的特点，也同时促进各个学科的发展。面对我们所处的高度复杂的网络世界，也必须采用这样一门交叉学科的技术工具才能真正解决问题。

2.1.3. 对于密码学的误读

“**密码学**”（Cryptography）包含（但不限于）对称密码学和非对称密码学，分别研究对称密钥体系与公私钥体系。研究范畴包括隐私性（Privacy）和完整性（Integrity）。隐私性又称机密性（Confidentiality）保护信息不被攻击者获取。完整性保证数据不被攻击者篡改。隐私性和完整性可以作为同时满足的特性进行研究。

“**加密**”（Encryption）只是密码学中的一部分，加密必然对应着解密（Decryption）。加密是利用密钥从明文到密文的过程，解密是利用密钥从密文到明文的过程。Hash只是数字摘要算法（Digital Digest），而并不是加密算法，因为无法（有效的）从Hash的结果中恢复出明文。

今天“**Crypto**”这一词汇已经进化出许多新的含义，被广泛应用到各个场合，已经成为了新兴经济体的重要代称之一。

密码学	隐私性（Privacy）	完整性（Integrity）
对称密码学	对称加密（AES）	Hash（SHA256）
	非对称加密（ECIES）	数字签名（ECDSA）
		零知识证明（NIZK）
非对称密码学		可验证计算
	全同态加密（存在对称密钥的构造）	
	安全多方计算	

表1 密码货币（Cryptocurrency）中涉及的密码学技术

Cryptocurrency正确的解读是“**密码货币**”，而非“**加密货币**”。在原生的比特币系统中只是使用了Hash和数字签名算法，甚至没有使用加密算法。由于Hash和数字签名只是保护数据的完整性或者说不可篡改性，因此原生的区块链技术根本无法提供任何隐私保护。隐私保护只有在叠加后续的零知识证明、安全多方计算、全同态加密等算法之后才可能被真正实现。

与之相对应的Crypto Economics也应该被称为密码经济学，而非以讹传讹的“加密经济”

学”。密码学的整个体系才是支撑未来经济体系的基础协议与能力，而非“加密”而已。

2.2. PlatON中的密码学

在PlatON网络中，密码学将发挥无所不在的重要价值，我们高度重视并且长期致力于密码学的理论突破与工程实践，并从其他交叉学科中不断汲取养分。

密码学理论支撑了PlatON关于全数字化世界中公共基础设施的根本定位，不同的密码算法协同配置，以作为下一代互联网的基础协议。

密码学及其工程实践将可以逐步优化直至解决数据流动性的基本问题，为数字化世界中的“盲人”们，找到一条清晰可见的路径来参与到数据的流动当中来。

密码学及其他交叉科学的综合运用，将可以平滑的改良下一代互联网的治理结构，让各个参与方在相对自治、透明、公正的基础上共治、共享。

为此，PlatON将会长期面向全球各类型大学、学术机构、学者、研究者、工程师、爱好者们，发起和支持密码学的理论研究、培训教育、赛事会议，为密码学的欣欣向荣略尽微薄的力量，以此推动全球社区的进步。

2.3. 关于电路

电路是计算的一种基本表现形式，电路复杂性是计算复杂性的一个重要分支。任意形式的可计算模型都可由电路表示。电路最早可以追溯到数学家George Boole，布尔电路即是以George Boole命名。电路复杂性最早的研究可以追溯到Shannon。电路因为其基本组成部分的简易性，是在密码学中被广泛使用的计算模型。

电路是PlatON的基本表现形式和技术路线之一。我们相信全数字化世界将逐步、完整的向以电路为表现形式的公共基础设施转移。

06 电路是由各种不同的门（Gate）通过输入输出线构成的“复杂有向无环网络”。由逻辑门（比如：与、或、非、异或等）构成的电路称为布尔电路（Boolean Circuit）；由算术门（比如加法、乘法等）构成的电路称为算术电路（Arithmetic Circuit）。

07 电路是PlatON作为复杂网络的连接纽带。PlatON通过电路的形式垂直连接上层智能合约与底层共识算法，以达到计算可验证、可度量的根本目标。PlatON通过电路来水平的连

有向无环网络

有向无环网络指的是一个无回路的有向图。在图论中，如果一个有向图无法从某个顶点触发经过若干条边回到该点，则这个图是一个有向无环图（DAG图）。

布尔电路

一种通用的计算表现形式，由不同类型的门（gate）组成。由逻辑门构成则成为布尔电路（Boolean circuit），由算术门构成则叫算术电路（Arithmetic circuit）。

接各类算法，以到达计算的隐私性。电路作为安全多方计算、零知识证明、可验证计算、全同态加密共同使用的通用计算模型，以其超强的普适性串联各类算法。

电路是PlatON度量“计算”的基本单位。任何计算都可拆分为电路，电路以有限种类的门构成各类复杂的计算形态，如同生命一般，恰当的“简单”产生了极致的“复杂”。电路正是复杂性的最好诠释和缘起。对计算的度量可直接细化到门的数量和种类。各类计算中不同种类门的资源消耗不同，对各类门消耗的度量进而反映为对整个计算的度量，电路为计算的度量和定价提供了理论基础。

电路与下一代专用计算硬件无缝对接。PlatON中有关计算的表示、算法的实现都围绕电路进行展开。计算密集型与通信密集型的算法最终需要专用硬件支持以支撑复杂的应用场景与逻辑。PlatON中的电路形态及模型天然适合专用硬件的实现。

2.4. 安全多方计算

安全多方计算是保证数据安全流动，发挥数据价值的基本协议。是连接全数字化世界中数据孤岛的隐形桥梁。

安全多方计算不仅是密码学理论上的明珠问题，也为人类社会的数据安全共享打开了大门，是PlatON的重要理论基础和努力方向。

2.4.1. 基本概念

安全多方计算（Secure Multi–Party Computation，缩写为MPC）是在无中心条件下，多个参与方协同完成对各自数据的计算，并且保证各自输入信息的隐私。最早由姚期智先生以百万富翁问题的形式提出。百万富翁问题是两个百万富翁如何在没有可信第三方的前提下比较资产的多少，并且不向对方透露自己的资产。在此基础之上，抽象出一般的安全多方计算问题，并逐渐发展成密码学中非常重要的一个分支。

安全多方计算是指N个参与方 P_1, \dots, P_N 分别拥有输入 x_1, \dots, x_N ，共同计算函数（本文称为计算逻辑） $f(x_1, \dots, x_N)$ 得到相应结果，并且保证输入的隐私。安全多方计算有两个主要性质：正确性和隐私性。

■ 正确性

在协议执行结束之后，各方能够得到正确的结果。

■ 隐私性

隐私性是指整个协议不会泄露除结算结果外的“额外信息（Additional Information）”。这里并不意味着“不泄露输入数据的任何信息”，因此，有一些计算逻辑是不重要的（比如两个参与方计算加法），因为无论如何总能从结果和一方的数据中反推出另外一方的数据。

安全多方计算通常考虑两种安全模型：Semi-Honest（半诚实）模型和Malicious（恶意）模型。Semi-Honest模型是指攻击者（可能是参与者）严格按照协议执行，他仅能观察到协议的交互信息（如果是参与者，还包含参与者本身提供的信息）。

Malicious模型是指攻击者（可能是参与者）可以不按照协议规定进行计算和通信，尝试通过错误的信息获取其他参与方的输入数据。MPC协议在Semi-Honest/Malicious模型下是安全的指的是在Semi-Honest/Malicious模型下，攻击者无法获取除计算结果以及由此推出的信息之外的任何信息。

值得注意的是，MPC协议本身并不考虑输入数据的正确性和合法性。如何保证参与方提供正确、真实的数据需要其他技术手段来保证，比如审计、追溯、激励等。

2.4.2. MPC在PlatON中的应用

自姚期智先生提出概念开始，近40年的发展已经让安全多方计算成为密码学最活跃的领域之一。其可扩展性与性能一直是密码学界最为关心并致力于解决的问题，且几年来不断有许多令人惊喜的理论与工程结果相继出现。

PlatON不仅利用安全多方计算技术为数据的流动性提供平台，也为安全多方计算算法本身的理论突破和工程实践提供可落地的环境。依托于PlatON网络中的大量应用服务，不断为安全多方计算技术算法理论突破提供需求，其工程化实践进一步推动上层解决方案的完善，进而形成一个良性循环的生态。

PlatON将应用逻辑编译成电路，从Semi-Honest模型下的两方计算协议与多方协议开始，再逐渐进化到Malicious模型下的两方协议与多方协议。以Garbled Circuit和Oblivious Transfer为基本工具，并逐渐扩展支持其他工具，比如Secret Sharing等。

2.5. 零知识证明

零知识证明为PlatON数据交易提供完备的隐私保护，为全数字化世界提供隐形的共识。

2.5.1. 基本概念

零知识证明 (Zero-Knowledge Proof, 缩写为ZKP) 由Goldwasser, Micali, Rackoff提出，能够使证明者让验证者确认某一事实的正确性，而不泄露该事实的额外信息。

零知识证明所需证明的断言 (statement) 包含两个部分：实例 (instance) 和证据 (witness)。证明者 (Prover) 拥有证据，并且向验证者 (Verifier) 证明其拥有的证据witness满足该实例instance，并且不会泄露witness的其余信息。零知识证明拥有三个主要的性质：**正确性，可靠性，零知识性**。

■ 正确性

如果Prover拥有证据witness（可以不止一个）满足实例instance，那么按照规则生成的零知识证明，一定（或者以极大的概率）能被Verifier验证通过。直观的意思是：真实的证明者Prover一定能够生成合法的证明。

■ 可靠性

如果Prover没有证据witness满足该实例instance，则Verifier一定（或者以极大的概率）能够验证证明是错误的。直观的意思是：假的证明者无法生成合理的证明欺骗验证者。

■ 零知识性

验证者Verifier无法获得“证明者拥有某一个证据满足该实例”之外的其余任何信息。

自Goldwasser, Micali, Rackoff提出相关概念到最近几年，零知识证明，尤其是非交互零知识证明 (Non-Interactive Zero-Knowledge Proof, 缩写为NIZK) 大多只存在于密码学的理论学术研究中。非交互零知识证明是指Prover不需要同Verifier交互，可以直接生成证明，并由Verifier验证。分布式账本技术的不断成熟为零知识证明的落地和广泛使用提供了几乎完美的场景。

2.5.2. ZKP在PlatON中的应用

非交互零知识证明为PlatON中交易身份和交易内容的保护提供完备的解决方案。在分布式无中心的系统架构下，既能保证全体节点验证交易的合法性，同时保护交易中的所有隐私。从简单的转账交易，到复杂的智能合约，零知识证明都可以提供可证明的安全保护。

同样，现有零知识证明很难在证明长度、证明生成时间、证明验证时间上三者同时达到最优，依然需要有理论的突破和工程实践。PlatON集成最新的非交互零知识证明算法支撑上层隐私保护的需求，同时为非交互零知识证明算法本身的发展和进化提供平台。

PlatON在账户模型的基础上，从保护转账交易隐私开始，逐步进化成智能合约隐私的保护。结合合约计算化，将智能合约编译成电路，通过对通用电路可满足性问题的非交互零知识证明，进一步支持更为广泛和通用的计算形态。

2.6. 可验证计算

可验证计算是PlatON中并行计算和高效共识机制最为核心的密码技术，若想“一切皆可计算”，则需要“一切皆可验证”。

可验证计算有效的连接着“合约计算化”与“计算合约化”，最终真正实现利用全球异构算力进行并行计算。

2.6.1. 基本概念

可验证计算（Verifiable Computation，缩写为VC）能以极小的代价验证输出数据是否由输入数据按照规定的方法计算所得，也可按照场景需求决定是否保护输入数据的隐私。随着云计算和外包计算的兴起，可验证计算已经成为密码学研究中最为活跃的领域之一。

可验证计算研究的研究范畴是在计算能力不对等的场景下，计算能力弱的一方如何快速、准确的验证能力强的一方（比如，云计算）返回的结果是否正确。客户端将需要计算的数据 x 和需要计算的方法（称为计算逻辑） f 委托给服务端。这里一般 f 是相对复杂的计算逻辑以至于客户端本地的计算能力无法支持。

服务端提供足够的算力计算得到 $y=f(x)$ ，同时给出一个相应的证明。可以让客户端能够通过证明极为快速的验证（本地计算能力允许的前提下） y 是正确的。可验证计算一般满足三个条件：**正确性，不可伪造性（安全性），有效性**。

■ 正确性

如果服务端计算得到正确的结果 y ，则其正确生成的证明一定能被客户端验证接受。

■ 不可伪造性

服务端无法同时伪造假的 $y \neq f(x)$ ，且生成让客户端验证通过的证明。

■ 有效性

客户端验证证明的时间要远远小于其重新计算 $f(x)$ 的时间（否则客户端可以自行计算，无需委托给服务端计算）。

2.6.2. VC在PlatON中的应用

PlatON通过合约计算化，将计算/智能合约编译为电路。对于过于复杂的计算，以电路的形式分拆成多个子任务，再结合计算合约化，通过激励机制吸引网络中的闲置算力来进行子任务的计算。通过可验证计算技术，以极小的算力代价验证异构算力提供的子任务运算结果。可验证计算连接合约计算化与计算合约化，最终真正实现利用全球异构算力进行并行计算。

与传统的区块链技术不同，PlatON中每个节点不需要重复运行智能合约来验证交易。利用可验证计算，以及电路化的智能合约，节点只需在极短的时间验证交易的合法性，即验证新的状态是否由旧的状态通过智能合约运算而来。

2.7. 同态加密

全同态加密是密码学的圣杯—“The Holy Grail”。

全同态加密支撑PlatON网络实现可操作的全加密网络。在未来，一切数据主权在“我”，今天的互联网巨头们将会被解构成为“我”所用的“工具”。

2.7.1. 基本概念

同态加密 (Homomorphic Encryption, 缩写为HE) 的概念早在RSA算法之后不久即提出。**同态加密是指将数据加密后仍然可以对数据进行操作**。按照操作的范围可分为部分同态加密与全同态加密 (Fully Homomorphic Encryption, 缩写为FHE)。部分同态加密只能支持某一类操作，比如RSA算法支持乘法同态，Paillier算法支持加法同态。全同态加密支持任何计算，即任何由电路表示的计算。

(全) 同态加密可以是基于对称密钥也可以是非对称密钥。用 Enc 表示 (对称/非对称) 加密， Dec 表示解密。对于任何的明文 m_1, m_2 ，以及对应的密文 (一个明文可能对应着多个密文) $c_1=\text{Enc}(m_1), c_2=\text{Enc}(m_2)$ 。全同态加密的含义为，对于任意的操作“ \circ ” (考虑明文是比特，则该操作可以是XOR门或者AND门)，都存在一个密文上的操作“ \otimes ”，能够计算得到 $c_3=c_1 \otimes c_2$ ，并且 $m_1 \circ m_2 = \text{Dec}(c_3)$ 。

直观而言，全同态加密是指可以对任意计算，从密文的层面的操作“同态”映射到明文层面的操作，以实现加密的可操作性。

2009年，密码学家Craig Gentry基于格密码理论给出第一个全同态加密的理论构造。自此以后，全同态加密作为密码学的一个新领域空前繁荣，大量密码学家在Craig Gentry的

格密码理论

格理论是数学中研究具有周期性结构的离散点集合，格密码理论以格中困难的数学问题为基础发展起来的新型密码体系。

框架下不断进行理论和工程上的探索。

目前主流的构造全同态加密的工具是采用格密码理论，主要的方式是采用Oded Regev提出的基于Learning with errors (LWE)的带误差的加密方式（或者其对偶变形Dual Encryption）。在误差允许的范围内，可以通过私钥正常解密。随着对密文的操作的次数越来越多，误差会越来越大。为了能够减少误差以继续进行密文操作，Craig Gentry创新性的提出了Bootstrapping的技术，能够不断的刷新密文以减少误差。当前全同态加密领域基本是在Craig Gentry这个框架下进行理论创新和工程实现。

2.7.2. HE在PlatON中的应用

PlatON致力于打造全球第一个全加密网络，之上流通的所有数据、信息都经过加密。利用全同态的性质，对所有数据、信息的所需的任何操作都能同步保持。最终实现数据全方位、全生命周期的隐私计算网络。

同样，PlatON为全同态加密算法的理论和工程实现提供良性循环的生态。网络中新的应用和场景不断提供需求，进而新的、高效的全同态加密算法也可不断叠加在PlatON网络中进行实验和部署、运营。

■ 第三章/关于PlatON

3.1. 什么是PlatON

PlatON是面向下一代的全球计算架构，是全数字化时代的公共基础设施，我们则是新一代的数据管道工与梦想家。

这意味着，PlatON不仅是一个通常意义上的区块链技术体系，她本质上是下个时代的、面向服务的“运营商”。

PlatON是人类进入全数字化时代的“计算工厂”和“服务集市”。她是完备、完整的基于服务的计算架构，从数据的流动性视角提供完备的分布式网络框架、服务框架和生态体系。提供全面的计算、存储、通讯能力；将算力、算法、数据等一切基础资源作为服务提供。基于PlatON，**一切皆可计算**。

PlatON是全数字化世界的“通天塔”。致力于面向多源异构数据提供分布式的数据交换与协同计算，她也是多源数据与异构网络基础设施的连接器，从计算的角度超越原有孤立的价值本体，通过构造**以电路为基本表现形式的分布式计算网络**，将各种资源与应用服务化，形成跨地域、跨服务、跨账户、跨主体的公共基础设施。基于PlatON，**一切数据皆可流动**。

PlatON是“算法世界”的入口与守护者。将会是全球首个提供完备隐私保护能力的运营服务网络。我们主张个人以及任何实体的数据主权神圣不可侵犯，但我们相信完备的隐私保护是为了数据更加的开放。为此我们将基于密码学中的各种算法来支撑这一理念。基于PlatON，**算法即信任，认证即交易**。

PlatON是覆盖各种行业应用及服务中数据资产的“超级清算方”。为各类服务和应用提供评级、估值和定价的技术能力支撑服务。我们相信场景业务化、业务数据化、数据资产化、数据交换代币化的基本演进过程。PlatON提供运营商级的运营支撑体系，涵盖计费、支付、清算、结算、差错、争议处理等。基于PlatON，**一切数据的流动皆可清算**。

PlatON支持下一代计算架构中软硬件的协同进化。我们将会在适当时机推出支撑PlatON计算与运营需求的硬件架构，让用户使用更加方便简单。将理念的力量与机器生命融合一体。基于PlatON，**让计算更简单**。

3.2. 核心技术特征

PlatON是在过去十年分布式、密码学和区块链技术进步和社区进化的基础上开发的，吸取了大量区块链体系的理念和技术特点，也发展出了其自身特有的技术关键要素。可以概括为如下特征：

09

PlatON是一种去中心化的分布式RPC框架。基于RELOAD覆盖网络，PlatON实现了P2P服务发现机制，支持服务动态注册和发现、服务透明路由和访问，提供多语言支持的服务容器和服务编排、服务治理能力。在PlatON上，区块链也是一类服务，除了PlatON节点内置的计算服务、数据服务、存储服务、区块链等基础服务，用户也可发布自己的业务服务。

RPC (Remote Procedure Call)
RPC (Remote Procedure Call) ——远程过程调用，它是一种像调用本地方法一样地调用远程机器上的方法，而不需要了解底层网络技术的协议。

PlatON是一种全新的区块链计算模式。她将共识与计算解耦、将计算扩展到链下、支持算力线性扩容，并使用可验证计算算法防止欺诈计算；通过并行计算提高计算性能。

PlatON是一种区块链数据可信扩展。她通过MPC算法将链下多方数据在保证隐私性的前提下引入到智能合约，使用可验证计算和时间承诺的计算通道保证数据的有效性。

PlatON是一种可证明的状态转换函数。是基于零知识证明算法构建的状态转换函数，使得区块共识和同步过程中不需要在每个节点重复执行状态转换函数，可快速验证区块和交易的正确性。

3.2.1. 计算合约化

随着移动互联网、物联网、人工智能的高速发展，对数据的需求也日益臻于精准性、广泛性，与之相应的计算也越来越趋向于复杂化、规模化。如何有效获取计算资源和数据，是大规模复杂计算面临的巨大挑战。

大规模计算缺乏有效的激励手段。包括SETI（外星智能探索）项目、IBM的“World Community Grid”（WCG，全球网格大同盟）项目、BOINC（伯克利公开网络计算基础设施）在内的全球公共资源计算项目，都是致力于利用一切闲置的计算资源来进行科学的研究，如清洁水源、癌症治疗和清洁能源等。这些全球计算项目靠志愿者贡献计算资源来进行，只能吸引小众志愿者参与，缺乏有效的手段激励全球闲置计算资源的加入，并定义和执行相应的权利和义务。

大规模计算带来新的数据隐私问题。随着数据主权意识的觉醒，人们开始意识到数据的价值。人们在享受着推荐算法、语音识别、图像识别、无人车驾驶等智能的技术带来的

便利的同时，基于数据隐私的考虑，对于共享自己的数据疑虑重重。

为此，我们提出了“计算合约化”这一基本方式来面对以上问题。

PlatON支持大规模复杂计算合约化。PlatON用智能合约让计算具备相应的法律和经济属性，使得计算能以自组织的方式进行执行和激励。智能合约可以“释放数据的力量”，在鼓励数据充分共享的同时高度保护数据隐私。

3.2.2. 合约计算化

通过众多的POC（概念验证）应用，智能合约被验证可以应用到广泛的业务场景，但从目前的发展状况看，其性能问题和隐私问题仍然十分突出。

在PlatON中，创造性的将计算和共识解耦，将合约当中的计算部分分离出来，构造更高效、安全的计算。其特性包括：

- **计算本质化**

PlatON智能合约的计算逻辑均编译为布尔电路，回归计算本质。

- **计算并行化**

基于布尔电路，将计算任务拆分成更小的计算单元，分发到不同的提供算力的计算节点上进行计算，将实现真正意义上的并行计算。

- **计算扁平化**

基于布尔电路的计算逻辑直接在专用计算硬件中执行，省却一切中间环节。

- **计算隐私化**

全面使用安全多方计算、可验证计算、零知识证明等多种前沿密码学技术，用于强力的保护用户隐私、保障数据安全，以及验证计算结果的正确性。

3.2.3. 元智能合约

PlatON致力于服务计算世界，创造性的提出面向计算的智能合约体系“元智能合约（Meta Smart Contract）”。

- **多源数据支持**

元智能合约同时支持访问链上数据和链下数据，根据数据来源不同将元智能合约分为状态合约、无状态合约和混合合约三种类型。

■ 数据隐私保护

采用同态加密和安全多方计算算法保证数据的隐私安全。

■ 并行计算

PlatON中将元智能合约的计算逻辑拆分成多个子任务分，发给多个计算节点并行计算，提高元智能合约的计算性能。

3.2.4. 可验证计算证明共识Giskard

10 —— 11 —— 12 ——

主流的区块链技术体系目前还是使用PoW /PoS /DPOS 等共识机制或其变种，这些共识机制不可避免地普遍存在着以下问题：

■ 算力浪费

绝大部分共识都依赖于Hash挖矿，这种方式被公认存在极大的算力浪费。挖矿机制使用交易过程本地重放的方法来验证交易，也进一步浪费了大量算力，并造成共识周期过长，进而极大的影响了区块链的性能。

■ 算力中心化

据统计比特币和以太坊50%以上的哈希率分别在前四大矿工和前三大矿工手中，形成隐形寡头的权力治理架构。这已经偏离了中本聪设计比特币的初衷。

为解决这些问题，PlatON提出了基于可验证计算的加权权益证明共识方法Giskard。

■ 共识与计算分离

PlatON将共识与计算分离，算力只用于执行实际交易的计算工作，而不是用于挖矿，从而避免了算力浪费问题。交易的计算逻辑被进一步拆分成更小的计算任务，并可通过部署的一系列普惠策略将其分配给多个计算节点展开并行计算，配合有效的治理架构和激励体系，以此激励全球的闲置算力都能参与到真实的计算中来。在避免算力浪费的同时，也将网络中的权力解耦、分散，避免整个网络的算力中心化，从而求得开发者群体、计算者群体与数据提供者群体各方的动态博弈平衡。

■ 基于密码学证明的计算和交易验证

每一个计算节点在执行计算任务时都需要提交一个证明，用于验证计算结果的正确性。PlatON的共识节点打包的区块中直接包含交易结果及其证明，验证节点可通过密码学算法进行快速有效的验证，不需要采用交易本地重放的方法来验证交易，避免算力的浪费，同时也从整体上提升了区块链的共识效率。

PoW (Proof of work)

PoW (Proof of work)
工作量证明最早应用于
Adam Back 1996年提出的Hashcash中，而后被
中本聪改造为以“挖矿”
形式实现区块链一致性
的共识机制。PoW中，
矿工通过计算符合要求
的区块哈希值竞争生成
新区块的资格，同时获得
相应的币作为奖励。
而这整个过程中，矿工
贡献的算力就是上面所
说的“工作量”。

PoS (Proof of Stake)

PoS (Proof of Stake)
权益证明与PoW一致，
PoS也是需要提供一定
的证明来获得生成新区
块的资格，同时获得相
应的币作为奖励。不过
PoS (权益证明) 是用
“拥有的币龄”来证明自
己有资格写入区块链。

DPOS (Delegated Proof of Stake)

DPOS (Delegated Proof of Stake) 委托权
益证明的出块节点（见证人）由持币用户选举
投票产生，每个用户的
投票权重则按照用户持
币占系统总量比例计
算。选出的出块节点的
权利是完全相等的。从
某种角度来看，DPOS
有点像是议会制度或人
民代表大会制度。

■ 计算贡献值和诚实度评估

PlatON中，验证正确的计算工作量累积为计算节点的计算贡献值。计算贡献值相当于在PlatON体系中的信用评分及相应等级，用于衡量节点的计算贡献和诚实度。

■ 计算贡献值加权选举

为提高共识效率，PlatON以选举的方式选取部分节点参与共识。PlatON鼓励算力贡献者和诚实计算者，因此选举以计算贡献值加权后的权益为依据。每个用户拥有的选票数按照计算贡献值加权权益计算。共识节点候选人通过竞选产生，候选人排名也需要计算贡献值加权计算。

■ PBFT共识出块

13

选举出来的多个共识节点通过PBFT机制出块。

3.2.5. 专用计算硬件

PlatON中，智能合约的计算逻辑被编译成布尔电路进行计算，整个计算回归到与、非、异或等处理。而布尔电路的操作，天然与FPGA的架构相匹配，通过将智能合约转换成FPGA的布尔电路并通过FPGA来执行这些逻辑单元，就能够极大的提高运算效率和降低功耗/成本。

PlatON将在适当的阶段推出基于FPGA/ASIC的专用计算硬件，会极大提升整个区块链平台的交易性能，真正实践下一代计算架构当中的硬件部分。

3.2.6. 同构多链架构

PlatON为同构多链架构，根据应用场景不同可构建多条作为子链的应用链。PlatON的多链架构具有以下特点。

PBFT (Practical Byzantine Fault Tolerance)

PBFT(Practical Byzantine Fault Tolerance)是Miguel Castro (卡斯特罗)和Barbara Liskov (利斯科夫) 在1999年提出来的。PBFT是一种基于消息传递的一致性算法，算法经过三个阶段达成一致性。PBFT具备 $1/3F + 1$ 的情况下一致性是可能解决，N为总计算机数，F为有问题的计算机总数。

■ 用户账户统一

PlatON中，用户只需要创建一个统一账户，就可以直接使用多个应用链。

■ 资源多链共享

PlatON网络内置服务发现机制，节点提供的计算、存储、数据、路由等服务为基础服务，发布到整个网络，各应用链均可发现并集成。在PlatON中，应用链本身也是服务，网络中的节点可发现并加入任何应用链。

■ 多链路由

在PlatON网络中，区块链服务是“一点接入，全网服务”，即PlatON用户可以通过网络上

任意节点发起交易到任意应用链，而无需与目标应用链的任意节点建立直接连接。

■ 跨链转移及汇兑

每条应用链可独立发行度量衡体系，并可自由转移及汇兑。

3.3. 应用生态

3.3.1. 应用体系

PlatON将致力于建构基于下一代计算架构的全球价值交换网络，面向价值互联网时代数据资产化之后的流动性需求，建设面向全球的、跨行业的数据交换与协同计算基础设施，覆盖金融、医疗、物流、交通、传播、内容、零售、商业服务、供应链以及其他普惠民生的多个垂直领域。

PlatON亦将不断推出标准化服务，涵盖存证、溯源、积分、对账、清结算等基础服务，来供应用体系模块化使用，并基于此灵活的开发新的应用服务。

3.3.2. PlatON联合体

PlatON将会全力支持基于其之上的联合体，为各个应用链提供端到端、可交付的基础设施运营支撑和技术服务。

基于生产级的分布式计算架构、全球领先的密码学技术，以及全球合作网络强大的业务与技术运营能力，为加入PlatON的合作伙伴提供分布式、可扩展、可信任的数据交换与协同计算服务，保障数据安全及隐私保护前提下的数据共享。

PlatON从分布式商业基础设施这一原点出发，不断为生态级的合作伙伴提供更为完备的数据交换与转接清算服务，从基础的计算服务迭代升级到面向广义的数字权益、数字凭证、数字资产的转接交换基础设施服务。包括从传统中心化体系中单一的信用账户发行与受理方的服务模式，进一步过渡到为跨行业应用、跨数据主体、跨应用服务、跨网络节点的全账户数据提供“超级清算方”服务。

3.3.3. 开放的生态建设

PlatON是一个弹性网络，对身处其中的学术科研机构、开发者社区、ISV/SP、数据提供方、算法及应用提供方、算力提供方都将秉承公正、公开、透明的原则，相信自由市场带来的长期积极变化。

我们坚定的相信社区的力量，是因为我们充分相信开放性带来的冗余与激励正是PlatON

可以长久存续的根本原因和原生力量。

我们将致力于聚合社区的智慧与活力而不是唯我独尊、闭门造车；

我们将尊重各方的数据主权、隐私保护和治理共识而不是寻求主宰和控制；

我们将坚定的致力于社区的长期共同利益、鼓励温和且合理的经济利益与激励相容而不
会牟取暴利，或者其他不当的短期利益；

我们将全力谋求在全球各个国家和地区的合规安全，符合当地法律和行业监管要求，亦
尽最大可能契合当地社会不成文的风俗与约定；

我们将秉承开放社会理念全力以赴支持与其他社区的协同、共享与融合。

3.4. 隐私保护与合规性

3.4.1. 数据保护监管

自欧盟出台“史上最严格”的数据保护监管条例（《一般数据保护条例》）后，其他国家和地区均开始关注或着手制定相关政策法规。PlatON将坚定拥护和支持各国对个人数据保护的监管政策，我们将坚持“个人及任何实体的数据主权神圣不可侵犯”这一理念，并在PlatON平台上通过各种隐私保护算法和机制深刻践行。

3.4.2. PlatON的合规性

欧盟颁布的《一般数据保护条例》中，定义了“数据主体”，“数据控制者”、“数据处理者”、“数据接收者”、“第三方”等角色，并规定了数据控制者对数据主体的各项责任和义务，规定了数据控制者和处理者在数据处理、组织管理方面需遵从的规范。条例的出台使得各国拥有个人数据的企业或机构不仅需花费大量成本进行整改，而且很多依赖于个人数据的业务也将受到影响。

PlatON为数据控制者们提供了一种全新的数据处理模式——带有隐私保护的协同计算。不同于以往数据先被归集再处理的方式，PlatON的MPC算法可以在数据不离开本地的情况下仍能进行协同计算并得到期望的结果；不同于以往数据委托处理需转移数据给数据处理者的方式，PlatON的元智能合约可将计算任务而不是数据本身分发给各算力提供方进行计算。

PlatON将使大量的企业从“数据控制者”或“数据处理者”变为PlatON中定义的“计算请求方”或“算力提供方”，不再因拥有个人数据而承担相应的义务，从而节省大量合规成本；一部分“数据接收方”也将转变为“计算请求方”，不再获取数据，而只获取协同计算后的结果，另外，“计算请求方”或数据使用方的范围可能在符合监管要求的前提下扩大，如跨境的数据协作将成为可能；同时，因无需担心个人隐私遭到滥用或泄露，个人用户也更倾向于将数据授权给机构使用以获取经济上的或非经济上的收益，其“数据主体”的地位将更加牢固和安全，其对数据的主权、处置权等各项权利将牢牢掌握在自己手中；而PlatON将作为“第三方”，为平台的参与者提供完备的计算架构和运营服务。

第四章/技术架构

4.1. PlatON网络协议

4.1.1. 网络协议栈

¹⁴ PlatON的基本实现是全分布式结构化拓扑（Decentralized Structured Topology），完全基于RELOAD（REsource Location And Discovery）基础协议[RFC6940]和Kademlia协议[Kademlia]。下图为PlatON网络整体分层结构。

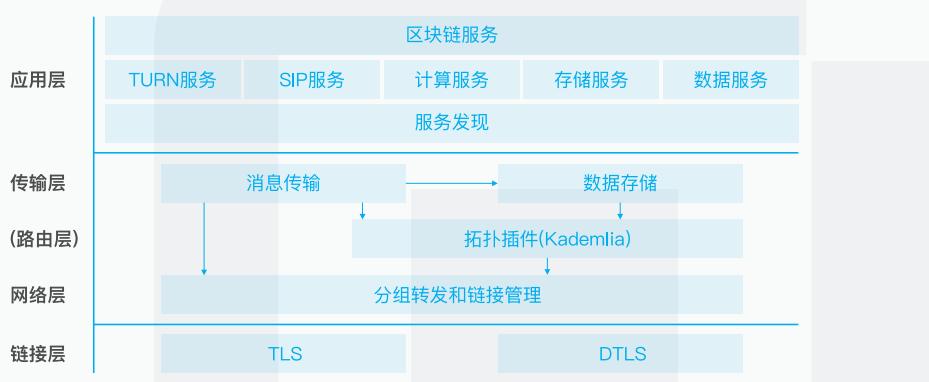


图1 PlatON网络协议栈(参考自RFC6940)

4.1.1.1. 链接层

链接层定位于实现数据的安全传输，提供多种传输协议来防止窃听、篡改、消息伪造；提供安全、可认证的连接；保证消息来源认证和消息数据的完整性。

本层实现安全传输层协议（TLS）和数据包传输层安全性协议（DTLS）。

针对密码算法，PlatON扩展实现为插件机制，可灵活支持国际标准算法（包括SHA256，SHA3，ECDSA、RSA、3DES、AES、RSA-OAEP、ECIES等）。同时将率先支持中国国密算法（SM2，SM3，SM4，SM9等）。

4.1.1.2. 分组转发和连接管理

负责提供分组转发服务来实现存储路由表，同时负责点对点建立连接，¹⁵ 包括位于NAT设备和防火墙后的节点。RELOAD使用ICE方法[RFC5245]实现NAT穿越。

全分布式结构化拓扑
全分布式结构化拓扑是P2P网络的一种拓扑形式，主要采用分布式散列表（Distributed Hash Table，简写成DHT）技术来组织网络中的结点。

4.1.1.3. 拓扑插件

RELOAD是一个P2P网络框架，支持扩展不同的拓扑算法来实现全分布式非结构化拓扑

NAT穿越 (NAT traversal)
NAT穿越 (NAT traversal) 涉及TCP/IP网络中的一个常见问题，即在处于使用了NAT设备的私有TCP/IP网络中的主机之间建立连接的问题。

或全分布式结构化拓扑网络。

拓扑算法可利用消息传输组件来管理消息的收发，利用存储组件来管理数据的存储。

拓扑算法与分组转发和链接管理层紧密配合，提供多种路由功能来满足不同需求。

PlatON网络采用Kademlia算法来实现全分布式结构化拓扑网络。

4.1.1.4. 数据存储

负责数据的存储，通过与拓扑插件的配合完成数据的复制、迁移等动作，同时与消息传输组件配合完成数据消息的收发。RELOAD支持字符串、数组和dictionary类型的数据存储。

4.1.1.5. 消息传输

负责对应用提供可靠的点对点消息传输服务。PlatON在RELOAD基础上扩展了分区泛洪算法来进行消息的快速全网广播。

4.1.1.6. 应用层

利用RELOAD底层的通信、存储能力来构建服务发现扩展，以及基于服务发现的TURN服务¹⁷、SIP服务、计算服务、数据服务、存储服务、区块链服务等。

以下章节主要描述应用层各服务的网络协议。

4.1.2. 服务发现

在P2P覆盖网络中，有些节点负责对外部提供服务，有些节点负责向其他节点请求服务，比如中继服务、语音邮件服务、网关定位服务、转码服务等。PlatON中也需要部分节点提供算力服务、TURN服务、SIP服务等。其中服务发现是关键问题所在。

4.1.2.1. ReDiR树

在P2P网络中，最简单的方式是在DHT中以一个特定的KEY保存所有提供某个服务的节点ID。但使用这种方法，将使存储节点的存储负载过大，而且会导致路由到存储节点的服务查询请求过多，造成消息处理负载过大。

为解决以上问题，PlatON使用ReDiR（Recursive Distributed Rendezvous）[RFC7374]来实现服务发现机制，ReDiR可以支持数万的服务提供节点及服务查询节点。

ReDiR使用树状结构实现P2P服务发现机制。同时使用RELOAD覆盖网络的存储能力保存数据，每一类服务都存储为一棵ReDiR树，树节点保存服务提供节点的信息。当某个节

TURN (Traversal Using Relay NAT)

TURN (Traversal Using Relay NAT) 是 STUN/RFC5389的一个拓展，定义了一种中继协议，使得 Symmetric NAT后面的主机能使用中继服务与对端进行报文传输。

SIP (Session Initiation Protocol)

SIP (Session Initiation Protocol) 是由IETF制定的多媒体通信协议。SIP是一个基于文本的应用层控制协议，用于创建、修改和释放一个或多个参与者的会话。这些会话可以是 Internet多媒体会议、IP电话或多媒休分发。

DHT (Distributed Hash Table)

DHT (Distributed Hash Table, 分布式哈希表)，是一种分布式存储方法。在不需要服务器的情况下，每个客户端负责一个小范围的路由，并负责存储一小部分数据，从而实现整个DHT网络的寻址和存储。

点请求查找指定服务的提供者时，对ReDiR树做有限次的查找就可以找到离请求节点最匹配的服务提供节点。

ReDiR树节点使用RELOAD的dictionary结构存储服务提供节点，每一个ReDiR树节点属于ReDiR树的某一层（level），ReDiR树的根节点为第0层，根节点的子节点位于第1层，第一层的子节点位于第2层，以此类推。

ReDiR树每层容纳的节点数取决于分支因子 b ，每层最多容纳 b^{level} 个节点，每个节点用 (level, j) 来唯一标识，其中level为节点所在的层数， j 表示该节点为相应层中第 j 个节点。在每一层中， b^{level} 个树节点把第level层分为 b^{level} 个KEY空间。

所有服务节点映射存储到相应的KEY空间，每个KEY空间由一个树节点负责存储，树节点 (level, j) 包含的KEY范围为 $2^{\text{BitsInKEY}} b^{\text{level}}(j + \frac{b}{b})$, $2^{\text{BitsInKEY}} b^{\text{level}}(j + \frac{b+1}{b})$ ，其中 $0 \leq b < b$ 。树节点 (level, j) 中保存的资源ID取值为 $\text{hash}(\text{service}, \text{level}, j)$ 。

下图为分支因子为2的ReDiR树。

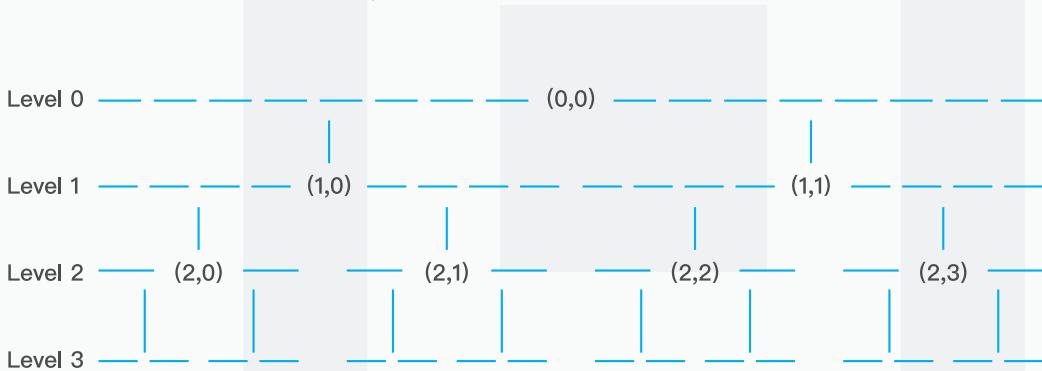


图2 分支因子为2的ReDiR树（参考自[RFC7374]）

4.1.2.2. 服务发布

在RELOAD覆盖网络中，节点ID为n，KEY为k的节点发布服务s的步骤如下：

■ 步骤一

选择一个初始层 $l = l_{\text{start}}$ ，一般为2。

■ 步骤二

节点n发送查询请求到负责KEY空间 $I(l, k)$ 的树节点，获取该树节点存储的服务节点列表。

■ 步骤三

节点n发送存储请求将自身信息存储到负责KEY空间 $I(l, k)$ 的树节点中。

■ 步骤四

检查第一步返回的结果，如果节点n的KEY值k是其中最大或最小的，则将当前level $l \leftarrow l - 1$ ，重复第2–4步，直到节点n的KEY值不是最大或最小，或者到达根节点为止。

同理，从 $l = l_{\text{start}}$ 层往下层遍历处理，直到满足以下条件为止：负责KEY空间 $I(l, k)$ 的树节点中，节点n为唯一一个服务节点。

4.1.2.3. 服务更新

注册到ReDiR中的服务状态都是动态的，服务节点需要定期重复服务发布流程来更新服务状态。若超时未更新，负责存储的树节点需要将其从存储中删除。

4.1.2.4. 服务查找

■ 步骤一

查找满足KEY为k的提供服务s的节点的方法跟服务发布类似，也是从一个初始层 $l = l_{\text{start}}$ 开始，每一步获取到KEY空间 $I(l, k)$ 中的服务节点列表，按照以下方法处理：

■ 步骤二

如果没有返回任何服务节点，则表明KEY(k)对应的服务节点存在更大的KEY空间，将 $l \leftarrow l - 1$ 然后重复查询，如果当前level为0则查询失败。

■ 步骤三

如果在返回的服务节点中，k不是其中最大或最小的，则表明对应的服务节点一定存在 $I(l, k)$ 的子空间中，将 $l \leftarrow l + 1$ 然后重复查询。

否则，返回的结果为最接近KEY(k)的服务节点，查询成功。

4.1.3. TURN服务

RELOAD使用ICE方法[RFC5245]实现NAT穿越，因此需要网络中部分节点提供TURN服务[RFC5766]。

节点在发布TURN服务时，使用服务发现扩展协议进行服务发布和更新，将自己发布到KEY空间 $I(l, \text{NodeID})$ 中，NodeID为服务节点ID。节点在发布TURN服务前，需要检测节点本身是否已经在NAT设备或防火墙后，如是则不能对外提供TURN服务。

需要使用TURN服务的节点在覆盖网络上查找TURN服务节点时，查找KEY空间 $I(l, \text{NodeID})$ ，NodeID为自身节点ID，用于查找最接近自己的TURN服务节点。

4.1.4. SIP服务

得益于PlatON网络中RELOAD作为基础架构呈现出的高度灵活性，基于P2P能力在应用层实现了SIP服务，支持P2P之上的SIP会话能力。这样PlatON可以方便地在节点之间建立会话，用于多方计算的协商，也可以用于构建上层的IM应用。

PlatON的SIP服务实现P2PSIP协议[RFC7890]，参考模型如下：

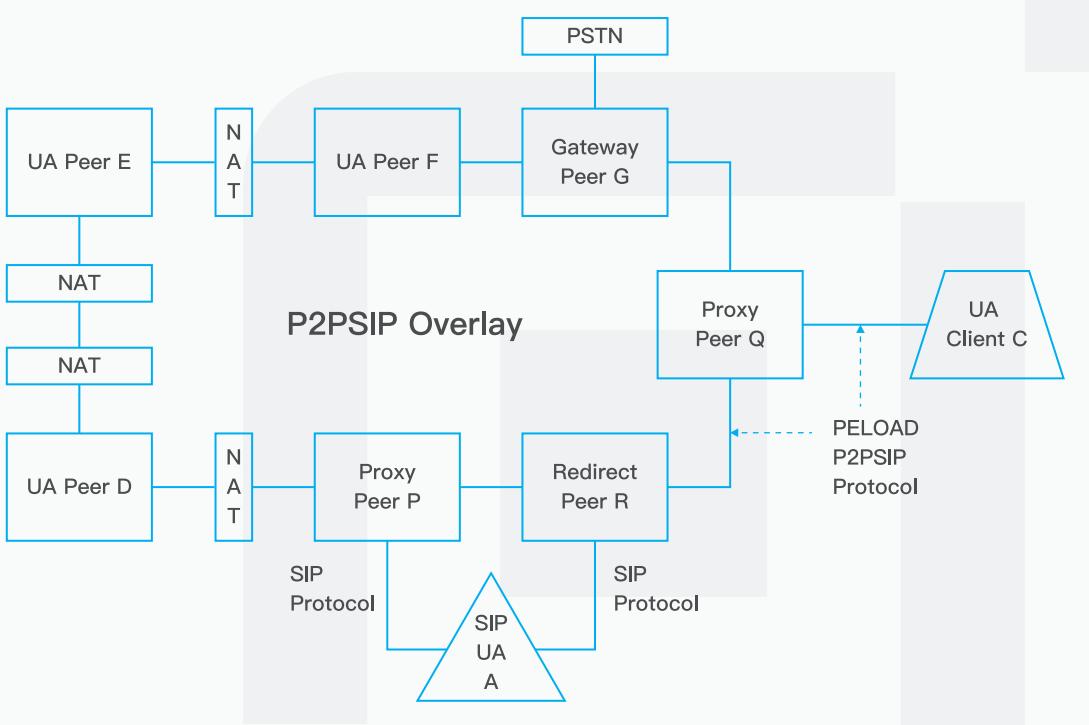


图3 P2PSIP覆盖网络参考模型(参考自[RFC7890])

上图中，由多个节点和一个客户端构成一个典型的P2PSIP覆盖网络（Overlay Network）。

尽管节点D和E位于NAT网关之后，这两个节点仍然属于P2PSIP覆盖网络，并参与资源信息存储和消息路由。

客户端C使用RELOAD协议跟代理节点Q通讯。C使用RELOAD协议从覆盖网络中获取信息，但是自己不加入覆盖网络，也不参与资源信息存储和消息路由。

图下方的A也不是覆盖网络的一部分，只是作为普通SIP节点或客户端。A使用传统的SIP协议跟节点P或Q交互，通过P或Q跟覆盖网络其他节点进行通讯。

P或R实际充当了普通SIP设备与覆盖网络之间的协议适配器。

19

同样，G的作用也是覆盖网络与PSTN之间的协议适配器。

PSTN (Public Switched Telephone Network)

PSTN (Public Switched Telephone Network) 即我们在日常生活中常用的电话网，是一种以模拟技术为基础的电路交换网络。

4.1.5. 计算服务

如何高效的进行计算节点间通信在PlatON中变得十分重要。建立在RELOAD协议基础上的计算服务，实现了计算服务的发布、计算服务的发现、计算会话的建立等。

4.1.5.1. 发布算力服务

计算节点加入PlatON网络提供算力服务，在注册为算力服务提供方之前，需要利用²⁰STUN协议[RFC5389]来判断出自己是否在NAT设备后面。如果已经在NAT设备后面，则需要通过服务发现找到一个TURN服务来为自己提供公网的服务能力。计算节点需要把自己的IP地址或从TURN服务获取到的Relay地址注册到PlatON网络。

计算节点在发布算力服务时，使用服务发现扩展协议进行服务发布和更新，将自己发布到KEY空间 $I(l, power)$ 中，power为节点提供的算力。

STUN (Session Traversal Utilities for NAT)

STUN (Session Traversal Utilities for NAT) 是一个轻量级的协议，可以被终端用来发现其公网IP和端口，同时可以检测端点间的连接性，也可以作为一种保活(keep-alive)协议来维持NAT的绑定。

4.1.5.2. 发现算力服务

PlatON计算时，需要根据算力匹配计算节点，使用服务发现扩展协议查找KEY空间 $I(l, power)$ ，power为需要的算力参数。

4.1.5.3. 计算任务分发

PlatON在RELOAD基础上封装了计算任务分发协议，把计算任务通过P2P通讯分发给提供算力服务的计算节点。为保证计算的可靠性和性能，计算任务分发保持一定的冗余度，即同时分发给多个计算节点。

4.1.5.4. 安全多方计算协议

PlatON在RELOAD基础上封装了GC和OT的协议，以支持安全多方计算。安全多方计算中多个数据方通过SIP协议建立计算会话。

4.1.6. 区块链服务

区块链服务的节点使用RELOAD框架的消息传输组件进行交易数据的转发和区块数据的同步，以及共识过程中的点对点的通讯。

4.1.6.1. 区块链节点的加入

多个区块链可以同时运行在PlatON网络中，区块链在PlatON网络中也作为一种特殊的“服务”存在，节点选择加入指定的区块链时，需要使用服务发布方法将自己发布为指定区块链服务（服务名为指定区块链名称）的提供者。

客户端发起交易时可以使用服务发现方法根据区块链名称查找到指定区块链的节点，并向其发起区块链交易。

4.1.6.2. 交易数据的转发

利用RELOAD消息传输组件的快速广播能力，区块链交易能够迅速扩散到全网并打包到区块中。

4.1.6.3. 区块数据的同步

PlatON中，每个全节点都保持一份区块链的完整副本，区块经过共识后广播到整个RELOAD覆盖网络，各节点接收验证成功后保存到本地。

区块数据使用RELOAD消息组件的广播功能进行同步。

4.1.6.4. 可验证计算证明共识协议

Giskard共识算法中，基于计算贡献值加权权益选举出共识节点，该选举过程就是区块链交易。选举出来的多个共识节点通过PBFT协议出块，PBFT协议基于RELOAD协议实现。

4.2. PlatON网络结构

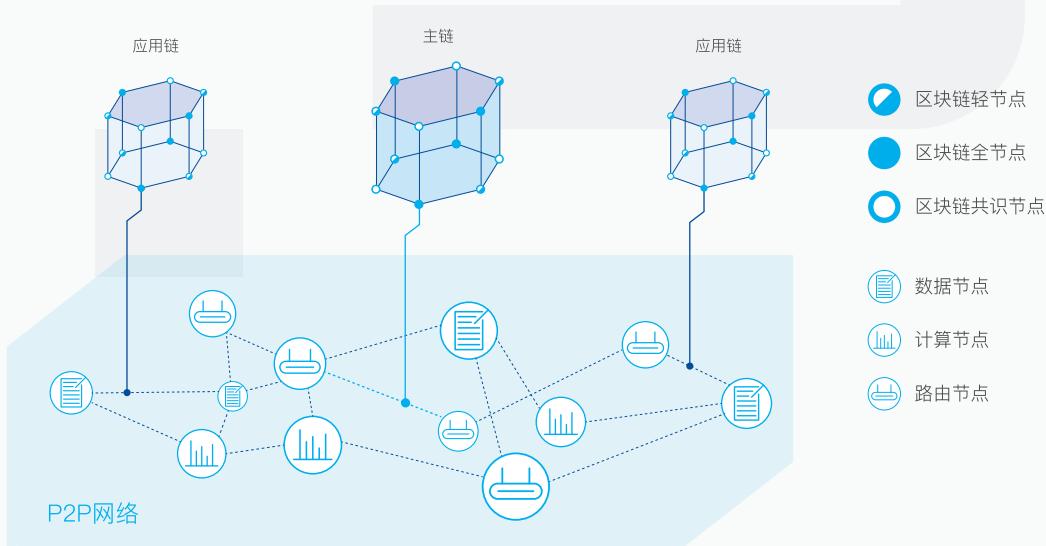


图4 PlatON网络结构

PlatON网络是一个RELOAD覆盖网络，所有节点都需要加入到RELOAD覆盖网络；每个节点拥有自己的节点ID，因此可以在RELOAD覆盖网络上根据节点ID找到任何节点的路由信息。

在RELOAD覆盖网络之上，存在多条逻辑意义上的区块链，每个节点可选择加入某一条或多条区块链，成为该链的节点。在RELOAD覆盖网络中，每条区块链就是一类服务；加入一条区块链，也就意味着该节点在RELOAD覆盖网络上把自己注册成为相应区块链服务的提供者。

PlatON网络中的节点还可以独立于区块链之外提供一些特定服务，如TURN服务、SIP服务、计算服务、数据服务、存储服务等。这些服务可以供网络上所有区块链使用。提供服务的节点可以获取不同形式的、可度量的经济激励及社区奖励。

4.2.1. PlatON节点

按照提供服务类别，PlatON网络中的节点分为两类：

4.2.1.1. 基础服务节点

■ 计算节点

为PlatON网络提供算力服务的节点，负责完成各种计算任务。

■ 数据节点

为PlatON网络提供数据服务的节点，负责为各种计算任务提供数据。

■ 路由节点

PlatON网络的节点可以部署在私有网络内，私有网络内的节点可通过路由节点实现NAT穿越，路由节点提供STUN和TURN服务。

4.2.1.2. 区块链节点

■ 轻节点

不保存所有区块的数据，只保存区块头信息以及跟自己相关的信息，依赖全节点进行快速交易验证。轻节点参与交易和区块信息的全网广播。

■ 全节点

保存了所有区块的数据，可以在本地直接验证交易数据的有效性。全节点参与交易和区块信息的全网广播。

■ 共识节点

负责执行交易并把交易数据打包成区块。在Giskard共识协议中，共识节点基于计算贡献值加权权益选举产生，并通过PBFT协议达成共识。

4.2.2. 多链路由机制

在PlatON网络中，区块链服务是“一点接入，全网服务”，即PlatON用户可以通过网络上任意节点发起到任意区块链的交易，而无需知道目标应用链的节点地址。这意味着区块链路由对于用户来说是透明的。

在PlatON网络中，每条区块链就是某一类服务，每个区块链节点加入指定区块链的同时，也将自己注册成为相应应用链的服务提供者。区块链节点使用服务发现协议进行服务发布和更新，将自己发布到相应区块链服务的KEY空间 $I(l, \text{NodeID})$ 中，NodeID为区块链节点ID。每个区块链服务在整个PlatON网络上最终构成一颗ReDiR树。

PlatON用户可以连接到网络上任意节点，通过该节点在指定区块链的ReDiR树当中查找 KEY空间 $I(l, \text{random})$ ，其中random为随机Hash值，用于随机查找一个指定区块链节点。查找成功后，就可以直接连接到相应节点向指定区块链发起交易。

4.3. 共识与计算解耦

包括以太坊在内的传统区块链技术体系存在一个共同问题，即交易执行和区块共识都严重依赖共识节点串行处理，整个区块链网络仅能支持单机的计算性能，全网算力得不到充分利用，从而造成性能瓶颈。如果将交易执行从共识节点分离，从而改由独立的计算节点来并行计算，将能切实的提高交易性能。

传统区块链也是一个封闭的计算环境，智能合约只能访问区块链内部数据。基于数据主权和数据隐私考虑，数据拥有方不愿意将数据保存到链上，使用密码学加密保存会导致数据量的急剧扩张和智能合约处理能力的降低。

然而，即使数据拥有方愿意将信息上链，但如果所有信息都上链，则必然会导致区块膨胀和智能合约处理能力的降低。

只有独立的计算层才能够解决以上所述问题，这也是PlatON网络的核心设计思路。

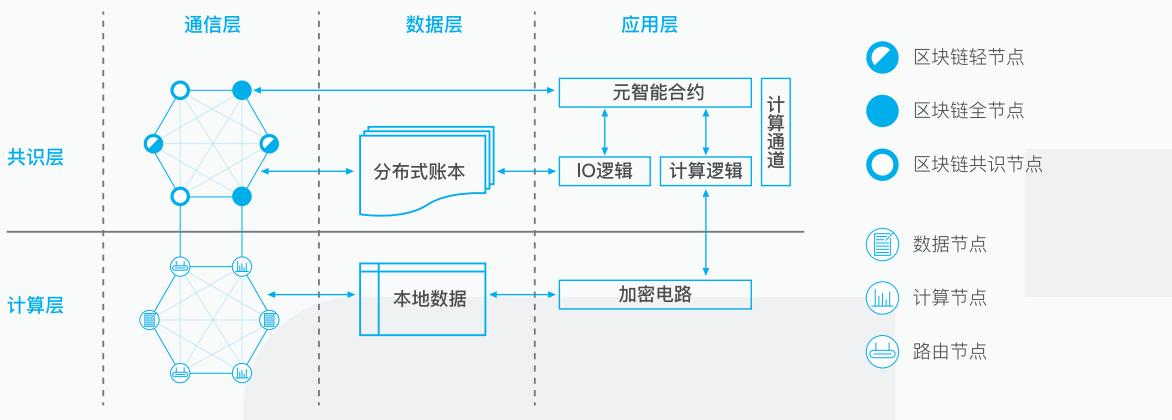


图5 共识与计算解耦架构

PlatON中的智能合约被定义为新型智能合约“元智能合约”。

元智能合约是数据和算法的封装，其数据源可以是链上分布式账本，也可以是链下数据节点的本地数据。但不管链上还是链下数据，其计算处理过程是一样的，因此PlatON设计为将共识层跟计算层解耦，并定义为元共识和元计算。

外部客户端通过交易触发元智能合约执行，元智能合约的执行由共识机制选择的共识节点来执行。共识节点同时负责将交易和分布式账本的更新数据打包成区块。

元智能合约包含IO逻辑和计算逻辑，IO逻辑负责读写链上数据，计算逻辑被编译成布尔电路（Boolean Circuit），并分拆为多个并行计算任务，通过PlatON网络将计算任务分发到空闲的计算节点进行可验证计算。

如果涉及到多方数据（包括链上数据，链下多个数据提供方的本地数据），为保证数据隐私，各个数据提供方（共识节点作为链上数据的提供方）将联合执行安全多方计算（Multi–Party Computation）来获取计算结果。

为进一步保证计算的安全性和有效性，计算凭证和结果证明需要写入一个名为计算通道的系统合约。计算通道数据保存在分布式账本中。

通过将计算和共识分离，提高了PlatON的吞吐能力和交易性能，同时也避免了算力的过度集中，从而进一步提高PlatON网络的安全性。

4.4. 元计算框架Monad

计算本质上由算法、数据和算力构成。

PlatON元计算框架的目的就是有效整合全球范围内异构的算法资源、数据资源、计算资源，从而深刻而广泛的促进数据交易和算力交易。

PlatON采用的元计算框架在使用并行计算和专用计算硬件提高计算性能的同时，也集成了多种密码学算法保证计算的可验证和数据隐私。

PlatON元计算框架集成了安全多方计算、可验证计算、同态加密、零知识证明等密码学算法。

4.4.1. 元计算定义

Monad是一种区块链扩容计算的实现。通过将计算扩展到链下，使得算力可以线性扩容；使用并行计算和专用计算硬件提供计算性能的同时，集成多种密码学算法来保证计算的可验证性和数据隐私。

4.4.2. 元计算参与方

在元计算框架中，计算参与方按能力类型分为计算发起方、算法提供方、数据提供方、算力提供方、计算协调方。

4.4.2.1. 计算发起方 U

一般指外部用户，其通过客户端发起元智能合约的调用，从而触发计算。

4.4.2.2. 算法提供方 A

特指元智能合约的发布者。算法包含在元智能合约中，其定义了计算逻辑和输入输出数据格式，计算逻辑被编译成布尔电路（Boolean Circuit）。算法随元智能合约一起发布到PlatON平台。

4.4.2.3. 数据提供方 D

在PlatON平台中，数据提供方也称为数据节点，数据保存在数据节点的本地数据库中。

数据提供方根据算法定义的输入数据格式，提供相应数据用于计算。

共识节点是一类特殊的数据提供方，共识节点实际上是链上数据的提供方。

4.4.2.4. 算力提供方 P

接收并执行计算任务（包含算法和数据）。在PlatON网络中也称为计算节点。

4.4.2.5. 计算协调方 C

计算协调方负责获取数据，并将数据和计算逻辑一起构成计算任务分发给算力提供方进行计算。计算协调方一般而言也是数据提供方。

4.4.3. 元计算任务

4.4.3.1. 计算数据源

元计算任务的数据可分为单源数据和多源数据。

■ 单源数据

数据来源于单个数据提供方，该数据提供方如果是共识节点，则数据来源于链上。

■ 多源数据

数据来源于多个数据提供方，包括链上和链下的多个数据提供方。

4.4.3.2. 计算分类

元计算支持多种形式的计算任务。可分为可验证代理计算和隐私代理计算。

■ 可验证代理计算

计算过程中不需要保证数据的隐私，当算力提供方完成计算后，在返回计算结果的同时也返回正确执行的证明，由计算发起方进行验证。

对多源数据而言，各数据提供方各自进行可验证代理计算。

■ 隐私代理计算

计算过程中需要保证数据的隐私。单源数据和多源数据都适合进行隐私代理计算，但是使用的密码算法不一样，后面章节将会分开阐述。

4.4.4. 计算通道

PlatON的计算通道（Computing Channels）实现为一个特殊合约，该合约通过可验证计算和时间承诺保证计算的有效性。

计算通道预扣交易发起方一定量的Energon作为计算任务的质押，任务结束且完成结算之

后，再将剩余的Energon返回给交易发起方。

计算结束时，每一个参与方都可以往计算通道合约中发送一个交易，从而关闭这个通道并启动一个结算过程。但计算通道不会马上进行结算，会先启动一个时间区间，在该区间内任何参与方均可对于计算过程提交异议申诉。

因此区块链就可以被视为某种“密码学法庭”，作为PlatON网络中一种成本较高的仲裁手段。这是用于提供交易安全性的最后手段，也因此极大的降低了造假和欺诈的动机。

当然，经过长期验证的有效工作量证明和交易结果证明已经可以很好的保证计算的有效性，这种仲裁手段仅作为交易安全的强有力补充和最终保障。

4.4.5. 计算任务执行

4.4.5.1. 计算资源分配

当计算节点加入网络时，将自己发布为计算服务。发布服务时，该节点会自动检测和评估自己的计算能力并发布为服务能力参数。

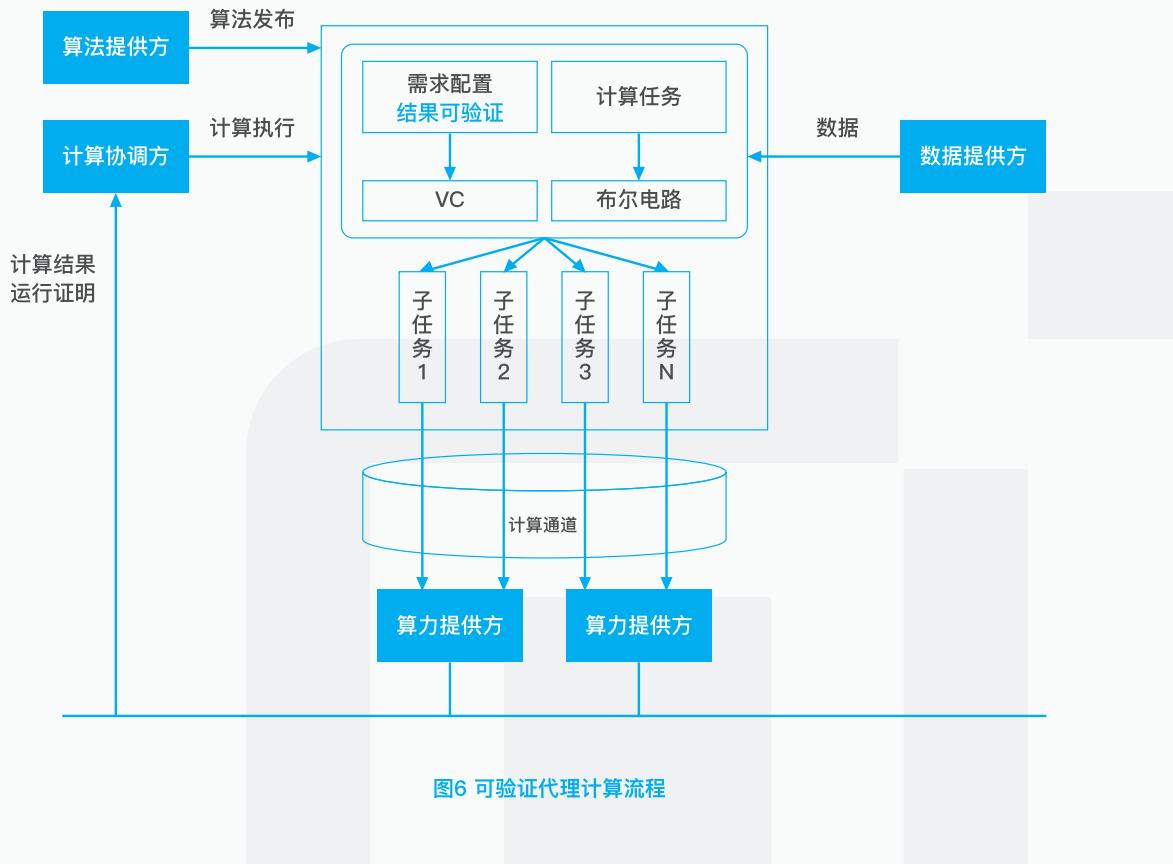
当计算协调方试图发起计算任务的分发时，首先需要从网络上查找能力匹配的计算节点。使用服务发现协议在网络上随机查找符合算力需求的计算节点，并根据计算贡献值排序，选择计算贡献值高的计算节点。为保证公平性，鼓励更多的节点提供算力服务，还将随机选择一部分新加入的计算节点。

4.4.5.2. 可验证代理计算

计算发布者在发布计算逻辑时指定“可验证”为计算需求。合约执行时，计算协调方配置VC算法的相应参数，并将合约中的布尔电路拆分成多个子电路。

计算协调方将VC算法参数、子电路以及输入数据整合成多个子任务，并分发给多个计算节点。为保证计算的可靠性，同一个子任务会同时分发给多个计算节点，从而保留一定的计算冗余度来做相互校验。

计算节点在进行子任务计算的同时，利用VC算法生成正确执行的证明，并返回给计算协调方。证明验证通过后，计算协调方按照算力提供方计算的门电路个数，累加加权计算贡献值之后按照一定比例分配奖励。



4.4.5.3. 单源数据隐私代理计算

单数据源可在不泄露原始数据的前提下利用全网的计算资源。当合约执行时，计算协调方配置同态算法以及VC算法的相应参数，并将合约中的布尔电路拆分成多个子电路。

计算协调方将数据进行同态加密后结合VC算法参数把计算任务拆解为多个子任务，并分发给多个计算节点。为保证计算的可靠性，同一个子任务会同时分发给多个计算节点，保留一定的计算冗余度。

计算节点根据子电路进行密文的同态计算，同时采用VC算法证明其执行的正确性。计算节点把加密的计算结果以及计算证明返回给计算协调方。计算协调方首先在验证证明的有效性后，对密文进行解密获取结果。计算协调方按照算力提供方计算的门电路个数，累加计算贡献值，并按一定比例分配奖励。

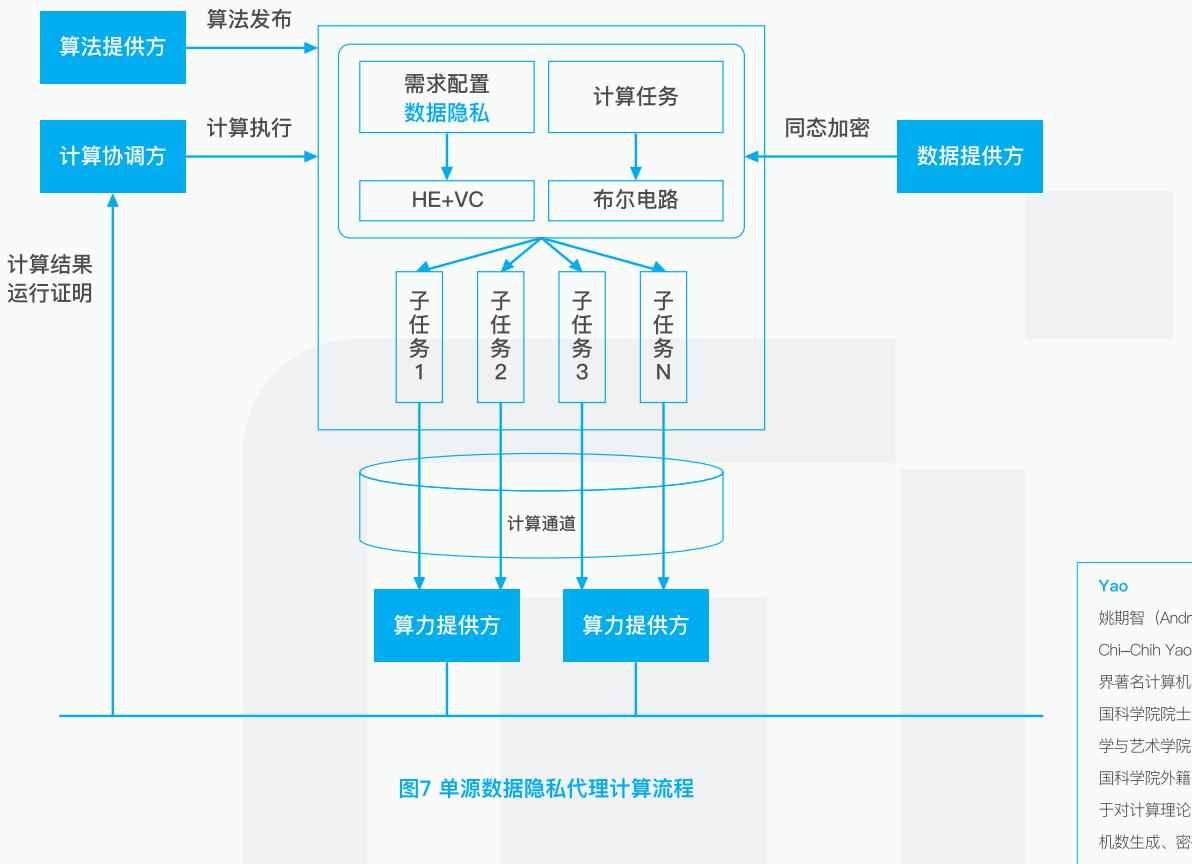


图7 单源数据隐私代理计算流程

4.4.5.4. 多源数据隐私代理计算

多个数据源可协同发起计算任务得到计算结果，并且保证各方对数据的所有权。多源数据计算的隐私保护采用MPC算法。

²¹ ²² 安全多方计算采用经典的Yao 的加密电路 (Garbled Circuit) 方法。简单而言，加密电路方法有一个生成方和执行方。

生成方按照电路将电路中的每一条线选取一个随机数作为标签 (label)，并按照电路的逻辑对每一个门用输入的标签加密输出的标签。最后将普通的布尔电路转化为加密电路。执行方与生成方之间运行OT协议获取与双方输入相关的标签，解密电路最终获取计算结果。

合约执行时，共识节点作为GC生成方发布计算任务，配置GC生成算法和VC算法参数。共识节点随机选取标签（标签的选法与具体的GC算法相关），将计算任务按子电路及标

Yao
姚期智 (Andrew Chi-Chih Yao) 先生，世界著名计算机学家，美国科学院院士，美国科学院与艺术学院院士，中国科学院外籍院士。由于对计算理论包括伪随机数生成、密码学与通信复杂度的突出贡献，2000年获得图灵奖。

加密电路 (Garbled Circuit)
加密电路 (Garbled Circuit) 最早由姚期智先生提出的对电路进行加密的方法，是安全多方计算中最常用的工具之一。

签分成多个子任务并分发给多个计算节点计算，最终得到多个加密子电路。计算节点在进行子任务计算时，同样需要用VC算法生成正确执行的证明，并返回给共识节点验证。

同时，数据提供方作为GC执行方与GC生成方之间运行OT协议，获取与其输入相关的标签。这个过程可以和GC生成方发布计算任务并行进行。

GC执行方在获得标签和加密电路后，可以再发布计算任务对电路进行解密。其发布方式与GC生成方发布的方式类似，只是为其计算需求配置的为GC解密算法。

通过将消耗资源的电路加密和解密过程以计算任务的形式分发给计算节点，利用激励机制引导各种算力来参与进行并行计算。将可以充分利用闲置计算资源，极大的促进数据的安全流动和隐私保护。

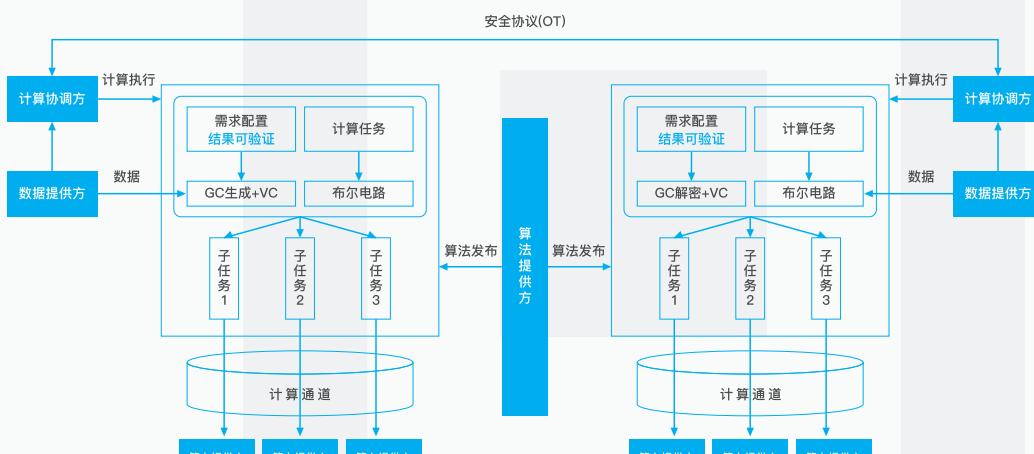


图8 多源数据隐私代理计算流程

4.4.6. 专用计算硬件

在PlatON中，每个元智能合约的计算逻辑都被编译为相应的布尔电路，构成布尔电路的基本门电路天然地和硬件架构匹配，通过硬件平台来执行布尔电路将可以极大的提高运算效率，并降低功耗及成本。

PlatON将会分为以下几个阶段来推进专用计算硬件的研发与部署：

■ 第一阶段

设计适用的硬件IP，并利用FPGA实现相应的硬件设备；

■ 第二阶段

23

将IP授权给ASIC/ASSP/SOC厂商，协助这些厂商集成在其设计中，支持PlatON的计算框架加速；

ASSP

ASSP (Application Specific Standard)

Parts, 专用标准产品)

是为在特殊应用中使用而设计的集成电路。

■ 第三阶段

实现ASIC芯片，为生态合作伙伴提供芯片级的解决方案。

PlatON将会秉承开放态度与生态体系的各类合作伙伴充分合作，以推动下一代计算架构的全面部署。我们坚定的相信只有通过软硬件的协同进化才能彻底的提升网络性能，以此践行我们对于下一代计算架构的设想。

4.5. 可验证计算证明共识Giskard

为避免算力浪费和提高共识效率，Giskard共识不采用PoW方式，PlatON将会以选举的方式选取部分节点参与共识。

为选取真正积极参与和诚实计算的节点，将不采用传统DPOS的方式。

Giskard的选举以计算贡献值加权后的权益为依据。计算贡献值可衡量节点的贡献度和诚实度。

4.5.1. 计算贡献值

PlatON采用多维度、多属性的账户体系。账户体系中包含资金余额、计算贡献值等属性。这样的账户体系可更准确的刻画用户在整个网络中的行为画像。

计算贡献值是用户提供的经过验证的有效算力。PlatON中所有计算都展开为电路化，计算的消耗与门电路的个数成正比，并且每个门的消耗权重也各不相同。PlatON为每个门电路定义了计算贡献点，节点的计算贡献值为所有计算贡献点的累计值。

4.5.2. 可验证计算证明共识

“劳心者治人，劳力者治于人”。这一治理架构在全数字化世界将会面临全新的解构和解读。

计算是一切事务的基本过程和本质。劳心者与劳力者貌似分处不同阶层，但本质上都参与或者发起了计算过程。

在PlatON网络中，我们相信劳动创造价值。劳心者的一切权力源于劳力者，也应当从劳力者中产生，其所产生的所有决策也应当且需要满足劳力者的自然权利。当然劳动创造

价值的方式是多样化的，作为一个有包容性的社区，应该兼容包括计算贡献值维度在内的多种衡量标准，来做综合加权评估。这一理念将通过恰当的算法机制予以保障。

在PlatON网络中，共识节点通过选举产生。选举采用持续实时投票方式，选票根据包括计算贡献值在内的多维度因素进行综合加权评估，每隔一个时间周期根据投票情况重新确定下一轮参与共识的节点。

共识节点采用优化的PBFT算法出块并达成共识。恶意节点将被取消其作为共识节点的资格，并给予一定的计算贡献值扣除及经济惩罚。共识节点在执行打包交易时，将交易中的计算逻辑拆分到多个计算节点并行计算，每个计算节点在反馈计算结果的同时返回正确执行的证明。共识节点将结果与证明打包到区块中，其他节点只需验证证明确定区块的合法性，可以大大减少区块验证时间，提高交易性能。

候选节点的选举、投票和出块机制不仅是一个技术问题，更多的是社区理念和治理模式选择问题。在本技术白皮书中不做过多探讨，将会根据社区反馈意见在适当时机发布的生态治理方案中提出。

4.6. 元智能合约Sophia

PlatON 所采用的智能合约体系完全不同于传统智能合约。PlatON将致力于服务计算世界，创造性的提出面向计算的“元智能合约”。

4.6.1. 元智能合约分类

PlatON本质上是一个去中心化拓扑结构下的Serverless架构的分布式服务平台。元智能合约就是部署于其上的FaaS²⁴ (Functions as a Service) 应用。

用户只需要提交元智能合约代码到PlatON平台，就可以对外发布服务，且只需要为执行代码过程中消耗的资源付费。

PlatON将元智能合约分为以下三种类型：

FaaS (Functions as a Service)

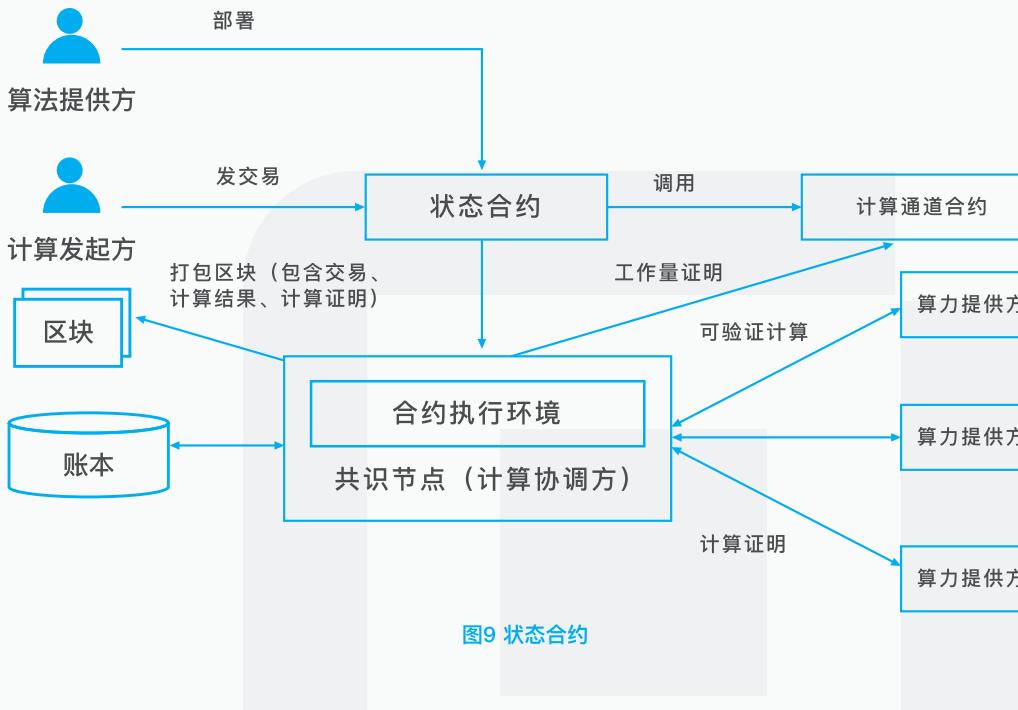
FaaS(Functions as a Service)是一种无服务器架构(Serverless Architecture)，FaaS 将函数转换为无状态服务，同时管理服务的生命周期，FaaS的每个函数都拥有快速启动和短暂生命周期的特性，在运行的时候才消费资源。

4.6.1.1. 状态合约

状态合约类似于传统的智能合约。

这类智能合约需要在链上保存状态，状态合约执行时输入的数据来自链上分布式账本，每次合约执行会导致合约的状态变更，所有变更均会被记录在分布式账本中。

合约的计算拆分成多个子任务分发给多个计算节点，合约开发者可以选择隐私计算的方式，以保证数据不透露给计算节点。



4.6.1.2. 无状态合约

无状态合约在链上不保存任何状态。

无状态合约执行时输入的数据来自链下数据提供方的本地数据库，可以是单个数据提供方，亦可是多个数据提供方。

单数据提供方的计算过程跟有状态合约相同；如果是多个数据提供方，则多方使用MPC算法进行协同计算，保证各方对数据的所有权。将实际的计算拆分成多个子任务分发给多个计算节点，合约开发者可以选择隐私计算的方式，以保证数据不透露给计算节点。

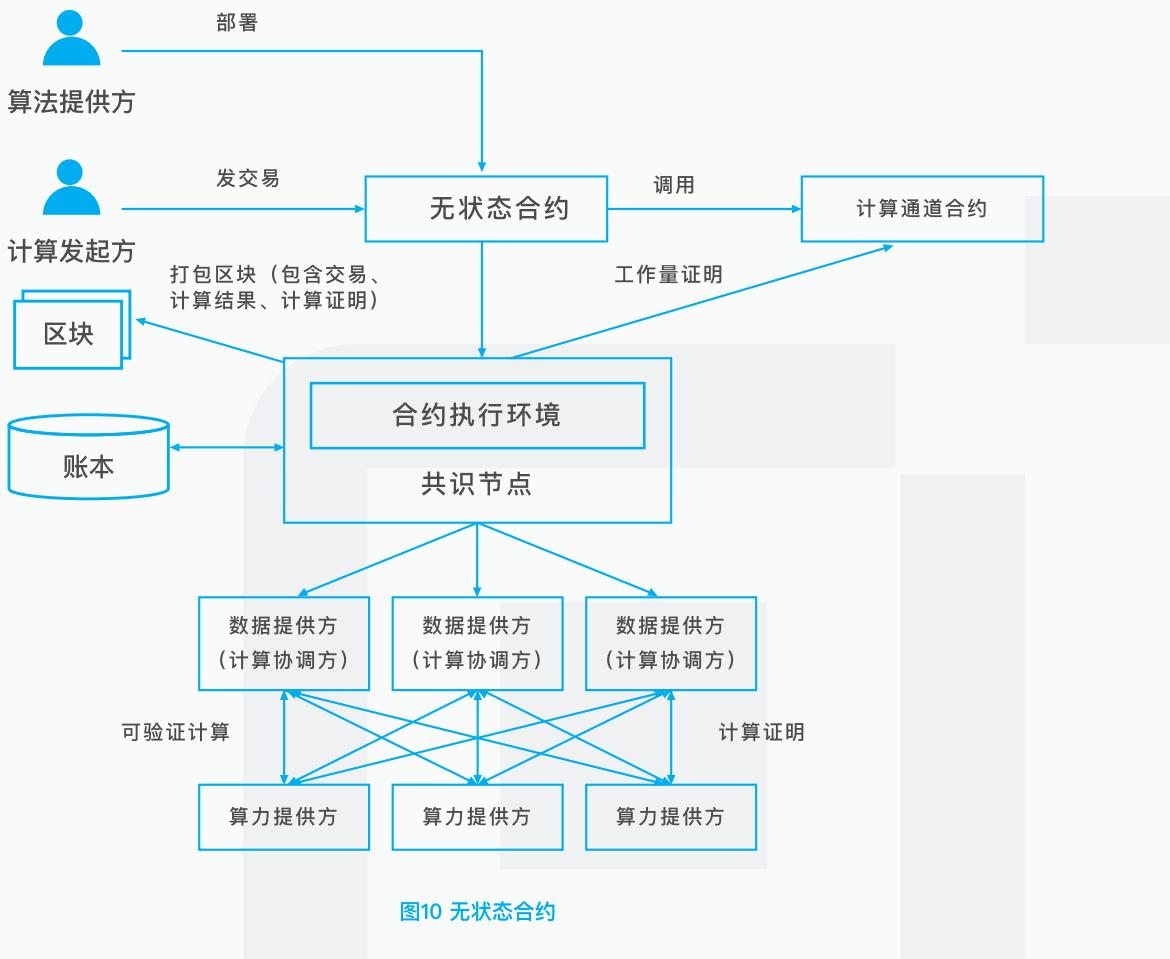


图10 无状态合约

4.6.1.3. 混合合约

PlatON也允许智能合约在链上保存状态，又存在有链下数据参与计算，这类合约称为混合合约。

混合合约本质上是一种多源数据计算，共识节点作为链上状态数据的数据提供方参与计算。混合合约典型的使用场景是把链下的数据计算结果保存到链上，并参与到下一次的计算中。

4.6.2. 元智能合约虚拟机

为适配并行计算和专用计算硬件，加速计算性能，PlatON把元智能合约编译成布尔电路来执行。元智能合约使用Java语言开发，PlatON提供编译器将元智能合约中的计算逻辑编译成布尔电路。

除了提供能直接运行元智能合约的专用计算硬件，PlatON也提供元智能合约虚拟机，可在各种软硬件环境下运行元智能合约，也供其他区块链项目集成使用。

第五章/能量块Energon

PlatON由一条主链和多个应用链构成。各链业务上相互独立，逻辑上相互平行。主链是PlatON网络的初始链，应用链是为解决特定行业问题而衍生出来的垂直链。

5.1. 能量块 (Energon)

PlatON是一个基于服务的计算架构，除了提供计算、数据、存储、网络等基础服务外，应用开发者也可在PlatON上发布自己的应用服务。PlatON上每个应用的运行都要消耗一定的资源（包括算力、带宽、存储、数据等）。为实现资源的公平合理使用，避免资源的滥用，PlatON通过一系列算法实现资源的合理调度和有效性验证，并使用Energon来度量资源的使用。Energon也是驱动PlatON这个“计算工厂”运转的能量。

25 ATP为PlatON主链的Energon，各应用链也可以创建自己的应用Energon。在PlatON网络中，用户只需要一个统一账户就可以管理和使用自己的Energon。不同链的Energon可以自由跨链转移。

关于PlatON当中Energon的定义、价值、发行、回收、费用等基本问题请参见PlatON经济生态红皮书，其中会有更进一步的详尽阐述。

ATP

ATP为PlatON主链中发行的Energon，可以跟内部应用链Energon进行转换和交换，也可以跟外部数字资产进行交易。ATP这个缩写可另表述为三磷酸腺苷 (ATP adenosine triphosphate)，是由腺嘌呤、核糖和3个磷酸基团连接而成，是生物体内最直接的能量来源。亦被称为生命体的“能量货币”。

5.2. 能量块交换合约

PlatON网络中Energon的跨链转移是通过名为能量块交换合约 (Energon Exchange Contract, 简称EEC) 的特殊合约来进行的，EEC合约内置在主链和各应用链中。EEC智能合约中使用双向锚定[Two-way Peg]和原子交换[Atomic Swaps]技术实现Energon的跨链转移。

5.3. 去中心化交易所

未来随着PlatON的不断应用和发展，PlatON上内部Energon间、内部Energon与外部数字资产（如USDT、BTC、ETH等）间转换和交换的需求也会不断地增加。中心化交易所提供了高效的交易性能，但也面临着巨大的内部欺诈和外部黑客攻击的风险，给用户带来资产安全问题。PlatON内置一个去中心化交易所，采用“链上挂单，链下撮合，链上交割”的方式，保证用户资产安全的同时，也兼顾交易撮合的性能和用户使用的体验。

PlatON去中心化交易所支持以下几种类型的交易形态：

■ 内部跨链Energon转换

PlatON通过设立Energon储备池实现内部Energon的转换，Energon储备池根据市场行情动态调整转换汇率，用户可通过跟储备池交易将某一条链上拥有的Energon汇兑成另外一条链上的Energon。储备池使用双向锚定[Two-way Peg]保证跨链转换的安全性。

通过Energon储备池，PlatON可增强Energon流动性，监控市场变化，并平抑市场投机。

■ 内部跨链Energon交换

用户可通过EEC合约进行链上挂单，链上交易可保证交换的透明性，交易同步到链下进行高效撮合，最后交换双方通过原子交换[Atomic Swaps]进行Energon交割，确保用户对Energon的完全控制，保证跨链交换的安全性。

■ 外部数字资产交易

PlatON支持在主链上通过抵押ATP来创建锚定外部数字资产(比如USDT、BTC、ETH等)的储备池，外部数字资产储备池根据市场行情动态调整汇率。通过外部数字资产储备池，PlatON可实现ATP跟USDT、BTC、ETH等外部数字资产进行交易。

第六章/用户客户端Edge

PlatON网络提供一个跨平台的通用客户端Edge（包括Web、Android、iOS等平台），以作为PlatON用户的统一门户。

Edge设计为社交风格，为用户提供易于使用的操作界面。Edge将全面支持以下各部分功能：

6.1. 数字钱包

支持PlatON网络私钥和Energon的安全管理，提供方便的点对点Energon交换。

- PlatON将发行硬件钱包用以安全保管用户密钥。硬件钱包实现签名、同态加密、零知识证明等密码算法。
- 使用MPC算法实现密钥多中心协同托管和恢复。
- 支持扫码等便捷的转账和收款方式。

6.2. 即时通讯 (IM)

Edge提供P2P版IM功能，计划采用以下技术实现点对点加密通讯（包括文本消息和音视频通话）：

- 基于ICE协议的NAT传输。
- 基于RELOAD协议的SIP/RTP/RTCP/RTSP协议栈。
26
- 音频Codec使用Skype的SILK。视频Codec支持VP8和H264。
27 ————— 28 —————
29
- AEC回声抑制算法，NetEQ算法等WebRTC音频技术。

6.3. Dapp 门户

开发者可以在PlatON网络上部署自己的Dapp（去中心化应用）。Edge是Dapp的统一门户。在Edge上可浏览查找部署在PlatON网络上的Dapp。Dapp可直接在Edge上运行。
30

SIP/RTP/RTCP/RTSP

RTP/RCP/RSP是一组定义为传输音频、视频等实时数据的传输协议，RTP是实时数据传输协议。RTCP是RTP的控制部分,是用来保证服务质量,和成员管理的。RTSP是开始和指引流媒体数据从流媒体服务器。

音频Codec

Audio Codec，音频编解码器，是指一种能够对数字音频流进行编码和解码的设备或计算机程序。常见的音频编解码器有AAC、AMR、Speex、SILK、MP3等。

视频Codec

Video Codec，视频编解码器，是指一种能够对数字视频流进行编码和解码的设备或计算机程序。常见的视频编解码器有H263、H264、MPEG4、VP8等。

WebRTC

WebRTC (Web Real-Time Communication)，是谷歌2010年以6820万美元收购GIPS公司而获得的一项技术。WebRTC提供了视频会议的核心技术，包括音视频的采集、编解码、网络传输、显示等功能，其中回声抑制 (AEC)、噪声抑制 (NR)、自动增益 (AGC)、自适应抖动控制及语音包丢失隐藏算法 (NetEQ) 是WebRTC中的几个极具价值的技术。

Dapp (Decentralized Application)

Dapp (Decentralized Application) 是运行在底层区块链平台上的分布式应用。Dapp是基于智能合约的应用，由智能合约和前端App构成，智能合约运行在去中心化的区块链节点上。

6.4. 前端应用运行环境ERE

31 —

ERE (Edge Run-time Environment) 支持React Native 环境，前端应用可直接基于H5/JavaScript开发，并可直接在运行环境中运行。ERE内置PlatON网络协议，前端应用可直接访问PlatON，无需开发区块链网关提供中转。

React Native

React Native（简称RN）是Facebook于2015年4月开源的跨平台移动应用开发框架。RN使用Javascript语言以及CSS来开发移动应用，因此熟悉Web前端开发的技术人员只需很少的学习就可以进入移动应用开发领域。

6.5. Energon转移

用户可在Edge上便捷地进行Energon的安全转移：

- Edge实现友好的原子交换客户端，用户可直接进行无需信任的点对点Energon交换。
- Edge实现去中心化交易所客户端，用户可便捷地进行内部Energon间的转移、内部Energon与外部数字资产（如BTC、ETH、EOS等）间的交易。

第七章/应用与生态

PlatON将全面支持全球开发者社区基于本平台启动各类开发计划。我们诚挚的邀请来自各个领域的伙伴在PlatON上开发各类组件、算法、服务和应用，并可以针对某一特定技术方向或垂直领域开发应用链。各种应用以及应用链间通过主链交互和协作，建构全球一体的复杂网络和生态体系。

7.1. 数据交易

PlatON平台提供了全球数据协同计算的公共基础设施，在PlatON上可以建立安全的数据交换应用链及应用，为机构和个人提供安全可靠的数据交换和协同计算服务，让他们在数据共享的同时保护数据隐私，在保有数据所有权的同时享受数据再利用的经济收益。PlatON不仅提供了内置多种算法和协议，还搭建了数据交易市场，激励更多的参与者贡献自己的数据、算法和算力。

■ 协同计算和隐私保护

通过PlatON平台，可以整合全球多源异构数据资源和计算资源进行协同计算，并应用安全多方计算、可验证计算等密码学技术保证数据隐私和计算的可验证性。

■ 数据交易市场

在数据交易市场，拥有数据的机构和个人可以有效地对自己的数据进行管理和授权；数据需求方可以提出数据交易和计算请求，获取更多的维度、更大规模的数据或其计算结果；适用于更多场景的计算逻辑和商业逻辑将由算法提供方或运营方提供，并封装在智能合约中对外发布；而分散的算力资源也在此得到整合和利用。在这里，数据可以得到合理的定价，并进行充分的交换和共享，产生更大的价值。

■ 即时清结算

计算通道作为计算的控制验证层和结算层用于保证计算的有效性，为数据提供方、算法提供方、算力提供方等提供即时的清结算。

■ 高计算性能

在元计算框架中使用并行计算和专用计算硬件提高计算性能，可支持大规模的、更复杂的商业应用。

7.2. 科学计算

随着数据规模的爆发和人工智能等算法的优化，计算越来越趋于密集化，如大整数分解，外星智能探索（SETI）计划，气候数据分析等大规模的科学计算需要消耗大量的计算资源，通过PlatON平台，可激励和整合全球闲散的计算资源共同参与科学计算，让算力得到充分利用，让科研机构和商业团队能够进行更低成本、更有效率的科学计算。

■ 计算任务分解

科学计算的计算任务通常比较复杂，PlatON中“计算合约化”的特性可以将计算任务分解成大量分布式的子任务，由PlatON全网计算节点共同执行。

■ 算力路由

PlatON提供了算力发布、发现和路由的功能，可将计算任务通过P2P通讯分发给提供算力服务的计算节点，并以一定冗余保证计算任务执行的可靠性。

■ 经济激励

用PlatON的智能合约发布了计算任务后，智能合约即可以以自组织的方式进行执行，同时通过VC等算法提供计算正确执行的证明，为正确完成计算的节点给予经济奖励，以鼓励全球更多的计算资源参与。

7.3. 身份认证

基于PlatON的去中心化身份管理系统能够解决传统中心化系统存在的单点失效、恶意收集和滥用用户隐私数据等问题，实现去中心化的身份认证与管理。

■ 统一认证

去中心化身份管理系统可为用户生成链上唯一的身份标识，让用户在不同应用间实现统一的身份认证。

■ 用户画像拼图

个人或机构可能存在多种身份属性。去中心化身份管理系统可以将多种身份属性关联认证，利用PlatON上带有隐私保护的协同计算方案拼凑出完整的用户画像，帮助各机构更好的识别用户，以做出更优的商业决策或满足合规性要求。

■ 多重认证和交叉验证

对于每一次身份的认证均有记录，形成不可篡改的认证链条，实现信任的强化和传递。

同时，可设计身份数据的交叉验证机制，有效识别虚假信息，提高作恶成本。

7.4. 医疗健康

现有医疗IT系统建设在很大程度上非标准化，导致医疗机构之间系统存在数据格式不统一、接口不兼容等问题，难以实现数据的交换共享和协同计算，导致在现有系统下医疗领域的海量数据难以实现交换与互操作，进而限制了数据的进一步使用。

个人的医疗健康和基因数据在所有数据领域中隐私性要求最高、数据量最大。基于PlatON平台可构建医疗信息统一开放服务平台，为其设计统一、通用的数据共享和数据交换标准、实现不同组织机构间异构数据的互联互通，从而促进医疗和基因数据的进一步分析和使用。

基于PlatON平台构建医疗信息统一开放服务平台，医疗机构作为数据源和网络节点，可以动态加入/离开，满足系统弹性伸缩的要求。但实际数据仍然保留在医疗机构的本地系统，做到了对现有系统的最小化改变，充分保障了数据安全、各医疗机构的历史投资以及相关方利益。

■ 全球基因医疗数据库

可基于PlatON搭建数据索引、查询及交换的平台，整合全球各医疗机构和研究机构的医疗数据、基因测序数据、试验数据等，形成全球医疗健康数据库或数据目录，配合PlatON的安全多方计算和隐私计算等算法，促进医疗信息的共享和流通，以更好的服务于公共健康分析、药物研发、罕见病研究、专项病防治等需要大量数据协同的领域。

■ 个人统一健康账户

通过整合医疗、基因数据、个人自己产生的运动健康数据等，可形成个人全生命周期的健康情况追踪、连续的医疗信息和疾病预警等报告，在此基础上政府和各相关机构可以为公民提供更好的个人医疗服务、公共卫生服务、保险服务以及其他生活服务。

■ 数据医联体

PlatON将可以支持包括个人医疗咨询与服务、公共健康分析、药物研发、医疗研究、CRO、专项病防治在内的多个领域组建数据联合体，同时提供高效的审计监管和追踪溯源。

医疗数据、健康记录，以及用户产生的数据，如穿戴设备、运动监测、健康APP等数据，加

密和签名后存储在机构或个人的本地系统，确保数据的本地归属和安全，同时每一条数据的标签、Hash摘要存放在权限许可的应用支链上，通过严格的权限管理、智能合约、密码学技术，进行数据的安全查询、交换或交易。

经由PlatON网络的数据交易服务，可以有效降低交易摩擦和交易成本、全面对接各类数据拥有方和需求方。充分的实现医疗数据的流动性。

7.5. 征信体系

传统征信体系面临着典型的“盲人摸象”问题，深陷可信第三方数据来源单一和数据共享的困境。社会信用体系的建立依赖于大量个人信用数据的整合和分析，而传统中心化方式下只能依赖于可信第三方来进行数据归集和处理，数据以金融信贷信息为主，信用模型单一、应用受限。

除了传统的身份信息、银行信贷信息以及公共事业信息外，得益于社交网络、移动支付以及物联网的发展，还产生了更多可以反映个人信用的数据，如人际关系、行为偏好、非银信贷、健康运动等信息。这些海量数据直接导致中心化的数据存储及处理面临日益严重的效率和隐私保护问题。

基于PlatON，将可以全面重构隐私保护前提下分布式的社会信用体系，整合多源数据，开发不用场景下的信用模型，完善社会信用体系。

PlatON通过分布式数据交换与协同计算方式，对分散的个人信用数据进行安全计算，得到更准确的信用评级结果，降低全社会的信用成本、进一步完善社会信用体系。同时，PlatON可以提供一套激励机制和市场机制使得数据提供方、算法提供方、算力提供方均可获取一定收益，间接的为数据提供定价，从而激活海量数据的潜在价值。

■ 信用钱包

PlatON可为个人（数据提供方）提供一个安全的“信用数据钱包”，可以让个人在不担心泄露隐私的前提下管理本人的信用和数据；为企业（数据使用方）提供算法、算力和计算结果，助其做出更高效准确的判断；为生态中其他成员（如算法和算力提供方等）提供更多参与行业生态建设的机会，催生新的商业模式。

■ 完善的信用数据

除在金融机构中产生的信贷数据外，个人在非金融机构（如民间借贷）产生的借贷数据、身份属性信息、行为偏好信息、人际关系信息等也可被记录在区块链上，并纳入信

用体系中，减少多重借贷、作假等行为，构造更完整、可信的数据基础。

■ 联合征信

应用MPC进行协同计算，多机构间可进行联合征信，得到更准确的信用评级结果，大大缩短征信时间，降低征信成本。

■ 共享信用模型和结果

数据的丰富和完整使得各机构可以根据业务场景不同建立多样化的信用模型，引入不同的参数和算法，对用户进行更精准的评价和服务。同时，这些模型和分析结果也可在数据隐私保护的前提下为其他机构所共享，提供方可二次获利，使用方也可降低成本，构筑良性的生态循环。

7.6. 社交网络

基于PlatON平台，可以构建下一代社交网络，支持跨地域和跨应用域的点对点人与人、人与物和物与物的通讯和数据交换，不依赖中心化的机构独立运作，具有去中心化、保护隐私、安全、激励相容等优势。

■ 价值创造与利益共享

社区可自定义规则，包括但不限于奖励创建和维护内容的用户、提供存储和算力贡献的用户、观看广告的用户等，鼓励所有用户创造更多有价值的内容，正向吸引更多用户参与，以使系统具有强大的内生驱动力。

■ 数据所有权

用户产生的数据所有权归属于用户个人，包括但不限于用户自己创造的文字、照片、视频、绘画、音乐等，这些创作的数字证明具有时间戳和Hash摘要，是一个天然的存证和版权登记载体。

■ 隐私保护

用户对属于个人的信息和数据可以灵活设置可见权限，设置为私有属性的信息，采用非对称加密保护，平台或任何其他人无法看到这部分数据，彻底保证用户隐私和数据安全。

■ 信用建立

用户在PlatON网络中的创作、活动参与、事件评价等行为，写入区块链后具有不可伪造、不可篡改、不可销毁的特点。用户将可以在数字世界建立个人的信用、品牌与影响力。

7.7. 物联网及工业互联网

PlatON可以有效解决物联网发展中面临的大数据管理、信任、安全和隐私等问题，为大规模物联网部署提供基于数据安全和隐私保护的基础设施和依托于算力共享平台的边缘计算能力，促进物联网在智能制造、车联网、农业、智慧城市、分布式能源管理等领域应用模式的扩展，促进商业模式创新。

■ 高可信基础设施

基于强大的密码学算法与技术实现，PlatON为物联网提供可信的设备身份认证、多通道数据传输、数据存储等服务，确保数据的所有权和隐私权，加强物联网设备和系统的安全。

■ 算力分享平台

基于PlatON的新一代计算架构，可为物联网应用提供强大的算力支撑。可以将边缘计算的需求发布给平台，在平台内临近的计算设备之间进行及时、安全的计算，而无需每次返回中央服务器，以全面提升服务的时效性。同时，物联网设备也可将其多余的算力贡献给其他应用共享，从而提升物联网设备的使用效率和附加值。

■ 跨运营商设备数据的协同计算

物联网设备可能属于不同的服务提供商，基于PlatON提供的数据隐私保护能力，可以支持跨运营商物联网设备的数据协同分析，实现不同物联网应用的有效协作，提供更加复杂和多元化的服务，同时保障设备本体对其数据的所有权。

专用计算硬件加速

PlatON平台提供专用计算硬件生态支持。针对边缘计算的不同数据处理需求，可以提供FPGA/ASIC等专用算力支持。并可以根据应用端对参数的训练和固化需求，提供软件到FPGA/ASIC等多种资源，从而有效支持算法的参数训练或实时计算的算力支撑。

除以上案例之外，PlatON可被广泛应用于各个领域。以下是部分业务场景：

金融服务

资产权益证明和交易
数字票据
金融审计
支付清算
保险管理

教育

档案管理
学历和成绩证明
网络学习社区

智慧城市

公共安全
城市服务
智慧政务

社会管理

身份认证
社会信用体系
公证
社会公益

数字版权

数字版权认证与管理
数字内容分发和交易
侵权行为识别和维权
版权众筹

物联网

设备管理和认证
数据存证和交换
边缘计算
分布式能源管理

供应链管理

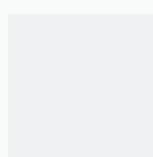
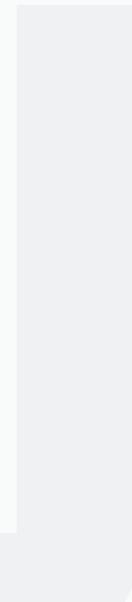
溯源和认证
物流仓储管理
供应链金融

共享经济

闲置物品共享和交易
能源共享
知识技能交易

医疗健康

病历共享
个人健康档案
全球协同研究
基因检测和追踪



■ 第八章/技术路线图

PlatON项目的技术路线如下图所示：



- **贝莱世界 (Baleyworld)**：实现完整的RELOAD覆盖网络和区块链服务，支持服务发现、元智能合约、两方MPC计算。
- **川陀 (Trantor)**：实现完整的多方安全计算、多链路由和去中心化交易所。
- **端点 (Terminus)**：实现并行计算、可验证计算、Giskard共识。
- **盖娅 (Gaea)**：实现软硬件一体化，发布专用计算硬件。

■ 第九章/社群的进化

9.1. 技术的进化

PlatON网络是一个处在开发初期、尚不足够完备的系统。目前给出的只是PlatON作为下一代计算架构的基本描述。必须指出的是，PlatON创造的复杂网络面临巨大的技术挑战，无论是分布式架构、密码学算法、博弈论机制的设计、硬件实现和网络建设都存在诸多问题，有待于学术界的理论突破和工程上的点滴探索。有些问题甚至是全人类共同面临的智力挑战。我们将依托全球社区的力量逐个解决、持续进化，并在未来的路线图中不断更新迭代。

9.2. 组织的进化

组织的进化某种程度上就是治理模式的进化。我们相信改良的力量，而不妄谈颠覆。人类社会在不同的组织结构和治理模式中试错、选择，以此循环往复求得最终的进步。

区块链开源社区在过去几年中也遭遇了多次类似的问题，社区的分裂、分叉、黑客攻击、合约漏洞、合规性挑战等等。但仍然保持了鲜活旺盛的生命力。

作为一个全球化的自组织形态的社区，PlatON在治理模式的设计和实践过程当中也会面临同样多的挑战，但会持续秉承共治、共享、共识的基本理念来解决所面临的治理挑战和异常。

PlatON的参与方也会从现有提供智能合约的开发者社区、提供算法和理论的学术社区、提供算力的计算社群、提供数据的数据社群和需求方，递次演进至更多参与方和参与者。其间利益必然有所不同，产生的矛盾分歧也必然不都是技术或者算法可以解决的。我们将会根据社区各个群体的反馈，逐步梳理和发布社区治理方案以适应未来。

PlatON作为一个复杂网络，不会刻意偏袒任何一方，只会一如既往的鼓励和支持更多方、更多机构、更多利益群体、更多个人参与这一网络。越是如此“复杂”，网络就越是强大和健壮。

我们坚信在数据主权日益彰显的时代：“部分不知道整体、整体不知道部分”。这既是密码学理论对隐私保护的实现，也是共识机制的价值之所在。

PlatON组织的进化，其逻辑基础源于共识，源于“同意的计算”。

9.3. 网络的进化

PlatON依托于全网共识、依赖于全球算力、数据、算法的共享、建构在社区共治的基础之上。其中网络基础设施是举足轻重的一部分。

我们将从现有互联网出发，始终跟随全球移动互联网、天基互联网建设运营的步伐，支持、适配乃至发起各种不同类型的网络基础设施和计算基础设施，最终目标是基于空、天、地一体的网络基础设施来推进PlatON的进步。

PlatON的网络进化过程，将会极大拓宽社区的视野，持续提升社区达成共识的能力。具体工作计划将会以网络建设白皮书的形式在适当时机发布，并定期更新。

脚踏实地，尔后，仰望星空。

以此九章“算”术，就此展开未来。

在未来，**一切皆可计算。**

术语表

中文	英文	缩写	解释
电路	Circuit	-	一种通用的计算表现形式，由不同类型的门（gate）组成。由逻辑门构成则成为布尔电路（Boolean circuit），由算术门构成则叫算术电路（Arithmetic circuit）。
安全多方计算	Secure Multi-Party Computation	MPC	无可信第三方场景下多个参与方协同计算，获取计算结果，并不泄露各自输入信息。
零知识证明	Zero-Knowledge Proof	ZKP	证明者让验证者确信某个事实的正确性，并不泄露其他任何信息（零知识）。
可验证计算	Verifiable Computation	VC	可有效验证结果数据是否按照原始数据依照指定逻辑计算而来。
(全) 同态加密	(Fully) Homomorphic Encryption	(F)HE	在密文上进行计算，既能保证隐私又能提供可操作性。全同态是指支持所有操作的计算。
半诚实模型	Semi-honest model	-	一种安全模型，指攻击者严格按照协议规定执行，被动获取网络传输的信息。
恶意模型	Malicious model	-	一种安全模型，指攻击者可不按照协议规定执行，主动篡改协议、试探诚实参与方，以期获取更多的信息。
加密电路	Garbled Circuit	GC	最早由姚期智先生提出的对电路进行加密的方法，是安全多方计算中最常用的工具之一。
不经意传输	Oblivious Transfer	OT	一种安全的传输协议，允许两方对按照输入比特安全选取标签，是安全多方计算中常用的工具之一。
秘密共享	Secret sharing	-	一种将秘密值分享成多个碎片的技术，并且从碎片恢复秘密值的过程具有一定的容错性。是安全多方计算中常用的工具之一。
全分布式结构化拓扑	Decentralized Structured Topology	-	全分布式结构化拓扑是P2P网络的一种拓扑形式，主要采用分布式散列表（Distributed Hash Table，简写成DHT）技术来组织网络中的结点。

中文	英文	缩写	解释
/	REsource LOcation And Discovery	RELOAD	RELOAD协议由IETF P2PSIP (Peer-to-Peer Session Initiation Protocol)工作组提出的一个P2P网络协议框架提案，已经成为RFC6940标准。RELOAD协议定义了统一的叠加网对等体和客户端协议，实现抽象的存储和消息路由服务。
/	Kademlia	-	Kademlia是由Petar Maymounkov与David Mazières所设计的P2P重叠网络传输协议，以构建分布式的P2P电脑网络。是一种基于异或运算的P2P信息系统。它制定了网络的结构及规范了节点间通讯和交换资讯的方式。
/	Recursive Distributed Rendezvous	ReDiR	ReDiR在RELOAD基础上定义了一种服务发现机制，已经成为RFC7374标准。
/	Interactive Connectivity Establishment	ICE	ICE是一个用于在offer/answer模式下的NAT传输协议，主要用于UDP下多媒体会话的建立，其使用了STUN协议以及TURN协议，同时也能被其他实现了offer/answer模型的其他程序所使用，比如SIP。
/	Session Traversal Utilities for NAT	STUN	STUN是一个轻量级的协议，可以被终端用来发现其公网IP和端口，同时可以检测端点间的连接性，也可以作为一种保活(keep-alive)协议来维持NAT的绑定。
/	Traversal Using Relay NAT	TURN	TURN是STUN/RFC5389的一个拓展，定义了一种中继协议，使得Symmetric NAT后面的主机能使用中继服务与对端进行报文传输。
/	Session Initiation Protocol	SIP	SIP是由IETF制定的多媒体通信协议。SIP是一个基于文本的应用层控制协议，用于创建、修改和释放一个或多个参与者的会话。这些会话可以是Internet多媒体会议、IP电话或多媒体分发。
公共交换电话网络	Public Switched Telephone Network	PSTN	PSTN即我们日常生活中常用的电话网，是一种以模拟技术为基础的电路交换网络。

中文	英文	缩写	解释
现场可编程门阵列	Field-Programmable Gate Array	FPGA	FPGA是指一切通过软件手段更改、配置器件内部连接结构和逻辑单元，完成既定设计功能的数字集成电路。FPGA是作为专用集成电路（ASIC）领域中的一种半定制电路而出现的，既解决了定制电路的不足，又克服了原有可编程器件门电路数有限的缺点。
专用集成电路	Application Specific Integrated Circuit	ASIC	专用集成电路(application specific integrated circuit) 是针对整机或系统的需要，专门为之内设计制造的集成电路，简称ASIC。
专用标准产品	Application Specific Standard Parts	ASSP	ASSP(专用标准产品)是在特殊应用中使用而设计的集成电路。
系统级芯片	System on Chip	SoC	SoC称为系统级芯片，也有称片上系统，意指它是一个产品，是一个有专用目标的集成电路，其中包含完整系统并有嵌入软件的全部内容。
工作量证明	Proof-of-Work Consensus	PoW	PoW机制最早应用于Adam Back 1996年提出的Hashcash中，而后被中本聪改造为以“挖矿”形式实现区块链一致性的共识机制。PoW中，矿工通过计算符合要求的区块哈希值竞争生成新区块的资格，同时获得相应的币作为奖励。而这整个过程中，矿工贡献的算力就是上面所说的“工作量”。
权益证明	Proof-of-Stake Consensus	PoS	与PoW一致，PoS也是需要提供一定的证明来获得生成新区块的资格，同时获得相应的币作为奖励。不过PoS（权益证明）是用“拥有的币龄”来证明自己有资格写入区块链。
委托权益证明	Delegated Proof-of-Stake Consensus	DPOS	DPOS的出块节点（见证人）由持币用户选举投票产生，每个用户的投票权重则按照用户持币占系统总量比例计算。选出的出块节点的权利是完全相等的。从某种角度来看，DPOS有点像是议会制度或人民代表大会制度。
实用拜占庭容错	Practical Byzantine Fault Tolerance	PBFT	PBFT是Miguel Castro (卡斯特罗)和Barbara Liskov (利斯科夫) 在1999年提出来的。PBFT是一种基于消息传递的一致

中文	英文	缩写	解释
功能即服务	Functions as a Service	FaaS	性算法，算法经过三个阶段达成一致性。PBFT具备1/3的容错性，即在 $N \geq 3F + 1$ 的情况下一致性是可能解决，N为总计算机数，F为有问题的计算机总数。
去中心化应用	Decentralized Application	Dapp	FaaS是一种无服务架构(Serverless Architecture)，FaaS将函数转换为无状态服务，同时管理服务的生命周期，FaaS的每个函数都拥有快速启动和短暂生命周期的特性，在运行的时候才消费资源。
计算节点	Computing Node	-	Dapp是运行在底层区块链平台上的分布式应用。Dapp是基于智能合约的应用，由智能合约和前端App构成，智能合约运行在去中心化的区块链节点上。
数据节点	Data Node	-	为PlatON网络提供算力服务的节点，负责完成各种计算任务。
路由节点	Routing Node	-	为PlatON网络提供数据服务的节点，负责为各种计算任务提供数据。
轻节点	Light Node	-	PlatON网络的节点可以部署在私有网络内，私有网络内的节点可通过路由节点实现NAT穿越，路由节点提供STUN和TURN服务。
全节点	Full Node	-	不保存所有区块的数据，只保存区块头信息以及跟自己相关的信息，依赖全节点进行快速交易验证。
共识节点	Block Producer	-	保存了所有区块的数据，可以在本地直接验证交易数据的有效性。
元计算框架	Meta Computing Framework	-	负责执行交易并把交易数据打包成区块。在Giskard共识协议中，共识节点基于计算贡献值加权权益选举产生，并通过PBFT协议达成共识。
			元计算框架有效整合全球范围内异构的算法资源、数据资源、计算资源，从而深刻而广泛的促进数据交易和算力交易。元计算框架使用并行计算和专用计算硬件提高计算性能

中文	英文	缩写	解释
计算任务	Computing Task	-	的同时，也集成了多种密码学算法保证计算的可验证和数据隐私。
计算发起方	Computation Requester	-	PlatON中，计算逻辑编译成布尔电路，并拆分成子电路进行并行计算，每个子电路及其输入打包成一个计算任务。
算法提供方	Algorithm Provider	-	一般指外部客户端，其通过客户端发起元智能合约的调用，从而触发计算。
数据提供方	Data Provider	-	特指元智能合约的发布者。算法包含在元智能合约中，其定义了计算逻辑和输入输出数据格式。
算力提供方	Computing Power Provider	-	数据提供方根据算法定义的输入数据格式，提供相应数据用于计算。
计算协调方	Computing Collaborator	-	对外发布算力服务，接收并执行计算任务。
计算通道	Computing Channels	-	计算协调方负责获取数据，并将数据和计算逻辑一起构成计算任务分发给算力提供方进行计算。
元智能合约	Sophia	-	计算通道作为计算的控制验证层和结算层用于保证计算的有效性和算力交易的安全性。
计算贡献值	value of computing contribution	-	PlatON中的智能合约，不同于传统智能合约，元智能合约同时支持对链上链下数据的访问。
可验证计算证明共识	Proof-of-Verifiable-Computation Consensus	-	计算贡献值是用户提供的经过验证的有效算力。
能量块	Energon	-	PlatON的共识机制，Giskard基于计算贡献值选举出共识节点，共识节点使用优化的PBFT协议出块。Giskard有效解决算力浪费和算力集中的问题。
			Energon是PlatON资源使用的度量衡，也是驱动PlatON这个“计算工厂”运转的能量。PlatON上每个应用链可独立创建自己的Energon。

中文	英文	缩写	解释
/	ATP	-	ATP为PlatON主链中发行的Energon，可以跟内部应用链Energon进行转换和交换，也可以跟外部数字资产进行交易。ATP这个缩写可另表述为三磷酸腺苷（ATP adenosine triphosphate），是由腺嘌呤、核糖和3个磷酸基团连接而成，是生物体内最直接的能量来源。亦被称为生命体的“能量货币”。
双向锚定	Two-way Peg	-	双向锚定(Two-way Peg)是2014年Adam Back等人提出来的一种侧链技术。PlatON中，双向锚定用于实现Energon在多链间的安全转换。
原子交换	Atomic Swaps	-	原子交换（Atomic Swaps）是T. Nolan在比特币开发社区提出来的一种代币点对点交易方案。PlatON中，原子交换用于实现Energon在多链间的安全交换。

■ 参考文档

[RFC6940]

C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, and H. Schulzrinne,
"REsource Location And Discovery (RELOAD) Base Protocol",
RFC 6940, January 2014,
<<http://www.rfc-editor.org/info/rfc6940>>.

[RFC5245]

J. Rosenberg , "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols",
RFC 5245, April 2010,
<<http://www.rfc-editor.org/info/rfc5245>>.

[RFC7374]

J. Maenpaa, and G. Camarillo, Ericsson"Service Discovery Usage for REsource Location And Discovery (RELOAD)",
RFC 7374, October 2014,
<<http://www.rfc-editor.org/info/rfc7374>>.

[RFC5766]

R. Mahy, P. Matthews, and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)",
RFC 5766, April 2010,
<<http://www.rfc-editor.org/info/rfc5766>>.

[RFC7890]

D. Bryan, P. Matthews, E. Shim, D. Willis, and S. Dawkins,
"Concepts and Terminology for Peer-to-Peer SIP (P2PSIP)",
RFC 7890, June 2016,
<<http://www.rfc-editor.org/info/rfc7890>>.

[Kademlia]

P. Petar, Maymounkov, David Mazieres.
Kademlia: A peer-to-peer information system based on the XOR metric[DB/OL].
<www.cs.rice.edu/conferences/IPTPS02/109.pdf>.

[Atomic Swaps]

T. Nolan, Re: Alt chains and atomic transfers,
<<https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949>>, 2013.

[Two-way Peg]

A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille,
Enabling Blockchain Innovations with Pegged Sidechains,
<<https://blockstream.com/sidechains.pdf>>, 2014.

[Homomorphic Encryption]

- [1] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, 1978.
- [2] C. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. STOC, 2009.

[Zero-Knowledge Proof]

- [1] S. Goldwasser, S. Micali, C. Rackoff , "The knowledge complexity of interactive proof systems" , SIAM Journal on Computing, 1989.
- [2] B. Manuel, F. Paul, M. Silvio "Non-Interactive Zero-Knowledge and Its Applications". STOC, 1988.

[Multi-Party Computation]

- [1] A. C. Yao, Protocols for Secure Computations (Extended Abstract). FOCS, 1982.
- [2] A. C. Yao, How to Generate and Exchange Secrets (Extended Abstract). FOCS, 1986.
- [3] O. Goldreich, S. Micali, A. Wigderson:How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. STOC, 1987.

[Verifiable Computation]

- [1] S. Micali, "Computationally Sound Proofs". SIAM Journal on Computing, 2000.
- [2] B. László, F. Lance, L. A. Leonid, S. Mario, "Checking Computations in Polylogarithmic Time". STOC, 1991.
- [3] S. Goldwasser, Y. T. Kalai, G. N. Rothblum. "Delegating Computation: Interactive Proofs for Muggles".STOC, 2008.
- [4] G. Rosario, G. Craig, P. Bryan. "Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers". CRYPTO, 2010