

Ether Data (ETD) 白皮书

2021年7月 v.2.6



目录

序

1. ETD
 - 1.1 BOINC简介
 - 1.2 从BOINC到ETD
 - 1.3 ETD本质
 - 1.4 设计理念
2. 技术架构
 - 2.1 EMP2P网络
 - 2.2 双盲匹配算法
 - 2.3 M:N匹配过程
 - 2.4 公链特性
 - 2.5 ETD算力机
 - 2.6 技术优势
3. 凭证发行
 - 3.1 ETD贡献值凭证
 - 3.2 出块规则
 - 3.3 分配规则
 - 3.4 治理机制
 - 3.5 锁仓机制
4. 生态建设
 - 4.1 链委托与链结算
 - 4.2 跨链支付和流通
 - 4.3 ETD记账节点
 - 4.4 激励机制
5. 凭证运用场景
 - 5.1 时间银行
 - 5.2 智慧城市

- 6. ETD基金会
 - 6.1 ETD通用计算实验室
 - 6.2 创新工场
- 7. 核心团队
- 8. 风险提示与免责声明

序

随着区块链行业拥抱理智、走向成熟，参与者普遍放弃了中心化-去中心化对立，监管-民主对立，浪费-环保对立的二元叙事结构，抽身于中本聪原教旨主义的宏大许诺与加密货币炒作乱象之外，转而探索区块链的多元实用价值。其中，一部分探索者把目光投向了人类科学共同体，因其天然具有无国界、有共识机制、有广播行为、产品（即知识）可自由流通等特征，与区块链的多项基本特性高度类似，两者在底层意识形态上无可置疑地具有合作的前提。

用比特币为科研机构捐款是最容易想到的途径之一，而现在我们相信，这只不过是一种最为原始和低效的途径，因为让区块链社群成员直接参与现实世界科学研究，实现人人贡献、人人享有的整套公开透明的技术方案已经成熟，不仅解决了所有主要技术难关，并且构建了符合经济学逻辑的生态法则，这就是以太数据（Ether Data，ETD）。

ETD的构想来源于分布式计算与时间银行两个概念的碰撞。时间银行概念最初在十九世纪被提出，核心理念是每个人的单位时间的价值都是平等的，因此银行发出的交易凭证上只记录时间，不记录价格；任何人今日贡献的两小时，可以在未来换取他人的两小时。而在分布式计算中，每个节点贡献的单位算力，价值同样是平等的，大量节点互相通信、汇集成算力足以匹敌超级计算机的集群，或者说组成了一个地理位置分散在全球各地的虚拟超级计算机，而在所有人类事业之中，最能够跨越地域与文化障碍，团结海量参与者自愿贡献算力的事业，在当今世界非科学莫属。

在迄今为止的几次科学范式转移中，“计算”的地位不断提高，含义也发生了演变，甚至其本身已经成为一门显学。数字化革命以来，科学家不再能够像第一、第二次科技革命时一样，单枪匹马加一叠稿纸就做出世界级发现；而万物互联的大数据时代到来后，一个团队加数十台电脑的模式也因其有限的算力——无论是人脑还是电脑——而逐渐被淘汰。由OpenAI开发的人工智能GPT-3，从全网收集了45TB的文本数据，才训练成为当今顶尖的自然语言处理模型。

同时，互联网早期的共享精神正在式微，不仅全网用户数据被数个寡头瓜分；而且在科学界，以Sci-Hub为代表的免费论文网站也被学术出版财阀围追堵截而面临关停。这不仅导致学者必须缴纳高昂的出版费用，还在科学发现传播给公众与潜在投资人的过程之中设置了人为壁垒。互联网已不再互联，科学界需要下一代的互联网——一个算力强大、价格合宜的计算平台；一个开放透明、人人可用的信息流通中介。公众需要下一代的

互联网——如果将人类科学事业作为一间上市公司，那么所有人都是持股人，因为科学对现实的塑造无微不至，即使对科学漠不关心的人也概莫能外。

通过分布式计算整合分散在世界各地的聪明头脑和计算资源，通过作为金融技术的时间银行让每个科研团队与普通资源贡献者劳有所得，最终构建一个符合人类长远利益与经济学激励机制的良性博弈生态圈，就是ETD的愿景。

1. ETD

ETD(Ether Data)是结合以太坊智能合约和共享区块链DSB (Disk Storage Banking) 分布式存储和安全计算技术，旨在为伯克利开放式网络计算平台(BOINC)和其他科学计算平台贡献公众算力的分布式网络通用计算系统。其共识算法采用全新的PoCS (Proof of Computation-Storage)机制，即综合了PoW和DSB PoS，定位为易用的高性能应用区块链平台，同时满足现实科研机构的计算需求、网络应用的存储和计算需求，以及算力贡献者获取回报的经济需求。

为什么是以太数据，而不是以太坊？首先，以太坊、比特币等现存区块链，共识目的仅为记账，而ETD在获得共识的同时还解决了科学计算问题，为共识赋予了记账之外的价值。其次，在以太坊上只能执行智能合约，不能直接解决存储和计算问题，因此进行一笔科学计算要花三笔费用：gas费、可能十分高昂的Swarm存储费、以及支付给算力提供者的报酬。与之相比，ETD的技术架构集成了计算和存储功能，拥有更完整的用户隐私保护与身份认证机制、更低成本和更高效率，以及基于以太坊并且更契合多样化计算需求的智能合约，可为不同身份的认证实体及应用快速建立一个去中心化、资源共享和自组织的生态网络。

1.1 BOINC简介

BOINC是(Berkeley Open Infrastructure for Network Computing)的简称，由加州大学伯克利分校计算机科学系主导开发，是一个用于志愿者计算和网格计算的开源中间件系统。BOINC最初是为了支持SETI @ home项目而开发，后来成为一个用途广泛的分布式计算平台，涉及领域包括数学、语言学、医学、分子生物学，气候学，环境科学和天体物理学等。

BOINC旨在汇集分散在全球各地的志愿者的个人计算机，形成巨量运算资源以提供给科研人员。截至2021年6月3日，BOINC在全世界共拥73,006名志愿者，636,158台活跃主机，24小时平均算力为26.185 PetaFLOPS。在2020年3月的巅峰期，受到COVID流行病的公众对科研的热情，BOINC的24小时平均算力达到41.548 PetaFLOPS，最大算力在浮动间可以匹敌全球排名第五至九名的单个超级计算机。

| 排名 | 名称 | 地理位置 | 供应商 | CPU核心数 | 最大算力 |
|----|---------|-------------------|-------------------|------------|---------|
| 1 | 富岳 | 日本RIKEN计算机科学研究中心 | 富士通 | 7,630,848 | 442,010 |
| 2 | 高峰 | 美国橡树岭国家实验室 | IBM | 2,414,592 | 148,600 |
| 3 | Sierra | 美国劳伦斯利佛摩国家实验室 | IBM | 1,572,480 | 94,640 |
| 4 | 神威·太湖之光 | 中国国家超级计算无锡中心 | 中国国家并行计算机工程技术研发中心 | 10,649,600 | 93,014 |
| 5 | Sierra | 美国英伟达公司 | 英伟达 | 555,520 | 61,445 |
| 6 | 天河-2A | 中国国家超级计算广州中心 | 中国人民解放军国防科技大学 | 4,981,760 | 94,640 |
| 7 | FZJ | 德国于利希研究中心 | 源讯 | 1,572,480 | 44,120 |
| - | BOINC | 分布式 | 全球志愿者 | - | 41,548 |
| 8 | HPC5 | 意大利埃尼公司 摩国家实验室 | 戴尔 | 669,760 | 35,450 |

图表：超级计算机全球排行（2020年11月）

曾经和正在利用BOINC进行科学计算的项目均在其官网列出，其中比较有代表性的几个包括：

Rosetta@home - 研究蛋白质的折叠，近期致力于为COVID19寻找治疗方案

Docking@Home - 深入研究蛋白质键结和反应的原子等级构造和细节，用于研发药物

GPUGRID.net - 分子动力学

Climateprediction.net - 气候预测

Einstein@Home - 搜寻脉冲星的引力波

LHC@home - 模拟粒子加速，协助设计及改善LHC粒子加速器。

SETI@home - 搜索外太空文明

ABC@Home - 尝试解决ABC猜想

World Community Grid - 由IBM主持，主要目的为利用分布式计算来帮助寻找人类疾病的治疗方法，和改善人类生活的相关研究。

SZTAKI Desktop Grid - 搜索广义二进制数系

这些项目各自独立运作，有些设在大学和研究实验室，有些由私人团体或个人经营。贡献者(Crunchers)可以选择项目来贡献。目前一共有34个项目获得BOINC网站验证并维护的白名单资格；贡献者也可以填写特定的项目URL以加入其他项目。

BOINC由服务器系统和客户端软件组成，它们相互通过HTTP协议通信以分配和处理工作单元并返回结果。客户端可以远程控制。一项完整任务流程分为五个步骤：

1. 贡献者的主机从项目的调度服务器获取一组任务；
2. 主机从项目的数据服务器下载可执行文件和输入文件。如果项目发布其应用程序的新版本，则可执行文件将自动下载到主机；
3. 主机运行应用程序，生成输出文件；
4. 主机将输出文件上传到数据服务器；
5. 主机将完成的任务报告给调度服务器，并获取新任务。

1.2 从BOINC到ETD

BOINC自身拥有一个积分体系，每单位贡献被称为1 Cobblestone，由于BOINC作为最主流的分布式科学计算平台之一，拥有IBM等机构的巨额注资，无需寻求盈利途径，所以官方强调Cobblestone没有货币价值或其他价值，其唯一用处即记录每台主机贡献算力的多少，Cobblestone无法用于向其他志愿者换取算力，也无法跨平台流通。

BOINC作为开源系统的开放性质及其自身积分系统的全封闭特征，二者之间的矛盾构建出了一个巨大空间，使得任何为BOINC贡献算力的子网络，在理论上都能够采用区块链技术，制定与Cobblestone线性关联而又外在于BOINC，并且无法篡改的去中心化外部积分系统，从而令贡献者获取公认的、可自由交易的积分凭证。但是，由于科学计算任务的海量和非同质化特性，主机从BOINC服务器接到的每一项任务都由不同类型的运算组成，而且运算量极大，所以现存区块链平台（包括以太坊）无论从硬件还是软件层面都难以达成这一需求。而ETD区块链技术正是为这一目的而开发，其专有的分布式计算技术架构、凭证发行规则与生态建设原则，能够在为BOINC提供算力、获取Cobblestone的同时，按比例生成ETD通证，通过ETD时间银行机制和依托于ETD公链的分布式应用（DApp，Decentralized Application）生态圈，在时间和空间上都实现价值的自由流通和赋予，达成算力资源的深度共享与最优化调配。

1.3 ETD本质

志愿者通过ETD向BOINC和其他分布式科学计算平台献出的计算和存储资源，都将获得永久记录在链的凭证：真实，公开，透明，可查。以ETD凭证为流通手段，促进全球志愿者算力的合理共享与再分配，最终助力科学发展。通过ETD算力机完成科学运算而获得贡献值凭证的用户，将同时自动ETD算力贡献者身份。贡献值凭证可存入时间银行以获得利息，在有需要的未来提取，用于为自身换取计算资源；亦可通过公共流通池，在算力贡献者之间自由流通，打通科学界内外分野，自发实现全球计算资源最优化配置。无论个人或是机构，均可在ETD平台上搭建具有特定功能的分布式应用，提供各类互联网服

务，丰富凭证运用场景，吸引更多人主动加入全球志愿者社群，成为活跃主机之一，解决科学问题的同时得到实用回馈。

得以实现这一切的前提，在于ETD作为一个全新的区块链体系架构，在设计上实现了高速、稳定、安全及易用特性，使得它尤其适合进行分布式科学计算，并使得基于区块链技术的DApp开发者享有更广阔的创新空间及更高的效率。ETD平台提供丰富的模块化应用和免费插件，不仅便于科学工作者在其上实现特殊的计算功能，而且可以实现其他行业的多样化要求，安装简单，操作方便，大幅降低开发、运营、交易及推广成本。

ETD生态网络有三个重要特性：

- 即时确认：
如果一个交易遵循智能合约的协议执行，则该交易会即时确认
- 操作确定：
用户在确认成交前，明确交易价格和流通量，交易风险较低
- 多种通证流通池优化智能应用计算的感知模型：
针对不同应用计算对资源的要求和负载情况，资源按需申请分时复用。ETD生态为用户贡献各种通证，通过公共通证流通池，方便用户实现ETD凭证与其他区块链通证和与计算资源的相互转换。智能压缩感知技术对计算任务和数据结构的优化调度，减少因网络带宽瓶颈和数据传输所带来的时间损耗。

ETD平台由专业团队负责底层架构的搭建、测试和维护源码，在任何时候都不会控制任何用户的账户，并且所有操作和交易都可以在公链上查到。即使平台遭到黑客攻击，用户持有的资产也不会受到影响。

第三方开发者可以通过ETD生态网络的公开API接口，将自己系统中的交易和信息通过调用ETD生态网络的智能合约接口实现。相较于目前市面上常见的链下（off-chain）协议接口和混合接口，ETD采用的链上协议接口将使得数据和信息的对接更高效。同时，整个对接环节无需第三方机构参与及信任背书，提高了整个接入过程的效率，简化了对接流程。

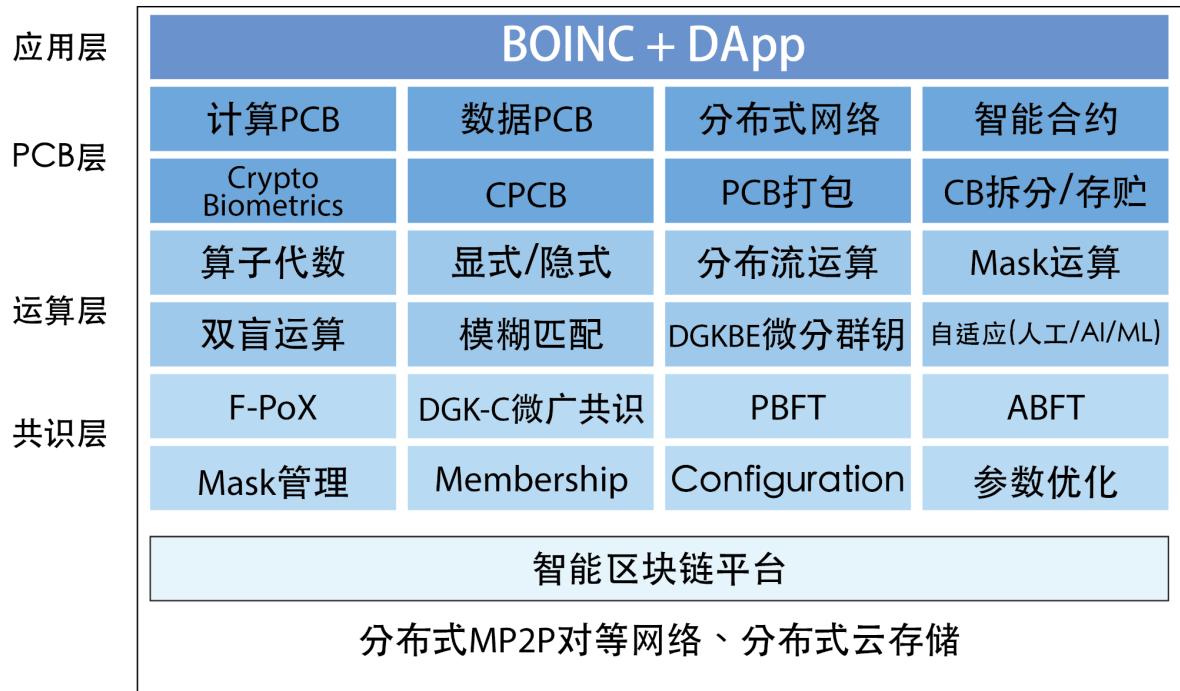
1.4 设计理念

- 从底层保证生成凭证的同时，必然为科学计算贡献算力产生真实价值，拒绝投机炒作与能源浪费
- ETD算力机一机多用，网体复用，支持各类分布式计算和数据存储应用
- 平均每台算力机仅有36W功率，耗电量相当于一盏家用台灯，低碳环保
- 个人零门槛，人人参与，成为志愿者，助力人类科学事业
- 机构零门槛，一键发链，快速部署计算和存储应用
- 全面支持智能合约，满足各种应用落地
- 独创链上质押体系，保障分布式计算机运行稳定
- 实现全球志愿者/算力贡献者联盟

2. 技术架构

ETD技术包含底层共识算法的高效实现，分布式存储、运算、和验证的算力运营层，物联网嵌入式系统，区块链操作系统，分布式存储系统，分布式安全系统，智能合约，大数据

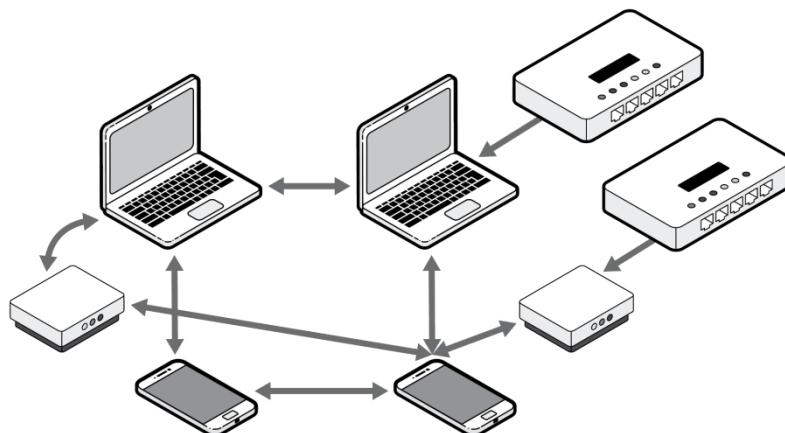
分析和人工智能，以及科学计算与DApp支撑系统等完整体系，解决区块链应用中的信用、性能、安全等核心技术问题，促进生态内所有互联网应用与超越国界的人类科学共同体协同进化和发展。



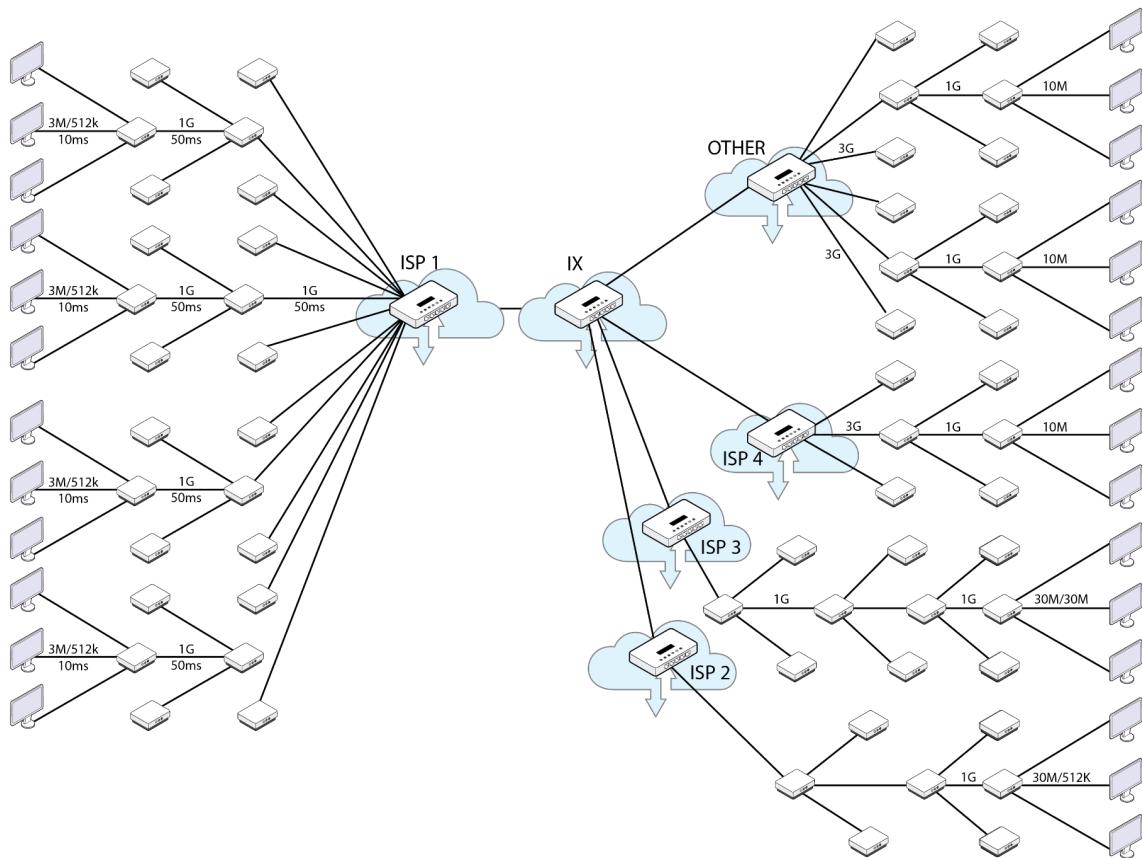
图表：ETD整体技术架构

2.1 EMP2P网络

分布式MP2P(Managed P2P)对等网络是可管控的逻辑网络，通过社区超级节点竞选和社区经营，可以推广到服务整个互联网的海量用户。ETD底层的分布式MP2P网络运行独特的EMP2P(ETD Managed P2P)协议，包含多个高性能网络协议栈：EMP2P PCB能力交互协议栈 (PMC/PCB list, Mask, Coordination); EMP2P对等节点协议栈 (TS - Tracker Service); EMP2P性能监控协议栈 (MS - Monitoring Service)等。



图表：超级节点 EMP2P协议栈



图表：EMP2P对等网络用户

EMP2P协议结合了通用P2P对等网络的特点和为ETD应用服务的安全Projective Crypto Biometrics (PCB) 运算功能，为双盲匹配应用提供了一个实用、可优化、可管控的网络平台。它具有如下显著优势：

- 兼容性：支持任何用户终端（软件/硬件）
- 可扩展性：易拓展，可支持海量应用，不受加密方式瓶颈限制，系统能力和参与的节点（运算/存储/带宽）数量成正比
- 高效性：对DApp低延迟可控
- 鲁棒性：对节点崩溃和恶意攻击鲁棒（攻击成本极高）；超级节点有差错复原功能
- 互动性：支持用户通过手工、人工智能、机器学习等方式参与生态网络搭建

2.2 双盲匹配算法

ETD首创应用双盲匹配技术，用于应对分布式计算和大数据应用中的数据安全问题。由于每个节点只包含部分节点的分布式数据，因此计算/索引只能根据其所见数据，需要所有节点协同运算完成求解匹配问题。同时，辅助运算的节点，对于匹配双方的数据，作为中间运算节点，双向数据是加密的（双盲）。实现双盲的数据PCB是CPCB（即加密可交换运算PCB，Commutative PCB），支持共识验证算法则采用微分群钥广密。

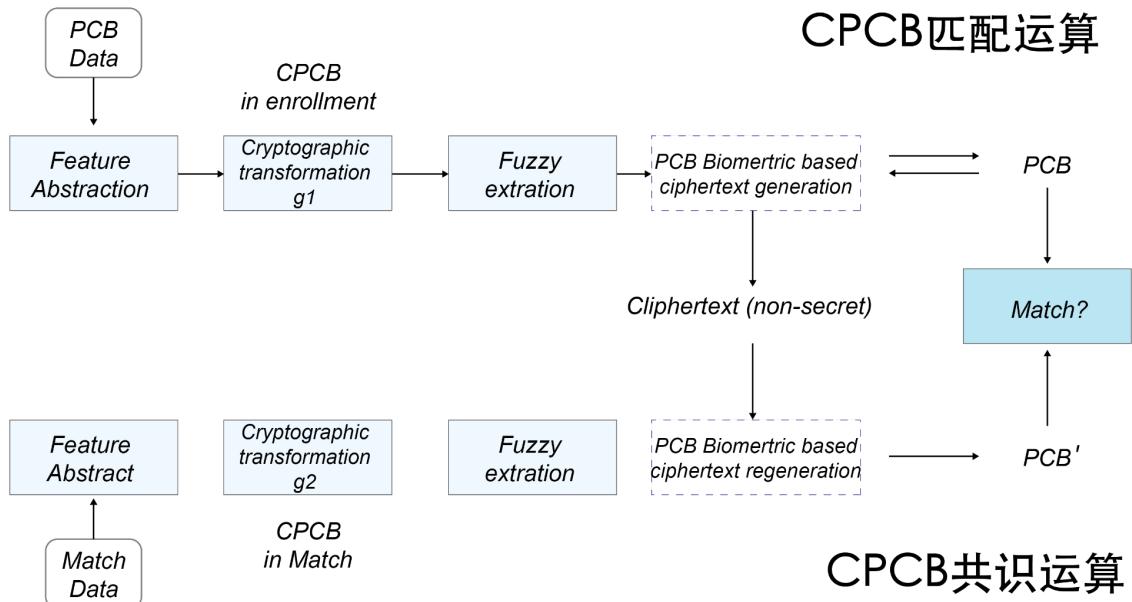
比起任何现存公链，CPCB的巨大优势的是可以用户生物特征（如指纹、声纹）或唯一性硬件特征（如相机CMOS感光元件）来加密/解密PCB数据，而无须使用/存储/记忆一长串的秘钥/公钥，更加安全与实用。同时，利用唯一、不可复制的内置用户身份绑定秘钥和

硬件模块，使识别密钥和安全管理机制更“坚固”，大大减少用户数据暴露于外界网络和环境的机会，提供硬件级别的保障。



图表：生物特征加密/解密

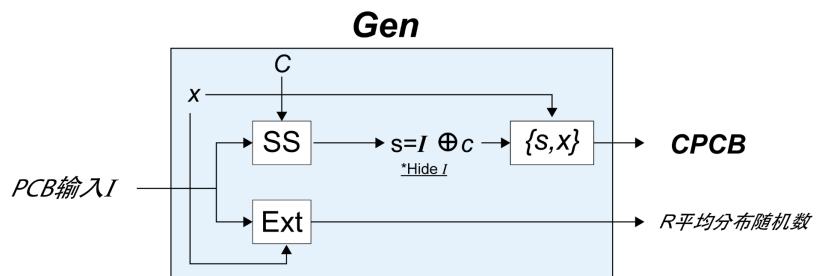
- 双盲匹配系统架构：



图表：双盲匹配系统架构

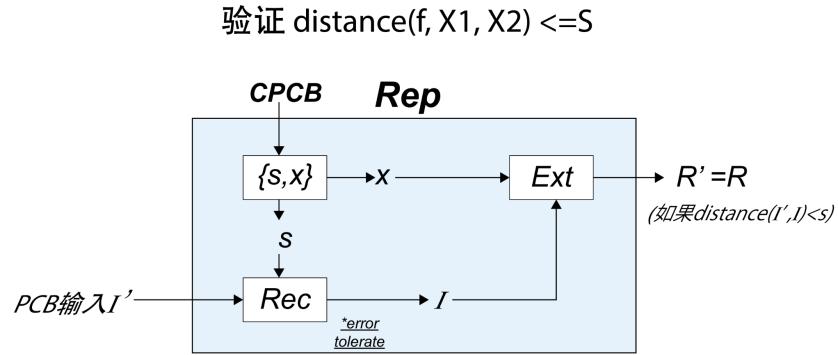
- CPCB匹配运算：

求解 $\text{distance}(H(f), g(X_1), g(X_2)) \leq s$



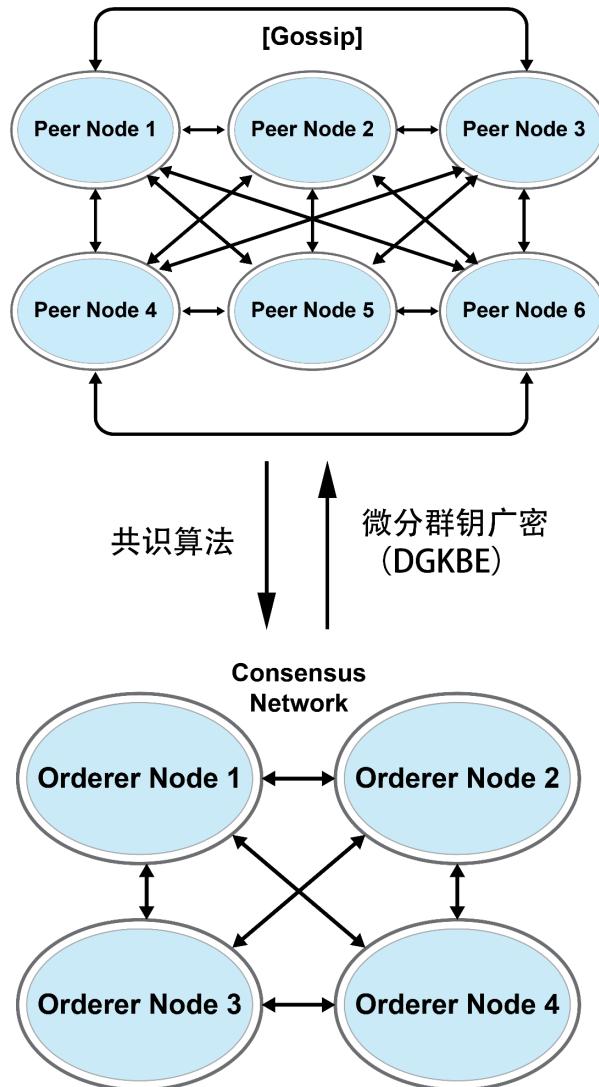
图表：CPCB匹配运算

- PCB匹配验证：



图表 : PCB匹配验证

- CPCB共识运算 :



图表 : CPCB共识运算

分布式CPCB双盲匹配运算模型分为三层 :

- 顶层是dapp，实现加密PCB双盲匹配的分布式dapp，如搜索，配对，exchange, ads, etc.
- 第二层是加密PCB双盲匹配运算层：分布式节点通过gossip protocol 交换计算需求（智能合约）和其他节点数据列表，并进行双盲匹配运算，符合匹配规则的匹配对传给共识机制层
- 共识机制层接收双盲匹配对数据，运行Proof of Computation-Storage共识算法

ETD设立独立的计算层和共识机制层以解决去中心化的数据存储问题。现有公链在本地节点包含所有数据（full node），这对双盲匹配的大型科学计算中的海量用户数据是不现实的。ETD将海量用户数据通过CPCB分散存贮于P2P网络中。

- 共识机制

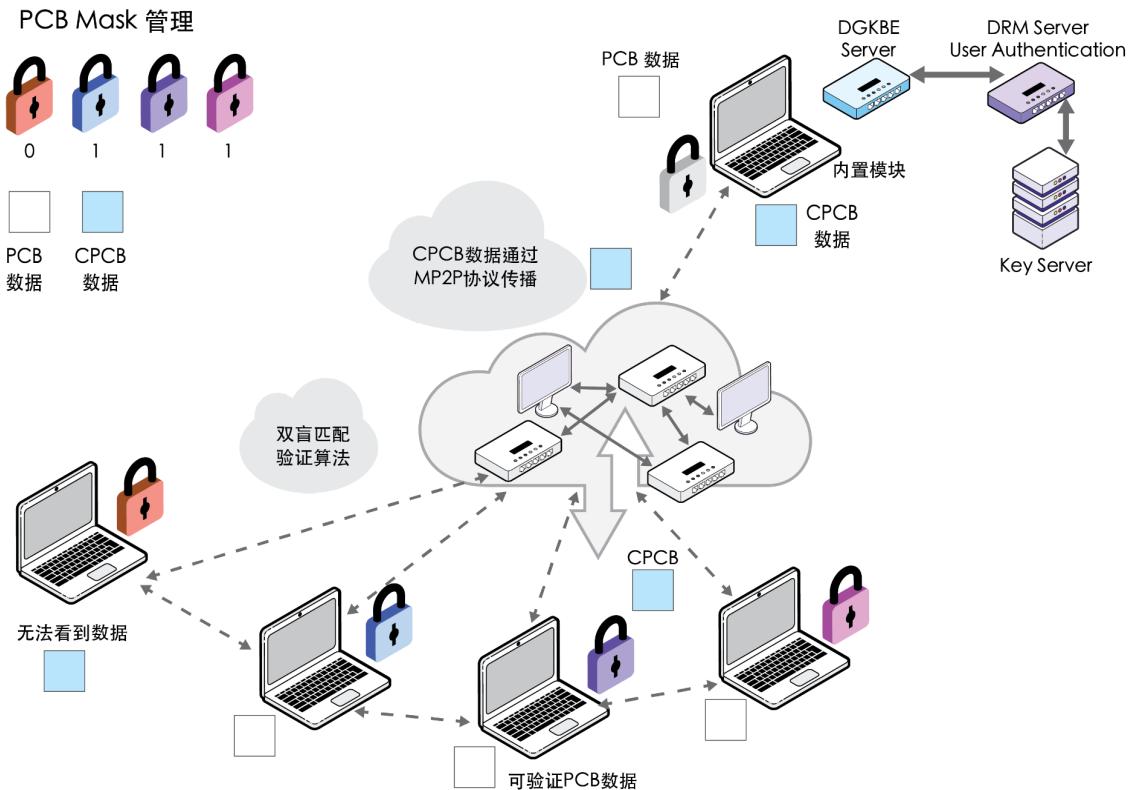
ETD采用结合Proof of Computation (PoC) 和Proof of Existence (PoE) 的Proof of Computation-Storage consensus algorithm共识机制。

共识机制的选择是由双盲匹配问题的要求决定的——它是一种通用分布式计算平台，目标是最优化核心资源的利用，包括分布式的计算模型，分布式存储模型，P2P对等逻辑网络通讯（带宽）模型，和双向数据隐私保护需求。为实现通用PCB匹配，双盲匹配的运算是核心。本质上PCB共识是一种工作量证明（配对是通过一定的计算而得到/发现的）。但是计算需要数据以及传递数据的网络带宽，除非所有的数据都在本地节点。因此数据资源的提供，和计算工作量(PoC)一样重要（否则计算将无从下手）。为了确保双盲匹配运算的数据来源安全，PCB数据存储采用Proof-of-Existence（存在证明）机制。配对数据可以由节点提供（PoE）；或者数据片段由本地或者其他节点提供，再通过计算得到所需PCB数据（结合PoC和PoE）。加密生物识别PCB能有效取得PoE中的证明而无需解密全部加密数据。

- 微分群钥广播加密（DGKBE）

由于现行公钥平台无法应对大量、并发多、用户广、实时、跨平台的海量P2P加密数据运算需求，因此，ETD使用微分群钥广播加密（DGKBE）技术，带来了以下突破：

- 高速（可用于海量分布式P2P，如PCB）
- 安全（160位的DGK=1024位RSA）
- 大规模可扩展（处理亿级水平）
- 固定存储容量（客户端仅60比特）
- 低CPU要求（低至10MHz）



图表：微分群钥广播加密

DGKBE在区块链平台上对DApp应用端（如IoT/电脑/手机）实现了用户数据安全、可靠、高效的处理，它使PCB数据安全加密运算可以成为晶片解决方案的有效组成部分，支持物联网级别的各类应用。

DGKBE加密算法包括三个主要的算法模块：

1. DGKBE密钥引擎：其主要功能是生成公共密钥和一组相应私有密钥。
 - 产生一个p-指数(p为质数)的双线性映射群G，及其相应的椭圆曲线G^N
 - 初始系统随机化；随机产生一个群G的生成子元素g，满足相应椭圆曲线的要求
 - 系统随机化；从模数整数群Z_p中随机产生一个元素a
 - 对 $i=1,2,\dots,n,n+2,\dots,2n$, 利用椭圆曲线G^N和双线性映射，生成： $g_i=g^{(a^i)}$
 - 随机选取模数整数群Z_p中和a双线性互质的元素r
 - 计算椭圆曲线上的对应点v= g^r
 - 生成公钥 $PK=(g,g_1,\dots,g_n,g_{n+2},\dots,g_{2n},v)$, 属于 $G^{(2n+1)}$
 - 对每个用户 $j=1,2,\dots,n$, 其相应私钥 d_j 由椭圆曲线的双线性映射产生：
 $d_j=(g_j)^r$

2. DGKBE CPCB引擎：其主要功能是生成CPCB密钥(Session Key)以及公共密码文本(存放于的CPCB数据流内)。

- 系统随机化；随机生成模数整数群 Z_p 中满足双线性互质的元素 t
- 生成 $g_1, g_{(n+1)}$
- 利用双线性映射计算椭圆曲线上对应于映射 $e(g_n, g_1)$ 的点
- 利用双线性映射及椭圆曲线计算 $e(g_{(n+1)}, g)$
- 利用双线性映射及椭圆曲线生成会话密钥 $K = e(g_{(n+1)}, g)^t$
- 生成公共密码文本 H ：

$$H = \left(g^t, (v \cdot \prod_{j \in S} g_{n+1-j})^t \right) \in \mathbb{G}^2$$

3. DGKBE解密引擎：其主要功能是利用公共密钥、完整的文件头和私有密钥来恢复一个CPCB密钥，然后使用这个CPCB密钥来对加密后的CPCB数据进行运算。

- 系统随机化；生成椭圆曲线上的相应配对序列
- 提取完整的文件头中的用户掩码 S

- 利用双线性映射及椭圆曲线计算 $\prod_{j \in S} g_{n+1-j}$ 和 $\prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}$
- 提取完整的文件头中的公共密码文本 H
- 利用双线性映射计算 (C_0, C_1)
- 利用双线性映射及椭圆曲线计算

$$e(g_i, C_1) / e(d_i \cdot \prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, C_0)$$

- 计算会话密钥 K ：

$$e(g^{(\alpha^i)}, (v \cdot \prod_{j \in S} g_{n+1-j})^t) / e(v^{(\alpha^i)} \cdot \prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, g^t)$$

2.3 M:N匹配优化过程

- 分布式M:N双盲匹配问题

假设 M 个课题组， N 个用户，课题组根据用户的数据匹配，为其科研课题募集算力/资金/志愿者/产品试用者，在课题组数据和用户数据互相双盲的情况下，如何通过ETD链上Dapp应用来实现分布式双盲匹配计算，使得在双方数据都不泄漏的情况下，借助所有 $M+N$ 群体的帮助（计算，存储，和通讯带宽资源），使课题组可以找到合适的用户？

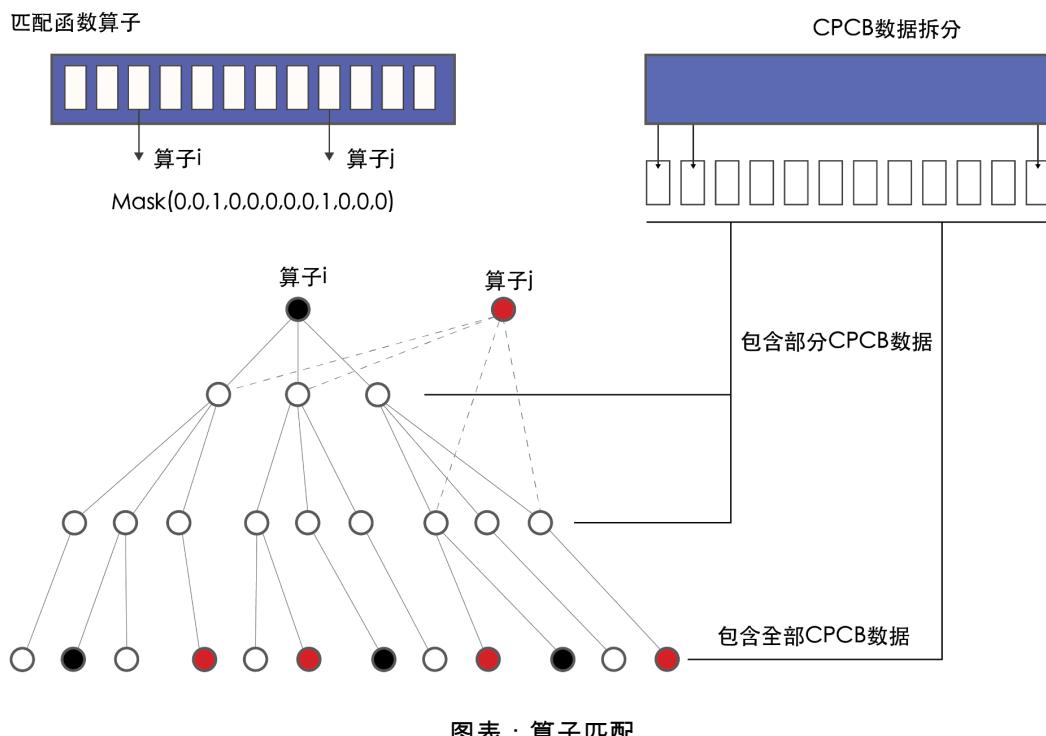
- 双盲匹配的假设

匹配优化运行函数

- 匹配距离函数是逻辑可拆分的，可以用并行算法（对等分布式网络计算模型）
- 任何复杂函数都可以分解成有限逻辑算子的基本逻辑算子组合，如序列($E1;E2$)，并连($E1 \wedge E2$)，同时($E1 \wedge E2$)，限制(Any(n) $E1$)等，这些逻辑算子用函数 f 表达， f 可是显示函数 $y=f(x)$ – 因果关系明确已知，或者隐式函数 $f(x,y) = 0$ – 因果关系未知

匹配优化运行数据

- 用户数据是可以无限（任意）拆分组合的，数据拆分的计算量相对匹配计算量或者网络带宽资源很小（甚至可以忽略不计），因此用户数据可以任意拆分组合
- 加密运算对匹配函数的逻辑拆分，和用户数据的任意拆分，在双盲匹配条件下满足算子交换率Commutative property（如此条件不满足，则需要定义复合算子和数据拆分的函数表达，以额外的运算成本换取数据双盲（数据保护），如弱双盲匹配 Weak Commutative Computability）
- 假设相比双盲匹配运算复杂度，反向验证匹配的结果的真实性运算量很小，ETD 使用高效的微分群钥广播加密算法（DGKBE），实现最优的O(1)级的双盲验证算法。



图表：算子匹配

图中算子i（黑色）有三个双盲匹配，算子j有四个匹配（红色）；所有数据CPCB双盲。匹配结果的验证通过EMP2P网络上的微分群钥广密运算完成。

2.4 公链特性

通过ETD算力机控制的节点、CPCB绑定分布式计算/存储数据的信令传递，将分布式应用

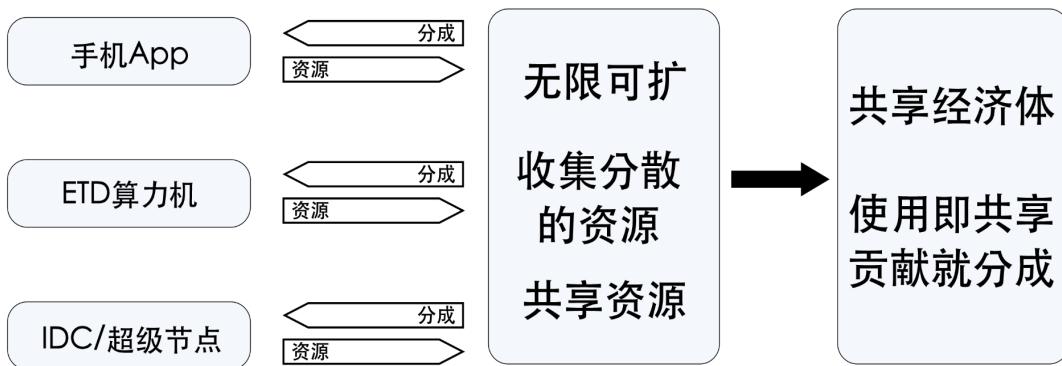
DApp的计算程序解耦成可交换的CPCB算子，维持面对对象的ETD计算的有效封装和应用。ETD节点系统内部状态只能通过传递消息来改变，数据的传输和消息的发送不会被阻塞，在多个线程上可以有效平行安排并行的计算和应用程序，充分发挥CPU和GPU在分布式云存储平台上的混合算力资源，优化组合、高效运行。

ETD公链具有更高的性能

- 提高存贮/读写性能：计算/存贮即计算机制。分布式计算/存贮在加密PCB的条件下，实现了高效的匹配运算机制，instead of（加密运算+传播+解密运算+匹配运算）乘以N，乘以M，PCB实现了($O(1)$ 加密匹配运算)* $\log N * \log M$ 的计算。数据存贮从 $N * \text{Size L} * \text{replication factor K}$ （一般K是20-100的范围-如IPFS）变为Crypto PCB的 $(\log N)^2 * (\log L)^2 * k$ (here k is greater than 1 but less than 1.2 ~ 1.3)。
- 提高通讯性能：通讯性能的提高是在保证数据加密的条件下实现的，简单Merkel tree无法提供加密数据的计算支持(如子数枝干的计算和搜索)。Crypto PCB使用微分群钥广播加密的算法，将数据的加密和数据结构的优化（节省通讯带宽资源）绑定在一起，以实现 $O(1)$ 的数据通讯需求（相比基于Merkel tree或者DAG图等数据结构的 $O(\log)$ 的需求）。
- 提高公链数据运算性能：1) 计算/存贮/通讯的综合优化目标；2) Biometric Crypto PCB的密钥分布机制，避免了密钥的传输和分布，提高安全性和运算效率；3) 可定制的计算或存贮/通讯模块；4) 抗统计学习的复合PCB算法；5) 匹配算子的并行细分，支持并行算法和中间/部分匹配结果；6) PCB数据随机/任意细分的分布式存贮，支持加密状态下的重组和复合算子，例如计算和存贮的权衡。7) 支持PoC/PoE共识机制，以及任何通用或者定制的共识算法；

只有双盲匹配运算的结果上链，匹配运算的结果产生CPCB加密文本ctxt和相关的参数，如对应请求i的掩码模具 S_i （一个大小为总用户数N的二进制掩码）。ctxt和 S_i 将被包括在区块头的数据中。任何在 S_i 中相应位置所对应的二进制值为True的用户都可以使用其加密生物特征输入数据解密密文，并验证请求 i 满足他的条件。同时，其他位置的二进制值为False的节点将无法解密密文，因此不会知道请求 i 的内容，更无法看到其他用户的私人数据。

由于双盲PCB匹配的数据加密特性，ETD计算平台可以有效抵制来自网络的恶意攻击（攻击的成本是不但要耗损计算资源-因为数据的加密特性，难以发动针对某个节点或是某个应用/服务的攻击，除非对数据进行解密运算-同时还要耗损网络带宽和存贮资源）因此，算力场的分布可以针对Dapp进行adaptive设定。在双盲匹配的运算环境下，节点可以通过历史数据的积累和分析，即使在双盲的情况下，还是可以通过机器学习，储存高频的服务请求或者高频的配对用户（尽管不知道具体的服务和用户名字-由于数据加密）。这样节点可以只存贮高频的数据，使系统失去了公平性（或者对于低频服务和用户，系统服务性能大幅下降），为了保证服务质量，可以提高低频数据的奖励机制，或者通过固定算力场的计算机制（比如算力场的计算份额在30%-50%浮动，以确保足够的算力和存贮解决任何高低频匹配需求）。另外，可以引入嵌套PCB(composite PCB, 或者PCB of PCB技术，例如PCB(PCB)算法），由于PCB函数f是对用户数据的双盲加密运算，另一组PCB双盲加密运算g所产生的加密数据 $g(f(X)+p)$ - 这里p是一个系统随机参数 - 将使节点对PCB函数f的任何大数据历史分析和学习变为毫无意义(类似asynchronous randomization algorithms)。



图表：ETD共享分布式公链

ETD具备独立的智能合约体系，可以平行兼容以太坊智能合约，并提供了一套包含堆栈操作、流程控制、逻辑运算、算数运算、密码学运算、字符串操作、数组操作的指令集。ETD可以创建独立的虚拟硬件，并以接口的形式开放给智能合约来使用，使得合约可以在运行时取得平台相关的数据、分布式存储以及其他网络资源。由于PCB具有硬件层面的安全机制，可以保证使合约的行为安全可控，通过合理编写虚拟硬件提高安全性。

2.5 ETD算力机

网络中有两种类型的节点，计算节点和记账节点。计算节点可以运行程序、执行计算、广播、接收和转发交易、同步区块等，而记账节点参与分布式共识并创建区块。记账节点是区块链的核心角色，它保存完整的历史数据并监听广播交易。ETD系统中的记账节点分布在全球多个拥有算力的矿池中。

算力贡献者的ETD算力机对于维护ETD算力和整体系统安全性是至关重要的。在比特币和以太坊等公链平台上，算力贡献者是通过PoW或者PoS(equivalent to PCB's PoC and PoE)来取得记账权和获得回报，共识机制是保证帐本的安全可靠和一致性，公链本身不支持任何应用层的复杂Dapp计算模型(以太坊有简单的智能合约计算，复杂计算将极其昂贵—例如GAN或者Neural Network算法根本无法支撑；并且数据来源严重受限，必须由本地节点提供，或者是第三方Oracle service，不支持P2P网络分布式存贮模型)。而ETD公链的PoC/PoE模型，将分布式计算/存贮模型统一在公共的ETD链上，算力贡献者的匹配计算，即解决Dapp的应用计算(存贮)问题，同时又提供了共识机制保证计算/存贮的账本安全可靠和一致性。因此，任何宝贵的计算/存贮/网络资源都没有浪费，而是用到了解决实际Dapp问题和提供记账功能。每个节点既是用户，又是算力贡献者，而且可以任意组合。用户可以选择任何分布式计算策略，分布式存贮策略，以及P2P对等网络通讯策略和协议，以谋求最大化其计算效率和回报—也就实现了匹配的效率(需要计算和数据存储)。

例如，用户A对网络电商推广的匹配app具有优势(他有商家资源或者优秀客户资源)，他可以针对商家推广的策略函数f，最优化地使用他有限的计算和存贮资源—比如商家的推广策略通过他发布到ETD链上，他可以最先/最广收到双盲匹配结果。

ETD硬件的算力取决于节点运算内核的数量和种类，以及内存和数据储存空间的大小。根据信息熵理论与分布式计算特性，存储空间可以用来存储运算的结果，因此在计量节

点的算力上，给定同样的运算任务，存储空间可以置换一定量的运算算力，反之亦然。由于存储的数据可以为多个计算单元使用(multiple read)，而运算单元一旦使用只能用于一项计算任务，因此采用存储单元的大小来代表算力机静态的算力。算力机实际动态算力是由存储和与其绑定的计算单元综合决定的。例如通用的ETD算力机以静态4T存储为单位，可以有4T、8T、16T三种配置。4T机器的算力固定，由硬件CPU/GPU绑定。而8T与16T机器可与分散在网络中的任何CPU和显卡远程配对而执行通用计算任务，算力更大、产生的通证数量更多。

2.6 技术优势

- 通过区块链技术在凭证与算力交易环节中确真，确信，确价，确权；
- 如果一个交易遵循智能合约的协议执行，则该交易会即时确认，实现支付秒到账；
- 多种通证流通池优化智能应用计算的感知模型，实现多种数字资产通证的自由兑换与交易；
- 超大数据量的处理与运算过程的安全和高效；
- 定制化智能合约，可根据不同DApp 应用场景中对共识算法的个性化需求实现定制化；
- CPCB算法解决数据安全隐患，实现用户身份认证关联数据可被查询与追踪，让每笔交易公开透明可查；
- 双向匿名隐身镜像身份验证，对每个参与数据交易的实体认证身份在区块链上实行双向完全匿名记账，彻底保护交易双方的隐私；
- 社区节点投票系统，让整个社区投票节点达成共识，统一使用去中心化的通用工具来完成社区自治与良性发展

3. 凭证发行

3.1 ETD贡献值凭证

ETD贡献值凭证 (ETD Credit) 简称ETD，是ETD区块链原生通证，获取途径包括：

- 使用ETD算力机，为ETD贡献算力获得
- 在ETD生态系统之内，通过他人转赠、DApp奖励等参与双方自愿的流通途径获得
- 在其他数字资产交易平台买入

3.2 出块规则

ETD(Ether Data)规划产生贡献值凭证总数为2,100,000,000(21亿)张，每2100天减半，理论上可持续产生超一百年。

规划表：

| 年 | 出块/日 | 区块贡献值 | 日贡献值 | 年贡献值 | 总计贡献值 |
|---|------|-------|--------|-----------|-----------|
| 1 | 8640 | 57.87 | 500000 | 182500000 | 182500000 |
| 2 | 8640 | 57.87 | 500000 | 182500000 | 365000000 |

| | | | | | |
|----------|------|--------|--------|-----------|------------|
| 3 | 8640 | 57.87 | 500000 | 182500000 | 547500000 |
| 4 | 8640 | 57.87 | 500000 | 182500000 | 730000000 |
| 5 | 8640 | 57.87 | 500000 | 182500000 | 912500000 |
| 6(7.5个月) | 8640 | 57.87 | 500000 | 112500000 | 1025000000 |
| 6(4.5个月) | 8640 | 28.935 | 250000 | 35000000 | 1060000000 |
| 7 | 8640 | 28.935 | 250000 | 91250000 | 1151250000 |
| 8 | 8640 | 28.935 | 250000 | 91250000 | 1242500000 |
| 9 | 8640 | 28.935 | 250000 | 91250000 | 1333750000 |
| 10 | 8640 | 28.935 | 250000 | 91250000 | 1425000000 |
| 11 | 8640 | 28.935 | 250000 | 91250000 | 1516250000 |
| 12(5个月) | 8640 | 28.935 | 250000 | 37500000 | 1553750000 |
| 13 | / | / | / | / | / |
| 14 | / | / | / | / | / |
| 15 | / | / | / | / | / |
| 16 | / | / | / | / | / |

ETD区块链每10秒钟产生1个区块，每天理论产生8640区块。为了对BOINC提供更好的支持，ETD系统不进行预挖，全部凭证通过区块产生。前5.75年每年计划投入50万T算力；后续每5.75年每年计划投入减半算力。

3.3 分配规则

- 为了促进ETD生态运转，ETD供应总量21亿张，并且永不增发，每2100天出块数量减少。每日日产分配，具体分配规则如下：
 - 75%进入算力贡献者
 - 15%用于各个DApp的奖励分成
 - 5%进入以太数据基金会账户，由社区治理委员会拨出
 - 5%进入算力平台运营基础设施建设，用于抵消运营风险，每日分配一次
- ETD算力机接入即可运行，为了保障ETD作为全球分布式超级计算机的稳定运行，避免被投机客利用，算力机持有者需按照以下规则进行质押：
 - 每T质押100张凭证，打入绑定节点的ETD地址，以获得正常算力
 - 质押凭证锁定期为540天释放
 - 每次减半质押翻倍，未提高质押者，贡献值所得降低50%

3.4 治理机制

在区块链ETD生态中，所有的贡献均会获得ETD激励，同时，所有的对于资源的使用，都需要消耗ETD。ETD激励由共识机制根据贡献权重进行分配，而消耗ETD则由对于资源的具体使用度来衡量。

ETD是衡量价值传递的一个标准，同时也是建立在ETD生态上众多资产的基础资产。ETD激励算力贡献者去更好的劳动和创新，并且让那些失去劳动和创新能力的人也能够被保障生存。

3.5 锁仓机制

算力贡献者和DApp获得的ETD当天可以释放20%，其余按照每天180分之一释放，以此类推。减持时所有ETD分配都智能合约自动执行，无人为干预。

基金会和算力平台运营基础设施建设获得的ETD锁仓期为1个月，次月释放上月的10%，以此类推。减持时，所有ETD分配都依照智能合约自动执行，无人为干预。

4. 生态建设

ETD是分布式计算集群的技术基础设施，为开发去中心化应用提供了强有力的技术支持，最终将发展成ETD生态。全球性的ETD高校与科研机构合作网络和持续的人才培养是实现ETD生态的重要基础。

4.1 链委托与链结算

信任机制是区块链底层技术的重要部分。ETD在进行价值资产数字化的过程以此为基石，构建出整个ETD生态。权益托管（链托管），采用合格资质第三方机构对权益资产进行托管并且所有数据写入区块链。权益结算（链结算），采用合格资质第三方机构对权益资产进行结算并且所有数据写入区块链。

4.2 跨链支付和流通

用户从任何渠道获取的ETD（包括贡献算力、消费终端、交易平台等），均可在ETD生态中自由交易，并且与其他交易平台数字资产之间跨链无缝连接实现自由支付和流通。

4.3 ETD记账节点

ETD记账节点是基于PoW+DSB PoS共识机制、兼容多种跨平台通证的完全节点，支持ETD公链运行计算与存储功能，提供一站式通用计算服务。ETD主链具备多样化用途潜质，通过技术将算力的价值进一步释放，给用户带来更高回报。换句话说，这些算力可以用来做其它事情。算力贡献者可通过竞选成为ETD记账种子节点，而接下来在更多基于PoW+DSB PoS共识机制下的通用计算业务上线之后，算力贡献者只需通过委托投票的形式就能参与计算，获取贡献值凭证。

4.4 激励机制

传统的点对点通讯网络将焦点关注于信息传输，有点像互联网1.0时代的应用，一切都是公开和共享的，而其并没有达到区块链技术所达到的震动效应，一方面是因为缺少有效的共识机制将分散的节点协同参与工作（仅限于点和点的共识），而更重要的是因为一切人类行为需要经济逻辑驱动，在缺乏有效的经济规范趋势下，人类的行为只能受到社会规范约束，使得大部分需要共同完成的目标，对个体缺乏约束力。

比特币网络通过PoW共识机制，并以贡献算力获得记账权从而获得比特币奖励的方式激励节点参与共识，无疑是一项了不起的设计，我们认为通证经济模型是区块链价值的核心也不为过。以太坊基于同一种底层共识机制，允许智能合约开发者发行自己的通证，并且使用ETH作为GAS费用支付共识成本，既统一了共识成本的计量单位，又允许在相同的共识成本下，能够根据通证所用于的生态获得不同的价值输出，使用者至少能够计算最佳的投入与回报的平衡点，如今许多人诟病在以太坊上发行ERC20的代币太过容易导致鱼目混珠，却很少有人意识到以太坊设计初衷的重要意义。

站在ETD生态的角度，所有服务的价值都有一个源头，由于区块链平台本质是一个公平的价值流通市场，因此所有的经济行为的成本底层在于交易成本，ETD就是交易成本的载体，从这个立足点出发，ETD凭证用于以下激励用途：

- 记账奖励
- 算力贡献奖励
- 其它角色包括算法提供者（通过发布智能合约的形式）的运行激励
- ETD生态的开发者会因其开发应用的实际产生价值而获得ETD奖励，这种奖励往往用于实际补贴其共识记账或算力支付开销的成本方式给出

节点参与通用计算的收益：ETD生态系统的运行离不开各个节点对网络的支持，在ETD完全去中心化的网络里，ETD系统希望创建更多的节点来维护ETD网络的稳定运行。

ETD节点是要为整个网络提供持续服务的全节点，需要质押机制作为保障。质押凭证可以保存在本地离线钱包中，从而完全确保安全。普通地址和多签地址都可以使用，当节点被激活时，它可以为网络提供通用计算服务，并在此过程中获得丰厚的回报。节点数量的增加会导致质押凭证数量同步线性增加，有效平衡了ETD在交易市场的流通性，给予凭证不断升值的支撑。

5. 凭证运用场景

5.1 时间银行

依循古典时间银行“人人时间平等”的理念，ETD作为分布式通用计算集群，相应的内核是每个算力贡献者的单位算力的价值都是平等的。ETD时间银行为算力贡献者提供比传统银行更多元和便宜的服务，包括三个业务板块：

- **时间钱包**：相当于面向个人的零售银行服务，用于凭证的存储、便捷转账、收款收单，并提供ETD与其他加密货币的兑换业务
- **金融业务**：将传统金融市场的成熟业务模式搬迁到ETD生态圈中，例如理财、借贷、支付、保险；量化交易、不良资产处置、分期、众筹、上市公司的并购或资产重组、市值管理等

- 为专业投资机构提供的业务：建设金融数据上链、风险控制模型上链、生态内征信上链、金融资产上链的体系

5.2 智慧城市

- 产业集群。基于公链提供的智能合约工具开发的海量DApp，在各行业中落地之后，自发形成个性化、可裂变的产业集群，促进线上线下融合，打通多领域协同，提升服务体验；
- 募资与投资。处在孵化阶段的项目可公开募集ETD，并将募集到的ETD直接用于交换ETD生态体系自身提供的算力或合作方提供的各类服务，例如云计算、数据托管、金融服务等，大大减少中间环节、降低创业成本；与此同时，个人和社区投资者向项目注资也将更加便捷。算力贡献者还可将ETD作为抵押，兑换所需法币；
- 企业链改。相比其他区块链平台，ETD在安全性、可靠性、高效性与灵活性方面的显著优势，将在企业对其现有业务流程进行区块链改造时，体现出巨大效益，实现实体产业与区块链技术融合，形成互联、互通、互促的生态圈。

6. ETD基金会

基金会将从事以ETD为核心的区块链生态建设和生态投资，进行基金金融产品发行与管理、社群资讯发布、区块链IPO、股权投资、通证经济研究等工作，为所有算力贡献者持有的ETD凭证保障流通价值。在投资过程中，基金会着眼尖端产业发展，聚焦高回报率的现金流投资项目，纳入交易所、钱包、学院、通用计算、产业科技园等多个维度，稳步推进相关DApp落地，成为在区块链上中下游全产业链进行战略布局的母基金。基金会还将负责未来的开源架构拓展与ESG（环境，社会和企业管制）标准的达成。

6.1 ETD通用计算实验室

我们计划与世界各地的高校及附属科研机构合作，在校内捐助成立ETD通用计算实验室，在其中架构ETD完全节点，让无力自行负担购买/租赁超级计算机使用费用的科研团队，在有需要时通过节点接入ETD平台，拥有相当于超级计算机的运算与存储能力，在不需要时则将节点富余算力共享给他人，过程中获取的ETD凭证将直接注入团队科研资金池，以供进一步科研投入或相应发明、专利的商业化投产。

科研团队的发明成果可以使用ETD的模块化工具，方便地转化为用户友好的线上应用，开放给全网公众使用（免费或收取ETD）。科学家将无需自行负担雇佣应用开发者、市场营销人员、财务人员的成本，并得到与心血相匹配的收益。与此同时收集到的用户数据也可以反过来帮助科学家继续完善、优化其成果。这同时意味着，高校的研究如果需要大数据支持，例如：自然语言翻译算法的课题、人类基因组相关的医学、历史、社会科学课题，那么也可以选择作为付费方，付出ETD在全球招募志愿者/受访者。课题组可以借此节约支出，而且因为ETD格外完善的隐私保护机制与匿名性质，志愿者无需顾虑通过网络向课题组传送自身数据带来的泄露隐患。ETD基金会作为基金管理者，将从综合科研实力、基础学科研究能力、当下热门领域突破能力三个维度来考察并选择合作高校。

6.2 创新工场

我们将参照硅谷模式，在ETD生态体系中打造一个全球顶尖的科技项目孵化器，换句话说，即是一个系统化、自动化、分布式的硅谷——其位置分散在世界各地，不再受限于现实空间约束；其功能通过区块链智能合约而执行，大幅提升效率、缩减信用成本，并且无需如以太坊一般高昂的费用；其经济价值体现为参与方的协同博弈最终导向共赢。我们深信，在长期的未来，这将成为整个人类科学共同体的研究成果走向技术化、市场化、平民化的主流模式。

基金会的合作机会一方面向科学界开放，另一方面也开放给包括风险投资机构与大型科技企业在内的专业投资人。投资人可以选择与基金会一同捐赠成立ETD通用计算实验室，也可以单独投资旗下某一个课题组。他们将花费更少的尽职调查成本并得到更多元的合作机会。项目成功市场化之后的经济收益将在高校、投资人与ETD基金会三者之间分成。

值得一提的是，我们特别关注环境与气候科学，首先，其研究对象是整个人类经济和文明的根基；其次，诸如海洋生物多样程度、大气清洁程度等指标都难以衡量、更无法买卖，任何在传统金融世界找得到原型的模式，都难以帮助其研究成果的实用化。基金会将与科学家合作，探索自然资源通证经济的可行性，设计特别的金融激励机制，让自然资源（或其具体指标）成为区块链上的加密资产，从而获得公开可信的质量评估、透明性和可交易性，避免公地悲剧的发生。

7. 核心团队

- **Nikolay Tasev**
以太数据基金会联合创始人

Nikolay Tasev 是一名程序员、密码学家、密码分析家和密码朋克。Nikolay 致力于倡导广泛使用密码学和隐私技术以提高个人和社会福祉。作为年轻的程序员，他曾赢得过两次黑客马拉松奖项，其中一个应用程序被一家价值超过 5000 万美元的领先社交网络公司采用。在Android成为行业垄断者之前，他是早期开源移动操作系统的核心系统程序员和开发者。Nikolay开创了安全工作的先河，将物理不可克隆函数与公钥密码学结合起来，为伪随机性、零知识证明、安全随机函数等领域的密码算法实际实现做出了贡献。他的研究兴趣综合了计算的复杂性、安全的繁琐性、物质的随机性以及人性中谬误和想象的不一致性之间的相互作用。

- **J. Robert Bo Collins Jr.**
以太数据基金会顾问，MGH董事

Collins是一名积极的企业家和区块链践行者，目前担任MGH集团（Mercantile Global Holdings）董事长，及其旗下银行Mercantile Bank International的首席执行官。他于2019年创立了圣胡安数字资产交易所（San Juan Mercantile Exchange）与伙伴银行San Juan Mercantile Bank & Trust International，为机构客户提供加密货币与法币的交易和托管服务。

他于2001年至2004年担任纽约商品交易所（NYMEX）总裁，在任职期间，他领导NYMEX获得了A++标普信用评级，被评为2004年“年度最佳交易所”；推出了第一个取得商业成功

的OTC清算平台Clearport Clearing;策划了迪拜商品交易所的成立。离开纽交所后, Collins 创办了对冲基金MotherRock, 并曾在国际衍生品清算集团(International Derivatives Clearing Group, IDCG)担任高管, 是备受业界尊敬的金融技术专业人士。

- **Michael Gaard**

以太数据基金会联合创始人 , Contata Solutions高级副总裁

Michael在IT战略、业务转型、软件开发和服务交付方面有充沛经验。他担任过埃森哲旗下安盛咨询公司(Andersen Consulting)和普华永道(PWC)合伙人, 负责北美零售银行业务。他曾在软件开发公司Information Advantage任总经理, 在医疗保健与金融服务行业中获得了领先的软件开发和部署经验。随后, 他在优利系统公司 (Unisys)领导北美金融服务业务。现在, 他是云数据智能解决方案提供商Contata Solutions的高级副总裁。

- **Timothy Perez**

以太数据基金会技术顾问 , QBKEY发明者

Perez是来自比利时的计算机神童, 7岁开始接触计算机硬件设备, 13岁写出第一个软件。他是数据与网络安全专家, 密码学领域的领军人物。他曾为微软、Adobe、育碧和Canonical等公司担任安全顾问, 专长于通信协议设计, 嵌入式系统和跨平台软件解决方案。他设计的QBKEY是一款便携式生物识别数据加密设备, 带有嵌入式指纹传感器, 可供个人和企业加密与管理数据, 安全地共享和浏览文件, 并支持任何本地存储设备和云存储服务。他目前所在公司是苹果、戴尔等科技巨头与汽车品牌的芯片代工商。

- **Matt Kelly**

以太数据基金会联合创始人 , facebook高级工程师 , 硅谷云储存服务Kloud.io工程师

Matt是资深软件工程师和数据库架构师, 在软件开发、体系结构、数据库设计、区块链版本管理、测试以及基础结构、网络搭建和智能合约等方面具有丰富的专业知识和实战经历。

8. 风险提示与免责声明

8.1 风险提示

系统性风险 : 是指由于全局性的共同因素引起的收益的可能变动, 这种因素以同样的方式对所有证券的收益产生影响。例如政策风险——数字资产在世界上部分国家已进入监管, 如果司法机构政策变更, 存在一定的因政策原因而造成参与者损失的可能性; 市场风险中, 若数字资产市场整体价值被高估, 那么投资风险将加大, 参与者可能会期望项目的增长过高, 但这些高期望可能无法实现。同时, 系统性风险还包括一系列不可抗力因素, 包括但不限于自然灾害、计算机网络在全球范围内的大规模故障、政治动荡等。

团队间风险 : 当前区块链技术领域团队、项目众多, 竞争十分激烈, 存在较强的市场竞争和项目运营压力。ETD项目是否能在诸多优秀项目中突围, 受到广泛认可, 既与自身团队能力、愿景规划等方面挂钩, 也受到市场上诸多竞争者乃至寡头的影响, 其间存在面临恶性竞争的可能。

项目统筹、营销风险：ETD团队将不遗余力实现白皮书中所提出的发展目标，延展项目的可成长空间。目前ETD已有较为成熟的商业模型分析，然而鉴于行业整体发展趋势存在不可预见因素，现有的商业模型与统筹思路存在与市场需求不能良好吻合、从而导致盈利难以可观的后果。同时，由于本白皮书可能随着项目细节的更新进行调整，如果项目更新后的细节未被参与者及时获取，或是公众对项目的最新进展不了解，参与者或公众因信息不对称而对项目认知不足，从而影响到项目的后续发展。

项目技术风险：首先，本项目基于密码学算法所构建，密码学的迅速发展也势必带来潜在的被破解风险；其次，区块链、分布式账本、去中心化、不同意篡改等技术支撑着核心业务发展，ETD团队不能完全保证技术的落地；再次，项目更新调整过程中，可能会发现有漏洞存在，可通过发布补丁的方式进行弥补，但不能保证漏洞所致影响的程度。

黑客攻击与犯罪风险：在安全性方面，单个支持者的金额很小，但总人数众多，这也为项目的安全保障提出了高要求。电子代币具有匿名性、难以追溯性等特点，易被犯罪分子所利用，或受到黑客攻击，或可能涉及到非法资产转移等犯罪行为。

目前未可知的其他风险：随着区块链技术与行业整体态势的不断发展，ETD可能会面临一些尚未预料到的风险。请参与者在做出参与决策之前，充分了解团队背景，知晓项目整体框架与思路，合理调整自己的愿景，理性参与。

8.2 免责声明

本白皮书对ETD项目的基本情况介绍、说明，不是也不能被视为对任何特定或不特定主体的投资、合作的要约或承诺，不是也不能被视为项目团队对项目的承诺或保证。项目团队保留对本文件进行修改、删节、增加、废止、解释等相关行为的全部权利。对本项目有参与、投资、合作意向的人员务必明确了解本项目的全部风险。参与者对本项目的参与应当订立书面的合作协议，合作协议应明确、完整、清晰的载明合作、参与或投资事项。参与者应当以书面或口头形式表明其自身已充分了解并接受项目已产生或可能产生的全部风险，并自行承担相应的责任。

您在阅读和使用本文件之前，应了解以下注意事项： 本文件不应也不能被视为项目合作、投资或任何合同的内容、标准或条件。任何项目参与者与项目团队法律关系的产生、变更和消灭应以书面订立的合同为准。本项目所称ETD作为非载于项目团队服务器的数字资产，具有完整且独立于项目团队的价值，其价值完全取决于市场相关主体对其使用价值、交换价值的认可，不是也不应被视为债券、证券或任何形式的有价证券，也不是对项目团队、公司的股权、股份、所有权或控制权。基于本项目产生的ETD，ETD的价值受到市场环境、市场主体认可程度的影响，项目团队不能也无法保证ETD的价值。ETD存在遗失、被篡改、被盗、被骗的风险，项目团队不能也无法保证对相关虚拟财产进行保管、回复、修改。鉴于世界各地政府对区块链技术、加密货币或无体财产的监管变化，项目组保留随时根据各地区法律法规及实际情况修改、删节、增加、废止本文件部分或全部内容的权利。您确认自己对项目团队及项目服务中的内容能够自行加以判断，并承担因使用本文件内容而引起的一切风险，包括因对本文件内容的正确性、完整性或实用性的依赖而产生的风险。项目组无法且不会对因您自身的 behavior 而导致的任何损或损害承担责任。