GAIA.WORLD
高效可信的分布式应用平台

前言

2008 年中本聪的论文《比特币：一种点对点的电子现金系统》开创了区块链的概念，这套系统“基于密码学原理而不是基于信用，使得任何达成一致的双方能够直接进行支付，从而不需要第三方中介参与”。区块链的出现不仅仅是催生了“比特币”这一全新的货币体系，更是带来了互联网去中心化的一次革命。区块链技术从诞生至今，经过 10 年的持续迭代，已经大大超过最初的“点对点电子现金系统”的定义，成为一种革命性的互联网底层架构。区块链技术将构建一个高效而可靠的价值传输体系，推动互联网成为构建社会信任的基础设施。

GAIA.WORLD 致力于将这一愿景变为现实。基于全新的区块链架构，我们试图建立一套去中心化的、自由稳定的互联网信任体系，并重点解决以游戏等强交互应用为典型代表的泛娱乐领域的开发痛点，推动区块链技术的普及和应用。

目录

1. 区块链技术的发展和现状 1

2. 区块链技术面临的问题。 1

2.1 性能问题和“挖矿”带来的资源浪费 1

2.2 算力竞争造成交易成本高昂 1

2.3 单一网络造成低效和不安全 2

2.4 与现实世界交互的难题 2

3. GAIA.WORLD 核心技术 2

3.1 共识机制 3

3.1.1 CPoS 3

3.1.2 锻造委员会 3

3.1.3 锻造组 3

3.1.4 主锻造委员 3

3.1.5 投票权计算 4

3.1.6 奖励和惩罚 4

3.1.7 形成共识 5

3.1.8 最短出块时间 5

3.1.9 锻造过程 5

3.1.10 可验证性随机 8

3.2 平行链 8

3.2.1 侧链树 8

3.2.2 跨链事务 8

3.2.3 侧链的独立性 9

3.2.4 侧链的灵活性 9

3.2.5 主链与侧链的互利关系 10

3.2.6 解决生产力问题 10

3.2.7 节点安全问题 10

3.3 神盾协议 10

3.3.1 封闭或扩展 12

3.3.2 如何定义安全 12
3.3.3 分布式事务 13
3.3.4 权益 13
3.4 仲裁委员会 13
3.4.1 仲裁者 13
3.4.2 仲裁机制 13
3.4.3 初级仲裁 13
3.4.4 中级仲裁 14
3.4.5 最高仲裁 14
4. GAIA.WORLD 的链上应用方案 14
4.1 高性能要求的应用 14
4.2 与链外世界交互的应用 15
4.3 在侧链上开发应用 15
4.4 时间区块链应用 16
4.5 需要可验证随机数的应用 16
4.6 链上娱乐时代 16
4.7 全新的区块链生态 17
5. 团队 17
5.1 核心团队 17
5.2 顾问 18
5.3 合作机构 18
6. 法律 18

1. 区块链技术的发展和现状

诞生于 2008 年的比特币作为第一个稳定运行的大规模区块链网络，被人们定义为“一种能够让整个世界就一个公共拥有的数据库的内容达成一致的机制”。在完成电子货币的功能后，如何让区块链技术服务于货币之外的领域成为第二代区块链技术发展的方向——2014 年由 Vitalik Buterin 发起的以太坊（Ethereum）是最成功的一次尝试。

以太坊最成功之处在于设计了一个功能完善、图灵完备的智能合约，它允许用户编写具有一定复杂度的合约、自治代理和关系，以太坊的用户可以通过内置的脚本语言来实现任意交易类型，包括定制货币、金融衍生品、身份系统甚至更复杂的去中心化应用。

智能合约最通俗的定义是“一个包含价值并且只有满足某些特定条件才能打开的加密箱子”。因为图灵完备同时具备价值知晓（value-awareness）、区块链知晓（blockchain-awareness）和多状态等特性，以太坊通过智能合约可以实现许多过去难以想象的交互。

目前基于以太坊已经衍生出数千种应用，涵盖金融，物联网，虚拟资产交易，游戏，博彩等诸多行业。去中心化应用让许多原本无法运行或运行成本过高的运营模式成为可能。目前比较知名的应用有：

The DAO，用以太币资金创立，目标是为企业和非营利机构创建新的去中心化营业模式，项目开始仅 2 个月便遭到黑客攻击，超过 360 万个以太币被盗，最终以太坊基金会决定以分叉处理此次攻击；The Rudimental，让独立艺术家在以太坊上进行众筹创作；FreeMyVunk，虚拟物品交易平台；Ujo Music，使用智能合约进行音乐销售。

2. 区块链技术面临的问题。

2.1 性能问题和“挖矿”带来的资源浪费

现有区块链普遍采用工作量证明达成共识，而工作量证明是对资源和能源的极大浪费。目前市面上的加密货币包括比特币、以太坊等均使用工作量证明，考虑到摩尔定律带来的性能增长，具体实践中通常会随着参与竞赛的算力增加而提高寻找猜测值的难度，以维持相对稳定的出块速度。

作为目前使用最广泛的共识机制，PoW 简单可靠，相对公平，投入越多的算力就有越高的几率得到记账权。而作恶者必须投入超过总算力一半的计算能力（51%攻击）才能保证篡改结果，这使得攻击成本非常高昂，难以实现。

但是，由于记账权（得到奖励的概率）与计算能力成正比，节点为了赚取更多的奖励必然会不断增加自己的运算能力，而大部分的算力都浪费在毫无意义的计算上，这导致了巨大的资源和能源浪费。有数据指出，目前全球范围浪费在记账权争夺（又称：挖矿）上的电能已经超过一个小型国家的总使用量。遗憾的是，尽管付出了极为高昂的代价，基于工作量证明（PoW）的区块链网络性能扔远不能满足需求。以目前最被看好的以太坊为例，以太坊网络平均每秒仅能处理 10 笔交易。这种交易速度远远无法满足现代互联网应用的要求。

2.2 算力竞争造成交易成本高昂

节点为了争夺记账权的过程本质上是算力的比拼，这必然带来节点硬件成本的暴涨，而成本最终会转嫁给终端用户。

以以太坊为例，在以太坊区块链上进行的交易涉及的费用最终都以以太币（Ether）来结算。每笔交易必须指定一定数量的“Gas”，以及支付每单元 Gas 所需的费用。交易执行期间的所有操作，包括读写数据库、发送消息以及每一步的计算都会消耗一定数量的 Gas。同时，支付的交易费用越高，节点就更有积极性来打包和处理这笔交易。高峰期，以太坊中进行转账交易所需支付的交易费用为数美元，这使得基于以太币的小额交易变得不可能。以太坊设计中，一笔复杂合约交易的每一个步骤都需要消耗一定数量的 Gas，甚至于在执行某些复杂的智能合约时需要支付的交易费用已经超过交易本身。

2.3 单一网络造成低效和不安全

如今的区块链网络几乎都使用了单一网络结构，这种结构不便于扩展和安全隔离，在面对复杂应用场景时，其弱点会暴露无遗。

以以太坊为例，以太坊的成功得益于智能合约的创新，这极大的拓展了区块链的应用场景。开发者甚至可以通过 ERC20 协议直接在以太坊中发布自己的代币，包括 EOS、XUC、OMG、ITC 等知名项目均在以太坊上发布了对应的代币。

代币智能合约的出现极大的降低了项目融资的难度，也让以太坊市值如日中天。然而，运行智能合约也为以太坊带来了巨大的负担。以 CryptoKitties 为例，一款应用就占据了 20%的交易量，并且造成网络严重堵塞，部分交易时长超过 24 小时。不难想象，如果以太坊网络同时有多款热门应用，以太坊将几乎陷入瘫痪状态。据不完全统计，目前运行在以太坊上的代币或智能合约数量已达数千种，以太坊已不堪重负。

更严重的问题在于：整个网络环境极容易被污染。由于智能合约并没有进行严格的形式化验证，合约本身的安全性完全取决于研发工程师的个人水平，这使得以太坊上充满了各种不安全的智能合约。一旦其中一个合约发生严重 BUG，就将使得整个以太坊网络受到巨大影响。The Dao 事件就是典型的例子。

作为史上最成功的众筹项目之一，The DAO 智能合约代码中的致命漏洞造成了史上最大的数字抢劫案——黑客利用漏洞窃取了 The DAO 项目 30%的以太币，按当时市值计算约价值 5500 万美金。The DAO 事件暴露了单一网络体系的巨大问题，没有网络隔离，一旦发生 BUG 将影响到整个区块链网络的安全。

2.4 与现实世界交互的难题

区块链世界和现实世界之间存在天然的屏障，与现实世界的交互是现有区块链项目面临的一大难题。智能合约在一定程度上缓和了这一问题，可以通过多重签名等方式和现实世界进行弱交互。然而，在面临复杂问题时仍然无能为力。

用户在设计智能合约时面临的最大问题就是运行在虚拟机中的代码无法访问和调用区块链网络之外的数据。举例而言，金融衍生品是智能合约最常见的应用，也是最易于用代码实现的应用。在实践过程中的主要挑战是大部分金融衍生品合约都需要配合一个专门用于数据发布的合约，而这需要依赖某特定机构定期进行维护和数据更新，并提供一个接口使其他合约能够通过发送查询消息来获取关键的金融数据。现有的区块链网络缺乏一个智能预言机系统实现和现实世界的交互。

3. GAIA.WORLD 核心技术

3.1 共识机制

POW 作为第一代共识机制解决了分布式系统中的共识问题。PoW(Proof of Work)是基于算力计价的共识机制。矿工通过解决一个复杂而无实际意义的数学问题来创建一个区块，并获得一定数量的币作为奖励。每个矿工解决问题的能力完全取决于自身的算力，为了赚取奖励，矿工会互相竞争，不断升级自己的算力，白白耗费大量的资源和能源，导致交易费用不断升高，却无益于提高交易速度。除此之外，持币者无法参与任何决策，决策权集中在少数几个矿池手中，与去中心化理念背道而驰。

PoS(Proof of Stake)是基于链上货币计价的共识机制。PoS 用持币代替了算力，能够让持币者更多的参与到挖矿过程中，而且不需要计算复杂的数学问题，避免了资源和能源的浪费。已有的 POS 解决方案主要分为四种：基于拜占庭容错的 PoS，基于链的 PoS，Pow/Pos 混合, 基于授权的 PoS(DPoS)。基于拜占庭容错的 PoS 容错率较低，故障节点和恶意节点不超过矿工总数的 1/3，且为了达到较短的确认时间限制了验证者的数量。基于链的 PoS 本质上是 PoW 的一个货币计价改编。PoW/PoS 混合只是一个过渡方案，最终仍会被一个纯粹的 PoS 机制所取代。基于授权的 PoS 通过选举代理人达成共识，牺牲了去中心化的概念，不适合公有链。在研究了已有的 PoW 机制和 PoS 机制之后，GAIA 提出了一个全新的 PoS 方案：基于竞争的 PoS(CPoS)

3.1.1 CPoS

Gaia.World 总计产生 10,000 亿 GAIA 币。在创世区块中生成并且分配 9,000 亿 GAIA，1,000 亿 GAIA 作为锻造奖励预计 10 年发放完毕。短期而言，锻造者的奖励主要来源于锻造奖励和交易手续费。随着社区的发展，锻造奖励会逐渐减少直至最终取消，交易手续费会成为锻造者最主要的收益来源。之所以在项目早期设置锻造奖励，是为了防止因为前期交易过少，而导致的诚实锻造者消极出块，使得安全性降低。

3.1.2 锻造委员会

锻造委员会是区块链的一个基础底层模块，其中包括一个拥有创建区块权利的地址的集合。集合中的每一个地址都是一个锻造委员，每个锻造委员都有机会创建区块。为了激励锻造，成功锻造一个区块将会获得该区块中的所有交易费。

所有地址都可以申请加入锻造委员会，在加入锻造委员会时，会提交一个 bls 加密算法的公钥，自己保留私钥，公钥会用来验证该锻造委员产生的随机数。锻造委员会收取最少 1,000GAIA 作为保证金，保证金和锻造者的权益值相关，如果锻造者故意作恶，保证金会被罚没。收取保证金是为了防止节点作恶，最低限度设置为 1,000GAIA 是为了防止微资金地址加入锻造委员会。GAIA 认为保证金较高的地址，作恶的可能性更小。如果一个保证金少于 1,000GAIA 的地址申请加入锻造委员会，保证金会被罚没，罚没保证金是为了防止恶意的加入申请。

锻造委员的职责是创建新的区块。锻造委员可以主动申请退出锻造委员会, 该地址的保证金会被扣留 256,000 个区块高度。扣留保证金是一种惩罚机制，用于惩罚不能正常完成其职责的锻造委员。之所以不设置退出机制，是为了防止恶意节点，将大部分节点剔除出锻造委员会，实施长程攻击。

3.1.3 锻造组

所有人都可以查询到每个锻造委员的当前投票权。锻造委员首次将被按照地址的后 8-bit 进行分组，后两位地址即是分组编号，分组编号相同的为同一组，总共 16*16=256 个组。设当前区块高度为 H，则 H%256=N，N 号锻造组负责本轮的锻造。首次按照地址分组是为了让锻造委员尽量加入锻造委员较少的组，使得每组委员数不会相差过大。同时，由于单一用户可以拥有无限个地址，所以即使只有一个用户也能够占满 256 个分组。

3.1.4 主锻造委员

当前锻造组中投票权最高的锻造委员当选为主锻造委员，后续锻造组都倾向于验证和认同主锻造委员锻造的区块。

本组内所有的锻造委员都可以创建区块并且全网广播，其他节点收到区块后将进行验证。

为了优化不必要的计算和网络广播和建设分叉，如果主锻造委员在上一个区块产生 N 秒之后仍然没有全网发送新区块，则当前锻造组中投票权第 2,3 高的锻造委员则会立即锻造区块并广播。如果再过 1S 仍未产生区块，则投票权第 4,5 高的锻造委员则会立即锻造区块并广播。以此类推，直到锻造出新的区块。这个策略可以降低分叉的可能性，同时兼顾区块创建速度。

3.1.5 投票权计算

锻造委员的投票权和保证金的数值相关，设一个锻造委员缴纳的保证金为 a 个 GAIA，则初始投票权 K 为 LOG10(a*0.01)*p。P 为一个在[1,4]之间的随机值，在锻造委员初次获得投票权时生成，且在投票权再次初始化时重新计算。一个新申请加入的锻造委员不会立即获得投票权，需要等待 256000 个区块高度以后才会获得投票权。之后每隔 256 个区块高度(即一轮)投票权一次性增加 K。随着区块高度的增加，投票权不断累积，投票权最多增加 2560 个区块高度，即初始投票权 K 的 10 倍，之后不再增加。用投票权进行委员排序，如果有多个投票权最高的锻造委员，则比较锻造委员的地址值，地址值更大的排名更高。在当前分组中排名前 10 的锻造委员会获得额外的排名投票权，设排名为 R，则排名投票权为 2 的(11-R)次方。总投票权为累积投票权与排名投票权之和。

每个区块都会生成一个随机值，区块高度 m 对应的随机值为$R_{(m)}$， $H_{(x,y,z)}$为一个 hash 函数，让入参被唯一映射到一个[1,4]之间的值。设锻造委员地址为 l，则 $p=H_{(R_{(m)},m,l)}$。如果一个锻造委员成功将区块添加到了区块链，则该锻造委员和当前分组中投票权更高的其他锻造委员的投票权都会被重置为初始投票权（p 值会重新计算），且都会被重新分组。分组依据为委员地址、当前区块高度、当前随机值三者 hash 的最后 8-bit 的值。之后随着区块高度的增加，投票权不断累积，直到最高为初始投票权 K 的 10 倍。之所以需要不断的更新分组和更新初始投票权，是为了防止恶意节点串通控制几个相连的节点进行双花攻击。

降低保证金数值和投票权的正相关程度是为了避免大额地址拥有过高的投票权。累计投票权随着区块高度增加而增加，是为了激励小额锻造委员也有机会成为主锻造委员。设置 10 倍的上限是为了控制小额锻造委员的数量，保证金过少的锻造委员在可信度和稳定性方面不如缴纳了大额保证金的锻造委员。排名投票权是为了降低被恶意委员联合攻击的风险。

3.1.6 奖励和惩罚

锻造委员的奖励由两部分组成：1. 主锻造委员创建新区块将获得该区块中所有交易费。2. 举报作恶锻造委员将获得该作恶地址的所有保证金。在没有双签作弊节点的情况下，锻造委员只能从交易费中获得奖励，不会获得额外的奖励。

类似比特币或以太币的额外的奖励会引发富者越富的副作用，而且区块的创建过程消耗的资源极低，即使只有交易费作为奖励，锻造委员已经有利可图了。

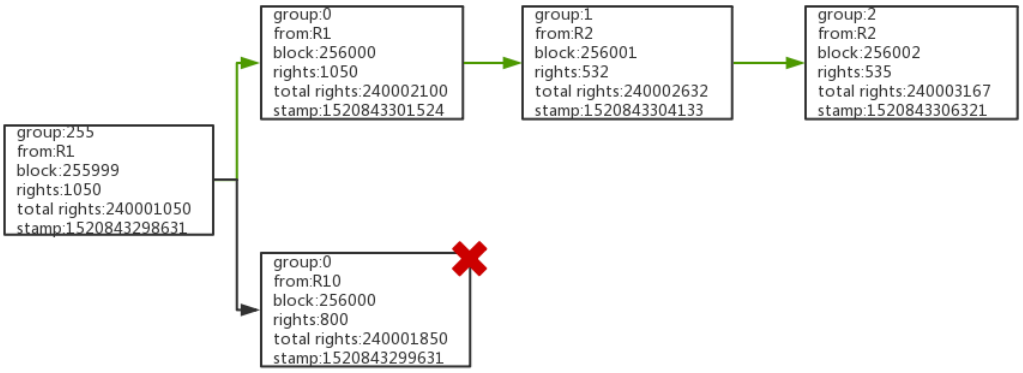
当锻造委员收到一个新的区块时，会验证区块高度、主锻造者签名、交易有效性，如果通过验证则会加入到自身的区块链上，如果没通过验证则会丢弃该区块。如果同一个锻造委员在同一个区块高度向其他锻造委员发送了两个不相同的区块，则该锻造委员被判定为作弊，将被罚没所有保证金。第一个举证该锻造委员作弊的锻造委员将获得被罚没的所有保证金。

3.1.7 形成共识

总投票权最高的链是主链。第 N 个区块的投票权等于主锻造委员在锻造该区块时的总投票权，区块链的总投票权为单个区块的总投票权之和。因为主锻造者的投票权极高，所以区块将会在极短的区块高度就达成共识，分叉将迅速被消除。

3.1.8 最短出块时间

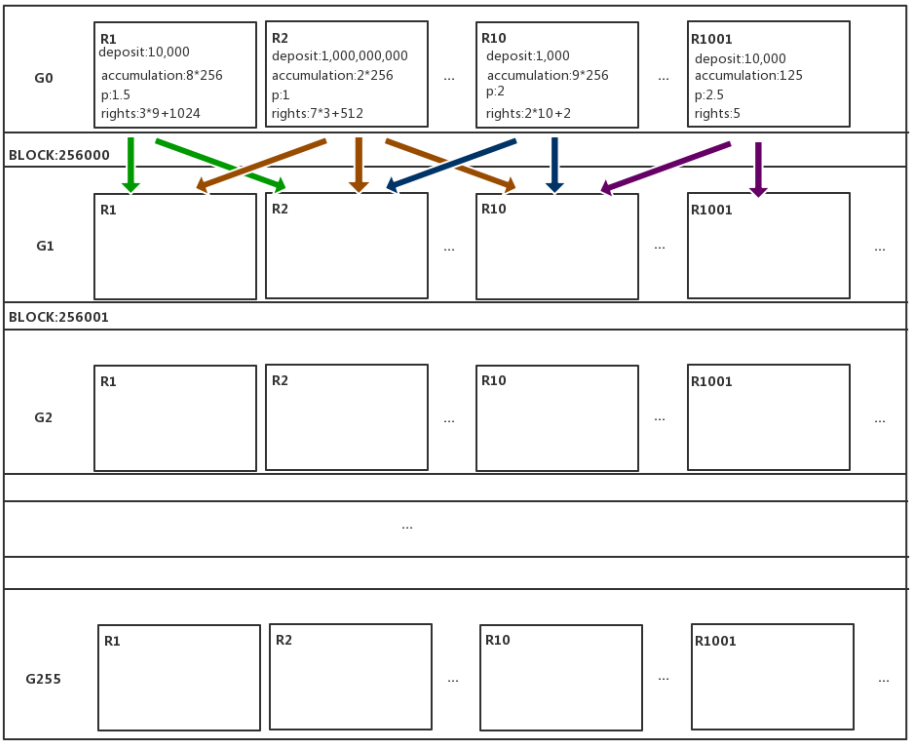
为了防止长程攻击(long-distance attack)我们在创世区块中会设定默认最短出块时间 T，如果出块间隔小于 T/2，则认定该区块无效。不同的侧链，可以根据需求设定不同的最短出块时间。具体过程如下：当产生一个新区块会在所有锻造者之间广播，锻造者以本机时间为准，如果新区块的时间戳大于本机时间则认为该区块无效，如果新区块时间戳和上一个区块的时间戳间隔小于 T/2，也认定该区块无效，无效区块会直接被抛弃，不会被广播。之所以是 T/2 而不是 T，是因为我们在一定程度上鼓励快速出块，也减小了锻造者本机时钟轻微误差造成的影响。例如，设定默认最短出块时间为 3S，如锻造者发现两个区块的时间戳间隔小于 1.5S，则认定该区块无效。



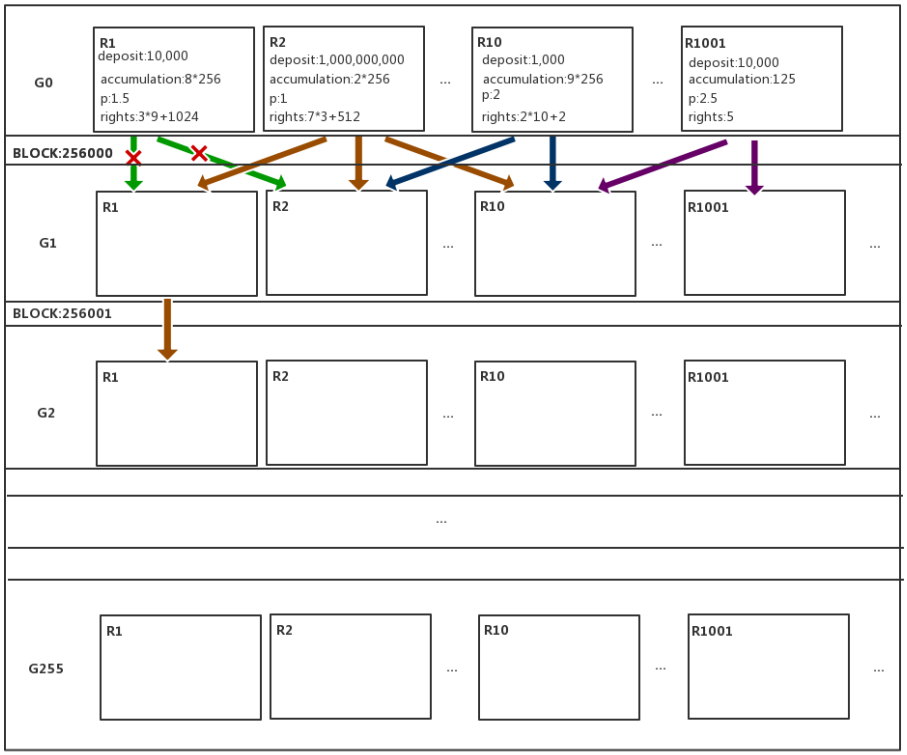
3.1.9 锻造过程

为了便于理解，此处只描述最高投票权锻造者和次高投票权锻造者的锻造过程和选择策略。实际情况更为复杂，但是原理相同。我们约定 Rn 代表分组中投票权排名第 n 位的锻造委员。

在区块高度 255,999, 所有组编号为 0 的锻造委员均有机会创建 256,000 号区块，其他分组无法创建区块。R1 地址为 0xdab12...00, 缴纳了 10,000GAIA 保证金, 随机值 P=1.5，总共累计了 2,304 个区块高度(即 9 轮)，累积投票权为 27，排名投票权为 1024，总投票权为 1051，设其创建的区块为 B1。R2 地址为 0xd12e9...00, 缴纳了 1,000,000,000GAIA 保证金, 随机值 P=1, 总共累计了 768 个区块高度(即 3 轮)，累积投票权为 21，排名投票权为 512，总投票权为 533，设其创建的区块为 B2。虽然 R2 缴纳的保证金为 R1 的 100,000 倍，但是 R1 却获得了更高的投票权, 避免了富者对投票权的垄断。所有组编号为 0 的锻造委员都可以将自己创建的 256,000 号区块进行全网广播。只有组编号为 1 的锻造委员们可以继续创建 256,001 号区块。由于总计投票权最高的链会成为主链，组编号为 1 的锻造委员们在理智的情况下都会在 B1 的基础上继续创建 256,001 号区块。

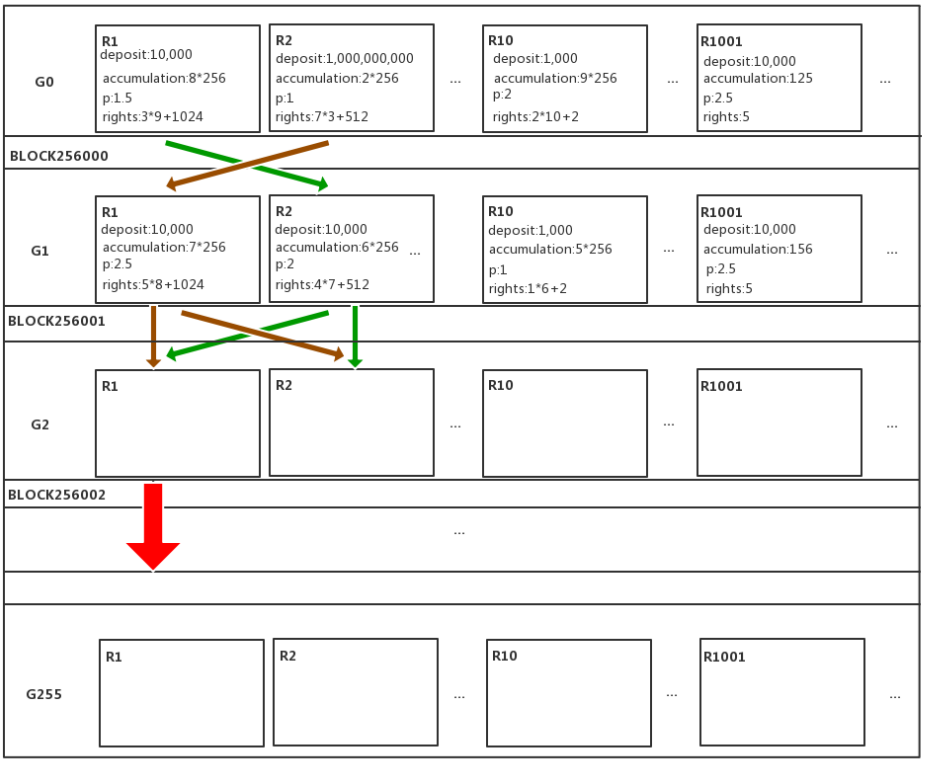


现实世界的网络环境极为复杂，投票权最高的投票委员有可能没有向下一个锻造分组发生新的 256,000 号区块。G1 分组锻造委员的最优策略是：等待 G0 分组 R1 一段时间，如果仍无响应，则接受 R2 创建的区块。愿意等待的时间和 G1 分组锻造委员自身的总投票权相关。自身总投票权越低的节点愿意等待的时间越长，因为这是在 256,001 区块高度打败同组更高投票权投票委员的唯一方法。G1 分组中 R1 会等待一段相对较短的时间，然后接受 G0 分组 R2 创建的区块。因为自身投票权最高，即使接受了投票权较低的区块，仍然有较大机会胜出。

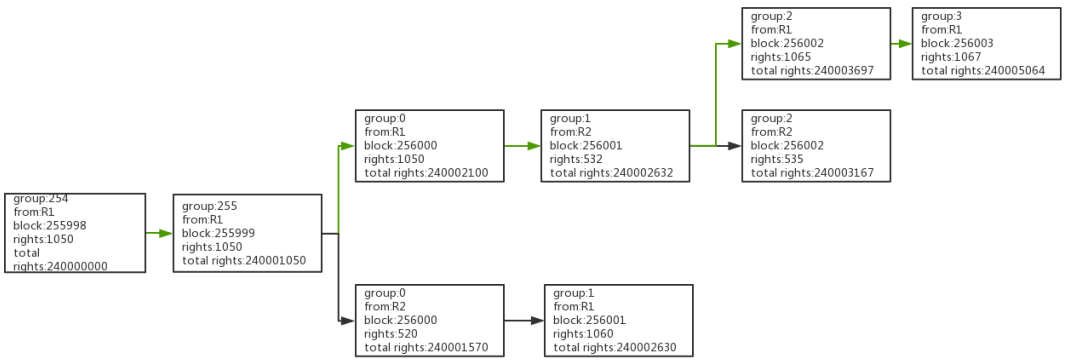


由于总投票权和分组、保证金、累积区块高度、排名投票权、地址五者相关，使得锻造委员难于串通作弊，但不排除由于网络原因或者其他未知原因导致的，最高投票权锻造者接受了上一个区块的次高投票权的锻造者创建的区块，如图所示。

G1 分组中的 R1 接受了 G0 分组 R2 创建的 256,000 号区块，而 G1 分组中的 R2 接受了 G0 分组 R1 创建的 256,000 号区块。G1 分组中的 R1 和 R2 都会向 G2 分组的锻造者提交区块。G2 分组中的 R1 选择总投票权最高的链继续锻造。



基于 CPoS 机制，分叉总是能在较短的区块高度被消除，如图所示。在区块高度 256,000 和区块高度 256,001 产生了分叉, 而 G2 分组的最高投票权锻造者选择了其中一条链，该链的总投票权显著增大，有极高概率胜出。G3 分组的锻造者会基于该链继续创建区块。



3.1.10 可验证性随机

每一个区块都有一个随机值，随机值由当前区块的锻造者产生。锻造者拥有一把特殊的 bls 私钥，用于生成随机数，而对应的 bls 公钥在锻造者申请加入锻造委员会时公布。设当前区块高度为 m，随机值为R_m，上一个区块随机值为，BLS 为签名算法，则$R_m = BLS(R_{(m-1),m})$，即使用上一个区块的随机值和当前区块高度来生成新的随机值。锻造者在当前区块高度，同时公布旧 bls 私钥和随机值，以及新的 bls 公钥。由于所有人都提前获得了旧的 bls 公钥，所以都可以对随机值进行验证，确保随机值的确是由旧 bls 私钥生成的。由于旧的私钥已经被知晓，所以锻造者需要更换新 bls 私钥，并公布新 bls 公钥。在随机数生成过程中没有加入交易信息等可人为控制的信息，是为了确保锻造者不会人为筛选交易，以获得对自己更有利的随机结果。

我们无需保证初始随机源的随机性，非随机的初始随机源，只会对最初的几个区块产生影响，对于后续区块，即使初始随机源是非随机的，后续产生的随机数仍然是随机的。

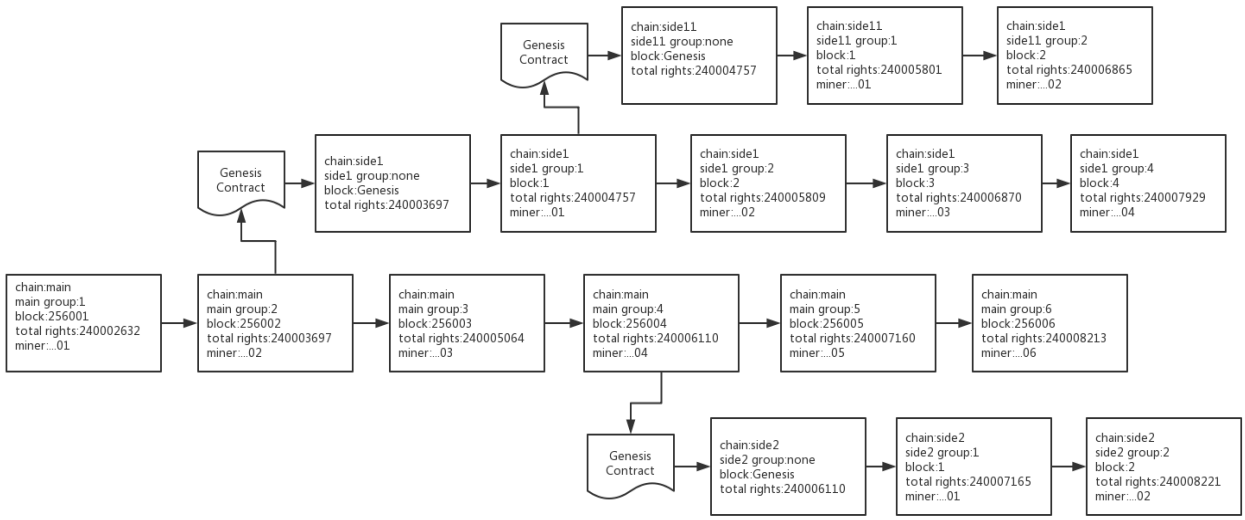
3.2 平行链

为了提高区块链的可扩展性和分散主链的网络压力，Gaia.World 设计了平行链架构。平行链由主链和侧链两部分组成。主链上只运行最基础的服务，所有应用级服务都在独立的侧链上实现。

侧链代码和主链相同，使用相同的共识算法（CPoS），有自己独立的区块链。和传统的 PoW 共识机制不同，PoS 占用的系统资源较少，使得侧链和主链可以共享网络节点资源，侧链从创建初就获得了较高的安全性。同时，侧链也能吸引更多的节点加入网络， 主链的安全性也会得到加强。

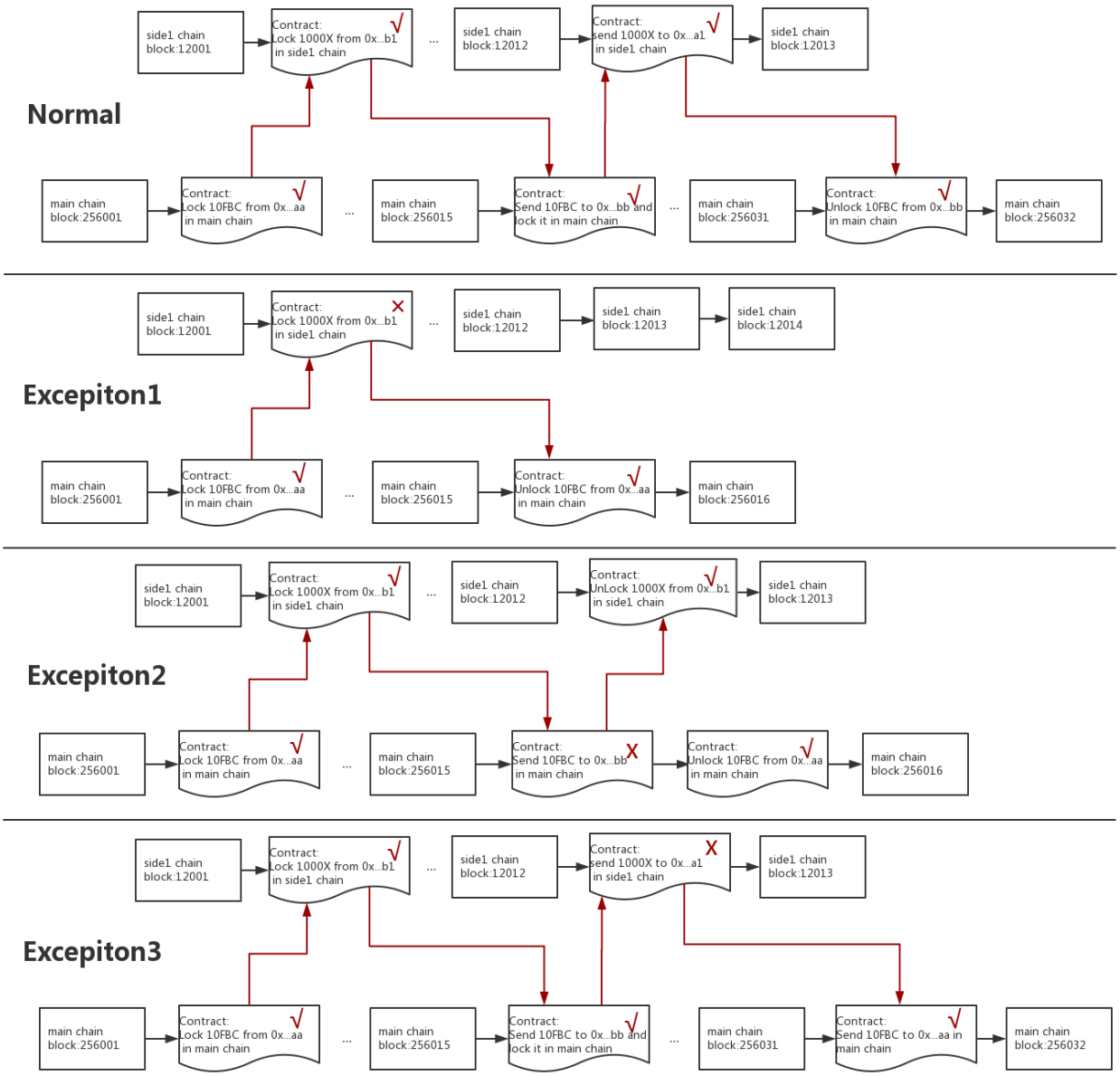
3.2.1 侧链树

平行链支持把指定的侧链作为主链，继续分叉成新的侧链。依次类推，从而形成一个侧链树，如下图所示。



3.2.2 跨链事务

在每条链上，智能合约或交易都是一个完整事务。由于侧链和主链处在不同的节点网络中，各自区块链的生成者、速度和规则都不一样，无法完成一个完整事务。因此我们制定了一个跨链事务规范来保证侧链和主链可以运行一个完整事务，如下图所示。



3. 2. 3 侧链的独立性

侧链架构的好处是数据独立，不增加主链的通讯和存储负担，避免数据过度膨胀和广播，也避免了代码 bug 被扩散到其他链上。主链上仅运行数字货币，身份验证等核心功能，其他应用都在侧链上开发和运行。遗憾的是，在传统区块链系统中，所有主链的节点并不会锻造侧链的区块，主链和侧链之间也无法进行价值的交换。

传统上认为，独立性既是优点，也是缺点。开发者在一个独立侧链上完成开发工作后，还要考虑运营问题，需要建立足够的节点来运行它，否则难以维持足够的安全性。而 GAIA 通过平行链实现了独立性和交互性的统一。

3. 2. 4 侧链的灵活性

侧链存在的主要目的是使得区块链核心逻辑和海量的应用逻辑区隔开来，提高整体运行速度和主链的安全性。

侧链也为开发者提供极大的灵活性。Gaia.World 建议大部分复杂应用都应该创建自己的侧链。侧链和主链通过相同的共识和特定的协议规范进行通讯，并不对侧链的运行细节做过多的限制，给开发者提高了较大的发挥空间。

3.2.5 主链与侧链的互利关系

主链与侧链之间是互惠互利的关系，主链为侧链提供基础设施，侧链则可以为主链补充更多的节点和开发者，以壮大整个系统。 侧链的开发者不需要提供机器，可以利用已经存在的主链节点，只需要节点拥有该货币。另外，主链和侧链可以用系统提供的跨链事务规范进行价值交换，相当于为侧链的资产提供了一种价值的媒介。 开发者就不需要考虑交易平台的问题。

3.2.6 解决生产力问题

GAIA 侧链具有极低的开发难度，开发者只需进行简单的参数配置并且发布该侧链，侧链就得到了自动的运行。对于大多数普通开发者而言，并不需要关心区块链的实现细节，只需要关心具体的业务逻辑。同时为了保证开发者代码的可移植性，GAIA 兼容以太坊只能合约代码，而且侧链内的智能合约也使用和主链相同的编程语言，还可以调用主链上的智能合约的代码库，共享相同的开发者社区。

3.2.7 节点安全问题

这里的安全问题与上面提到的因为节点不足或代码 bug 导致的问题不一样，这里说的安全问题是指侧链代码对节点造成破坏的问题。 我们希望每一个矿工节点都能信任并接受任意侧链，而且节点本身无需信任侧链的开发者。这就需要提供一种安全防范的措施，比如，防止侧链代码读取文件系统、过渡消耗网络、内存或 CPU 操作。 在我们的系统中，侧链代码会使用沙箱机制隔离的 javascript 虚拟机，然后我们为这个虚拟机植入一个定制的 require 和一些常用且安全的模块，最后再加载侧链的代码。 我们还通过容器技术来管理每个侧链的网络、内存或 CPU 的消耗，这样侧链的安装者就没有任何风险。

3.3 神盾协议

神盾协议，就是一个按照 Gaia.World 约定的安全协议规范，实现的一种特定的智能合约。该智能合约可以被智能合约虚拟机执行，从而和外部服务器进行通信。包括获取数据，或者完成一个完整事务。示例代码如下所示：

```
1.  //a committee for manage security function
2.  contract SecurityCommittee {
3.      //the struct for voter
4.      struct Voter {
5.          bool agreement;
6.          address voter;
7.      }
8.      //the struct for security function
9.      struct SecurityFunc {
10.         address applicant;
```

```
11.         address securityFunc;
12.         uint32 publickey;
13.         mapping(address => Voter) voters;
14.     }
15.     //the return value of call security function
16.     struct SecurityResult{
17.         uint32 sign;
18.         address securityFunc;
19.         any param;
20.         any result;
21.     }
22.     //global store for all security function
23.     SecurityFunc[] public securityFuncs;
24.     // submit a security function, only can be used after the application is pass
25.     function submit(SecurityFunc func){
26.         securityFuncs.push(func)
27.     }
28.     // vote for a security function, need 2/3 voter's agreement
29.     function vote(address securityFunc, bool agreement) {
30.         //TODO;
31.     }
32.     // check if a security function can be called
33.     function isPass(address securityFunc) constant returns (bool){
34.         //TODO;
35.     }
36.     // calculate the digest by sign and public key from security function
37.     function calDigest(address securityFunc , uint32 sign) returns(uint32){
38.         //TODO;
39.     }
```

```
40.     //calculate the Digest of result with param
41.     function calHash(SecurityResult result) returns(uint32){
42.         //TODO;
43.     }
44.     //check if the hash is just the same
45.     function isSameHash(uint32 src, uint32 dst) returns(bool){
46.         //TODO;
47.     }
48.     //call the security function by address with params
49.     function callSecurity(address securityFunc, any params) returns (SecurityResult){
50.         if(!this.isPass(securityFunc))
51.             throw;
52.         return securityFunc.call(params)
53.     }
54.     //check if the result value is generated by the
55.     function checkSecurityResult(SecurityResult result) returns (bool){
56.         uint32 digest = this.calDigest(result.securityFunc, result.publickey)
57.         uint32 hash = this.calHash(result.result)
58.         return this.isSameHash(digest, hash)
59.     }
60. }
```

3. 3. 1 封闭或扩展

在标准意义上的智能合约本质上是一段运行在虚拟机中的代码，代码所操作的数据全部存放在链上，在这种架构下，智能合约代码无法调用和操作区块链之外的数据。这就导致传统的智能合约无法和区块链外的数据进行交互。

在 GAIA.WORLD 区块链架构中，我们提供一个用户定义的外部函数调用，运行在 GAIA.WORLD 链中的代码可以通过神盾协议调用外部数据，这将极大的拓展智能合约的应用范围。

3. 3. 2 如何定义安全

智能合约是被锻造区块链的节点来执行的，我们俗称矿工。如果一个神盾协议没有被认为是安全的，矿工会拒绝执行包含该神盾协议的智能合约。因此，我们需要引入安全共识。

- 首先，提供神盾协议的智能合约会缴纳保证金。保证金是其提供服务价值的数倍，提高作恶的成本。
- 其次，锻造委员会会对该智能合约进行投票，如果多数矿工投信任票，则神盾协议就被信任，从而可以被调用。
- 最后，不信任投票随时可以进行，如果一旦超过半数，则保证金将被没收。

神盾协议应该尽力说服矿工相信自己的安全性。比如，提供源代码地址，提供权威性的证明材料。

3.3.3 分布式事务

在一个复杂的、需要保证严格一致的应用场景，比如多方交易。一个简单的神盾协议调用，是无法满足这类应用的。因此，我们定义了分布式事务神盾协议规范，保证了区块链可以和外部数据进行安全和一致的数据交换。

3.3.4 权益

提供神盾协议的外部服务器也是需要成本的，因此提供神盾协议的智能合约可以规定每次调用的交易费。有了收益，神盾协议的服务商就会有动力去提供更大的带宽，更大计算力。而且也会吸引更多人来提供神盾协议，从而引入竞争，降低成本。

3.4 仲裁委员会

为了有效的管理 GAIA 区块链系统，我们参照现有英美法和大陆法系的多级法院体系建立了三级仲裁委员会规范，部分思路借鉴了 ENS。仲裁委员会是 GAIA 区块链系统中的去中心化管理组织。当用户发现节点或神盾协议作恶，或其他恶意行为时可以像仲裁委员会举报，而用户间的纠纷也可以向仲裁委员会申请仲裁。

3.4.1 仲裁者

每一位锻造委员同时也是一位仲裁者。同时在 GAIA 区块链创建后便会投票选出 9 位最高仲裁者。全网获得认可度最高的 9 个节点会成为最高仲裁者。

3.4.2 仲裁机制

申请人发起一个仲裁需要缴纳押金，如果在这个仲裁中申请人胜诉，押金将退回，否则将会被扣除。为了保证仲裁者的判决不会影响到其他仲裁者的决策。仲裁者的判决需要分两步提交：

仲裁者作出裁判后，会生成一个随机私钥，同时用随机私钥对判决结果摘要信息进行加密并且公布。裁判的期限结束后，仲裁者必须在限定时间内公开他们的随机私钥和判决结果，然后任何人都可以以此验证这个判决结果的。如果判决结果和随机私钥披露失败，仲裁者（锻造委员）将受到惩罚。

为了阻止仲裁者相互勾结，如果任何人提前披露了某个仲裁者的随机私钥，那么这个仲裁者将会受到惩罚，而其押金的一部分会奖励给披露人。

3.4.3 初级仲裁

申请人缴纳一定的押金后可发起一个初级仲裁：

- 从所有仲裁者（锻造委员）中随机邀请 5 位组成初级仲裁委员会。如果其中某个仲裁者拒绝参加会受到轻微处罚，然后重新再选一个。
- 仲裁委员会将收到与仲裁相关的材料。
- 每位仲裁委员会提交被随机私钥加密之后的判决摘要信息。

- 等待仲裁期过后，仲裁委员公布判决结果和随机私钥。
- 若仲裁申请人胜诉，将收到退回的押金，和败诉方被扣除的押金。若申请人败诉将会被扣除押金。
- 投了正确票的仲裁者会得到奖励，而投错票的仲裁者会被扣除一部分押金。

3.4.4 中级仲裁

如果申请人不服初级仲裁中的判决，他们可以发起上诉（需缴纳更多的押金），中级仲裁将邀请网络中所有的仲裁者（锻造委员）组成委员会，委员会作出判决的流程与初级仲裁一致。如果中级仲裁的结果和初级仲裁不一致，所有初级仲裁中投错票的仲裁者都会被严厉惩罚。

3.4.5 最高仲裁

如果申请人不满意前两轮的判决，他们可以继续上诉至最高仲裁者，然后由 GAIA 中的 9 位最高仲裁者组成最高仲裁委员会。

4. GAIA.WORLD 的链上应用方案

GAIA.WORLD 作为革命性的互联网底层架构，其所能实现的功能远不止数字货币或电子合约，许多我们常用的工作、生活甚至娱乐或游戏应用将会以全新的形态在区块链上呈现。作为一套去中心化的协作体系，得益于技术团队带来的革命性技术，我们有能力将海量互联网应用以去中心化的方式进行重构，互联网将变得更安全、更可靠、更富有想象力。

4.1 高性能要求的应用

现代互联网应用对于响应速度和服务器处理能力的要求越来越高，以知名社交网络 Facebook 为例，作为社交网络的鼻祖，截至 2017 年 7 月，其月活跃用户数已突破 20 亿，每 5 次网页访问中就有一个指向 Facebook 这一全球最大的社交网站上。每天用户在 Facebook 上分享的内容超过 50 亿条，“赞”按钮点击次数超过 45 亿次。Facebook 目前存储了超过 3000 亿张照片，每月照片存储容量约增加 10PB（注，单位换算：1PB=1024TB）。

另一个对性能要求极高的应用是在线游戏。由于玩家在游戏中的大多数行为都需要和服务器进行交互和信息确认，传统游戏运营过程中，为了降低服务器的压力通常会分割出许多个独立的服务器。如果游戏应用完全在区块链网络中运行，这对整个网络的数据处理能力将是巨大的挑战。

面对如此庞大的数据量，哪怕将现有的区块链网络全部整合也无法满足需求。即使区块链的用户数量增长数倍，但受限于 PoW 设计上的低效率，区块链网络的膨胀并不能带来其处理效率的明显增长。相反，新增加的运算资源大多被浪费在算力竞争和防止意外分叉而进行的校验上。

相反完全基于 CPoS 技术的 GAIA.WORLD 能够极大地提高区块链的处理效率，在小规模的测试网络中我们已经可以实现 1000TPS 的处理效率，和以太坊网络每秒 10 次的低效率相比，这是一次巨大的飞跃。另一方面，由于 CPoS 区块链中节点不需要靠算力来竞争记账权，整个 GAIA.WORLD 网络的性能将随着网络规模的增加进一步提高，新增加的运算性能也不需要浪费在无意义的 Hash 竞赛上。在 GAIA.WORLD 的高性能区块链网络中，开发者可以实现许多传统区块链难以支持的应用模式，包括游戏、博彩、社交分享，轻博客等。

区块链的另一个重要应用方向即时通信。在以太坊区块链网络中，哪怕性能不造成瓶颈，高昂的交易费用也阻碍了这类应用的开展。可想而知，发送给朋友的每一条信息都要收取不菲的费用。何况，同样受限于 PoW 的设计问题，每个节点最主要的收入来自于争夺记账权成功得到的奖励（挖矿），而每笔交易支付的交易费和挖矿

奖励相比仅是九牛一毛。这种模式下每一个节点都花费大量的成本来提高运算性能，以提高自己挖矿的成功率。交易（记账）本身反而成为节点并不太愿意干的事情。可以预计，交易费用在将来还会进一步提高。

在 GAIA.WORLD 网络中，得益于优化的 PoS 机制，挖矿将成为历史。由于不比拼运算性能，任何个人计算机都能成为支撑 GAIA.WORLD 区块链网络的节点，而节点的收益也将全部来源于交易费。传统 PoW 网络存在的节点中心化问题迎刃而解，而节点充分竞争也将带来更低廉的交易费用。这使得开发者可以在 GAIA.WORLD 中构建完全去中心化的点对点或群组即时通信应用。除此之外，GAIA.WORLD 也能为小额代币支付，线上游戏这类金额小而交易频率极高的应用提供低成本的去中心化区块链解决方案。

4.2 与链外世界交互的应用

以以太坊为例，传统意义上的区块链“应用”通常是指某种进行简单条件判断从而自动处理交易的智能合约程序。问题在于，以太坊智能合约使用图灵完备的语言编写，理论上可以实现远远比这复杂得多的高级应用。可是事实上，这类应用大多仍然停留在纸面上。这固然有以太坊本身低性能高费用问题造成的影响，但更主要的原因是以太坊智能合约无法访问区块链外的数据。

以太坊中的区块链应用通常只能依靠人工维护的数据发布合约来实现获取外部数据，可人工的介入却违背了其“去人工化”的设计本意，而且还可能进一步带来出错的风险。而使用神盾协议则可以轻松实现这种应用。

而在 GAIA.WORLD 区块链上，开发者可以通过独创的神盾协议功能来解决这一问题。在区块链上将部署一套安全的、可防止被篡改的神盾协议系统。开发者可以让智能合约应用通过网关自动化获取区块链外的数据，这一过程是双向的，智能合约同样可以通过神盾协议向区块链外的地址发送数据。

利用这一特性，开发者将能够在 GAIA.WORLD 区块链上运行更高级的智能合约应用。以前文提到的社交类应用举例，开发者将可以实现内容的分享接口，让用户可以方便的将自己在其他平台看到的图片、文章等内容直接发布到区块链中的社交网络上。

另一方面，GAIA.WORLD 的链上应用支持接入第三方支付，包括各类娱乐应用，游戏应用，博彩应用等都可以轻松实现商业化。而对于第三方支付这类对安全性高度敏感的应用接口，开发者可以在智能合约中约定支付功能的细节和限制，例如支付频率，是否需要二次验证或设置支付限额。

4.3 在侧链上开发应用

一个区块链网络的复杂程度取决于链上运行的资产和应用的数量。对于某些复杂而与核心区块链资源（货币，身份验证等核心功能）交互并不频繁的区块链应用而言，直接在主链上以智能合约形式运行并不是一个好的选择。为此，GAIA.WORLD 提供平行链来实现这一功能。事实上，我们更鼓励开发者以平行链的形式创建自己的链上应用。

平行链由主链和侧链两部分组成，侧链在基础层面独立于主链，但提供通用接口供侧链和主链进行通信，侧链可以直接调用主链中的功能和数据，也可以和主链进行互相操作。开发者建立平行链后不同于比特币的分叉，不需要自行建立新的节点网络，原有的 GAIA.WORLD 节点会自动为由 GAIA.WORLD 衍生的平行链提供服务。

由于平行链支持树状多层侧链技术，开发者可以在侧链上再次衍生侧链，以社交网络为例，开发者可以在第一层侧链上运行社交网络的核心架构，例如账户和用户信息等。而将其他功能例如聊天，轻博客，或其他社交网络应用运行在第二层或第三层侧链中。这种架构可以使开发者方便的搭建和管理复杂的区块链应用。

此外，平行链也能为开发者提供安全和可隔离的应用开发与测试环境，侧链中出现的问题和 BUG 也不会影响到主链。类似以太坊“The Dao”的灾难性安全事故在 GAIA.WORLD 中将被严格隔离在侧链上。而复杂的应用运行在独立的平行链上既能提高应用本身的执行效率，也能大大降低主链的臃肿程度。独立侧链的另一个应用方向是开发者可以基于 GAIA.WORLD 主链发布自己的数字货币，而通过平行链的交互性，能够通过运行在主链上的智能合约实现完全基于链上应用的交易所。

4.4 时间区块链应用

GAIA.WORLD 可以分叉成仅保留特定长度的平行链，传统区块链保留从创始开始的所有区块，而 GAIA.WORLD 侧链可以支持只保留特定时间长度的区块，这能有效的减少区块链的长度，降低设备的运算和存储压力。这使得 GAIA.WORLD 侧链可以被部署到大部分性能较低的设备上。

此外，以传统游戏应用为例，对大多数用户常规操作而言，服务器通常仅需保留数小时到数天以供回溯查询，除了某些核心内容外，大多数数据并不需要保留太长时间。而如果开发者希望完全基于区块链开发游戏，由于传统区块链必须保存所有数据，这将会造成区块链被大量无用数据占据。而通过时间区块链技术，开发者可以选择仅保留一定区块长度的数据。游戏应用或即时通信类应用的性能能够得到明显提高。

4.5 需要可验证随机数的应用

众所周知，现代计算机无法自行生成真正的“随机数”。常见的替代性解决方案是通过专门的“随机数供应商”来获取随机数，而这类服务商通常使用自然界的某种天然具有随机性的事物来帮助生成随机数。而受限于以太坊虚拟机的封闭性，智能合约只能生成伪随机数，这在用于某些对真随机要求极高的应用时就会带来很大的安全隐患。

以在线游戏应用为例，可以说游戏建筑在随机数之上，游戏中涉及装备掉落、开宝箱等情况都需要使用随机数来控制玩家获得物品的概率，若使用伪随机数将会使得游戏中的概率性事件变的可以预测。另一个急需可验证随机数的应用例如基于区块链网络的线上博彩，所有博彩玩法本质上都是基于概率的游戏，相对于其他复杂的游戏而言，博彩玩法以代码实现是非常简单的，同时博彩行业天生对匿名性，安全性，反作弊能力要求极高，区块链技术可以说是博彩行业最有前景的发展方向之一。

目前虽然在以太坊上已经出现了很多链上博彩应用，但受限于以太坊本身没有提供随机数生成机制，博彩类智能合约只能使用形式各异的伪随机，受限于本身开发水平的差异，这类随机的公平性仍然无法得到保证。而一旦区块链底层提供了随机数机制，博彩应用将可以完全在区块链上运行，体现区块链透明和公平的原则。

4.6 链上娱乐时代

区块链应用通常被认为仅面向部分严肃领域，例如金融业，商业或互联网基础服务。但随着区块链技术的进步和计算机性能的提高，越来越多的开发者尝试在区块链上设计各种娱乐性应用。以目前流行的基于以太坊的宠物收集养成游戏 Crypto Kitties 为例，用户可以花费以太币获得一只随机的“猫”，同时消耗资源将猫养大。用户之间可以自由的交易自己拥有的猫，而猫的价值和稀有度相关。

在这款游戏中的“猫”本质上是以太坊中的一种以以太币定价的数字资产，“猫”的获得与交换都是以智能合约的形式在以太坊网络中进行。从某种意义上看，这就是一种由以太币衍生的“猫币”。然而这款游戏几乎也代表了基于传统区块链开发游戏的极限。市面上更多的看似更加复杂的“区块链游戏”本质上只是内嵌了某种

数字货币的交易功能罢了，其核心的游戏代码逻辑仍然是以传统模式运行在中央服务器上，并不能真正保护玩家的利益和彻底摆脱游戏厂商操纵的可能性。

而在 GAIA.WORLD 区块链系统中，得益于独有的平行链和神盾协议等特性，我们能够提供一整套功能完善的 API 使各类娱乐应用可以完整接入 GAIA.WORLD 区块链，享受安全和去中心化的全新娱乐体验，很重视游戏公平性的玩家将会欢迎甚至只支持区块链游戏。

4.7 全新的区块链生态

过去，一个稳定运行的区块链项目上的各个参与者赚取收益的主要模式只有两种。“挖矿”和收取交易费用。“挖矿”基于低效率的 PoW 算法，不仅制约了整个区块链的性能，还浪费了大量的算力和电力资源。同时正因为“挖矿”收益为主交易费收入为辅，造成了交易费高启，为了整额生态体系的健康，类似比特币或以太币那样极高的交易费用也是不可取的。

GAIA.WORLD 在设计上彻底放弃了 PoW 算法这种“挖矿”模式。同时 CPoS 为节点带来了极低的性能要求和全新的竞争模式。随着节点网络的充分竞争和进一步扩大，GAIA.WORLD 用户将能够享受极为低廉的交易费用。

与此同时，我们更为区块链网络带来了全新的商业生态。首先是提供神盾协议，作为 GAIA.WORLD 区块链体系中最重要的特性之一，可以为区块链应用提供更大的想象空间，而神盾协议的设计或提供者将能通过为其他开发者提供服务获得持续的收入。基于神盾协议提供功能的复杂性和服务质量进行竞争，这将成为区块链上重要的商业生态之一。

另一个重要的模式则得益于平行链技术的出现。GAIA.WORLD 平行链的一个重要特点是支持树状多层侧链结构，开发者可以在侧链上开发新的侧链，这为一个全新的侧链应用开发市场提供了基础。开发者将可以基于 GAIA.WORLD 平行链开发独立的区块链应用平台并面向细分市场建立自己的独特生态体系，这将成为 GAIA.WORLD 中最具想象力的商业模式。

基于以上生态模式的可能性，GAIA.WORLD 真正有望成为互联网上的分布式操作系统。在 GAIA.WORLD 区块链技术的商业生态构建蓝图中，毒瘤式的“挖矿”获利生态将会让位于以程序员开发共建为主获利的生态，获利更将是因为为其他人产生实际价值，也将使社会资源得到更加有效的利用，就如 uber 带来的共享经济惠及普罗大众，而不再是由少数人堆砌无用硬件把持的军备竞赛游戏。

让我们携手创造真正的区块链世界！

5. 团队

5.1 核心团队

发起人：Calvin Ng

资深游戏人和创业者，20 余年从业经验，各大游戏公司任职，曾将“魔兽世界”代入中国

Zmax leo

20 年从业经验，大型多人在线网络游戏商用开发引擎的创始人

Fenix （Berkeley）

5.2 顾问

Adam Stradling

比特币和区块链开拓者，Bitcoin.com 创始人

Tiago

Aptoide 创始人 AppCoins 发行人

Ryan Terribilini

Google Play 运营资深策略师，Ripple 平台合作总监

Gaurang Torvekar

Indorse 联合创始人，以太坊新加坡大会(Ethereum Singapore Meetups)的联合组织人

Andras Kristof

FRD 首席区块链架构师，比特币、以太坊和 Ripple 合作者，《数字代币手册》(Handbook of Digital Currency)合著者

5.3 合作机构

Aptoide

Gumi

Gobi Partners

Google Play

Bitcoin.com

Kyber

6. 法律