元一
Seele

# 共创价值互联网新纪元

全球首个引入全新的神经网络共识算法，并针对大规模异构节点高通量并发，构建“异构森林”价值交换网络的区块链生态系统

# Whitepaper

seele.pro

# 0 摘要

近几年来，各种区块链及其应用不断开疆拓土，向更广的领域和更深的应用发展。比特币、以太币等各种公有链和数字货币不断涌现，还有诸如 Fabric、Corda 等各种联盟链百花齐放，形成群雄逐鹿的局面。

随着区块链技术的发展和应用的不断深入，问题也逐渐暴露出来。性能无法满足大规模应用，功能不能支持多样性业务场景，以及不同区块链网络之间无法进行信息交换和资产共享等问题变得越来越突出。

针对这些问题，我们回归到区块链的核心价值，尝试从区块链的几个核心问题——共识算法、生态拓扑结构、价值网络协议、底层通信协议、协同融合计算和上层应用生态等取得突破，力图推进区块链和价值互联网的更广泛应用。

- 提出了神经网络共识算法(Neural Consensus)，对比拜占庭共识(BA)类共识算法[4]，在不损失性能的前提下，将容错性由 33%提升到了 40%；
- 提出异构森林 (HF, Heterogeneous Forest)网络结构，具有良好的可扩展性，可满足各种多样化应用场景，同时还能够具有完美的资源和安全隔离机制，可适用任何通用或者定制化的需求;
- 提出价值传输协议(VTP, Value Transport Protocol)和价值应用协议(VHTTP, Value HTTP), 实现价值互联网资产和实体的命名、发现和寻址服务，并能无缝兼容和融合链外(互联网)资源，打造区块链的底层协议和基础设施服务；
- 提出基于 TCP/UDP 的低时延的价值互联网传输层协议 QVIC (Quick Value Internet Connection )，相比目前区块链网络使用的传统互联网

TCP 和 UDP 协议，更好地适应和满足区块链价值网络在传输层和应用层面临的各种需求 ,在处理更多的连接、安全性、低延迟上具有明显的优势，特别是针对特定区块大小的数据包(1M,2M)的传输上进行了专门的优化，相比 UDP 的传输效率提高了近 1 个数量级。

# 1 命名

元一 Seele，Seele 在德语中是“魂”之意，"魂"不单指人的灵魂本身，也代表一个人的想法或行事的基本观念核心，元和一都有开创和初始的意思，也寓意了我们的目标：开创价值互联网新纪元。

# 2 使命和目标

- 价值互联网基础设施标准推动者，网络建设者，生态布道者；
- 在标准层面，融合信息互联网(Internet)基础协议分层模型的思想精髓，为价值互联网的资源互联互通，异构协同计算提供坚实的协议保障；
- 在网络层面，为全球各区块链内及链间的资源定位和发现，价值转移和转换，数据资产的自由安全流通提供强大的基础平台和高速管道；
- 坚持生态为本、合作共赢的战略，为开发者、服务提供方和用户提供数据资产注册、价值传递和交换的开放平台。致力于构建面向价值互联网的操作系统，为开发者提供方便灵活的设计、开发、测试和部署等一体化服务链，为服务提供方以最高效的渠道将服务呈现给用户，并且为用户和各方提供最简捷的通道进行价值传递和交换；
- 以代币经济鼓励社区贡献分享，共同打造元一生态系统，而不是中心化机构

搭建的软件平台；

- 构建全新的价值互联网生产关系，推动区块链向纵深发展，释放未来生产力。

# 3 设计原则

**开放式体系结构 （Open System Architecture）**：在基础协议和标准、功能框架和上层应用上满足可移植、可定制、互操作要求；

**效率优先**：为业务提供高效稳定的运行平台，快速准确进行价值传递；

**动态扩展：**根据不同业务需求，支持动态扩展区块链网络结构，实现计算资源和存储能力的动态规划和调整；

**资源隔离**：采用分区分层多链模式和区块链即业务的设计思路，避免多业务相互干扰；

**体验为王**:通过标准化的通信协议、模块接口规范、SDK 和 IDE、社区支持、开发者大会、行业应用协会等为元一用户提供全方面多角度的开发和服务支持;

元一作为下一代区块链标准倡导者和践行者，以异构森林、神经网络共识算法、链内外算力共享、向上可扩展的 TPS 为标签，打造区块链 4.0 的价值体系和生态体系。

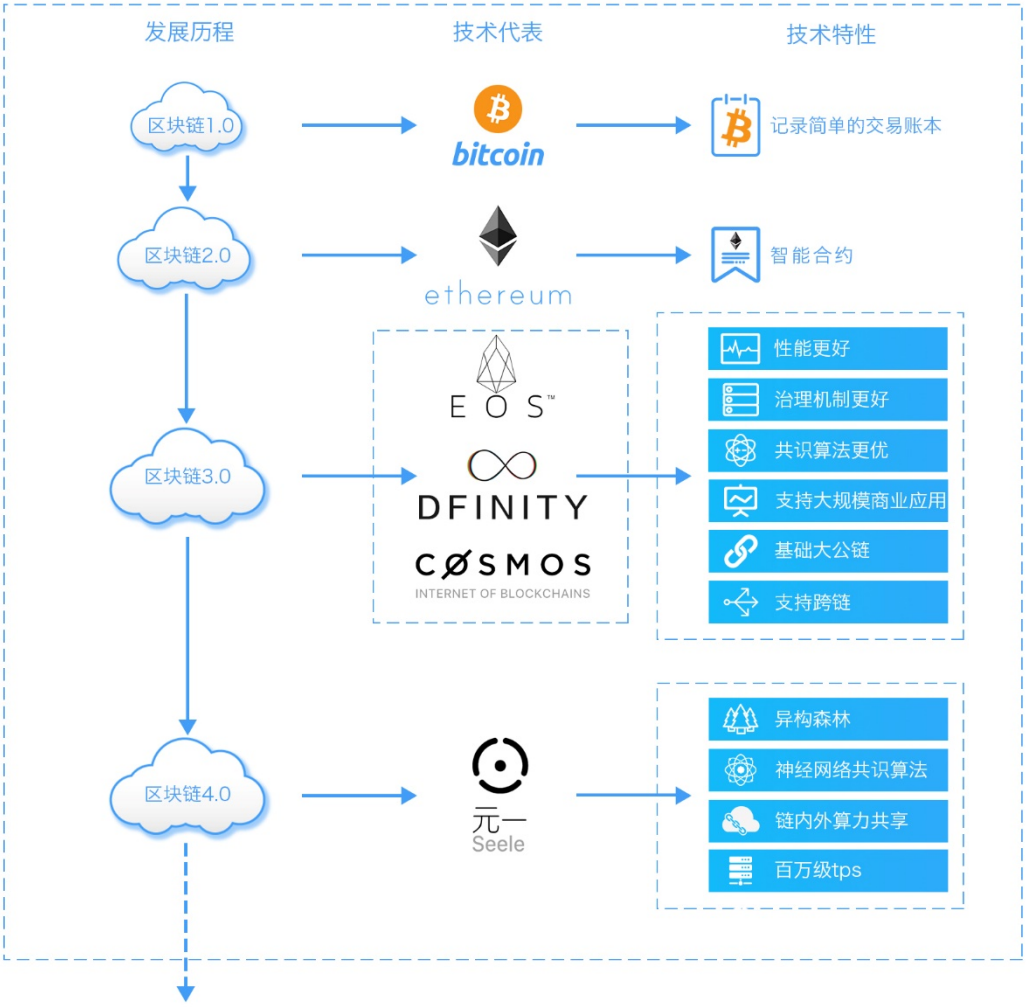



图 3.1 元一:区块链 4.0 代表

# 4 神经网络共识算法

## 4.1 现状

当前的共识算法，在规模(Scalability)、安全(Security),效率(Efficiency)上的不可调和，形成 SSE 矛盾。经典的 PoW 满足规模和安全的要求，但运算开销大；PoS 满足功耗的要求，但在规模和安全性上存在不足；DPoS 满足规模和功耗的要求，但安全性上存在不足；pBFT 满足安全和功耗的要求，但当节点规模特别大时，网络开销问题就会变得非常突出；Hashgraph 满足规模和功耗的要求，

但在安全性上存在不足，并且由于其结构和流程上的限制，比如结点的连通性不足，对部分交易的确认时延会比较大；Algorand 满足规模、安全和功耗的要求，但其对网络的整体连通性有比较严格的要求，在网络分片的情况下，共识时延会变得不可预测。

## 4.2 简介

元一综合当前主流共识算法的优缺点，提出了全新的基于“微实数”的异步排序技术（$\epsilon$ - differential agreement, EDA），将共识问题转化为对异步系统中大规模并发请求的处理以及在此环境下数据的排序问题。对于网络的整体连通性有非常强的鲁棒性，在非全连通网络的环境下甚至在网络连接比例小于 50%的系统中也能够正常运行。元一的共识算法的另外一大显著特点就是直线性扩展性，即性能随节点规模增大而线性加速，节点规模越大收敛越快，性能越好。在 100K 节点的网络环境下，元一的 TPS 达到了 10W，并首次将交易的确认延迟提升到秒级。

## 4.3 原理

EDA 通过多次不完全随机采样将逐步覆盖系统全部特征将传统共识协议的离散型投票 $[T|F]$，转变为连续型投票[0%,100%]。它通过具有收敛性的函数将系统内各投票值压缩以及收敛。当所有节点值范围小于预设的阈值$\epsilon$时，认定投票一致，投票值作为排序依据。通过符合相应要求的算法，使该参数在共识过程中得到收敛，当该参数的范围收敛至小于用于排序的数轴所要求的精度$\epsilon$时，即确保在该刻度范围内，仅存在一个区块。 随着节点增加，投票轮数会减少。

对于多个区块，通过彼此独立、互不影响的循环，将区块在数轴上不断进行定位，完成排序。

算法以一个虚拟数轴上坐标的位置作为区块排序的依据，使区块的排序不再依赖于前置区块的共识，完全摆脱现有一致性协议不能并行的性能瓶颈，为数据的大规模处理提供了有效实用的方法，大幅度提高了系统的效率。通过架构分离，将一致性协议与前端的重复性检验、后端的存储技术分离开来，拥有良好的可移植性。因对整个共识流程不存在对数据内容的处理或访问，其数据无关性的特点使其可以广泛的应用于金融、电子政务、溯源跟踪等多种场景。

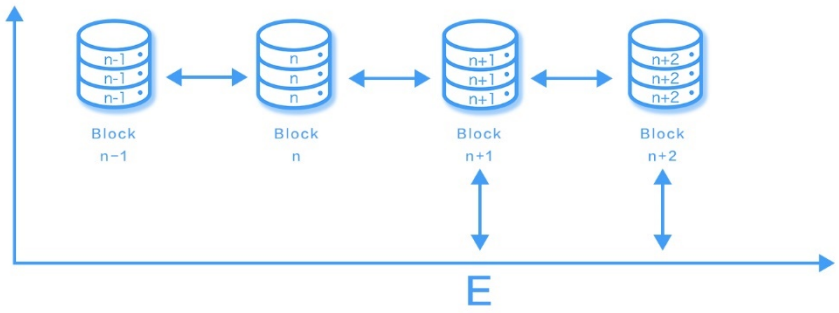



图 4.1 共识排序模型

## 4.4 亮点

- **共识过程的离散型投票变更为连续型投票**

传统共识中，节点间对区块的投票用 0 或 1 代表节点的意见，其投票为离散型，EDA 算法则是一个连续区间的概率取值，用以表示结点对本轮共识的置信度。

- **节能降耗**

不存在头节点的选取流程，无需节点自证性能（PoW）或权利（PoS），在完整维护无中心系统运行的过程中，充分降低能耗。此外，方案中除了对信息进行

摘要提取需要进行浮点运算外，其余运算、排序等过程均基于整数运算，对节点性能要求极低，可进一步降低社会经济成本。

- **低传输开销**

不需要像 PBFT 在共识过程中与大多数节点连接，并获取投票。这可以节省系统数据传输的开销，尽可能的降低节点对系统网络结构的依赖。

- **针对不同使用环境实现效率参数可调节**

本算法共识效率基于收敛区间$\epsilon$、采样率$s$等参数的选取，可通过实时调整相关参数，获得最优的系统效率。并行共识将异步系统的运行效率得到提升，充分发挥并行系统分布式计算的能力。配合异步系统多节点的设计，可以进一步提升系统的并发性能。

- **兼容多种网络结构**

EDA 共识算法对于传统的链结构和 DAG 结构都有很强的适应性。

## 4.5 安全分析

对于女巫攻击，根据参与共识的用户所持有的币值，为其分配权重，组合使用多次局域随机采样逐步特征覆盖。只要女巫结点拥有的总币值少于总价值的一半，元一的算法对女巫攻击就具有绝对的抵抗和免疫力，避免分叉和双花。

对于共识过程中的节点随机选择，元一使用随机可计算函数，用户根据其私钥计算得知其是否被选择中，并将结果反馈和广播给其它用户，这种随机选择的过程是非交互的 ,攻击者无法提前知道哪些节点被选择。在每一轮的共识过程中，被选择中的节点都是随机和不同的，这也增加了攻击的代价和成本。

## 4.6 实验结果

元一以 pBFT 算法为参照，使用了 2K 台亚马逊 EMC 云节点，算法收敛范围控制参数$\epsilon < 0.001\%$。

### 4.6.1 节点故障对共识过程的影响

分别使用如下三个场景进行测试：

A：故障节点数量占总体比例为 10%，即故障节点为 200 个；

B：故障节点数量占总体比例为 33%，即故障节点为 660 个；

C：故障节点数量占总体比例为 40%，即故障节点数量为 800 个。

对于 pBFT，当故障节点（含恶意节点和失效节点）总体超过 33%时，系统将无法运行，也即对于场景 C，pBFT 方案是无法运行的。EDA 方案可通过使用不同的采样率s （每次上升 10%，每一个 s 值实验 20 次）验证方案的效果。

对于场景 A，最多需要 6 次投票即可以完成共识，确定排序。

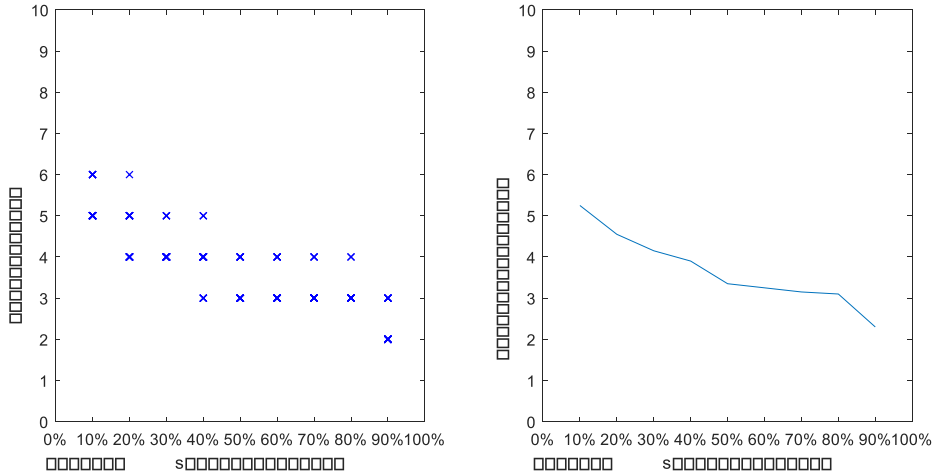



图 4.2 采样率 s 对共识次数的影响（故障节点占比 10%）

对于场景 B，最多需要 7 次投票即可以完成共识，确定排序。

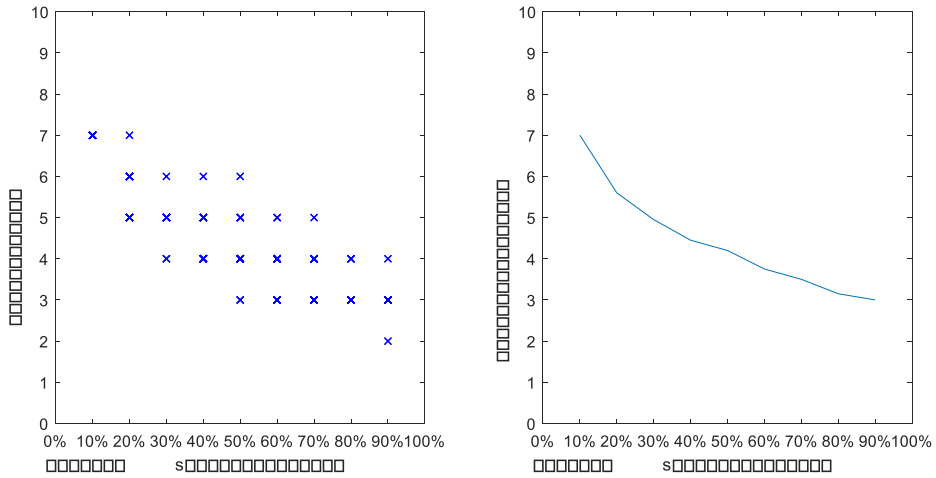



图 4.3 采样率 s 对共识次数的影响（故障节点占比 33%）

对于场景 C，当 s 不低于 20%时，最多需要 8 次投票，即可以完成共识，确定排序。而对于 pBFT，因为故障节点数量高于基本要求，在本环境中，PBFT 无法完成共识。

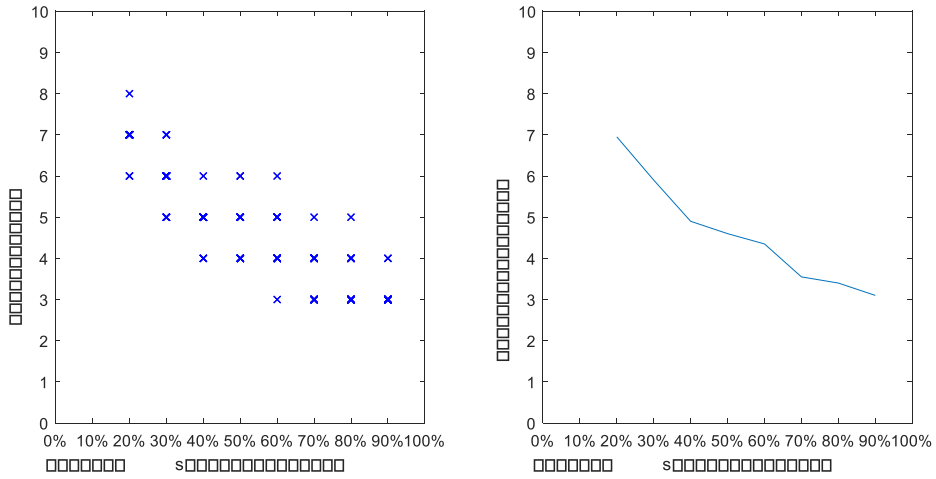



图 4.4 采样率 s 对共识次数的影响（故障节点占比 40%）

### 4.6.2 多次采样对总体的覆盖

大规模节点环境（N=10k），采样率 3%（n=300），两轮 EDA 后，任意正常节点已经接收到了全部节点 r-2 轮的投票；中型规模节点环境（N=100），采

样率 30%（n=30），同样在两轮后收到全部节点 r-2 轮的投票。

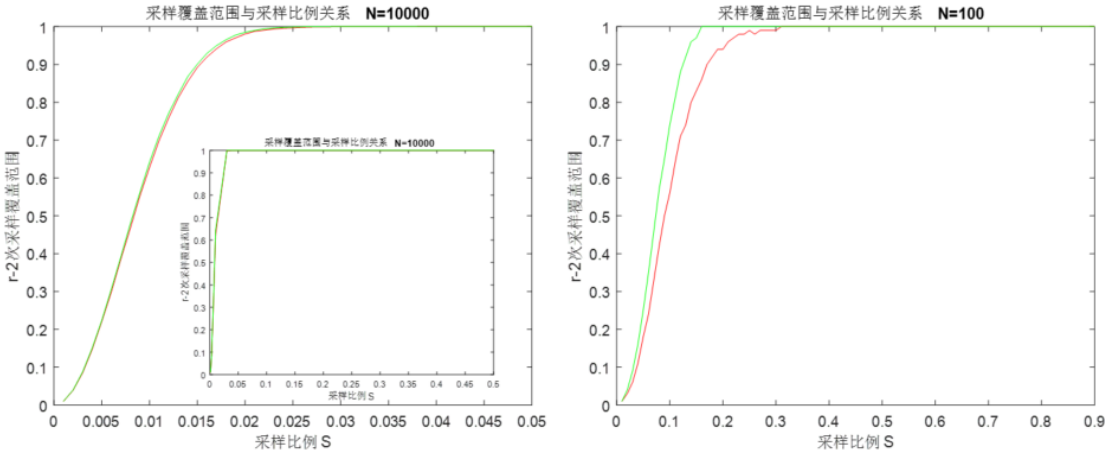



图 4.5 多次采样对总体的覆盖

### 4.6.3 采样通讯次数

大规模节点环境下，EDA 传输节省带宽效果明显；小规模网络下，EDA 与 pBFT 差距不大，当 r*s<2 时优于 PBFT；小规模网络下，网络带宽消耗可忽略不计，影响不大。

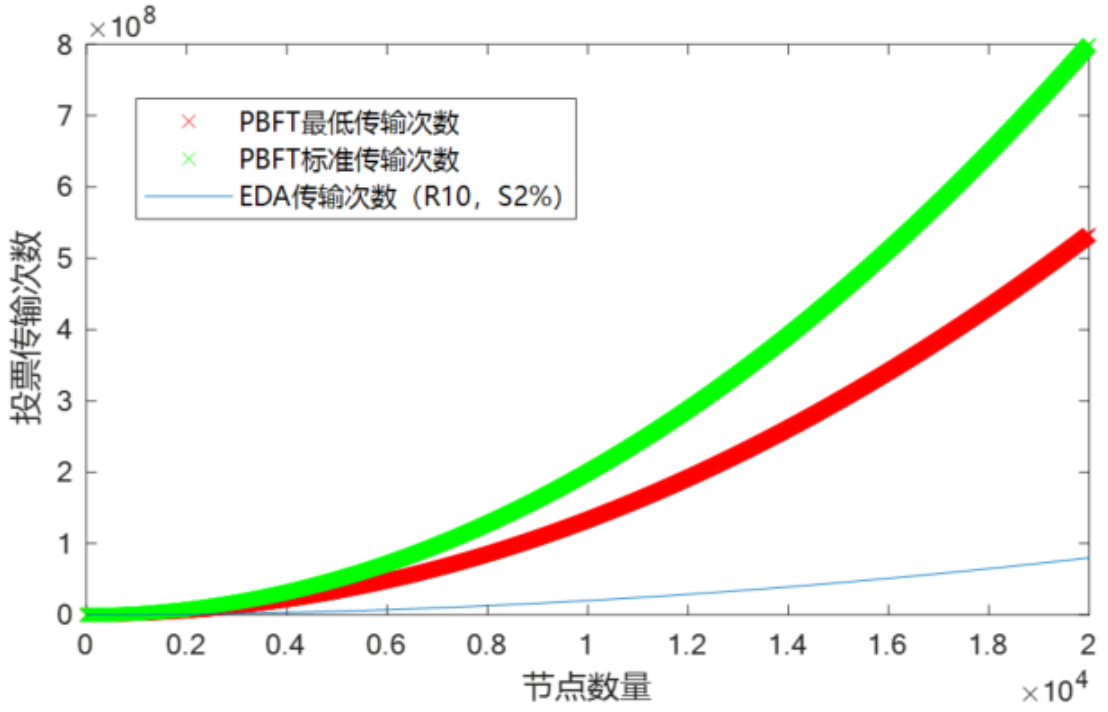



图 4.6 采样通信次数对比

### 4.6.4 可扩展性

节点 N=100K ,S=0.9%时 ,EDA 两轮覆盖 100%投票成分 ,与 PBFT 相同；节点 N=100K，S=0.9%，R<=10 时，传输次数远小于 PBFT；

PBFT 在并行投票中，产生的投票结果无意义，需要重新进行排序，并对排序再次进行共识；EDA 在并行投票中，产生的投票结果可直接作为排序依据。

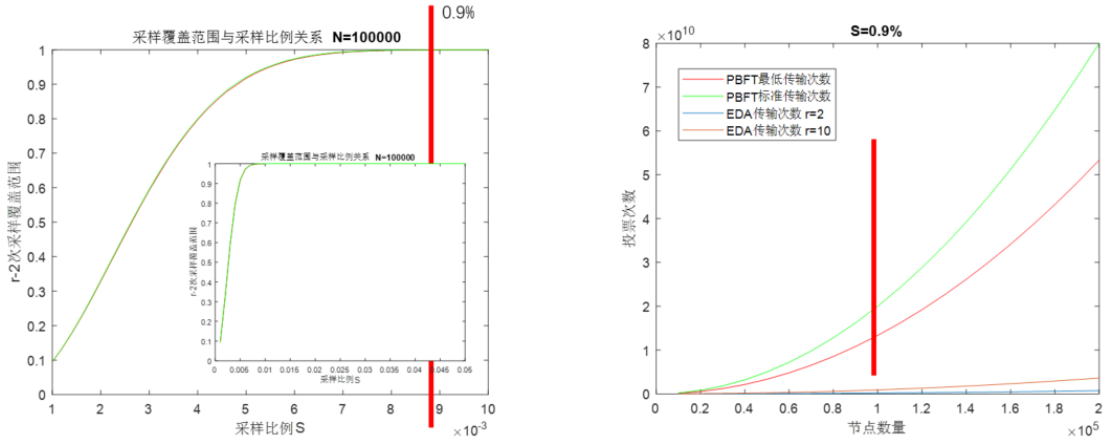



图 4.7 pBFT 和 EDA 的可扩展性对比

### 4.6.5 容错性

pBFT 的故障率超过 33%时会造成阻塞，EDA 允许节点继续投票，直至故障节点恢复正常。

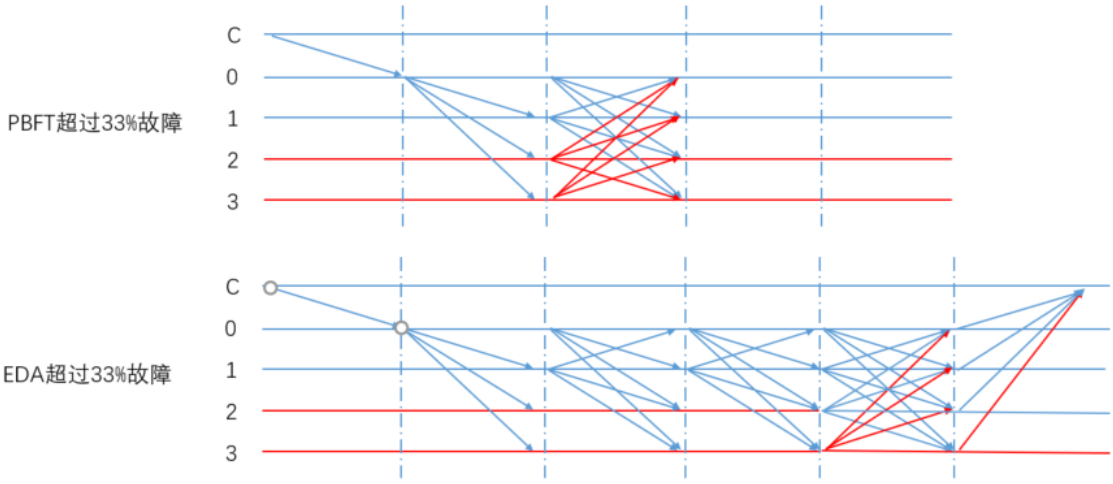



图 4.8 pBFT 和 EDA 的对故障率的容错对比

EDA 在小规模环境下：

定义采样 S=100%，E=100%：失去并行排序能力，退化为典型 PBFT;

定义采样 S=100%，E<100%：增加网络消耗（多轮次），保留并行排序能力;

定义采样 S=100%，E=0%：降低容错性能，允许并行排序;

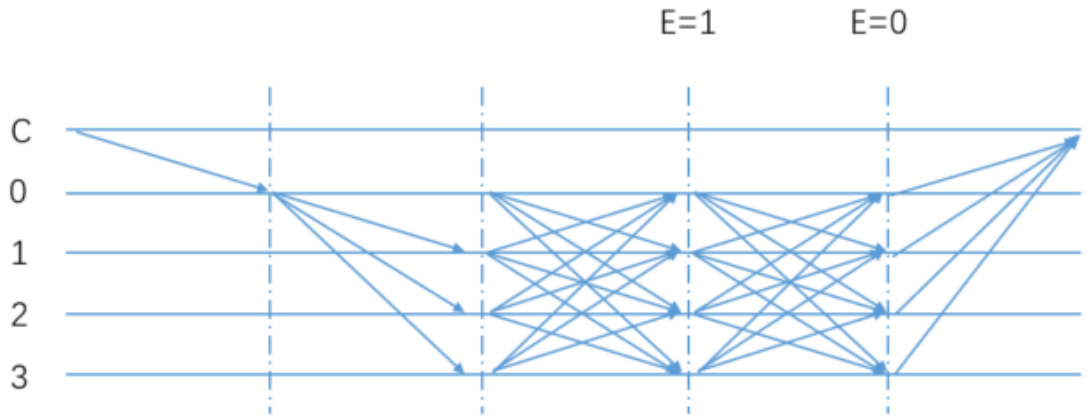



图 4.9 EDA 在小规模网络环境下的故障率比较

### 4.6.6 结论

由上述实验测试可以得出，在 s 不低于 20%的情况下，对于故障节点占比不超过 40%的系统，均能够实现整体系统的收敛。且 s 值越高，收敛所需要的次数越少，效果越好。

# 5 异构森林网络

## 5.1 概述

人类社会的发展历程经历了原始单部落模式，到多部落模式，到不同文化生境，再到不同体制的国家。互联网的发展也是经历了单机时代，多机简单互联，多机局域网，再到各种异构的局域网互联，然后到上世纪末的全球 PC 互联网，

再发展到今天的移动互联网和物联网。区块链的发展也相似，从最初始 1.0 时代以比特币为代表，发展到 2.0 时代以集成了智能合约的以太坊为代表[1][2]，再到今天各种多链（跨链）区块链产品。

## 5.2 单链结构

经典的区块链网络，比如比特币网络、以太坊等都是采用单链结构，所有的事务和交易都是在一条链上进行。

单链结构的优点是交易和共识流程比较简单，在区块链发展早期能够很好地满足用户需求。但是随着区块链技术的发展和市场对区块链的需求不断增强，单链架构逐渐暴露出很多无法解决的痛点：

- 整体吞吐量和性能存在瓶颈：比特币只有 7 TPS 以及需要 6 个区块的确认机制，以太坊出块间隔也需要 10-20 秒，这些都严重阻碍了日益增长的区块链业务发展需求;
- 链内业务相互干扰：单链架构很容易由于个别业务的繁忙而造成整个系统拥堵，比如最近风靡一时的数字加密猫(Crypto Kitties) 就使得整个以太坊网络的变得拥挤不堪，很多正常的交易都得不到及时处理和确认;
- 封闭的网络结构：无法实现不同链之间的跨链交互，无法满足多平台之间的业务交互需求。

## 5.3 多链结构

为克服单链结构的局限性，多链结构被提出，主要形态有多条平行链，主/侧链等，部分满足了业务多样化的需求，但在灵活性和定制化上还存在不足。

- 对于多条平行链，各条链的功能通常是预先设定好的，难以满足快速变化和多样化的业务需求，同时如何在多条链上共享计算和数据资源也没有得到很好的解决。
- 对于主/侧链结构，可以根据业务的增长和变化而派生出不同的侧链，但侧链的共识与主链耦合比较紧密，主链有可能成为新的中心和瓶颈。

## 5.4 森林链结构

传统的互联网，我们使用浏览器输入网址，进入网站，点击其中的页面链接访问站内或站外的资源，获取信息，用专业的术语来说，即在广袤的互联网中进行跨网调用访问，而在这背后，互联网的基础协议之一 DNS（Domain Name System）做出了巨大的贡献。

由区块链所构筑的价值互联网作为一个遍布全球的庞大网络集群，各条区块链，各个子网产生相同或不同的业务，提供不同服务，不同链网之间同样存在大量的跨链(域)请求，集群的稳定运转为人类提供一个良好的价值传输服务。借鉴 DNS 的成功经验，元一提出异构森林网络架构，为现实世界和数字世界搭建一座桥梁，以实现资源和资产在价值互联网上定义、存储、转移、转换，从而促进价值互联网业务与传统互联网业务的融合。

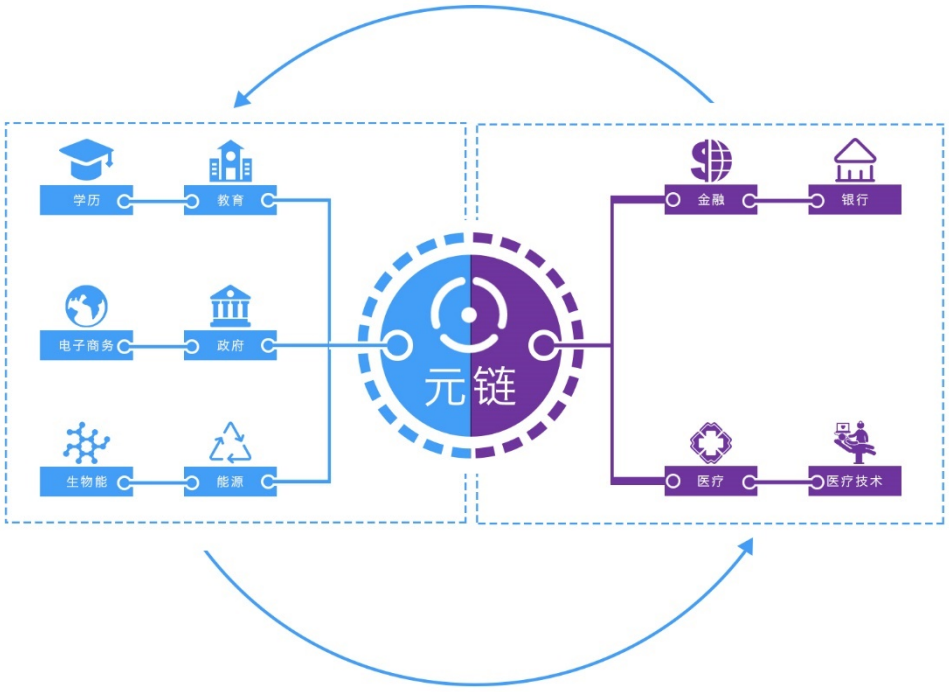



图 5.1 异构森林网络结构

异构森林网络由不同子网组成，每个子网可以看成是一个分层分区的树，在树的最顶端的链是一个全局服务链，称之为“元链”，它提供全局配置和调度服务。由此往下，是各种不同业务形态的链，根据业务场景、隔离机制、性能开销等不同进行划分，逐层往下划分，上层对下层提供寻址和调度服务。每一层可以独立设置治理机制，譬如访问权限、流量控制、安全机制等，每一层都形成多个相互独立的小生态，所有小生态构成一个完整的大生态圈。

由于现实世界的不同业务具有各种各样的特殊性，如前所述单链结构是很难完美的支撑多种异构业务的。在异构森林网络中，每一条链只服务于最小功能集合的业务，每个内聚型的业务运行在单独的链，这样既能做到有效的安全隔离，也能实现计算和资源的有效利用最大价值化，不同链之间通过跨链协议进行交互，实现价值交换。

异构森林网络结构能满足现实世界各种不同类型的复杂业务需求，不同类型不同特性的业务在不同的子链运行，比如计算密集型、IO 密集型、混合型分别

在不同链上良好地运行；不同安全等级要求的业务也可以在不同层次运行，比如针对银行的业务需求，在数据的保密和安全以及事务的强一致性会有更高的要求，因此可以隔离在最安全的一层。

# 6 VTP

## 6.1 互联网协议

传统互联网的大范围应用和成功，很大程度上是归因于有一整套规范的协议，把各种设备、网络连接起来，并对资源进行统一标识，使得资源交换极其便利。

- IP(Internet Protocol)：任何设备和软件，只要遵守和实现 IP 类协议，都是无缝接入互联网，共享资源;
- URI(Uniform Resource Identifier): 对互联网资源，例如图片、文字、视频片段等进行唯一标识，该标识允许用户对任何的资源通过特定的协议进行交互操作。

## 6.2 区块链现状

当前的各种区块链网络，各自拥有不同的数据、交易、代码、链接，相互之间不能共享数据，无法互通有无，形成一个个独立的区块链孤岛，例如比特币和以太坊两个网络，数据模型和交互协议完全不同，是两个完全无法兼容并行的独立系统。

对于比特币网络用户，其地址是一个形如如下地址的字符：

33YV5wC11kF67AuGSwTpUSpDTHBPTS4qDh

对于以太坊用户，也具有相同的地址形式。这种字符串是对机器和程序处理

很方便，但对人类的认知和记忆则非常不友好，这也极大地限制了区块链网络上的价值传输。虽然基于以太坊的 ENS 服务提供了类似 DNS 的命名服务，但在效率和覆盖面等方面都还存在诸多不足。

## 6.3 VTP

为解决各区块链网络之间无法有效地进行价值传输的痛点，基于异构森林网络架构，提出价值传输协议(VTP, Value Transport Protocol )。该协议涵盖了对链上资产的统一标识，对资产查找的路由策略，是一套完整的用于区块链价值网络的传输协议。

### 6.3.1 命名机制

对于区块链网络，其上的数据都是资产，对每个资产进行命名，标识其唯一性，对于资产的注册、发现、转移和转换都具有极大的意义。

基于 VTP 协议，我们定义了统一资产标识命令规范(UAI, Uniform Asset Identifier)，对资产采用分层结构化命名，方便人的认知、记忆，同时具备了唯一性、可用性、可扩展性等特征. 例如 CHAIN://edu.pku.cs/account/data，其中 CHAIN://是默认的协议头，edu,pku 和 cs 是从高到低的各个层次的链标识，account 是链上的账户（或者合约），data 该账户的某个信息，data 可以是账户的余额、备注、甚至是个合约的接口等。在异构森林网络中，兄弟链之间采用不同的命名空间，具有相同的父链命名空间，通过父子关系可以方便地进行内容的寻址和路由。

### 6.3.2 内容寻址

每条链都提供子链地址查询服务，由系统合约实现，在建链时进行初始化。当新增子链时，子链向父链发送注册请求，父链记录子链地址。”元链”是全局配置链，管理整个森林网络体系所有的入口地址，当查询一个信息时，根据 UAI 首先从元链找到入口，再依次往下查找，直到找到所要的子链，然后根据 account 和 data 字段的内容定位到特定的资产。“元链”不会成为性能瓶颈，因为路由满足局部性原理，可以被缓存处理。

### 6.3.3 路由缓存

为保证更高效的网络利用率、提高数据的可用性和访问效率，提升上层服务体验，引入路由缓存机制。在每条链上，由内置系统合约管理路由缓存，在建链时进行初始化。对于缓存的替换策略，主要有如下几种方式：

- 基于上一次被访问时间间隔的替换策略；
- 基于访问频率的替换策略；
- 同时基于上一次访问间隔和访问频率的策略；
- 基于随机的替换策略；

通过缓存路由寻址失败则立即清理缓存。当新的子链加入到异构森林网络，须向元链注册信息，由元链向下层传递消息以进行路由的更新。

### 6.3.4 VHTTP

为方便上层应用实现简便的跨链访问，借鉴传统互联网的 HTTP 协议，提出用于价值互联网的跨链传输协议 VHTTP(Value HTTP protocol)。该传输协议实

现链与链之间、链内和链外之间的价值交换。VHTTP 兼容 HTTP 协议，能够识别 HTTP 请求包格式，也即链外用户可以直接通过 HTTP 协议访问链内资产和数据。对于进入区块链网络的 HTTP 请求，自动建立方法之间的映射。

VHTTP 协议请求由三部分组成：请求包头、消息报头、正文。

请求包头以一方法名称开头，以空格分开，后面是请求的以 UAI 标识的资产地址和版本，格式如下：

```
Method UAI Version CRLF
```

请求方法类型如下：

GET：请求获取 UAI 所标识的资源信息

POST：创建资产(资产上链)

TRANSFER：在二个 UAI 之间进行资产转移

# 7 QVIC

## 7.1 简介

区块链网络结点分布广，网络环境复杂，各结点之间的距离相差巨大，不同结点跨运营商甚至是跨海跨洲，网络的抖动和延迟非常大，严重影响共识算法的性能以及各结点之间区块的同步。元一实现了基于 TCP/UDP 的低时延价值互联网传输层协议 QVIC( Quick Value Internet Connection )，相比目前区块链网络使用的传统互联网 TCP 和 UDP 协议，更好地适应和满足区块链价值网络在传输层和应用层面临的各种需求，在处理更多的连接、安全性、低延迟上具有明显的优势，特别是针对特定区块大小的数据包(1M,2M)的传输上进行了专门的优化，

传输效率提高了接近 1 个数量级。

## 7.2 技术优势

- 采用非透明代理模式，客户端就近连接服务器，由加速服务接管传输；
- 数据从源端到目的端，中间无须增加缓存，保证快速和安全；
- 对数据流进行编码，通过 UDP 数据包进行服务器间的传送；
- 可采用负载均衡，提高鲁棒性；
- 对丢包有高容忍，在高丢包的情况下，也可以正常使用；

## 7.3 协议框架

QVIC 协议，是在广域网情况下，针对网络抖动、丢包不稳定等特点，针对性地进行优化。既保留了 UDP 协议快速高效的特点，又提供了 TCP 数据传输的完整性。

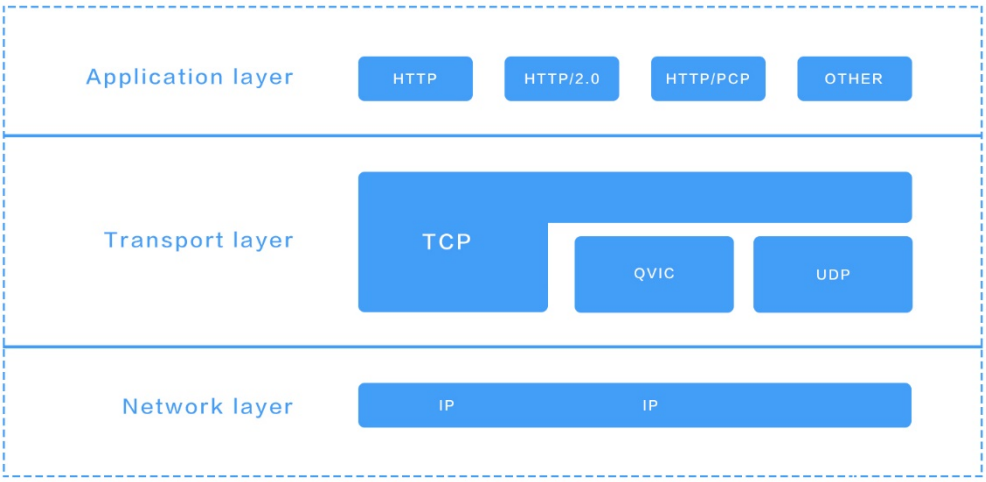



图 7.1 QVIC 协议框架

QVIC 协议采用预链接方式，握手控制在发送端完成，握手时间可以忽略，直接发送数据包，因此传输速率和效率得到了极大的提升。

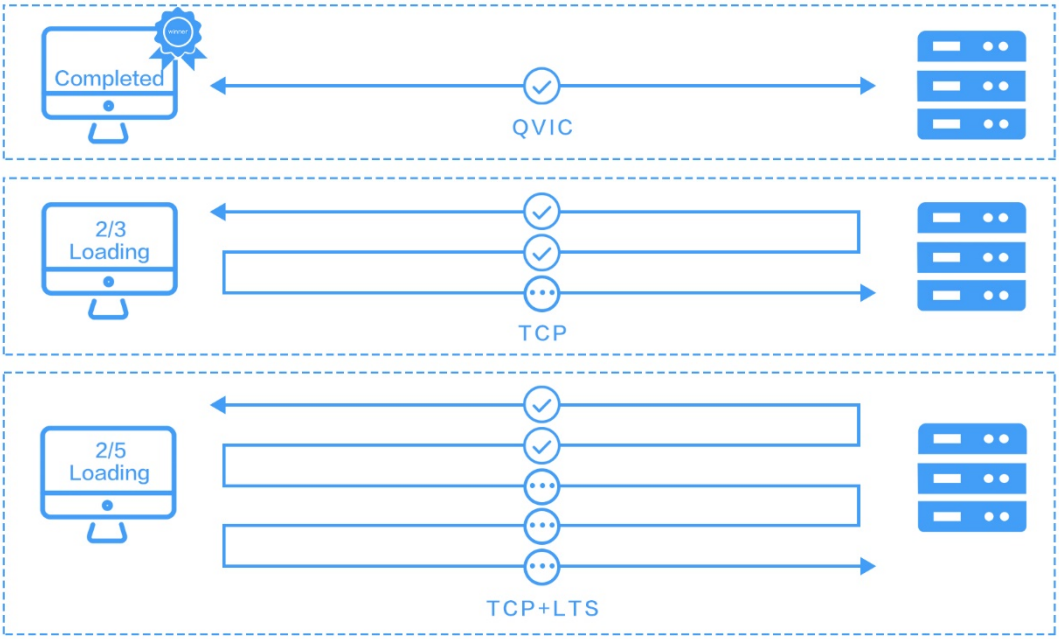



图 7.2 QVIC 协议握手机制与 TCP 对比

## 7.4 实验对比

使用分布在北京、上海、广州、伦敦四地不同数据中心的 50 台机器构建点对点数据传输网络进行测试，经过 QVIC 协议加速，对 1G 文件的传输速率由 100Kbps 提升到 1Mbps;在上述四个数据搭建元一测试网络，使用 1K 个节点进行测试，经过 QVIC 协议加速，由于共识过程中的数据传输效率和块同步过程的效率提升，单个交易的确认时间减少了 70%。

### 7.4.1 传输速度

由下图可知，对比 TCP 协议，QVIC 协议在传输速率上有了巨大的提升，对于 1GB 数据的传输，加速比达到了 500%。

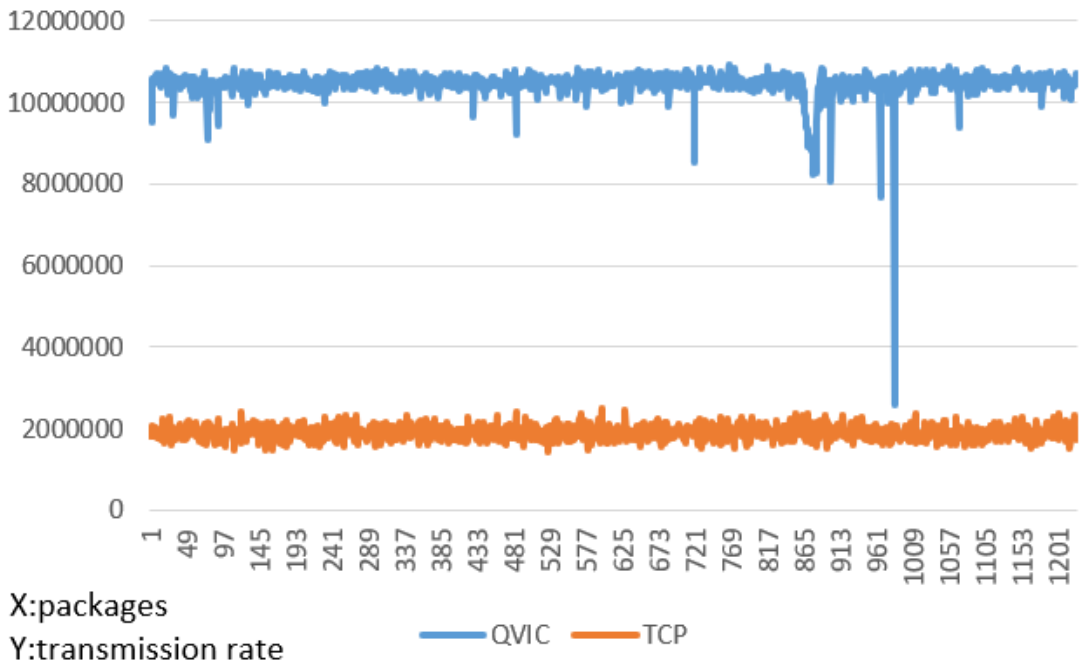



图 7.3 QVIC 传输速度与 TCP 对比

### 7.4.2 稳定性

在 UDP 的基础上，自定义传输控制算法和 FEC 动态补偿机制，与 TCP 相对，稳定性和效率也有明显的改善。

# 8 算力融合

## 8.1 现状

区块链上的资源以共识为基础，因为其可信任性、安全性和不可篡改性，让更多数据可以从中心化的存储转移到链上。但是，涉及到文件和数据的链上存储时，对于区块链本身的开销比较大。另外，包括政府、企业在内的很多机构，掌握着大量的高价值数据，但是数据开放共享的主要难点和挑战是如何保护数据的安全和隐私。对于计算而言，一方面传统的应用程序执行方式，无法保证计算过程中的数据安全性和结果的正确性，另一方面，对于数据量大和计算比较复杂的

场景，虚拟机无法提供更高的计算能力，需要提供额外的资源以满足更高要求的计算需求。

基于元一的算力融合定义了一种新型的技术，在区块链以及智能合约之上，对链外存储资源和计算资源进行了融合。网际存储解决了关于区块链存储的问题：

1. 通过区块链和 IPFS 的完美结合，弥补了现有区块链系统在文件存储方面的短板，将文件目录的哈希值加密后上链，节省区块链的存储开销。可以把文件加密后永久存入 IPFS 实现文件的分布式共享。
2. 元数据上链的方式解决了数据孤岛的问题，基于区块链的数据脱敏技术能保证数据私密性，为隐私保护下的数据开放提供了解决方案。在数据不上链的情况下，提供内网数据的可信交换，在共享交换过程中保证数据的隐私和确权。

网际计算提出了一种新形式的分布式云计算基础设施，以元一为基础实现较低运营成本的区块链计算。元一提供了两种不同的计算方式，链上合约虚拟机上的多方安全计算适合在低资源需求的应用程序安全之行的场景。另外，也提供了通过合约实体控制计算资源的链下桌面系统和分布式集群的计算方式。

## 8.2 链上资源定义

命名价值传输协议章节定义了一套完整的区块链价值传输协议 VTP，采用分层结构化命名方法对链上信息进行命名，这种结构化的命名方式（UAI）定义了协议头、链标示、账户和链上资源。本章节主要描述对于 UAI 链上资源的存储定义。

### 8.2.1 元数据目录描述法

元数据目录描述法（Meta-Data-Directory-Specification, MDDS）用来描述链外存储的原始数据特征，包括数据的基本属性、语义特征等静态描述和数据存储机制等动态描述。MDDS 已经在实际使用场景中得到了很好的验证。我们在基于区块链和智能合约的可信数据交换平台中使用 MDDS 对于原始数据的描述信息进行了链上唯一标识。

### 8.2.2 资源描述框架

元一对 MDDS 进行了扩展和延伸，提出了资源描述框架（Resource Description Framework, RDF）,RDF 是对 UAI 所包含的具体信息的描述协议，除了包括 MDDS 部分对于数据资源的静态描述和动态描述，增加对于计算资源的描述，通过区块链描述计算资源的特征，包括内存、CPU、硬盘等。对于计算资源请求描述的是执行分片任务做需要的最小资源量，如最小内存，最小 CPU cores 等信息。

自动寻址合约作为元一的分布式存储和计算的一个重要组件，通过系统合约进行内容寻址，根据 UAI 标识首先从元链找到入口，再依次往下查找，直到找到所要的子链，找到对应 account 下的 data 资源信息 RDF，发起对于 RDF 指向的链上（或链下）资源的请求，在请求得到数据拥有方的签名确认之后，智能合约可以匹配资源需求方和资源供应方。在实际应用场景中，对于资源供应方和需求方的自动撮合需要根据用户的实际需求来选择不同的策略。

每条链都提供一个子链地址查询服务，可以由系统合约来实现，在建链时初始化好。在新增子链时，子链向父链发送注册请求，父链记录子链地址。元链是

全局配置链，管理了整个森林体系所有入口地址，当查询一个信息时，根据 UAI 标识首先从元链找到入口，再依次往下查找，直到找到所要的子链，根据 UAI 中的 account 和 data 字段访问链上的资源。

## 8.3 存储和计算

### 8.3.1 网际存储

通过 MDDS，我们提供了两种基于区块链的分布式存储方式。以 IPFS 为核心的存储方式和元数据上链的存储方式。以 IPFS 为核心的存储方式是提供一个去中心化的网络，用户将数据存储在 IPFS 之上，允许每个用户定义文件的目录结构，目录结构包括指向 IPFS 文件的链接和文件的其他描述信息。用户上传数据到区块链，生产者通过广播确定数据被接受，其他的区块链节点通过 IPFS 网络复制文件。在区块链上，给所有发布的内容进行哈希值计算； 构建哈希值索引地址。当用户访问某个文件，会广播哈希请求，找到存储该文件的节点，传输给用户。

在公网环境下对自有数据进行可信交换数据的场景适合使用元数据上链的存储方式，可信数据交换在实际的产品中经过验证。通过公链提供的互联协议，用户也可以将自有数据存储中的文件原数据信息同步到区块链上，借助 MDDS，区块链上的数据目录和用户自有数据建立映射关系。

数据或元数据信息存储到链上需要保证数据的安全和隐私确权，除了采用传统的数据加密技术确保数据在链上的安全和隐私外，也要保证数据在传输过程不被泄露，还需要确保同一份数据，对不同用户有不同的访问权限和可读范围,也即我们需要基于数据加密基础上的细粒度的访问权限控制，公链使用属性加密和安

全沙箱来实现数据加密基础上的细粒度的访问权限控制。

### 8.3.2 网格计算

算力融合提供了基于区块链的分布式计算能力，基于公网环境下节点上的智能合约虚拟机，普适合约组成了一个可验证的分布式计算环境，这一点与以太坊类似。不同的是，在算力融合过程中，数据被安全的封装在沙箱之内，沙箱运行在合约虚拟机之上，保证数据在安全环境中进行计算。

在传统的数据交换场景下，C 要使用 S1、S2 和 S3 的数据，并使用算法提供方提供的算法 M，做法是，提供数据给算法提供方，由算法提供方在 S 提供的数据上运行其算法，得到的结果再返回给 C，但这种方式已将 S 的数据泄露给算法提供商。算力融合基于安全多方计算[3]提供了一种新的方式，数据提供方上传加密后的数据在合约虚拟机内计算，数据分成 n 分分发到 N 个合约虚拟机中，最后根据合约虚拟机在协议执行阶段所得到的中间结果进行数据重组，获得最后的计算结果。

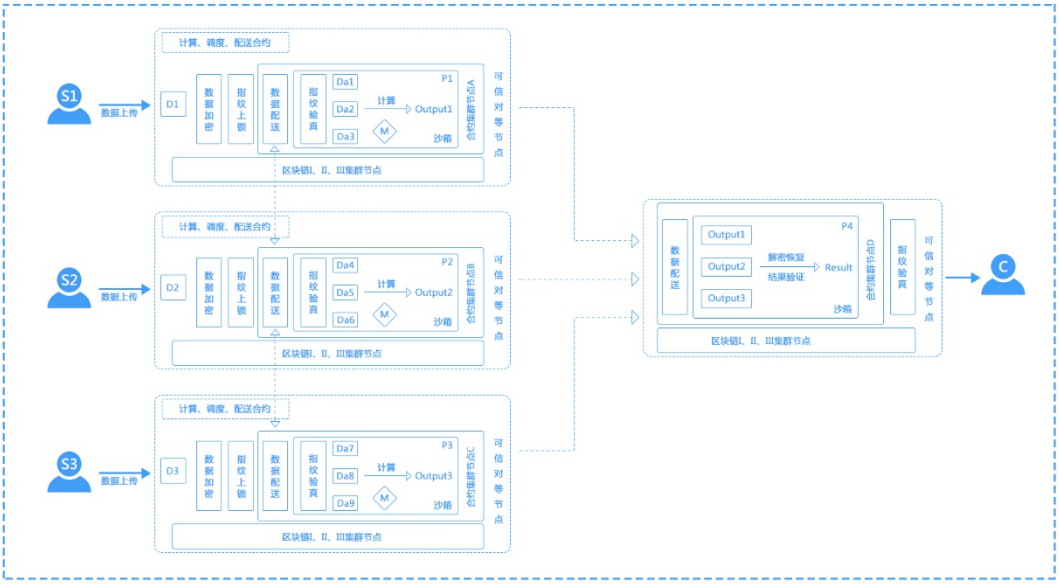



图 8.1 网络域计算框架图

在协同计算的基础上，元一提供了一种新的计算方式，通过合约控制和协调，分布式计算过程可以延伸到链外的计算资源提供方，数据通过沙箱配送到桌面系统或分布式集群等算力平台。并通过区块链验证计算过程和结果的正确性。

### 8.3.3 多域多级别调度

任务和资源调度是分布式系统非常重要的组件，调度器算法的设计优劣，直接影响整体集群的利用率。在分布式系统中，调度经过了单体调度、二级调度、共享状态调度、全分布式架构和混合式架构的演进。在智能合约集群中，我们设计了一种多域多级别调度，在合适的粒度下，基于安全和信任对于区块链划分了不同的域，对于用户要求的成本、性能以及安全等指标划分了不同的级别，同一调度算法中可以选择不同域和不同级别对任务和计算资源进行分配，并通过调度器精细调整、预测任务性能、降低邻居干扰支持用户关于计算的特殊需求。

以下场景描述根据用户不同需求做出的不同调度：A 客户对于任务的执行时间和数据安全要求不高，执行计算的时间会比较长；B 客户对于数据的执行时间有要求，数据安全要求性不高；C 客户对于数据的安全性要较高，这种情况下任务的执行时间较长，对于算力的花销也会比较高。

## 8.4 客户端设计

### 8.4.1 元数据上链

客户端对于元数据目录上联的存储方式提供了元数据目录抽取上链和元数据目录更新两种接口。

元数据目录抽取是指根据元数据目录结构描述，采用技术手段辅助人工手段，

从原始数据中提取元数据目录信息，并将元数据目录区分公开元数据目录和完整元数据目录（包括隐私信息）分别进行入链存储。

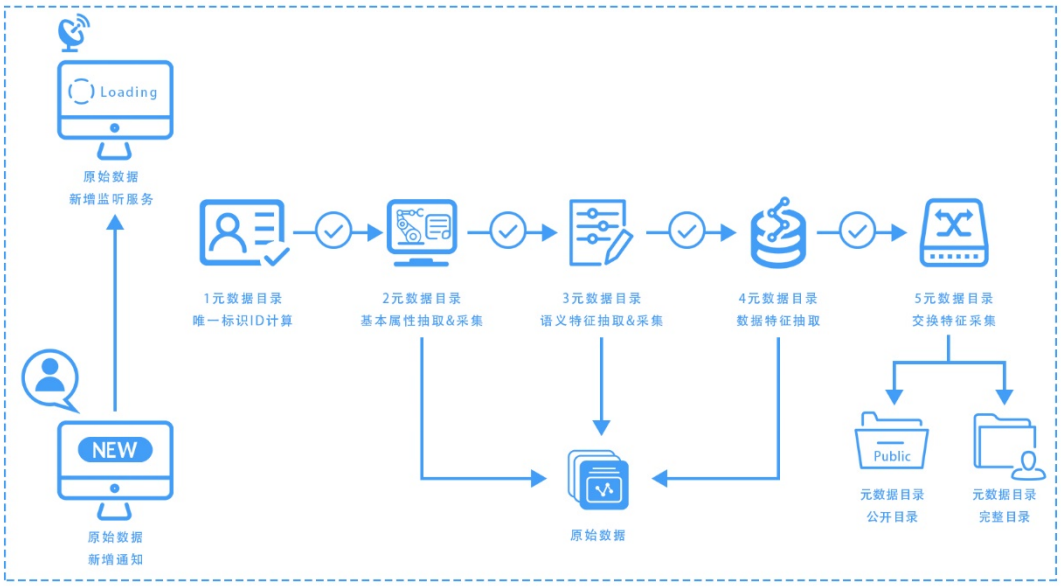



图 8.2 元数据上链流程

元数据目录更新是指当原始数据发生变更时，需要同步元数据目录，保持原始数据与元数据目录的一致性，其主体流程如下：

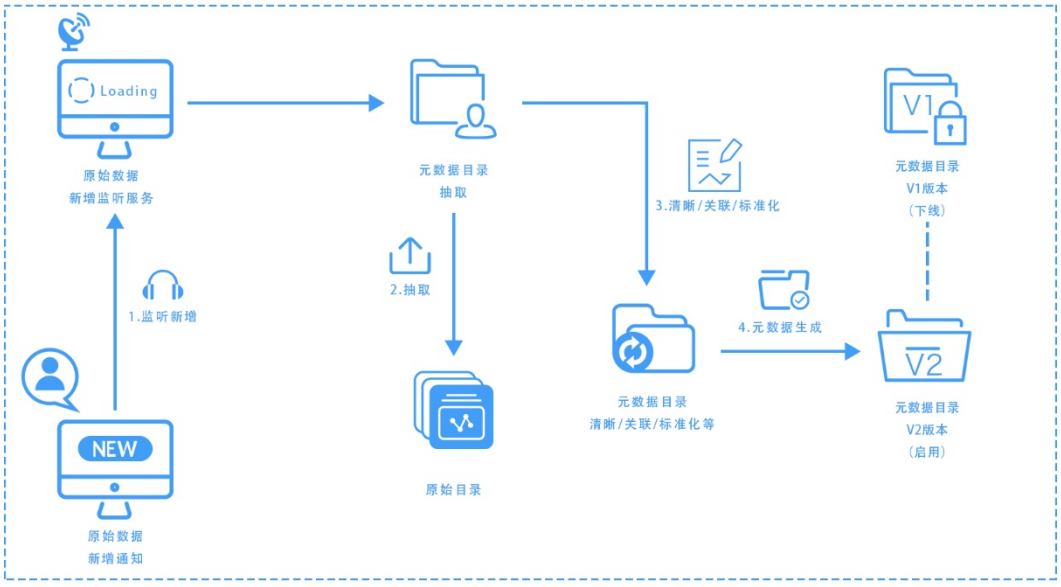



图 8.3 元数据更新流程

1. 监听原始数据的变更通知

2. 根据变更通知，按照元数据目录标准从原始数据中抽取元数据目录信息

3. 按照元数据目录标准针对抽取的元数据目录信息进行清洗/关联/标准化等操作
4. 将生成的元数据目录数据记录为 V2 版本，将元数据目录信息入链
5. 上层应用中启用新的 V2 版本元数据目录，将 V1 版本的元数据目录逐渐下线

## 8.5 数据的隐私和确权

通过智能合约，数据被封装的沙箱中调度到执行环境，执行环境分两种情况，在合约虚拟机上执行，在链外的计算资源上执行。

通过安全多方计算的密码学算法在不泄露各方原始数据的前提下，在智能合约集群的合约虚拟机上完成多方的数据联合计算，在确保用户数据隐私的前提下，进行业务的处理。对于在链外的计算资源上执行的场景，智能合约控制数据的配送和执行，将数据封装在沙箱之内配送到计算资源中，计算结果通过安全沙箱返回到用户。计算过程以及环境信息实时上链，用作现场检查和事后审计。

### 8.5.1 属性加密

属性基加密[5]本质是一种访问授权与认证服务技术，保证非授权用户没有资格访问特定的数据。属性基加密属于公钥加密机制，其面向的解密对象是一个群体，而不是单个用户，它使用群体的属性组合作为群体的公钥，所有用户向群体发送数据使用相同公钥。

属性加密属于公钥加密体系的一种，但它最大的特点在于用户的私钥和密文是依赖于某些特定属性的，比如用户的身份信息等。只有当用户的属性集与密文

的属性匹配时才能够正常解密。

安全沙箱在执行合约计算时，对接收到的加密数据，使用用户的私钥进行解密，在用户私钥的生成过程中，我们可以根据预定的用户的权限和访问规则来生成密钥，实现细粒度的限权、限时、限次、限内容安全访问控制。

属性基加密的函数定义：

**1.** 参数初始化：给定系统规模 $m$ 初始化参数，输出公开参数 $mpk$ 和主私钥 $msk$ ：

$Setup(m) \rightarrow (mpk, msk)$

**2.** 密钥生成：将主私钥 $msk$ 以及属性赋值 A 作为输入，计算输出用户私钥 $sk_k$ ：

$KeyGen(msk, \mathrm{A}) \rightarrow sk_k$

**3.** 加密算法：输入公开参数 $mpk$ 以及加密策略 Policy，计算会话密钥 $ek$ 和密文 $C$ ：$Encrypt(mpk, \mathrm{Policy}) \rightarrow (ek, C)$

**4.** 解密算法：输入公开参数 $mpk$ 、用户私钥 $sk_k$ ，计算恢复出会话密钥 $ek$ ：

$Decrypt(mpk, sk_k, C) \rightarrow ek \ \ iff \ \ \mathrm{Match(policy,A)=1}$

简单的例子说明：

建立下面属性值的集合:

大学名 := {……，“哈佛大学”，“斯坦福大学”，“清华大学”，……}，

部门 := {……，“生物学院”，“化学学院”，“信息学院”，……}，

年份:= {……， 2013， 2014， 2015， 2016，……}，

角色 := {……，“教授会”，“学术委员会”，“学位委员会”，……}。

可以为任何资源（包括文件、存储空间、网络信道、进程等）重新定义上述安全策略为

Policy := (大学名∈{“哈佛大学”， “斯坦福大学”} AND 年份= 2015 AND

角色=“学位委员会” AND 部门 ∉ {“生物学院”， “化学学院”})。

假设一个用户具有如下身份属性：

A:={大学名：=“斯坦福大学”，年份：=2015，角色：=“学位委员会”，部门：=“信息学院”}，

这表示该用户在2015年任职于斯坦福大学的信息学院，并且是学位委员会委员。显然，该用户的身份可以通过上述安全策略的认证，因此，将被允许访问由上述策略加密的资源。

### 8.5.2 安全多方计算

安全多方计算的理论模型在历史上提得比较早。1982 年姚期智先生提出姚氏百万富翁问题。1983 到 1987 年以色列的学者 Golderich 提出若干定义，完善安全多方计算概念。

在基于区块链和智能合约的数据协同计算的场景中，需要数据交换和计算的多方参与者，假定有 N 参与者，P1 到 PN，共同完成某一个计算任务，多方参与者既希望能够完成协作任务，又希望保留源数据所有权和控制权，而仅仅向对方开放有限的数据使用权。对于这种典型场景，我们采用多方安全计算技术来处理。通过安全多方计算的密码学算法在不泄露各方原始数据的前提下，在智能合约集群的合约虚拟机上完成多方的数据联合计算，在确保用户数据隐私的前提下，进行业务的处理。

# 9 生态/治理/激励

## 9.1 开发者生态

区块链和价值互联网的发展，不但需要先进的基础设施和技术架构，还需要给开发者营造一个良好的开发环境，吸引其投入到平台的生态建设和应用开发中来，促进社区的良性发展。

### 9.1.1 问题

对于以太坊的 dApp 开发，存在的主要问题有：

1. 开发工具和框架不完善，对于初学和入学者不友好；
2. 不同语言和框架的使用规范存在很多差异，资料的收集非常繁琐；
3. 文档虽多，但很杂乱，且更新不及时。网上虽然有各种示例，但经常会出现由于后续版本升级而文档没有同步更新，造成示例失效，从而误导开发者，浪费宝贵的开发时间；
4. 缺乏完善的跨平台接入解决方案。对于 Web 应用开发相对方便，但在移动端，没有良好的 SDK 支持，无法做到多端接入；
5. 存在各种面向私链、测试链和主链等的开发环境，但整个合约的开发、测试和部署，没有完善的指导流程，需要从头摸索。

### 9.1.2 方案

针对上述种种问题，在元一设计之初，就参考和借鉴游戏行业中 Unity 引擎的使用经验，构思了一个合约开发工具 SeeleEditor，主要优势如下：

1. 完善的应用开发工具链。可以在一个环境中，支持合约的开发、测试和部署；
2. 跨平台的 SDK 支持和技术文档的更新同步，提升开发的效率和不同平台上应用的多样性；
3. 建立类似于 Unity 的插件商城，提供合约开发的组件和示例程序等，提高开发效率，让开发者不仅可以开发具体的应用，还可以开发支持组件，获得收益；
4. IDE 自带社区模块，有任何关于开发相关的问题，可以随时在上面沟通交流，及时解决。

## 9.2 行业应用生态

区块链技术发展到现阶段，早已超越简单的账本功能。元一本质上已经是一个超级分布式云计算机，具有向上可扩展的 TPS 能力和完善的分布式链上链下融合存储系统。除了传统区块链技术所涉及的金融资产交易、代币发行，预测市场之类的应用之外，我们能支持落地更加丰富的应用。

1. 社交平台。构建类似于 Steemit 的社交平台，通过 Token 鼓励用户去创建更多好的内容,也可以搭建一个区块链直播平台，用户和主播直接点对点打赏,并且由于支付的透明性，也可以杜绝平台自消费和佣金不透明等诸多问题；
2. 链上游戏。基于以太坊的加密猫(CryptoKitties)的出现给游戏行业的发展指明一条新的方向，一只区块链上的猫，生于链、长于链、死于链，不会因为游戏发行商的倒闭而消失，它将是其主人的一个永久数字资产。这些

给链上游戏带来极大的想象空间。但一只猫就可以让以太坊拥堵不堪，让其交易费大幅提升，未来涌现出更多的现实，将使整个链网拥挤而不堪重负。因此，行业急需一个更好的基础设施来支撑游戏的开发，元一义不容辞；

3. 物联网。由于区块链在分布式，数据管理，安全和透明性上极具优势，所以区块链在物联网的应用具有很好的优势。但受限于传统区块链共识算法的高功耗和低效率，一直未能在物联网应用上取得良好的发展。元一的神经网络共识算法，参与结点越多，共识效率越高，具具有极低功耗和极高并发的特征。相对于 IOTA 的共识算法不能完全避免双花问题及 DDOS 攻击等弱点，我们的分层共识机制可以很好的克服这个弱点，具有很强的应用优势；
4. 其他企业应用。基于我们的异构森林网络，可以非常容易地针对某个特定的企业应用，单独创建一条应用链，基于它开发各种定制服务。通过 VTP 和 VHTTP 协议 ,这些企业应用可以非常方便地进行跨链通信和价值传递，给企业应用带来更多的灵活性和便利性

## 9.3 经济系统

### 9.3.1Token

元一的神经网络共识算法有一个良好的特性，越多结点参与，共识效率越高，交易确认时间越短。基于此，我们需要鼓励更多的节点加入网络中来，提高网络的性能，增加网络的安全性。

为此，我们引入令牌机制。主要用在两个方面：一是给参与的节点奖励令牌，这个也是我们最终货币发行的一种方式；二是收取交易费用。由于交易的过程中需要消耗整个系统的带宽和计算资源，我们需要通过收取费用来防止女巫攻击，收取的费用会用来奖励共识节点。

### 9.3.2 激励机制

现在主流的区块链，一般会给出块节点固定额度的奖励，以此作为货币发行的一种方式，另外还有交易费用也用来作为激励。交易费用的收取，当前区块链一般有三种主流的方式：

1. 比特币的机制，每一笔交易都会收取付款人一定的交易费，奖励给矿工；
2. 以太坊的 gas 机制，严格按照交易背后的计算和存储占用，来统计所消耗的 gas 值，然后给 gas 值一定的定价，两者相乘就是最终的交易费用；
3. EOS 免除交易费用，但其有一个前提，即发起交易的用户需要持有一定的令牌，才能享用系统中的资源，令牌的多少决定资源量的多少；

矿工在看到这些交易后，会选择费用高的那些交易，以达到收益的最大化。所以在激励体系的背后，本质是一个资源的分配问题：在有限的资源前提下，通过什么方式能提高资源的最大利用效率。对于这个问题，传统主流方式本质上其实是两种最为粗暴的解决方案：

1. 谁有钱谁就说了算；
2. 谁提前占坑谁说了算；

元一的激励机制的出发，即资源的分配不应该是采取这种简单粗暴的方案。参考现实社会中的治理方式，元一的原则是：兼顾效率和公平。在激励上，我们

采取基于参与和价值的分层激励机制。主要包括两个方面：

1. 交易共识的参与激励

因为我们共识的向上扩展，节点规模越大越稳定，相对效率也越高，系统的性能也越高。所以，我们需要鼓励更多的节点加入到网络中来，参与交易共识，以此提高网络的性能和安全性。对最终交易收敛节点，进行令牌奖励，这是一个代币发行的一种方式，获得数量会随着时间递减。另外，节点还可以获得一定的交易费用作为奖励。

区别于传统 POW 算力挖矿模式，我们的共识算法，无须强大的计算能力，只需要有良好的网络连接能力，通过节点的连接，就能更多地参与到交易共识中来，获得奖励。所以，我们节点的贡献能力取决于带宽和网络的从何性能，而且带宽的重要性大于算力。带宽资源是一种分布式的国家资源，很难出现集中的情况。这样就避免算力会趋向集中的问题。而且由于我们网络底层强大的打洞穿透能力，也可以让大量的内网节点参与到整个交易共识过程中来，大大增加节点规模。

2. 打包区块价值激励

节点每生成一个区块，系统都会根据其打包交易的价值来决定奖励出块者一定数量令牌。在这里系统会根据不同的类型的交易，给予相应的价值衡量。

这样，我们可以鼓励系统中价值更高的交易，能够更快地得到确认。以提高网络的效率。

在交易费上，我们跟以太坊的 gas 类似，通过计算交易所花费的 gas 来收取费用，但 gas 的费用会根据系统的运行状态，进行动态调节。这样就能够起到一定的公平性。

通过上述的机制，我们希望能够兼顾效率和公平，提高整个系统的使用效率。

### 9.3.3 治理架构

元一基金会将在新加坡注册成立，在新加坡会计与企业发展局（ACRA）的批准下，元一基金会将注册为非营利性基金会，类别为 Public company limited by guarantee。

元一基金会作为元一治理的主体，将规范管理元一技术开发和应用开发，维护元一币（SC）持有人的权益，宣传推广元一品牌。

此外，元一基金会还将与全球知名的慈善基金会联合推广基于元一的医疗产业落地应用，针对东盟地区提供针对胎儿与老人的远程医疗服务投放。

元一基金会计划与英国爱丁堡大学信息学院、英国伦敦大学区块链技术中心、香港城市大学信息系统系成立联合实验室，在数据库图计算、社会技术系统、商业服务与服务计算三个领域分别展开合作与学术研究。

# 10 核心团队

郑茂林博士 区块链研究院院长

中国北京市特聘专家

加拿大政府自然科学与工程研究委员会 NSERC 博士后

蒙特利尔商学院（HEC）博士后

前北京国政通科技有限公司首席科学家和 CTO

前宜信首席征信科学家

毕伟博士 首席科学家

牛津大学计算机科学硕士，伦敦大学博士、博士后、研究员，研究生博士生导师

中国区块链技术创新与应用联盟副秘书长

8 项区块链技术专利第一发明人（状态审核中，2017 年提交）

擅长区块链，密码学，数据分析，图像处理和视觉学科等领域，多次受邀参加大型国际学术会议，有多项国家发明专利，成果发表在新英格兰顶级学术期刊，文章、观点被 BBC， 英中时报，伦敦华语广播电台，Complex UK 等媒体报道。

Nick Smith 博士

分布式计算、云计算、网格计算工程师

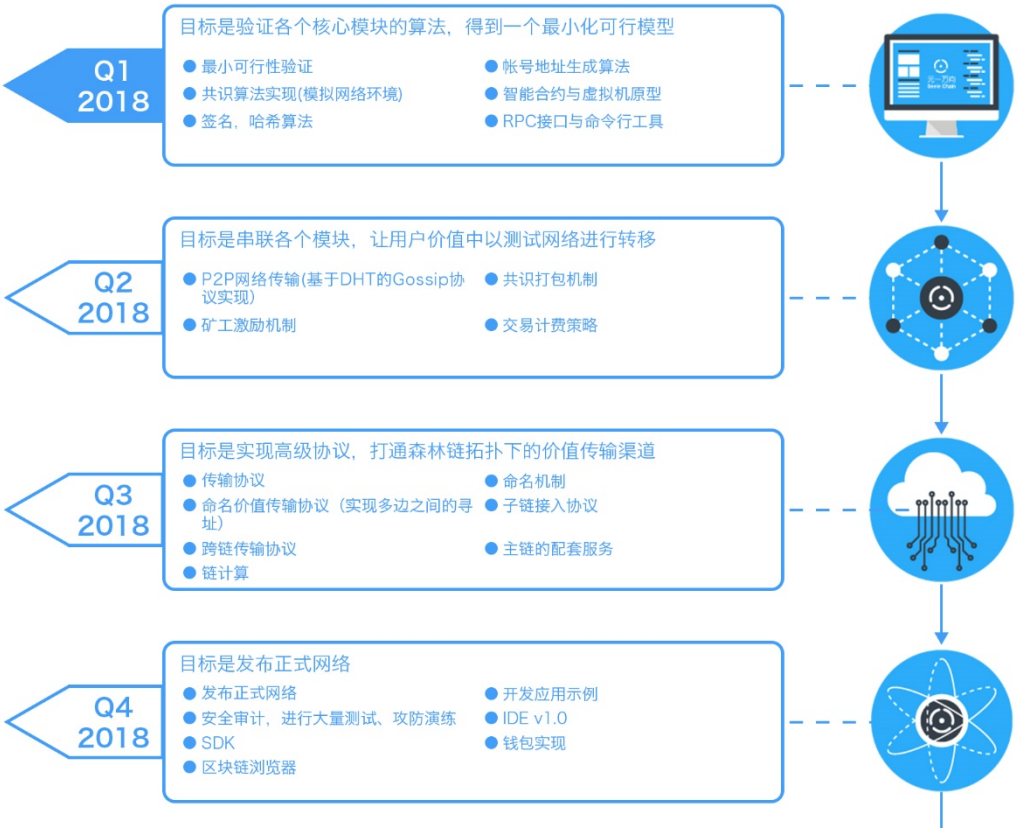
伦敦大学博士后、博士生导师

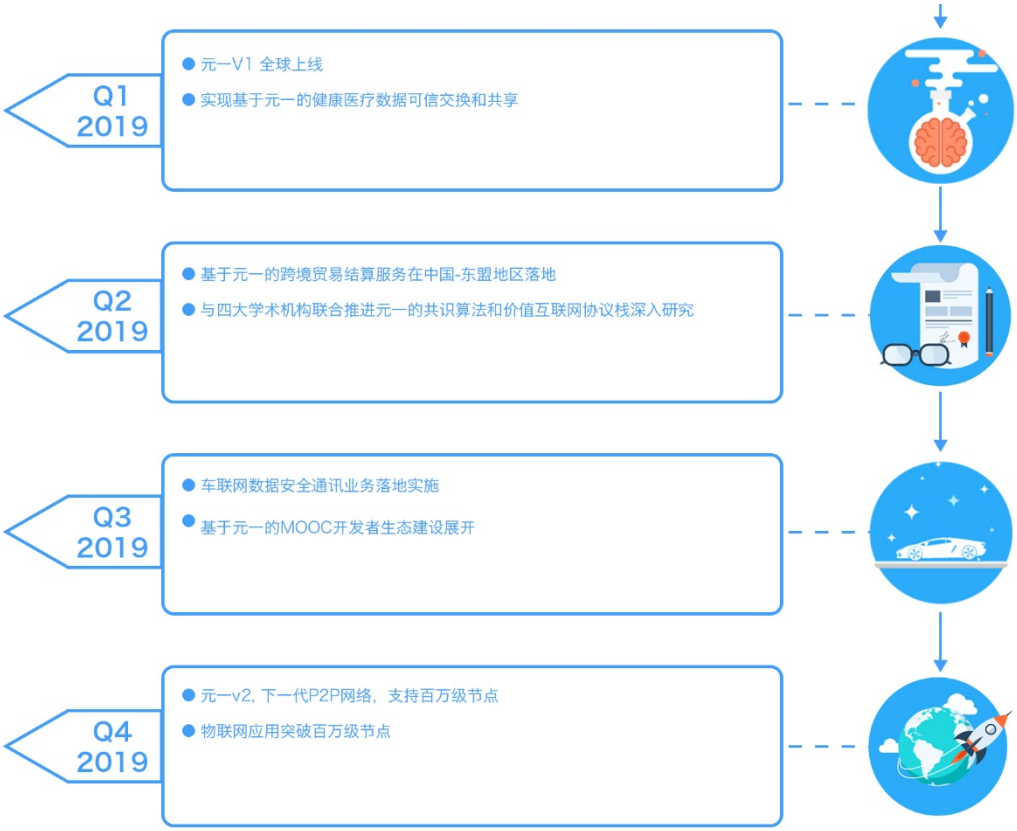
有多年分布式系统和云计算工作经验

擅长分布式网络架构设计、性能测试，并且有多年的数据分析、数据建模、图像处理和数据转换经验

现任英国 Moorfields 荣誉研究员

# 11 路线图


Q1
2018
目标是验证各个核心模块的算法，得到一个最小化可行模型
最小可行性验证
共识算法实现(模拟网络环境)
签名、哈希算法
帐号地址生成算法
智能合约与虚拟机原型
RPC接口与命令行工具
Q2
2018
目标是串联各个模块，让用户价值中以测试网络进行转移
P2P网络传输(基于DHT的Gossip协议实现)
矿工激励机制
共识打包机制
交易计费策略
Q3
2018
目标是实现高级协议，打通森林链拓扑下的价值传输渠道
传输协议
命名价值传输协议（实现多边之间的寻址）
跨链传输协议
链计算
命名机制
子链接入协议
主链的配套服务
Q4
2018
目标是发布正式网络
发布正式网络
安全审计，进行大量测试、攻防演练
SDK
区块链浏览器
开发应用示例
IDE v1.0
钱包实现




# 12 后记

本白皮书仅是对元一涉及的关键技术和生态系统的部分概览。技术的发展和进步无止境，新的应用形态也在不断涌现，元一的白皮书将随着技术的进步和应用的拓展而持续更新。本着共创价值互联网新纪元的宏大目标，元一欢迎全球开发者和服务提供商加入元一生态体系，共同营建一个创新发展、开放共赢的价值互联网新生态。

# 13 参考文献

1. Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, http://ethereum.org/ethereum.html

2. https://en.wikipedia.org/wiki/Smart_contract
3. Oded Goldreich and A Warning, Secure multi-party computation, 1998
4. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
5. https://en.wikipedia.org/wiki/Attribute-based_encryption