



eRoc  
商业白皮书

V1.90  
(内部文件)

实现App到dApp快速迁移的基础链

## 目录

摘要 :	1
术语说明 :	2
第一章 eRoc 项目背景 .....	4
1.1 区块链 3.0 逐渐兴起.....	4
1.2 区块链面临的挑战 .....	4
1.3 eRoc 的提出.....	5
第二章 愿景、使命、价值观.....	7
2.1 愿景 : App 秒变 dApp .....	7
2.2 使命 : 技术创新, 链接传统 App 和区块链 .....	7
2.3 价值观 : 贡献即价值 .....	7
第三章 eRoc 技术方案介绍 .....	8
3.1 App 迁移框架图 .....	8
3.2 eRoc 系统框架 .....	10
3.3 eRoc 系统设计 .....	13
3.4 eRoc 系统原理 .....	18
3.5 确定性随机共识机制 DRC .....	20
3.6 DRC 独创性分析 .....	21
3.7 智能合约的异步分片执行机制 .....	23
3.8 不可外包工作量证明机制 .....	25
3.9 诚实执行证明机制 .....	26
3.10 渐进式分片存储机制 .....	26
3.11 特别说明 .....	27
第四章 核心优势 .....	28
4.1 支持传统 App 到 dApp 的快速迁移, 秒变 dApp .....	28
4.2 独创快速共识算法, 节能高效公平 .....	28
4.3 数据分片存储, 量再大也不怕 .....	28
4.4 合约分片运营, 从容应对交易高峰 .....	29
4.5 支持多语言开发, 吸引全球 99% 的开发者 .....	29
4.6 微内核设计让高深的区块链技术进入组装年代 .....	30
第五章 经济模型 .....	31
5.1 设计思想 .....	31
5.2 eRoc TOKEN (ERT) .....	31
5.3 eRoc 经济模型特点 .....	33

5.4 eRoc 对 dApp 开发者的扶植及保护机制 .....	35
5.5 拥有 ERT 的价值 .....	35
<b>第六章 团队介绍 .....</b>	<b>36</b>
6.1 核心团队.....	36
6.2 顾问团队 .....	39
<b>结束语 .....</b>	<b>40</b>

## **摘要：**

eRoc Foundation 于 2018 年成立于新加坡 ,由来自 Intel、Microsoft、Oracle 等知名 IT 企业的一群技术大咖发起。

eRoc Foundation 认为基于区块链的落地应用太少 ,或者说区块链上的 dApp 太少 ,这极大的打击了从业者的信心。如何快速的落地一批 dApp ,并通过这些 dApp 的落地 ,给具体的业务带来价值 ,是目前区块链发展的核心中的核心。不解决这一问题 ,区块链就不能得到真正的发展和应用。

基于这一现状 ,eRoc Foundation 在全球首先提出了“实现传统 App 到 dApp 快速迁移”的一种解决方案 ,该方案包含服务总线 BSB( Blockchain Service Bus ) ,全新的区块链共识算法 DRC ( Deterministic-Random Consensus ) 、智能合约的异步分片执行机制 APESC ( Asynchronous & Partitioned Execution of Smart Contract ) 以及渐进式分片存储机制 PSS ( Progressive Sharded Storage ) 。

该方案的实现思路是 :首先 ,通过服务总线 BSB ,将链上数据访问封装成标准接口 ,实现传统 App 对链上数据的快速访问 ;其次 ,内嵌交易数据缓冲池 ,调和链上、链下性能差异 ,保证数据的平滑 ;最后 ,支持中心化、去中心化、“中心化+去中心化”混合部署 ,使得开发者在利用区块链优势的基础上 ,充分的保护原有投资。

eRoc Foundation 希望聚焦技术本身 ,真正解决区块链所面临的核心问题 ,帮助开发者将目前 220 万 iOS App 、 360 万安卓 App 以及 300 万小程序中的某些应用或者是应用中的某些场景迁移到区块链上来 ,彻底实现区块链的应用落地。

## 术语说明：

**区块链：**

是一种去中心化的分布式账本系统，基于密码算法、共识机制、时序机制等，实现了系统中各节点的数据持续记录、即时验证、极难篡改、无法屏蔽等特性，从而可用于建立一套隐私、高效、安全的共享价值体系。

**eRoc：**

eRoc，建立在“边缘共识异步分片智能合约协议”基础上的区块链平台，支持传统 App 到 dApp 的快速迁移。这个词本身为 CORE 的反写，代表着我们的平台对去中心化这一区块链精髓的坚持。

**DRC：**

确定性随机共识机制( Deterministic-Random Consensus, 简称 DRC ,已经申请专利 )，创造性的实现了“确定性”、“随机性”的相融；DRC 共识算法，由不可外包工作量证明机制 ( PoWFOP )、诚实执行证明 ( PoHE )、诚实存储证明 ( PoHS ) 等众多先进算法和机制来保证和实现。

**PoWFOP：**

不可外包工作量证明机制 ( Proof of Work Featuring Outsourcing-Proof, PoWFOP )：如果一个用户需要加入 eRoc 系统成为节点，则该节点需要进行不可外包工作量证明。不可外包工作量证明机制设定了一个动态的计算复杂度，用以保证当前系统的安全性。

**APESC：**

智能合约的异步分片执行机制( Asynchronous & Partitioned Execution of Smart

Contract, APESC )。eRoc 采用异步和分片的方式来执行智能合约，提高系统运行效率，避免拒绝服务攻击。

PSS :

渐进式分片存储机制 ( Progressive Sharded Storage, PSS )。渐进式分片存储机制把区块内容按照一定规律分片并分别存储在不同的节点上，使得节点的存储压力显著降低。

ERT :

eRoc TOKEN 的简称，是 eRoc 生态内流通使用的基于以太坊 ERC-20 智能合约生成的代币。eRoc 主链上线后，ERC-20 合约代币将以 1 : 1 比例被兑换为基于 eRoc 的代币 ERT。

sERT :

sub eRoc TOKEN 的简称，是在 eRoc 之上所发行的 TOKEN。

# 第一章 eRoc 项目背景

## 1.1 区块链 3.0 逐渐兴起

现在的互联网为“古典互联网”，区块链为“新式互联网”，或者称为“价值互联网”。不言而喻，这是对区块链技术蓬勃发展的一种期许。区块链的发展，与开发者对其所带来的全新价值传递方式密不可分。区块链技术具有巨大的创新潜力，它使金融和公共领域的消费者受益匪浅。

2010 年为区块链 1.0 时代，2011 年至 2017 年为 2.0 时代。进入 2018 年，区块链将迎来 3.0 时代，区块链技术应用也将席卷全球，一个新的风口已然到来，各行各业跃跃欲试，试图赶上这场飞跃之风。

区块链 3.0 的到来，将成为信息发展史上最波澜壮阔的进化浪潮。做为第三代互联网技术，区块链 3.0 使得全行业处身于一个时代开启的时刻，站在了从信息互联网往价值互联网转向的十字路口。新时代已经来临，我们每个人都身在其 中。未来，无论你在何处，你都在链上；纵然你孤身一人，你依然在世界之中。这些变化将进一步引起人们价值观念、社会意识的变化，从而社会结构和运行机制也将随之而变。

## 1.2 区块链面临的挑战

区块链一天，互联网一年。区块链的触角，已经触及到货币、金融、经济、社会等诸多领域，高速发展的同时，也面临诸多挑战：

一是目前区块链上的 dApp 太少，少的可怜。业内把区块链喊的这么热，但几乎看不到什么 dApp，这极大的打击了从业者的信心，也是导致 Token 价值暴

涨暴跌的根本原因。如何快速的落地一批 dApp，并通过这些 dApp 的落地，给具体的业务带来价值，是目前区块链发展的核心中的核心。不解决这一问题，区块链就不能得到真正的发展和应用；

二是 PoW 共识速度慢或是耗费资源多。为了解决效率问题，有人提出了权益证明机制 PoS 甚至 DPoS，但其实质是准中心化或中心化的系统，控制网络节点的永远是固定的持有大量权益的人。比如比特股，交易速度非常快，但是发行权控制在创始人手里，随意进行增发，导致比特币市值一落千丈。

三是吞吐量低，无法满足在很多实际场景的应用。从技术层面来看，将区块链技术应用至实际行业场景中，需要解决交易速度、数据共识、节点维护等问题。当前比特币网络每秒仅能处理 7 笔交易，而较为领先的超级账本技术也只能达到 200 到 300 笔的水平；这与每秒上万笔交易处理能力的中心化系统相比，还有一大段距离。

四是区块链发展有中心化的趋势，背离了区块链的初衷。目前比特币和以太坊都有算力集中的趋势，区块发布逐渐被算力寡头们垄断；而宣称的 TPS 过百万的有些所谓公链，其 TPS 值不仅只停留在纸面，而且还是在事实中心化的系统架构上实现的。

五是主流公链支持的智能合约开发语言偏少。以“以太坊”为例，从编程的角度来讲，Solidity 作为新生语言学习曲线较陡，而且除了编写智能合约外并无其他应用领域。

### 1.3 eRoc 的提出

来自 Intel、Microsoft、Oracle 等知名 IT 企业的一群技术大咖，加上区块链

商务精英，发起了 eRoc 项目，正在打造一款真正的区块链 3.0 的公链产品，势将成为未来一年最耀眼、最值得关注的基础公链项目。

## 第二章 愿景、使命、价值观

### 2.1 愿景：App 秒变 dApp

传统的互联网，已经积累了近千万的各种 App/小程序，涵盖了游戏、金融、餐饮、旅游、购物、酒店、娱乐、培训等几乎所有行业，并仍在快速发展中。怎么能让这些传统的 App 快速的变为 dApp 并迁移到区块链上，且在这个过程中能充分的享有区块链所带来的优势，是 eRoc 作为一条基础链所要解决的核心问题，也是我们最大的价值。

### 2.2 使命：技术创新，链接传统 App 和区块链

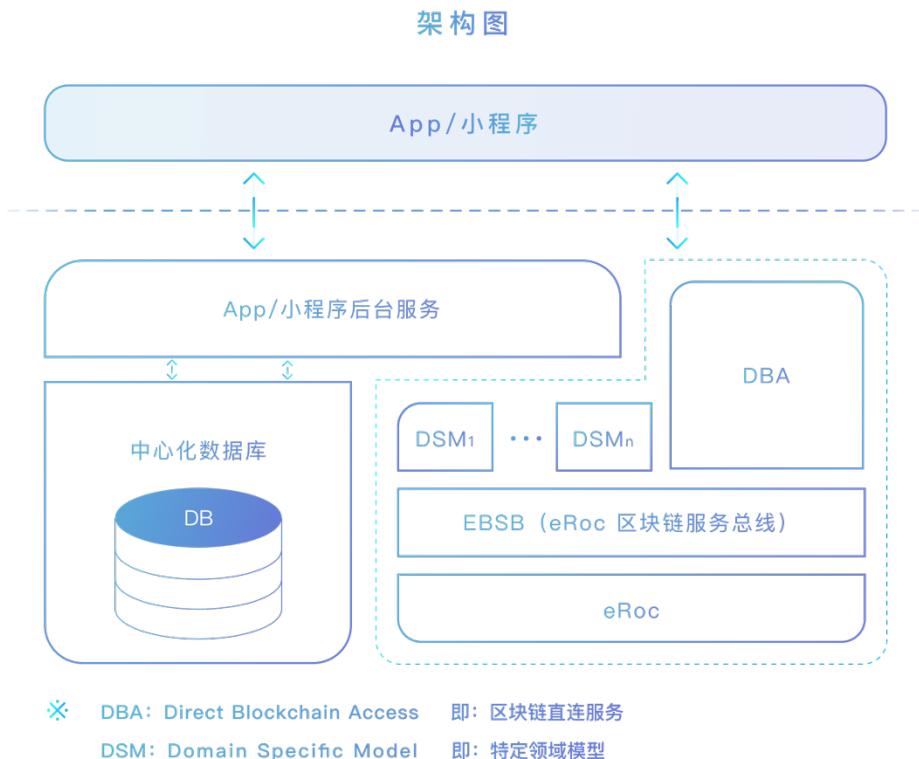
区块链是当前社会发生的一个重大的技术变革，会对未来经济产生重大影响。我们认为，只有专注技术创新，才能抓住这一历史机遇，才能使得 eRoc 成为传统 App 转型的基石，这是我们的历史使命。

### 2.3 价值观：贡献即价值

人的价值在于创造价值，在于对社会的贡献。任何人生存在这个世界上都不是孤立的个体，他都是这个社会大系统中的一员。他在依靠和享受其他社会成员劳动成果的同时，也在为其他的杜会成员作出自己贡献，并为此得到相应的回报。

# 第三章 eRoc 技术方案介绍

## 3.1 App 迁移框架图



目前在区块链圈存在一个很大的认识误区，那就是“去中心化一切”或者“区块链一切”，持有此误解的人或者鼓吹在区块链基础上开发全新应用，或者主张要把目前应用针对区块链进行全面重构，以至于把区块链和传统应用完全割裂对立起来。这种错误不仅阻碍了区块链应用（dApp）的普及推广，还造成了传统技术圈对区块链技术的严重抵触，非常不利于区块链技术的健康发展。而对区块链技术关注认可的传统 IT 圈人士，也因为掌握区块链技术本身及开发技能的学习曲线陡峭而心怀疑虑。

跟市面上常见的鼓吹“去中心化一切的”的看法不同，eRoc 团队从一开始就认为未来的区块链应用一定是中心化和去中心化的融合，即根据业务需求及技术指标，合理分配业务逻辑及数据到高性能的中心化系统和高可信的去中心化的系统中，各取所长，各补所短，在不影响用户体验的情况下，让区块链技术近乎对用户透明的方式在中间起作用。同时，我们也认为目前的存量应用中，很多也存在潜在信用问题，如果引入区块链技术，会显著提高用户的满意度，从而帮助他们在与同质产品的竞争中胜出。

基于这样的认识，我们在通用区块链体系之外，额外增加了一个针对应用开发者的软件开发包，当一个开发者需要使用 eRoc 区块链服务时，它需要在全节点之外，额外下载安装这个软件包，然后就能用自己原来的开发语言，如 Java 或 Node.js 来为应用增加区块链特性，包括小到把原先存放在数据库里的某些记录（如关键交易记录）或字段（如操作校验）上链，大到为区块链重新编写的业务逻辑。

这个新增的后台开发者模块，我们叫区块链中间件（BMW，Blockchain Middleware），主要由区块链服务总线（BSB，Blockchain Service Bus，即上图中的 EBSB，E 代表 eRoc），DBA（Direct Blockchain Access）组成，考虑到区块链在某些细分行业的用途更大并会被优先落地，我们又为这些行业专门增加了更加傻瓜式的 DSM（Domain Specific Model），让开发者可以直接用配置文件，或者极简代码方式来访问区块链的相关服务。DBA 的引入主要是让开发者可以用自己熟悉的方式编写纯区块链后端。

BMW 中间件的核心是 BSB，它工作在异步模式下，负责接收来自上层组件对区块链的添加和检索操作并进行必要池化，适时转换为底层区块链所能理解的

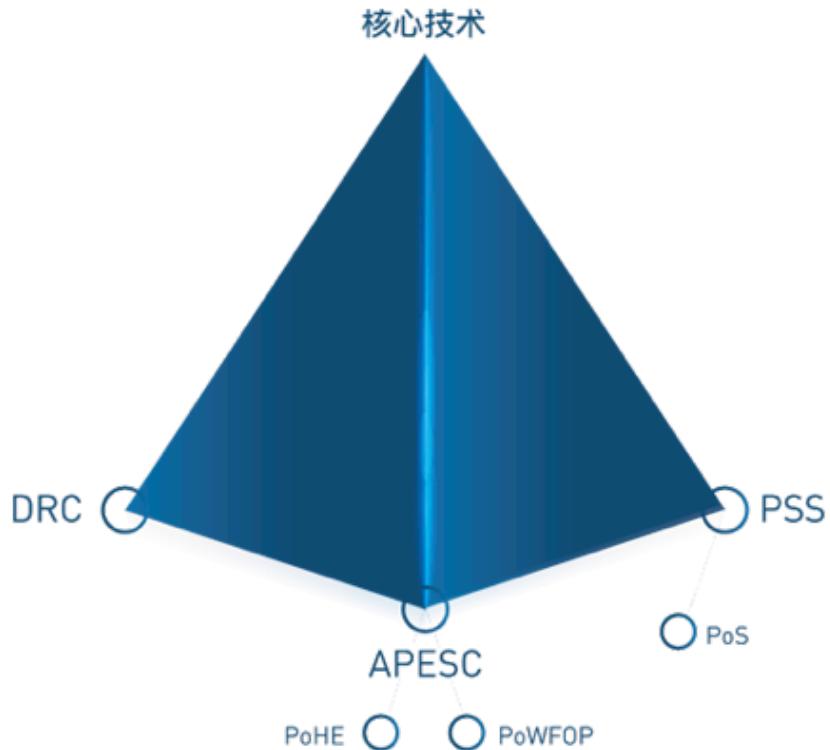
交易发布及读取请求，并在请求结束时，以异步/事件驱动的方式通知上层应用进行后续处理。在安全设计上，为了保证这个环节的数据不被篡改，系统将会生成单独的 ECC 密钥对，然后把请求时间、操作 hash 等更多校验数据打包进请求数据里，用私钥签名的方式进行发布。

在面向最终用户的界面展现上，eRoc 团队会推行一套界面设计指导，用无干扰的链接方式，允许用户点击相关位置并跳到区块链对应的浏览器应用中，来验证数据是否真的在链上。这个设计指导也是 eRoc 团队“Blockchain Ready”市场推广活动中的必要组成部分。

借助这个面向开发者的中间件，开发者打造去中心化应用的开发成本将大大降低，对外发布时间将极大缩短，从而使得去中心化应用的落地变得空前简单。

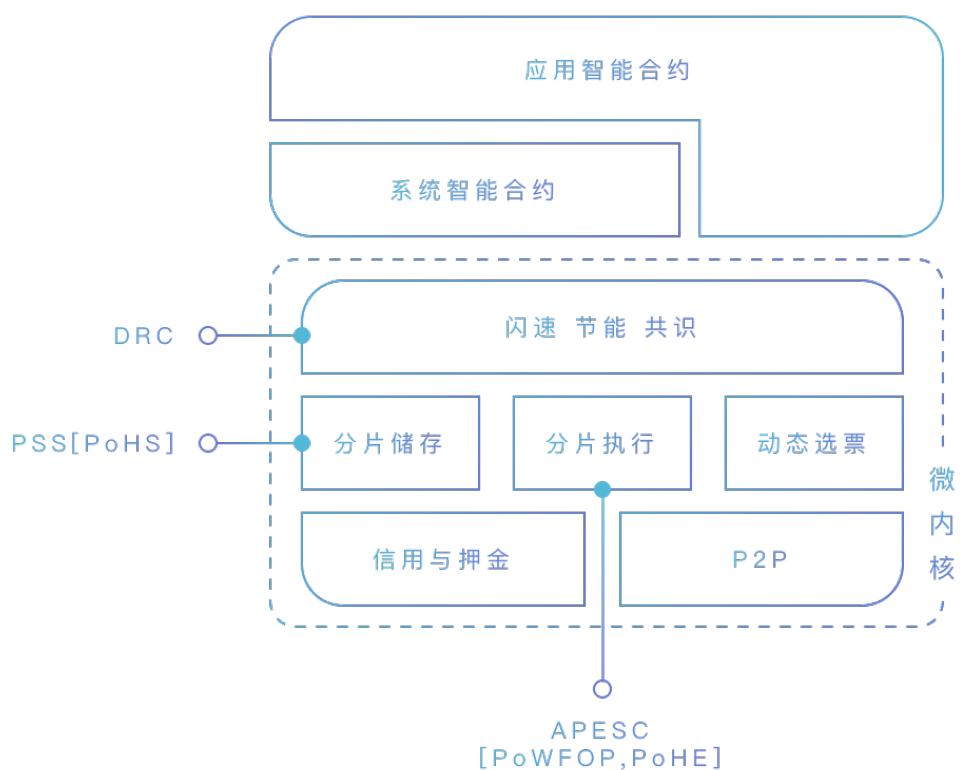
### 3.2 eRoc 系统框架

针对当前的区块链系统逐渐中心化、挖矿竞争过分激烈而导致资源浪费等问题，我们提出一个具有高度分布式特性和高效性的 eRoc 系统框架。该系统框架包含以下四项关键机制：确定性随机共识机制（Deterministic-Random Consensus, DRC）、智能合约的异步分片执行机制（Asynchronous & Partitioned Execution of Smart Contract, APESC）、不可外包工作量证明机制（Proof of Work Featuring Outsourcing-Proof, PoWFOP）和渐进式分片存储机制（Progressively Sharded Storage, PSS）。



本质上，我们仅使用了哈希函数和数字签名算法实现该系统，但是系统中的这四项机制对哈希函数和数字签名算法赋予了新的意义，使得系统的分布式特性和系统效率有了质的飞跃。首先，在安全方面，我们将表明如果系统仅实现简单的分布式记账功能，则安全性接近于比特币；如果系统实现智能合约功能，则安全性接近于以太坊。第二，在功耗方面，确定性随机共识（DRC）智能合约的异步分片执行和渐进式分片存储，这三大机制使得系统功耗远远低于比特币和以太坊，而不可外包工作量证明机制（PoWFOP）仅仅需要消耗与智能合约相近的计算开销。第三，在存储方面，我们提出的分片式存储机制不仅使得全网节点的存储压力显著降低，而且能够快速验证数据的正确性。第四，在分布式特性方面，工作量证明机制（Proof Of Work, POW）已经导致挖矿联盟，权益证明机制

( Proof Of Stake, POS ) 也促使财富过快集中 , 而我们提出的确定性随机共识机制 ( DRC ) 同时拥有的确定性和随机性 , 保证了高度的分布式特性。第五 , 在挖矿竞争方面 , 确定性随机共识机制 ( DRC ) 能够保证 eRoc 系统在相对安全的前提下 , 调节被选中节点数量以实现异步智能合约分片式运行 , 使得挖矿竞争压力可控而不是尽全力的提高计算能力以获得竞争优势。因此 , 与现有的区块链系统相比 , 我们提出的 eRoc 系统框架在安全性、系统效率、分片式存储、分布式特性、挖矿竞争这五个方面均有较大的优势。



### 3.3 eRoc 系统设计

比特币、以太坊，其巨大的技术优势早已得到社会的认可，但是其共识机制耗能高且逐渐失去去中心化特征。因此，我们提出 eRoc 系统框架，该系统的安全性与比特币和以太坊相近，但是其特性在于用确定性随机共识机制保障系统的高效性和去中心化特性。

在 eRoc 系统框架中，任意用户均能够通过简单测试、注册后进入系统，并在系统中产生一定活动行为，如交易。用户加入系统时，需要使用种子生成自己的私钥、公钥和公钥地址。由于公钥地址是唯一的，能够保障用户在系统中发起准确的交易请求。每笔交易单均记录了有关交易的具体信息，如付款人公钥地址，收款人公钥地址，付款金额，付款人签字，收款人公钥等信息；eRoc 系统中的用户交易是在智能合约中实现的。智能合约是指能够完成一定功能（包括交易）的函数，根据输入状态值，在多项式时间内输出另外一个状态值。

为保障系统安全性，eRoc 系统规定节点在执行智能合约的同时，还需要进行不可外包工作量证明或诚实执行证明。不可外包工作量证明是指通过运行一个不可外包计算的测试算法以证明节点本身拥有较强的计算能力，或能够完成计算复杂度较大的任务，而诚实执行证明则用执行步骤的正确性来佐证执行结果的正确，因此，与以太坊类似，我们提出的 eRoc 系统中的节点运行智能合约以完成交易或其他任务；而与以太坊不同，eRoc 系统节点需要运行与智能合约复杂度相近的不可外包工作量证明以保障系统安全性。

eRoc 系统中的节点有三种状态，分别为普通节点、幸运节点、领导节点。在系统运行的某一时刻，没有被系统选中的节点称为普通节点。普通节点不需要运行智能合约和不可外包工作量证明（或诚实执行证明）。在该时刻，被系统选中

的活跃的、希望挖矿的节点称为幸运节点。幸运节点运行智能合约和不可外包工作量证明（或诚实执行证明），且把智能合约结果和不可外包工作量证明结果广播给领导节点。

角色	主要职责
最新领导节点	收集交易、构造区块
前任领导节点	验证、汇总智能合约执行结果
幸运节点	执行智能合约
普通节点	验证、记录区块

为保障系统安全性和效率，系统通常会选中一定比例数量的幸运节点，而不会选择全部或较少的节点。同样，在该时刻，系统还会选择少数活跃的、希望挖矿的其他节点称为领导节点。一方面，领导节点收集上一时刻的领导节点广播的智能合约结果，进行有效性验证、并构造区块，然后广播到全网；另一方面，领导节点收集同一时刻的幸运节点执行的智能合约结果和不可外包工作量证明结果，验证其有效性并把有效的结果广播到全网，使得下一时刻的领导节点能够收集并验证有效性构造区块以广播区块。

原则上系统可以选出唯一的领导节点，但是在工程实现上，我们通常会取三个领导节点，分别称为第一领导节点、第二领导节点和第三领导节点，这样一方面可以因为防止突发事件，如停电或断网等造成的事系统停摆，也能避免自私挖矿行为。三个领导节点在规定时间范围内共同完成任务，但是 eRoc 系统区块跟随策略规定：首先跟随第一领导节点广播的区块，其次跟随第二领导节点广播的区块，最后跟随第三领导节点广播的区块。仅当第一领导节点广播的区块验证无效，或在规定时间范围内没出现时，才选择第二领导节点区块进行跟随，以此

类推。三个领导节点收集并广播智能合约数据和不可外包工作量证明数据，既保证系统区块创建的连续性和稳定性，又不会导致网络拥堵等问题。由于全网只有唯一的区块链，即每次仅一个领导节点广播的区块会被跟随下一时刻的领导节点跟随，因此，我们以下叙述中的领导节点默认为广播区块而被全网节点认可的领导节点，而不关注领导节点是第几领导节点。

与比特币、以太坊相比，eRoc 系统中的广播机制略有不同。幸运节点采用加密广播和明文广播方式。更加准确地说，幸运节点首先用领导节点的公钥加密智能合约结果，然后把智能合约结果密文消息与不可外包工作量证明结果明文消息一起广播到全网，使得全网节点（包括领导节点）均能够验证不可外包工作量证明结果的有效性，而仅有领导节点能够解密并验证智能合约结果的正确性。领导节点采用数字签名广播方式。更加准确地说领导节点收集智能合约结果密文消息与不可外包工作量证明结果明文消息，解密智能合约并验证智能合约和不可外包工作量证明的有效性。如果两项验证均成功，则对智能合约结果签名并广播到全网，使得下一时刻的领导节点能够收集。当下一时刻的领导节点接收到上一时刻的领导节点广播的智能合约结果及签名，则直接构造区块广播到全网。

eRoc 系统生成的区块内容包含上一区块的哈希值、本区块内容哈希值、序列号、时间戳、领导节点公钥、智能合约结果 Merkle 根、不可外包工作量证明 Merkle 根。一方面，在该系统框架中，领导节点收集并验证上一时刻的领导节点广播的智能合约的有效性并广播区块，以获得一定数量的系统奖励；另一方面，幸运节点运行智能合约并被领导节点认可并签名后广播给下一时刻的领导节点。以最快速度完成智能合约任务的少数幸运节点能够获得运行智能合约的交易费。因此，本系统框架中有两类挖矿活动，即领导节点挖矿和幸运节点挖矿。幸运节

点的数量可以由系统根据安全性和稳定性进行自动调节。因此系统能够控制挖矿竞争的激烈程度，而不需要节点尽可能提高计算能力以获得智能合约挖矿收益。因此，eRoc 系统实现了可调控的挖矿竞争，使得系统整体效率较高而不降低系统的安全性。

如果一个用户需要加入系统成为节点，则该节点需要进行长时间不可外包工作量证明。不可外包工作量证明机制设定了一个动态的计算复杂度，该计算复杂度是当前系统安全性的体现。当用户完成相应的计算工作量任务并广播到全网，则全网节点验证该用户不可外包工作量证明的有效性。如果验证有效，则存储该用户的公钥，即节点加入成功，否则拒绝，即加入失败。

为了降低系统的加入门槛，同时保证系统的安全性，eRoc 系统采用了信用积分与押金模式相结合的激励模式。在这一模式下，新加入的节点可以按照两种方式获得发块暨铸币权：一是通过长时间参与系统投票来证明自己诚实工作以逐步累积信用分，在到达阈值后可以参与发块权竞争，并在竞争胜出时获得系统激励，但每次获得代币后信用分将会被减去这一阈值，这样以来，工作在纯积分模式下的节点需要不断积累信用分来获取发块权；二是节点直接在账号里面直接押入一定数量的系统代币来获得持久发块权，存入越多的代币获得发块权的概率越大，但是随着存入代币数量的持续增加，这一概率的增加将趋于平坦。为了让两种模式平滑过度，押币下限为当前一次发块权所获得的系统代币数，也就是说一个节点在通过信用积分方式挖矿成功时，如果用户不把这部分代币提取的话，该节点工作模式将直接进入押金模式；反之，如果一个节点账号的押金低于阈值时，将自动切换到信用积分模式。为了避免有人用一次性加入海量节点并以恶意跟随的方式来影响投票的结果，从而用不诚实的方式获取铸币权，所有以信用积分方

式来工作的节点，在系统里面所投出的选票将不会记入区块得票。

在前面的叙述中，我们表明在系统运行的某一时刻，部分节点会被系统选为领导节点或幸运节点。该系统选择过程实际上是全网节点共同筛选完成的。因为输入值和计算过程是公开可验证的、公平的，而计算结果同时拥有随机性和确定性，所以该选择过程会得到全网节点的认可。因此，可以把全网节点共同筛选称为系统选择，而且该选择过程可以看作近乎绝对公平的随机选择。在筛选过程中，被选中的领导节点和幸运节点的筛选信息能够极快的从众多筛选信息中脱颖而出，领导节点和幸运节点能够立刻广播区块或运行智能合约。系统对幸运节点和智能合约进行分片，每片幸运节点执行对应的智能合约。

有可能产生的一个攻击场景是：所有节点把智能合约的运行外包到一个云服务器上，与服务器共同分摊挖矿收益，使得整个系统的智能合约运行实际上是中心化的。幸运的是，我们提出的 eRoc 系统中的不可外包工作量证明能够阻止智能合约外包。该机制要求节点运行一个具有一定计算复杂度的不可外包算法以证明其计算能力，使得智能合约外包在经济上不可行。

另一个挑战是，eRoc 系统长时间运行后会产生较多的数据，导致存储能力较低的用户无法成为节点，或产生巨大的存储压力。同样幸运的是，eRoc 系统中的分片式存储机制把区块内容按照一定规律分别存储在不同的节点上，使得节点的存储压力显著降低，并且能够快速验证存储区块的正确性。

最后，我们的 eRoc 系统框架中的确定性随机共识机制中其确定性和随机性保障系统的高分布式特性和高效性；确定性随机共识机制结合智能合约的异步分片执行机制使得系统具有可控的计算竞争和高效的系统性能；不可外包工作量证明机制使得智能合约外包在经济上不可行，从而保证系统分布式特性和安全性；

而渐进式分片存储机制使得节点存储压力得到显著降低，从而能够吸引更多的一般实体用户，而进一步提高系统整体的稳定性和分布式特性。

### 3.4 eRoc 系统原理

eRoc 系统采用与比特币、以太坊相同的方式进行网络通信，即节点通过点对点通信协议保持联接。该协议充分利用点对点网络鲁棒性好、生存能力强、易于扩展等优势。然而，与比特币、以太坊不同，eRoc 系统的用户需要完成不可外包工作量证明并得到全网节点的正确性验证后才能成为节点，从而参与挖矿以获取收益。如图 1 所示的 eRoc 系统框架，在某一时刻，确定性随机共识机制/算法选择一个领导节点（序号为 1，背景为红色）和多个幸运节点（序号为 2，背景为红色）。这些幸运节点以最快的速度完成运行智能合约和不可外包工作量证明并把结果广播给领导节点，以期望获得运行智能合约的收益；而领导节点收集上一时刻的领导节点广播的智能合约和不可外包工作量证明结果，并进行有效性验证以构造区块广播到全网，以获得系统奖励；此外，还收集幸运节点执行的智能合约结果和不可外包工作量证明结果，并对正确的结果进行数字签名并广播到全网；在下一时刻，确定性随机共识机制选择出下一个领导节点（序号为 1，背景为蓝色）和多个幸运节点（序号为 2，背景为蓝色），则该领导节点和幸运节点以相同的方式工作。再下一时刻，确定性随机共识机制选择出下一个领导节点（序号为 1，背景为绿色）和多个幸运节点（序号为 2，背景为绿色），则该领导节点和幸运节点以同样的方式工作，以此类推。因而，eRoc 系统实现了智能合约的异步分片执行。

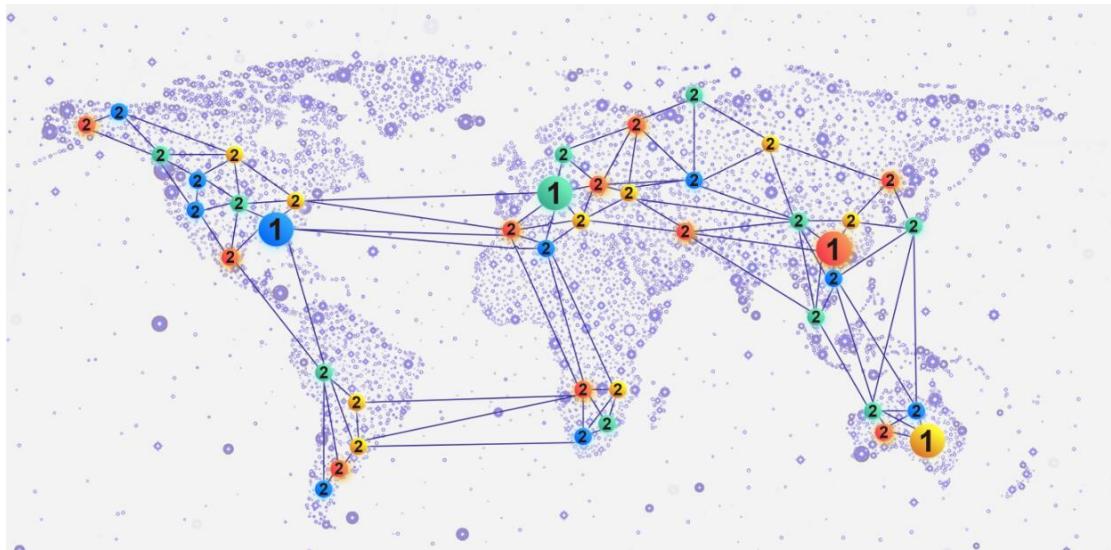


图 1

如图 2 所示 eRoc 全链，区块内容包含上一区块的哈希值、本区块内容哈希值、序列号、时间戳、领导节点公钥、智能合约结果 Merkle 根、不可外包工作量证明 Merkle 根。在图 2 中， $K=4$ ，则序列号为  $4n+1$  的区块为红色，序列号为  $4n+2$  的区块为蓝色，序列号为  $4n+3$  的区块为绿色，序列号为  $4n+4$  的区块为黄色，其中  $n=0,1,2,\dots$ 。

渐进式分片存储机制使得一般用户存储区块成为可能。如图 3 所示，某类节点仅需要存储浅红色的区块和其他区块的两个哈希指针，即上一区块的哈希值和本区块内容哈希值。如果系统节点数量较大，则能够对系统节点分为  $K$  类，使得各节点仅需要存储的数据量约为  $1/K$ ，从而显著降低存储压力。在工程中，为实现快速访问，我们规定  $K$  取值最大为 32。图 2 展示了 8 个区块，而节点仅需要存储其中对应的两个区块和其他区块的两个哈希指针。如果两个区块序列号的模  $K$  值相等，则两个区块相关，否则不相关。因此，我们把区块序列号的模  $K$  值称为区块相关系数。在渐进式分片存储机制中，如果节点的公钥的某个函数值与某个区块相关系数相等，则仅需要存储该类区块，而不需要存储其他区块。

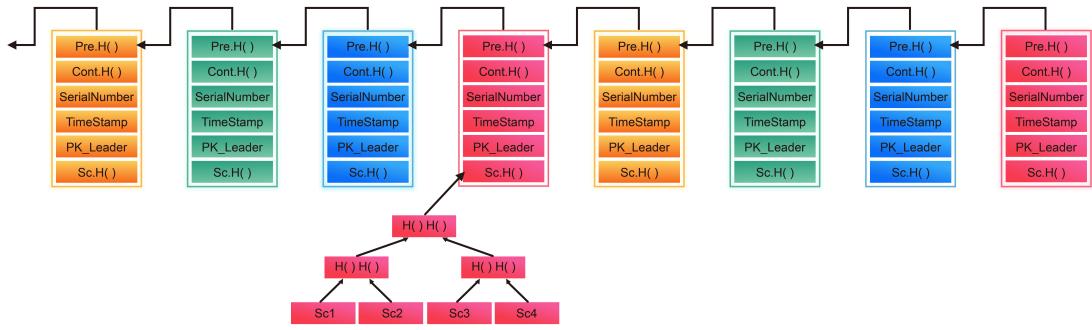


图 2

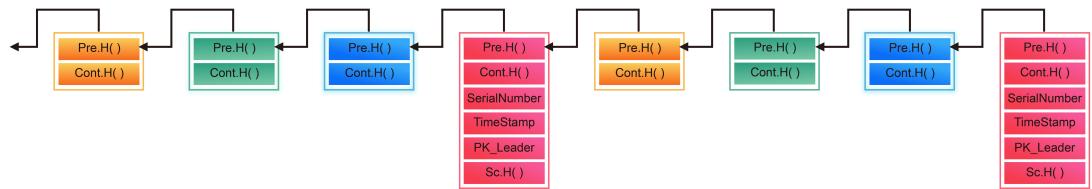


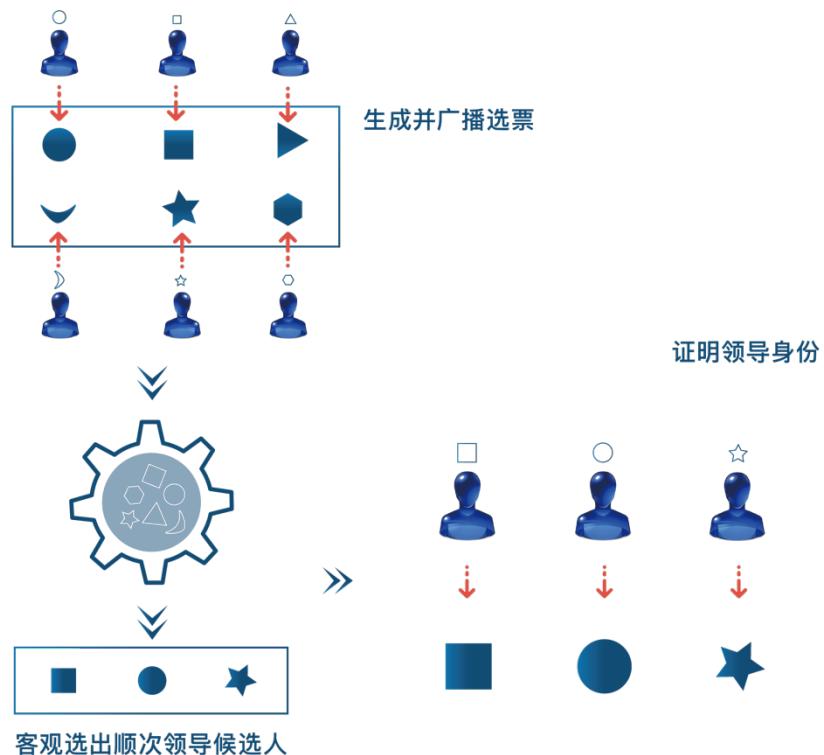
图 3

### 3.5 确定性随机共识机制 DRC

全网节点如何选出领导节点？选举过程是否公平？是否能够预测出下一时刻的领导节点？选举出来的领导节点是否在线？选举结果是否公开可验证？这产生了一系列问题。

幸运的是，我们的 eRoc 系统框架中确定性随机共识机制对上述一系列问题都能给出令人满意的答案。确定性随机共识机制规定：根据存储系数存储了当前区块的节点能够参与下一轮区块选举。这类节点根据系统种子和可验证随机函数，发布自己的区块，并在被投票节点多数跟随的情况下成为系统唯一确认区块。因为系统种子及可验证随机函数对全网节点来说均是公平的，所以能够计算的结果也是公平的。由于可验证随机函数不可预测，使得任意攻击者无法预测下一轮的区块来自哪个节点，从而无法对这些节点进行定点攻击。一方面，引言中已经说随机函数结果满足阈值的多个节点具有发块权且以最小值为跟随规则，因此，即

使发生突然事件，如区域性停电，也不会影响区块生成的稳定性。另一方面，被选中的一定比例数量的幸运节点需要通过竞争方式才能获得利益，因此系统具有可控的竞争压力。最后，算法所采用的限门哈希函数的计算复杂性低，不影响系统整体性能。



### 3.6 DRC 独创性分析

DRC 是 eRoc 独创的共识算法，与同样宣称节能快速的其他共识算法有显著不同。以下是 DRC 与 Algorand、Dfinity 的比较：

Algorand 共识机制：全网节点随机选择出一定数量的领导节点和验证节点。领导节点构造区块广播到全网，而验证节点对认可的区块进行数字签名以表明认同该区块。获得数字签名最多的区块则成为合法区块。

第一、Algorand 假设所有节点全部在线，且诚实参与方占  $2/3$  以上才能保证系统安全运行。假设节点全部在线不符合实际实际情况，即使节点全部在线，也存在节点不希望耗费计算资源而挖矿的节点，而  $2/3$  为诚实节点假设太强。

第二、广播的区块获得局部验证者（即少数节点）最多的数字签名，则被认为合法区块，因此验证方式为局部验证，即局部共识。

第三、Algorand 区块消息确认需要多次，即多个验证者对同一个区块签名，签名最多的区块则为全网共识区块。因此，多个领导节点广播多个区块到全网，被多个验证者签名，此过程网络资源占用最高。

第四、Algorand 算法在椭圆曲线群上基于计算性 Diffie-Hellman 困难假设，多次使用计算复杂度一般的数字签名算法以实现共识。

Dfinity 共识机制：全网节点随机选出一个委员会，该委员会包含随机灯塔和公证处。随机灯塔以去中心化的方式产生随机数，确定一定数量的分级用户。分级用户把区块广播到全网，经公证处认证后则成为合法区块。

第一、Dfinity 假设所有节点全部在线，且诚实参与方占  $2/3$  以上才能保证系统安全运行。与 Algorand 类似，这两个假设均存在较大的缺陷。

第二、分级用户广播的区块需要被公证处（即少数节点）认可，则被认为合法区块，因此验证方式为局部验证，即局部共识。

第三、委员会和分级用户由上一委员会随机选择出，因此是局部选择的。

第四、区块认证过程使用了门限签名算法，消息确认过程需要公证处节点数量 51% 的签名才能够形成正确的门限签名以构造合法区块。因此，多个分级用户广播区块而公证处验证并进行门限签名，该过程占用网络资源最大。

第五、Dfinity 算法在椭圆曲线双线性群上基于双线性 Diffie-Hellman 困难

假设，使用计算复杂度较高的门限签名算法以实现共识。

eRoc 共识机制：全网节点根据节点广播的选票值共同筛选出在线的且希望挖矿的领导节点和幸运节点。幸运节点运行智能合约和不可外包工作量证明并发送给领导节点。领导节点接收并验证智能合约和不可外包工作量证明的有效性，对有效的结果进行签名广播到全网，使得下一时刻的领导节点能够构造区块以广播到全网。

第一、eRoc 不需要节点全部在线，但要求 2/3 在线节点为诚实参与方。为了保证这一点，我们设计了信用积分与押金相结合的工作模式。

第二、广播的区块需要被全网节点认可，则被认为合法区块，因此验证方式为全网验证，即全网共识。

第三、系统确认区块的做法是后稳定的，按照系统种子和可验证随机算法所指定的动态投票团的选票多数来决定哪个区块最终胜出。在一般情况下，这一多数可以在网络状况良好的节点间快速达成，所以可以实现一定程度的异步性。

第四、发块节点由系统种子和可验证随机算法来指定，但是与投票团的算法彼此正交，从而可以有效避免定点攻击。而区块后稳的选票的多少不唯一取决于区块跟随规则，也取决于区块的扩散速度，这样实现一定程度上的发块异步性。

第五、eRoc 算法在椭圆曲线双线性群上基于离散对数困难假设的陷门哈希函数决定发块权，基于计算性 Diffie-Hellman 困难假设的多重签名算法决定投票权并对区块投票以实现共识。

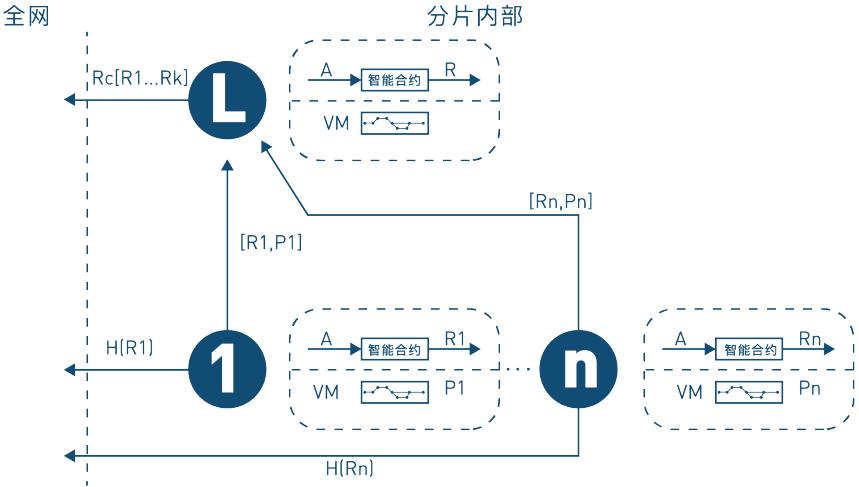
### 3.7 智能合约的异步分片执行机制

目前的区块链设计中，智能合约的执行都是在正常数据验证之外同步执行的。

然而恶意设计或低劣的智能合约会占据较长的运行时间 ,从而影响正常的记账行为 ,造成事实上的拒绝服务攻击。当前的智能合约经济模型分为权益保证和收费执行。两者在防止拒绝服务的处理上采取了不同的策略 ,前者要求智能合约必须在发块间隔内完成操作 ,后者则用经济方式来限制恶意行为的发生。

但是 ,这两个方式存在明显的缺点 :权益保证无法执行复杂逻辑的智能合约或者多层的智能合约调用 ,从而限制了分布式应用能力 ;收费执行看似比较合理 ,但是也存在两个缺点 ,一、气的消耗量与计算复杂度并不匹配 ,仍然存在利用廉价但耗时的操作进行拒绝服务攻击的可能 ;二、快速波动且高昂的气价导致智能合约执行成本昂贵。

我们在 eRoc 的设计实现上采取了不同的策略 :首先 ,采用异步执行方式来运行智能合约 ;其次 ,用分片执行的方式运行智能合约以避免拒绝服务及 SPAM 攻击 ;最后 , eRoc 系统中智能合约的执行采用了免费或者是支付发布者自己发行的 TOKEN 的方式 ,使得成本可控、发行成本低。



### 3.8 不可外包工作量证明机制

在 eRoc 系统中，所有节点都是被随机选择的，使得系统的运行效率极高。但是，执行智能合约需要一定的计算能力，而节点可能会把智能合约的运行外包到云服务器，从而与云服务器共同瓜分挖矿收益。一个极端的情况是：如果所有的智能合约均外包到一个云服务器上，则整个系统智能合约的运行实际上是中心化的，从而导致系统失去分布式特性。

因此，eRoc 系统要求幸运节点运行智能合约的同时，还需要完成不可外包工作量证明，防止智能合约外包问题，以保证系统的分布式特性。该机制要求节点运行一个不可外包计算的算法以证明节点本身具有较强的计算能力。更加准确地说，节点要证明其本身能够亲自完成比智能合约所需计算复杂度略大的计算任务。

因此，在该机制下，节点缺乏将智能合约外包的经济动力。

### 3.9 诚实执行证明机制

对于一个智能合约，节点对智能合约运行过程中的某些可验证的随机步骤和最终结果进行签名并发送给领导节点，使得领导节点能够验证并广播。因此，幸运节点必须保证智能合约中间过程和结果的正确性，否则将无法获得挖矿收益并失去挖矿权利。

### 3.10 渐进式分片存储机制

对于 eRoc 系统中的渐进式分片存储机制，主要考虑节点的存储公平、分片大小、快速访问、存储外包四个方面的问题。eRoc 系统长时间运行后，会给节点带来巨大的存储压力，容易导致存储能力较低的实体无法成为节点进行挖矿。

幸运的是，渐进式分片存储机制把区块内容按照一定规律分片并分别存储在不同的节点上，使得节点的存储压力显著降低。因此，如何公平快速地存储区块数据是 eRoc 系统的关键问题。

我们提出的 eRoc 系统采取随机分配策略，该策略规定各节点公开计算自己的存储系数。如果节点的存储系数与区块序列号相关，则存储该区块，否则拒绝。其次，如果渐进式分片存储机制把区块链分为过多的片，则其他节点之间的相互访问速度较慢，且存储不安全（因为存储特定数据的节点数量太少）。相反，如果分片取值太大，虽然区块存储安全，且访问速度很快，但是存储压力仍然很大。

因此，我们充分考虑存储压力、存储安全（或存储分布式特性）、区块数据访问速度这三者之间的关系。相关研究数据表明 如果区块数据较少，如低于 200G，

则存储全部区块链。如果区块数据较大，如超过 200G，则分片存储。因为 eRoc 系统中的区块包含两个哈希值，即上一区块的哈希值和本区块内容哈希值，所以任意其他节点能够快速读取并验证分配数据的正确性。

对于存储外包问题，渐进式分片存储机制中要求节点本地存储一定数量的区块，且其他节点可以快速验证该节点存储内容的正确性。

### 3.11 特别说明

《eRoceRoc 项目商业白皮》中仅仅是对 eRoc 技术部分做了概略性描述。如需详细了解具体算法、协议及理论证明等细节，请向 eRoc FOUNDATION 索要《eRoc 技术白皮书》。联系电子邮件：Xihua.Duan@eRoc.IO

## 第四章 核心优势

eRoc 有六大核心优势：

### 4.1 支持传统 App 到 dApp 的快速迁移，秒变 dApp

采用区块链服务总线，将链上数据访问封装成标准接口，实现传统 App 的快速访问切换；内嵌交易数据缓冲池，调和链上、链下性能差异，支持中心化、去中心化、“中心化+去中心化”混合部署。

### 4.2 独创快速共识算法，节能高效公平

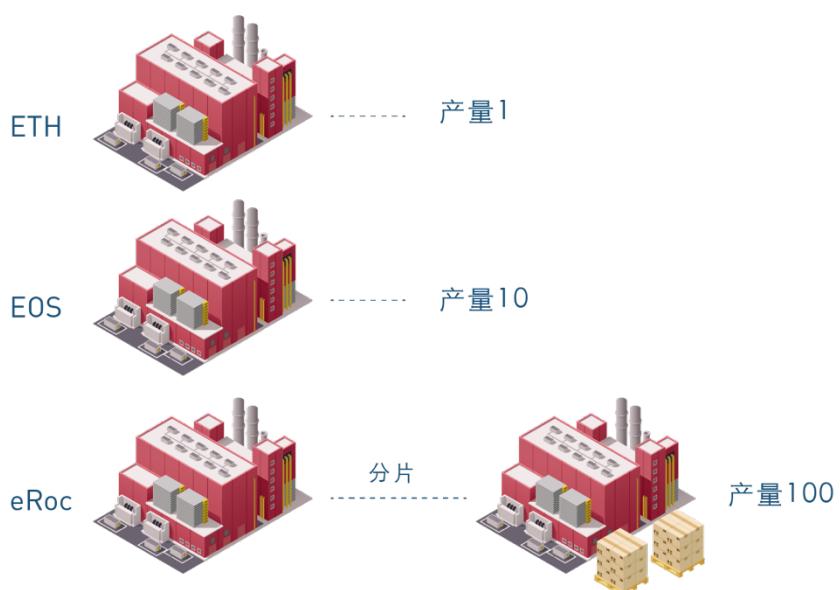
全球独创的去中心化共识算法 DRC：确定性随机共识机制（Deterministic-Random Consensus，简称 DRC，已经申请专利），创造性的实现了“确定性”、“随机性”的相融；DRC 共识算法，由不可外包工作量证明机制（PoWFOP）等众多先进算法和机制来保证和实现，没有过多算力消耗问题，真正的平民化、零门槛，从速度、效率、门槛、经济性、社会意义等角度优于 PoW、PoS 等共识算法。

### 4.3 数据分片存储，量再大也不怕

做为公链，随着时间推移，数据越来越多，存储面临着巨大的挑战。eRoc 独创智能分片式存储技术（已申请专利），一劳永逸的解决了公链数据不断增长的问题，使得海量数据的存储瓶颈不再成为公链发展的障碍，成为了极少数在创立之初就引入数据长期存储管理机制的稀缺公链。

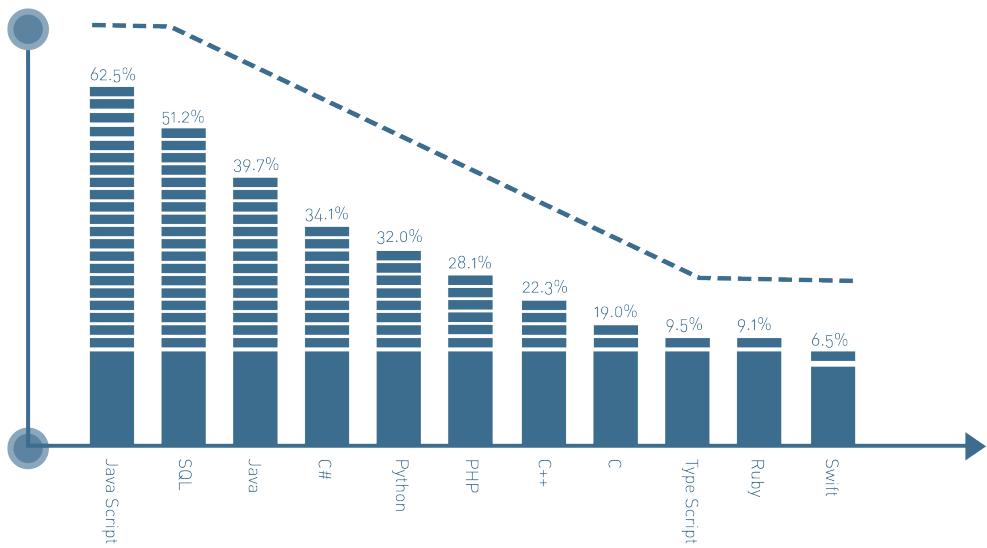
## 4.4 合约分片运营，从容应对交易高峰

完全基于自有技术的先进智能合约的异步分片执行机制，这种机制对整个网络的节点实行智能分片，形成多中心。每个分中心都同时执行不同的智能合约。通过节点级别并行的方式，极大的提高了智能合约的执行效率，增强了系统的吞吐能力。DRC 共识机制结合智能合约的异步分片执行机制使得整个 eRoc 系统具有可控的计算竞争和高效的系统性能，在系统效率、竞争压力、系统安全三方面达成了完美纳什均衡。



## 4.5 支持多语言开发，吸引全球 99% 的开发者

eRoc 支持使用更多的主流开发语言来开发智能合约。eRoc 将支持 Java、JavaScript、Go、C++ 等主流语言开发智能合约，覆盖了全球 99% 的开发者，为公链未来生态的发展打下了坚实的基础。



## 4.6 微内核设计让高深的区块链技术进入组装年代

英特尔将电脑模块化，人人都可以像搭积木一样组装属于自己的电脑，成为电脑进入千家万户的关键一步。eRoc 采用微内核技术，让区块链迅速适配各个行业的需求，正式进入个性化组装年代。微内核（Micro Kernel）把公链最核心的功能，如账本存储、共识、智能合约调度作为其核心，其他系统服务如节点都以系统智能合约的方式实现，提高了整个系统的灵活性、鲁棒性、可延展性。

# 第五章 经济模型

## 5.1 设计思想

eRoc 的经济模型，紧紧围绕着核心价值观“贡献即价值”而设计，重点是保证每一个 dApp 的开发者，都能利用 eRoc，在公平、公正的环境中，实现自己的创业梦想，贡献自己的独特价值。

eRoc 认为，TOKEN 网络价值=总交易量/速度。这是整个公链的价值基础。总交易量越大，说明需求越大，TOKEN 价值越大；速度越小，说明少人卖出，TOKEN 价值越大。

## 5.2 eRoc TOKEN (ERT)

好的经济模型，要实现 TOKEN 的高效、公平、可预期的生产及流转。

(1) 新增 ERT 的分配。通过自有独特共识算法 DRC，针对参与节点，实现了超快速度的共识确认以及不依赖计算能力的公平分配。

(2) ERT 的规模。ERT 总发行数量为 100 亿，其中一半(50 亿)用于节点奖励。公链上线后，头 4 年每年有 6.25 亿 ERT 给节点作为奖励，以后每 4 年发行量减半。

主要设计思想：为了维持一个经济生态的健康，一定数量的 TOKEN 是必须的，前期 dApp 数量相对不多，故每年有一定数量的 TOKEN 做为对节点的激励。随着 dApp 生态的丰富，节点的主要收入从挖矿转向智能合约的执行。ERT 的总量维持在 100 亿永久不变。

(3) ERT 在经济模型中的角色。eRoc 是一条公链，这就意味着，在 eRoc 之上

还有若干个子链，就是还有若干个智能合约，他们各自有自己的生态和 TOKEN（即 sub TOKEN，简称为 sERT），形成了自己的闭环。ERT 对 sERT 起到了锚定作用，这种思路，基本上是借鉴了金本位和美金的交互发展史。当然，不是所有的智能合约都有自己的 sERT，如，对 ERT 的转账，作为一个智能合约，就没有自己的 sERT。

金本位是通过纸币代表黄金的方法来保证纸币价值的信用货币制度。在金本位的后期，即在 20 世纪初期，各种金本位信用货币占全部使用货币的 70% 以上。可以说，那个时候金本位是国际货币的核心特征。这个过程在二战时被打乱。二战结束之后，美国战争中没有损失黄金，战后第一个宣布恢复金本位，一举奠定了美元的国际储备货币地位。但是，1971 年，美国取消了金本位制度，这其中当然有很多原因，但最主要的原因是，二战后随着世界经济的快速恢复和高速发展，黄金生产量的增长幅度远远低于商品生产增长的幅度，黄金不能满足日益扩大的商品流通需要，这就极大地削弱了金铸币流通的基础。就是说，经济发展太快，需要更多的货币来支撑，但依赖于黄金的保有量来发行货币，不能满足经济的发展需要。很多人说，放弃金本位，为各国货币普遍贬值、推行通货膨胀政策打开了方便之门，所以放弃金本位是错误的。但实际上，事物总有它的两面性。世界经济的体量和结构这些年发生了翻天覆地的变化，固守着黄金作为货币发行的锚定之物会阻碍经济的发展，至于由此引发的通货膨胀，虽是一个副作用，但人们此时应该做的是如何让自己的财物增长速度大于通货膨胀速度，而不是再回到金本位时代。

ERT 其实是借鉴了金本位和信用货币发行的优点，摒弃了其缺点。首先，ERT 是整个公链的锚定货币，与黄金类似，而子链上发行的 sERT，可以看作是类似

美金的信用货币 ;其次 ,公链上的各个子链 ,或者说各个子生态中所发行的 sERT ,其价值都是依照 ERT 来衡量。衡量的基本标准为 :sERT 的价值 = “子链发行者所拥有的 ERT”除以“发行的 sERT 的数量”。

#### ( 4 ) eRoc 中对参与节点的激励

主要有两个 :

第一个 ,就是前文中所提及的每年给节点的 ERT ,通过独特算法 DRC ,针对节点 ,实现了超快速度的共识确认以及不依赖计算能力的公平分配。

第二个 ,执行智能合约的节点 ,会得到 ERT 奖励或者是该合约所发行的 sERT 的奖励。

### 5.3 eRoc 经济模型特点

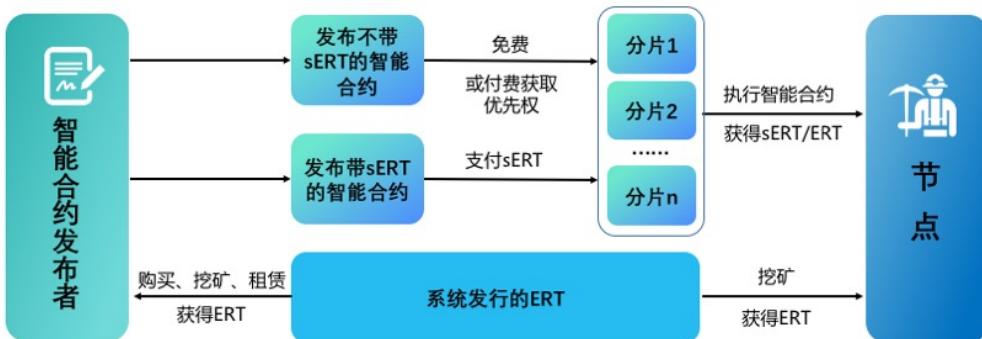
该经济模型的核心特点 :

( 1 )eRoc 经济模型的基础是 ERT 系统。该系统是吸收了金本位和信用货币的优点而构建的 ;

( 2 )eRoc 经济模型的核心是以 ERT 为锚定 ,以各个智能合约 ( 子链 ) 中所发行的 sERT ( 信用货币 ) 来作为具体应用场景的流转媒介 ;

( 3 ) 智能合约发行 sERT 时 ,必须以一定数量的 ERT 为锚定物。有了锚定物 ,使得 sERT 的价值有了衡量标准 ,其公式是 :sERT 价值 = 拥有锚定 ERT 的数量 / 发行的 sERT 的数量。这将做为智能合约执行优先顺序的标准。

#### ( 4 ) 模型示意图如下 :



### (5) 智能合约执行优先级

同一个分片中，先执行带 sERT 或愿意支付 ERT 做为费用的合约，谁的价值高先执行谁的；后执行免费的智能合约，谁拥有的 ERT 多，就先执行谁的；由于 eRoc 系统的智能合约是分片执行的，故不同的智能合约可能在不同的分片中，上述执行优先级仅仅是针对同一分片的。所以，从不同分片的角度看，并不总会是价值高的被优先执行。

(6) eRoc 落地场景：eRoc 的设计理念与其他的公链不太一样。eRoc 的核心是支持传统 App 往区块链上快速迁移，所以，落地的场景取决于传统 App 本身。eRoc 项目团队认为，未来众多商业场景，会是中心化和去中心化相结合，二者各取所需，各自发挥各自的优势，完全没有必要为了去中心化而去中心化。传统 App 中的财务/类财务数据、交易过程中的核心数据、重要操作的日志等，非常适合放在区块链上，做去中心化处理。

## 5.4 eRoc 对 dApp 开发者的扶植及保护机制

在为了保护广大 dApp 开发者、尤其是中小型开发者的合法权益，使得他们愿意、能够在 eRoc 上实现创业梦想，eRoc 从设计之初，就考虑针对开发者的扶植及保护机制：

- (1) 可以使用自己发行的 sERT 做为智能合约执行的费用，极大的降低了智能合约执行费用门槛；纵然未来 ERT 的价值再高，也不会影响智能合约的执行费用；
- (2) 独有的共识机制 DRC，使得节点无法形成算力垄断，保证了系统的连续性和一贯性；
- (3) 无论拥有 ERT 的多少，都能在 eRoc 拥有自己的舞台。拥有的 ERT 多，智能合约执行时，可以使用更多的资源；拥有 ERT 少，可以通过巧妙设计自己发行的 sERT 的数量，达到智能合约优先被执行的效果。所以，eRoc 系统不会忽略每一个 dApp 开发者，而是给他们每个人一个合适的舞台让他们贡献自己的价值；
- (4) 智能合约执行分片机制，使得不同的智能合约被随机分片，不会出现大户对资源进行垄断的现象。加入 eRoc 的节点越多，就可以有更多的分片，从而进一步提高了整个系统的 TPS。

## 5.5 拥有 ERT 的价值

由于 eRoc 支持传统 App 快速迁移到区块链、以及对广大 dApp 开发者的保护机制，使得基于 eRoc 的 dApp 生态蓬勃发展是大概率事件。

对于 dApp 开发者，您一定要拥有 ERT，越多对您的 dApp 生态越好。

不计划开发 dApp 的 eRoc 粉丝，也可以将 ERT 租赁给 dApp 开发者。

## 第六章 团队介绍

### 6.1 核心团队

段夕华：主导架构设计工作



毕业于复旦大学计算机系，硕士。原大路网、途安客 CTO。曾在高德全面负责与苹果和谷歌的新地图业务合作。在此之前，曾在全球最大芯片公司 Intel 工作 10 余年。从 1994 年开发商用软件 COK 算起，投身计算机信息技术行业已 20 余年。擅长技术团队管理、研发团队培养、新技术/新架构的实现，涉及从云到端的众多技术领域的研究、设计、开发、创新、布道、支持等工作，既有广泛技术积累与感悟，也有对商业和市场的敏锐度。

王晓光：主导研发及工程实现工作



毕业于清华大学信息系统和工程学院，硕士。原一起作业吧 CTO、聚美优品研发总监。专注于密码学、计算机网络和系统体系结构。他是 AnchorTech（信息安全）的创始人之一，Advance AI 的 CTO，是最大的虚拟专用网络之一的作者，SWFT 区块链的顾问。

### 陈绪：负责 eRoc 开源社区



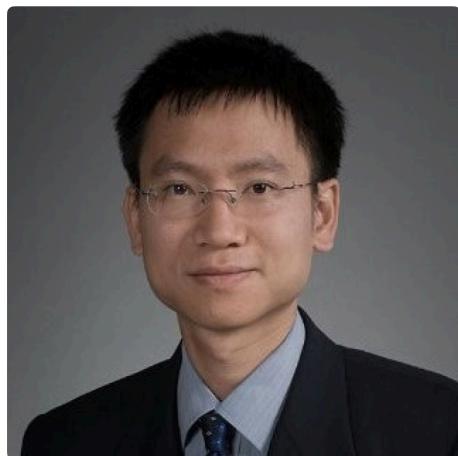
博士，曾任英特尔中国云计算战略总监、中国计算机协会会员、普适计算专委会委员、中国开源软件推进联盟常务副秘书长。1995 年至今，长期从事 Linux 技术和中国开源社区工作，2015 年荣获中日韩东北亚开源论坛最高奖项“特别贡献奖”。曾任 Sun 中国工程研究院高级工程师，北京泰宇科技有限公司技术总监。2007 年加入英特尔，历任 Linux 和开源战略经理，市场总监等职。陈绪先生 2002 年毕业于北京科技大学，师从中科院高庆狮院士，获工科博士学位。2014 年获得清华大学经管学院高级工商管理硕士学位。

### 华咤镇：负责研发



毕业于复旦大学计算机系。曾任职于富士施乐、微软公司，长期担任高级软件工程师、资深软件工程师。后任职于深圳创新投资有限公司，专长于互联网/高科技企业投资。2015 年创立美港通互联网金融有限公司。对系统软件开发、高新技术风险投资有丰富的经验。

### 欧嘉致：负责研发



毕业于美国名校卡内基梅隆大学计算机系。原任职于美国 eBay 公司，领导物流运输追踪团队的研发。在 eBay 之前，任职于美国微软公司，负责网络检索与搜索引擎的开发。在新技术的行业落地开发方面有着丰富的经验。

### 陈景伟：主要负责 dApp 开发伙伴孵化、市场推广、政府关系



湖南大学自动化专业毕业，后在中科院心理研究所深造心理学。曾在 Intel 任职 11 年，主要负责全国高新区/软件园创新中心 / 企业孵化器运营工作，支持、辅导、孵化与投资高科技创新企业。在 Intel 之前，在金蝶软件集团工作 8 年，曾任集团市场副总经理、PR 总监、公共关系总监等职。

## 6.2 顾问团队



Gansha Wu: 驭势科技 CEO , 原英特尔中国研究院院长 ;



Liang Zeng: 原微软中国副总裁、国际数字资产慈善基金会主席;



田甲: CortexLabs.AI 首席科学家、比特币早期投资者、Zcash 社区选举人、BitFinex 股东;



陈滢: 慧科集团副总裁 , 原 IBM 中国研究院副院长;



董耀祖: 英特尔首席工程师 , 全球知名虚拟化专家;



陈庆: 绿盟联合创始人 , 高级研究员 , 知名计算机安全专家 , 网名 " 小四 ";



魏育成: 中科院电子所教授级高工 , 博士 , 国产 FPGA 芯片公司中科亿海微总裁 ;



冯强: BOE ( 京东方 ) 集团高级副总裁 , 健康服务事业群 CEO;



周霖: 水木社区创始人 , 原搜狐技术副总裁 , 搜狐旗下狐狸金服联合创始人兼 CTO。

## 结束语

人类社会从来不缺少美好的愿望，只不过在过去漫长的岁月中，难以因为具体的动机而汇聚。eRoc 让这些已经存在着的、碎片般散落的点滴美好，瞬间汇聚出灼热的能量。eRoc 将使得每一个可能都不被忽略，每一个声音都面对着世界，每一滴水珠都等同于大海，每一个你都体现价值！



实现App到dApp快速迁移的基础链

Contact: Xihua.Duan@eRoc.IO

2018年8月21日