MAI

题目：以人工智能为中心的

去中心化的生态网络

作者：MAI 基金会

完成日期：2018 年 7 月 5 日

版本 1.1

免责声明：本文旨在提供相关技术概览，所涉及内容不以完整性为标准，也非涉及终稿。因此，非核心技术领域（如 APIs、协议、程序语言等）未有涉及。

目 录

摘要

目前，在绝大部分公链上运作的智能合约和共识机制是与现有的公平、效率和智能合约的合法性特质相悖。因而也产生了诸多问题，如转账效率低下、代理人机制（DPOS）的不公平、刺杀美国总统智能合约、博彩智能合约、编写智能合约困难等。而人工智能区块链以智能合约的合规性和完整性以及安全性为量化评级去决定谁拥有记账权我们称之为 PAI，能够充分解决上述现行公链所存在的问题。首先，PAI 的可伸缩性能够提供编写智能合约的人一个安全，符合法律法规的模板智能合约。其次，PAI 可将智能合约的写入权限限制在预先设定的一定范围内，从而消除智能合约不合法的可能。再次， PAI 通过对比智能合约使用频次、编写频次、安全性、合法性的相关信息得出谁拥有记账的可能性，从而提升 DAO 的整体性能、规范和使用频率从而衍生出更多好的 DAPP。支持智能合约和通证系统（数字令牌）的区块链具有激发设备之间自主合作从而创造使用价值的巨大潜能。然而，由于现有公链的特有属性，如消耗 GAS 数量、挖矿费电、相对不公平等问题，现有的区块链技术还是处于 2.0 时代。

本文所介绍的 MAI 是以人工智能为中心的区块链驱动公链的 3.0 时代，其具有以下四大创新点：

1) 前沿的链中链架构支撑起平衡性良好的分配网络，以高性价比的方式将可扩展性和隐私保护性最大化；
2) 依靠轻量级私密地址、无需可信设置的环签名应用，在区块链中真正实现隐私保护；
3) 具有即时最终性的高速共识机制大幅度提升网络吞吐量，并降低各项成本；
4) 灵活的轻量级 PAI 系统架构，精准对智能合约的生成和执行在公链中的应用起到较高的监管性和辅助性。

1 区块链

2008 年，区块链技术首次进入人们视野。此项技术的初次应用（比特币）出现在一年之后。中本聪于 2009 年发表了一篇名为《比特币：一种点对点式的电子现金系统》的论文。区块链在本质上是一种分布式的交易数据库，所有在网络中的节点分享数据。这是比特币的技术创新，它在这种交易过程中担任着公共分类账目的角色。系统中的每一个节点都拥有现存链上的区块副本，其中包含了所进行过的一切交易数据，每个区块以哈希值与前一个区块相连，这些相连的区块就形成了区块链。每个区块链都包含四个维度，数据层、共识层、应用层三个水平维度以及一个垂直的治理维度。

1） 数据层

作为底层水平维度，被记录的交易在节点间广播，完整的节点产生区块。作为区块链的基础，在区块链中发生数字资产与其伴随的价值的传输，通过椭圆曲线密码、哈希函数、默克尔树算法等加密手段实现账户安全。

2） 共识层

共识层是区块链的中间水平维度，体现区块链点对点式的特征。在此层中，网络中所有节点通过工作量证明算法（ PoW)、权益证明算法（ PoS)或其变体、拜占庭容错算法（ BFT)或其变体等技术对链的内部状态达成共识。区块链的可扩展性主要受共识层影响。通常认为，PoW(工作量证明算法）在扩展性方面不及 PoS(权益证明算法）。此外，双重支付问题和区块链可能遭受的状态篡改攻击还会直接影响共识层的安全性。

3） 应用层

以上两个水平维度构建了区块链的基本构架，而应用层对于区块链的实际应用至关重要，影响到包括区块链可扩展性和可用性的问题。举例来说，以太坊使用的智能合约具备可编程性，使得个体能依靠分布式的全球计算机执行合约条款。侧链技术与合并挖矿也极大地推进了可编程性的发展。闪电网络[7]所代表的二级协议发展状态通道技术，进一步加强了区块链在此层面的可扩展性。此外，应

用工具、软件开发工具包、框架结构、图形用户界面对区块链的可用性也尤为重要。应用层为开发者提供开发去中心化的应用软件(DApps)的平台，这是区块链实现其使用性和价值的重要环节。

4） 治理层

与任何有机体一样，成功的区块链也将是环境的最佳适应者。在区块链系统只有通过演化才能生存的前提下，初始设计固然重要，但在足够长的时间段里，可变化的机制无疑是最重要的，此机制就是我们所说的垂直层面治理。

2 现有公链的局限性

作为社会去中心网络化的体现，区块链公链之争已经迎来了白热化阶段。谁能成为区块链最多应用的区块链主链谁就能成为未来的巨头。然而，这场影响深远的变革才刚刚起步。相信大家都知道，现在的公链时代还是像当年的 DOS 时代，是处于行业为发展的最初期。公链就相当于操作系统一样，希望操作系统要快，要安全，要兼容性高。但是，就目前的种种公链来看，还没有一款可以做到。就以太坊而言，一个养猫咪就让以太坊遭遇了巨大的网络拥堵。尽管业界专家和消费者纷纷认定区块链将是网络时代的下一次革命，区块链的大规模发展和普及仍然受到三大问题的掣肘。

2.1 可扩展性受限

目前区块链中的公链都面临的一个很尴尬的局面就是区块链共识协议，这个协议限制着区块链的发展：网络中的节点对于信息的处理；网络中的节点都要都要对数据进行同步。因此区块链现在所处理信息的能力不能超过单节点处理信息的能力。现阶段，随着节点数的增加区块链变得更加孱弱了，因为节点间的延迟会随着每个新增节点呈对数性增长。吞吐量的限制也是造成这个问题的一个很主要的方面。

2.2 算力集中引起的再中心化

EOS 的创始人与以太坊的拥护者进行过一场激烈的辩论，他们就以下问题进行过辩论和讨论，从中我们可以看出现在区块链公链所面面临的一些风险如下：

1. EOS 通过设置 21 个超级节点来进行信息的处理无疑是对公平的一种挑战，虽然 EOS 解决了部分 TPS 的问题，但是还是牺牲了很大一部分的公平性；

2. EOS 同时指出了以太坊目前也是由 7-8 个矿池所控制的，中心化程度相较于 EOS 其实是有过之而无不及的。综合事实，他的反驳也不无道理。其实权利一直都在少数人手中的这件事已经很久了，人们期望区块链可以解决这个问题，对区块链抱有很强的期望，但就目前来看，还是有一定的距离的；

目前是基于算力来分配权利，如果不考量在算法上或者在其他方面进行升级的话会成为按财富分配权利的等价形式。以为允许任何人使用和接入就是公，不考虑底层如何进行权利分配结果，这是对公的一个曲解。

2.3 缺少完善的治理措施

公链在大家的认知内认为公链就是一个自由的世界，不可以被治理，是一个法外世界。因此对于治理有一种抵抗情绪，似乎认为公链上的智能合约应当是一切人类文明成果当中的一个法外圣地，在这里要排除掉其他的干扰和影响。这已经带来一系类的问题，争议缺乏协商解决以及管理机制机制，最后只能诉诸于丛林法则，这就距离公正、公道更加远了。表面上一切由代码来定义，由一开始设定的规则来规定，暗地里却可以使出各种底线之外的手段方式来施加影响。

3 AI 公链的机遇与挑战

人工智能对于信息的感知和感应、信息的转换与传输、以及信息处理是人工智能的专长。对于人工智能区块链而言，感知和感应层是自发式分布的，而后两个层面在现阶段的其他人工智能区块链尚未实现，这也是大部分可扩展性、隐私性以及可扩展性问题的根源。展望人工智能区块链的未来，我们希望它能成为区块链的脊椎和神经系统，精确而有效地应对前文提到的区块链三大问题。

3.1 存在的机遇

通过将人工智能技术引入区块链中，受益于人工智能特有的属性：

第一，具有自学习功能。例如实现图像识别时，只在先把许多不同的图像样板和对应的应识别的结果输入人工神经网络，网络就会通过自学习功能，慢慢学会识别类似的图像。自学习功能对于预测有特别重要的意义。预期未来的人工神经网络计算机将为人类提供经济预测、市场预测、效益预测，其应用前途是很远大的。

第二，具有联想存储功能。用人工神经网络的反馈网络就可以实现这种联想。

第三，具有高速寻找优化解的能力。

表 1 归纳了人工智能各属性与区块链各方面提升的对应关系。

表 1：人工智能属性对区块链的提升

人工智能属性	对区块链的提升
学习功能	增强智能合约的优化程度
联想存储功能	自动填充和弥补智能合约的不足
具有高速寻找优化解的能力	解决现有公平性的能力
可编程性	可延展性

1） 学习功能

增强学习的特点是通过与环境的试探性交互来确定和优化动作的选择，以实现所谓的序列决策任务。在这种任务中，学习机制通过选择并执行动作，导致系统状态的变化，并有可能得到某种强化信号（立即回报），从而实现与环境的交互。强化信号就是对系统行为的一种标量化的奖惩。系统学习的目标是寻找一个合适的动作选择策略，即在任一给定的状态下选择哪种动作的方法，使产生的动作序列可获得某种最优的结果（如累计立即回报最大）。

在综合分类中，经验归纳学习、遗传算法、联接学习和增强学习均属于归纳学习，其中经验归纳学习采用符号表示方式，而遗传算法、联接学习和加强学习则采用亚符号表示方式；分析学习属于演绎学习。

实际上，类比策略可看成是归纳和演绎策略的综合。因而最基本的学习策略只有归纳和演绎。

从学习内容的角度看，采用归纳策略的学习由于是对输入进行归纳，所学习的知识显然超过原有系统知识库所能蕴涵的范围，所学结果改变了系统的知识演绎闭包，因而这种类型的学习又可称为知识级学习;而采用演绎策略的学习尽管所学的知识能提高系统的效率，但仍能被原有系统的知识库所蕴涵，即所学的知识未能改变系统的演绎闭包，因而这种类型的学习又被称为符号级学习。

2） 联想存储

因为记忆数据，已经固化到一个具有某功能的神经网络结构中。这整个被训练好的神经网络，就是记忆。人脑记忆不能离开神经网络单独存在。要移植记忆，就要重构神经网络，不像下载电脑硬盘那么简单，它是功能性的。人一次就能记住，只是一次易忘，与人工神经网络多次训练才定下来不同。到底神经元及连接如何记忆，机制还待脑计划确定。用多个神经元的权值记录一个简单信息，当然可行，这也是一种编码表达方式，但它与存储器存储简单信息是一致的，存储器存储一个简单信息，也可以是多个字节，许多个位，你将每个字节可以看作一个权值，多个字节看作多个权值，部分存储器就可以看成是一个无主动响应能力的神经元权值网络。或者进一步，部分二进制位看作一个只有激活态与抑制态的神经元权值单元，多个位一样能编码表示复杂信息，那也能解释一些生物神经网络研究。所以，存储器能某种情况下近似对应生物神经网络的记忆。

具有高速寻找优化解的能力

寻找一个复杂问题的优化解，往往需要很大的计算量，利用一个针对某问题而设计的反馈型人工神经网络，发挥计算机的高速运算能力，可能很快找到优化解。

3） 可编程性

人工智能具有基本的可编程性，把人工智能程序嵌入到用户的钱包中，每次用户同步节点的时候都会更新钱包中的人工智能，让人工智能所学习的东西相互同步通过对于人工智能的不断优化加强对于整体智能合约的把控，让人工智能迅速成长起来，代替人们做一些人们不想做的事以及人们做不到的事。

3.2 面临的挑战

人工智能带来的机遇并不意味着几种算法就可以很好地融合在区块链当中。实际上，是有不少挑战的存在，现存的人工智能无一能应用于区块链解决上述的内容。

让电脑在没有人类教师的帮助下学习。

迄今为止最成功的机器学习方式被称之为监督式学习，方式与老师指着某个东西然后告诉我们名字非常相似。每次学习一项新任务时，系统基本上都要从头学起，需要人类在很大程度上进行长时间参与。

1） 理论上的挑战

目前，深度神经网络通过仿照人类大脑皮层的网状神经结构进行建模，实际构造的模型都是简化的 MNN，主要通过邻接层之间的连接来表达非线性映射关系。如果非邻接层或同层神经元之间也建立连接，能否提高深层网络的学习和表达能力?能否从神经学找到依据?能否构造一个深层神经网络，有效处理和人类智力水平相当的机器学习问题?如何构造深层神经网络，使得每一层提取特征的物理意义比较明确?相对于主流的两段式训练算法，能否找到一种完全无监督的在线训练算法?

2） 建模上的挑战

如果允许非邻接层或同层神经元存在连接，深层神经网络模型应该如何构造?如何对深层模型进行改进，使输入数据只需简单预处理即可输入模型，同时能够直接处理多模态数据?如何构造深层模型，使其减轻对有标签数据的依赖?如何改造深层模型使其实现并行加速?

3） 工程实现上的挑战

深层神经网络训练时间过长，易于过拟合，使得模型建模及推广能力较差，如何改造深层神经网络的训练算法，使其能够快速收敛到最优解，从而大幅度减少训练时间，而且模型推广性能良好，是一个需要解决的重要问题。如何改造深层模型，使其适用于多种类型的输入数据甚至多模态混合数据?如何改造深层模型，使其能够有效地结合 GPUs 以及分布式计算等并行加速技术?

3.3 相关探索

我们提出了 gcForest（multi-Grained Cascade forest，多粒度级联森林），以及一种全新的决策树集成方法。这种方法生成一个深度树集成方法（deep forest ensemble method），使用级联结构让 gcForest 做表征学习。当输入带有高维度时，通过多粒度扫描，其表征学习能力还能得到进一步的提升，而这有望使 gcForest 能注意到上下文或结构（ contextual or structural aware）。级联的数量能够根据情况进行调节，从而使 gcForest 在只有小数据的情况下也表现出优异的性能。需要指出，gcForest 的超参数比深度神经网络少得多；更好的是 gcForest 对于超参数设定性能鲁棒性相当高，因此在大多数情况下，即使遇到不同领域的不同数据，也能使用默认设定取得很好的结果。

4 设计与构架总览

4.1 设计原则

MAI 的目标是成为人工智能公链内注重法律法规、隐私保护和可扩展性的区块链系统。为了实现这一点，并应对上述提到的一系列挑战，我们的架构设计遵循以下原则。

1） 职责分离

将所有人工智能节点直接连接成一个单独的区块链是不现实的。除了不同的智能合约应用程序需要不同的区块链属性设置之外，在单个区块中，承载过多的节点对其规模和算力的要求直线上升，对人工智能来说计算量级过重。相反，职责分离可确保每个区块链与特定组别的人工智能节点进行互动，在有需求时才与其他区块链进行互动。这与互联网的构架相似异构设备首先形成一个内部连接的组，即内部网络。较小的内部网络进而构成一个更大的内部网络，最终连接到互联网中心并相互通信。职责分离通常会创建一个均衡的系统，以最大限度地提高效率和保护隐私。

2） 奥卡姆剃刀定律

每个区块链都有不同的用途和应用，应有针对性地进行设计和优化。例如，专用于交易传递的区块链不需要受图灵完备智能合约；运行在信任区域中的区块链无需过分注重交易隐私。

3） 简化计算

如前所述，区块链生态中充满了异构系统和节点，它们的算力、存储容量和功耗各不相同。由于强节点可轻易完成弱节点能够完成的操作，因此应该以弱节点为设计目标优化区块链操作。例如，操作需以轻量级为目标，从而节省算力、存储空间和能源等相关资源。

4.2 链中链架构

MAI 是由许多分层排列的区块链组成的网络，这些区块链在保持互操作性的前提下共同运行。 在 MAI 生态中，根链(root blockchain)管理着许多独立的区块链或子链(subchain)。子链与 AI 计算出的具有相似性的智能合约相连接，这包括功能的相同性、应用场景或级别相似性。如果一条子链在遭受攻击或遇到

DAPP 错误时无法正常运行，根链完全不受影响。此外，也可以进行跨区块链交易，将价值和数据从子链转移到根链，或者通过根链从一条子链转移到另一条子链。

根区块链是任何人都可以访问的公共链，它有三个主要目标：

1.以保护隐私的方式在子链之间传递数值和数据，以实现子链间的互操作性；

2.监督子链，例如通过没收定金(bond confiscation)惩罚子链上的运营方(bonded operators)；

3.计算和确定支付，建立子链信任。

有了具体目标，根链将专注发展其可扩展性，稳固性，隐私保护功能和协调子链的能力。

子链具有成为私有区块链的可能，并且依赖于根链作为中间站与其他子链进行交互。子链需具备灵活性和延展性以适应智能合约应用的多样化需求。子链很可能由在根链上存有定金的运营商运营。在另一种方案中，系统允许运营商提名一个或多个运营商在有/无特别绑定的前提下为其运作。运营商像根链上的轻量级客户端，作为子链上的完整节点来打包新区块。

详见表 2：根链和子链属性对照表。

表 2：根链与子链属性对照表

属性	根链	子链
公开性 VS 隐私性	公开	皆可
扩展性	必要	按需
稳固性	非常必要	必要
隐私保护	必要	按需
延展性	TuringComplete 非必要	TuringComplete
即时最终性	必要	必要

4.3 根链(Root Blockchain)

根区块链与以太坊一样使用基于内外部账户的模型，原因如下：

此公链是着眼于应用层面，所以不会采取比特币的 UTXO 模型；

节省大量空间（每笔交易只有一个输入、一个输出、一个签名）；简单编码；潜在的可拓展性；轻量级客户端。

潜在使用网络分片技术：

使用网络分片技术，如果你有 10000 个节点，通过工作量证明过程，它们将被随机分为 10 组，每个组被称为一个分片。每个分片处理一组不同的数据，并得出小组内一致同意的答案。然后，各分片将这些数据的摘要报告提交给一个名为目录服务委员会的分片，由它来统筹不同分片的数据摘要，并将它们组合起来形成一个更大的数据集，称为最终区块，最终区块的数据又会被返回所有分片。

从上面的分析可以看到，分片技术是一种去中心化的、安全的链上扩容方案，具有线性的扩容能力也就是说，节点越多，得到的吞吐量就越大。

分片技术有两种类型：网络分片和状态分片，以太坊正在开发的技术是状态分片。两种技术的不同之处在于，在网络分片中，不是每个节点都必须处理每条信息，但是每个节点都必须存储网络中其它分片的信息；如果使用状态分片，每个节点都只存储它们自己处理过的信息子集，虽然这减少了每个节点的负担，但分片之间的互通会变得复杂。

4.4 子链（Subchains）

MAI 通过低层基础设置为分布式区块链应用程序开发度身定制了可发展和增补的子链架构，人工智能可根据应用需求定制相对应的子链验证模型、规格、参数和交易类型。

MAI 子链使用以账户为基础的设计模型，使其易于追踪交易状态。子链包含类似于以太坊两种类型的账户，即常规账户和合约。由人工智能算出与根链相同的共识机制产生的有效交易被添加到区块中，以达到同等的结算速度，提高跨链通讯的效率。子链使用根链通证、MAI 通证或自行定义通证。开发者在子链上定义的通证可以通过通证销售或通过公共交易平台公开发行。

子链也同时支持智能合约，并且运行在轻量级且高效的虚拟机之上。我们目前正在测评 Web Assembly（WASM）[13]，这是一种用于构建高性能网络应用程序的新兴网络标准。WASM 效率高，速度快。我们同时也在探索其他可能性。通过人工智能生成智能合约，连接到相同子链设备以两种方式共享状态。

5 内置隐私保护交易机制

比特币和以太坊本身提供的隐私仅限于使用匿名地址，两者交易细节皆是透明的。任何人都可以轻易从透明的账本了解交易金额，被转让的资产以及该交易与其他交易的关系。在这种情况下，发送方的隐私，接收者的隐私和交易细节隐私三个方面是需要解决的议题。如表 3 所示，各种加密方案可用于解决以上所提的隐私问题。

表 3：区块链的隐私保护技术

技术	隐藏发送方	隐藏接收方	隐藏账户
隐藏地址	否	是	否
佩德森承诺协议	否	否	是
环签名	是	否	否
zk-SNARKs	是	否	是

MAI 的隐私保护技术通过隐藏接收方的地址，使用环形签名（ Ring Signatures）保护寄送方的隐私和使用佩德森承诺协议（ Pedersen commitment）来隐藏交易金额，进行了以下创新和改进：

使用 AI 推荐的隐藏地址让接收方不用计算整个区块链来确认交易；

优化环签名，使其体积更简洁并更具有可信赖的水平。

5.1 以可传递支付码隐藏交易接收方

隐藏地址技术源于 Cryptonote 协议[9]，它利用半轮（half round）Diffie-Hellman 密钥交换协议解决接收方的接收问题。这个技术的局限性在于目前接收方必须要扫描网络中的所有交易，或是要依靠可信的完整节点（在一定程

度上泄露隐私）的帮助以完成接收。支付代码的设计旨在解决隐藏地址的上述缺点，但仍有泄露交易隐私的缺点。

5.2 保密交易机制

本质上，区块链交易只是一个元组（{ pkin， i}，{ pkout， j}，{ vi， j}），其中{ pkin， i}是输入地址，{ pkout， j}是输出地址，{ vi， j}是输入和输出地址之间的交易金额。由于比特币交易是以明文形式存储在公共账本中，因此引发了很多安全和隐私问题。保密交易的目标是使只有交易的发送方和接收方能够知道{vi，j}值，并没有其他人知道交易双方以及{vi，j}值。此外，保密交易可以允许网络实体验证每个交易的有效性，但是交易的实际金额不会被泄露。区块链上的保密交易的实现需要许多先进的密码技术。

5.3 通过 Bulletproofs 模型证明交易金额范围

Bulletproofs 模型是为了替代佩德森承诺协议（Pedersen commitment）而被提出的。这是一种新的非互动零知识证明协议模型（ noninteractive zero-knowledge proof protocol），它仅需非常短小的证明签文（ proofs）并且不需要仰赖可信任的节点，因此可以在没有额外计算量的条件下，将范围证明（ range proof）的大小从线性减小到次线性，并进一步减少交易体量。由于 Bulletproofs 模型很好地符合 MAI 的设计原则，我们将把防弹协议（Bulletproofs）整合到 MAI 中。

6 PAI 高速共识机制

6.1 技术背景

工作量证明算法（PoW）是实现大多数区块链（包括比特币和以太坊）全球共识的支柱。工作量证明算法（PoW）使在计算上很难构建一个有效的区块并将其附加到区块链上。区块链变得越长，就越难扭转区块链以前记录的任何交易。攻击者必须拥有基于 PoW 的区块链网络整个计算能力的 51%，才能操纵该区块链。

虽然 PoW 为大型分布式区块链的全球共识提供了一个优雅的解决方案，但它也有一些固有的局限。维持共识整体计算成本很高，相当于 51%的攻击成本。这意味着即使大部分区块链参与者都是诚实的，他们仍然需要使用大量的电力来维护区块链，这不适合倾向于快捷的网络环境。另外，在单个设备级别上，使用 PoW 通常会花费大量的 GPU 周期和内存空间，造成不必要的系统浪费。

6.2 共识机制：AI 随机授权股权证明机制

为了设计和开发 MAI 的快速高效的共识机制，我们计划采用以下技术。

6.2.1 股权证明机制

为了避免以上提到的因 PoW 所带来的问题，这里有一个好的方案是权益证明算法（PoS）作为区块链达成共识的有效替代方案。PoS 的原理思想是随机选择一组节点对下一个区块投票，并根据它们持有以太坊量的多少（即权益）对他们的投票进行加权。如果某些节点行为不规范，系统可能会没收其链上的以太坊。藉由这种方式，不用通过高计算成本的 PoW，区块链依旧可以更高效地运行，除此之外可以实现链上的经济稳定性：参与者拥有的权益越多，其维护账本共识机制的动机就越大，其节点行为不当的可能性也就越低。 现在已经有一些根据权益证明算法（PoS）研发的设计和使用，例如 Tendermint[11]，已被许多应用程序采用[12]。

6.2.2 授权股权证明机制

授权股权证明（DPoS）改进了 PoS 的思想，即授权股权证明允许参与者委托一些代表来代表他们在网络中的部分股权。例如，Alice 可以向网络发送消息，

委托 Bob 代表她的股权并代表她投票。DPoS 为我们的 AI 区块链应用提供了以下优势：

小股权参与者可以将他们的股权集中起来，让他们有更高的机会共同参与区块链中的投票，然后分享奖励。

资源受限的节点可以委任代表，因此并非所有节点都需要保持联机才能达成共识。

代表可以是具有强大电力供应和网络条件的节点，也可以动态随机选择，因此我们在链上将获得更高的整体可用性，使网络达成共识。

使用 DPoS 的加密货币包括 EOS[3]和 Lisk[6]。

6.2.3 拜占庭容错算法

实用的拜占庭容错算法（PBFT）是 Castro 和 Liskov 在 1999 年提出的一种有效的抗攻击算法，用于在分布式异步网络中达成协议。我们前期计划使用 PBFT 作为我们 DPoS 共识机制的基础投票算法，因为它是一种简洁而且研究得非常好的算法，它提供了迅速的结算性，这对于构建高吞吐量 TPS 与可扩展的区块链至关重要。 正如 Castro 和 Liskov 的原始论文所证明的那样，只要低于三分之一的网络节点出现故障或恶意行为，PBFT 就可以为链提供可用性和安全性； 同时，PBFT 的网络成本非常低，仅为未复制网络系统成本的 3%。

基于 PBFT 的加密货币包括 Stellar[10]和 Zilliaq[14]。

6.2.4 基于 AI 选择的共识机制

如上所述，为了效率考虑，当要提出或选举新块时，系统将随机选择一小组节点。这种通过人工智能选择算法的设计非常重要，因为它影响了整个共识过程的公平性和安全性以及合法性。

6.3 轻量级用户 AI 定期检查点的创建

在区块链网络中，我们预计很多设备都是轻度使用的客户端，也就是参与者不会在本地记录完整的交易历史。 以比特币为例，目前存储完整比特币区块链需要的空间已经超过 100GB[1]，因此许多用户可能无法下载完整区块链。

为了缓解这一性能问题，以太坊的发明者 Vitalik 建议在区块链上创建定期检查点：epochs[2]，例如每隔 50 个区块设置一个 epochs。这样做的好处是每

个检查点都可以基于前一个检查点进行验证，运用这个方式轻量级客户就可以更快地同步整个区块链。

7 MAI 网络中的通证机制

本地数字通证（MAI TOKEN）是 MAI 网络生态的重要组成部分，它被设计成完全服务于 MAI 网络。在 MAI 主网启动之前，通证是以兼容 ERC20 标准部署于以太坊网络上的，待到主网发布后，通证会完全迁移至 MAI 主网上。

MAI TOKEN 通证作为一种虚拟加密燃料被用于在 MAI 网络上实现某些功能（比如执行转账和运行分布式应用），通过消耗 MAI TOKEN 通证激励社区参与者，维持 MAI 网络上的生态。在 MAI 网络上执行转账和运行分布式应用以及验证添加区块/信息需要占用很多的计算资源，因此我们需要激励这些提供服务/资源的网络参与者（即挖矿）以保持 MAI 网络的完整， MAI TOKEN 通证还被作为一种汇率单位用于支付占用计算资源所产生的费用。

MAI TOKEN 通证是 MAI 网络中不可或缺的一部分，如果没有 MAI TOKEN 通证，那么就没有一种汇率单位去支付这些费用，从而使 MAI 的生态系统无法持续。

MAI TOKEN 通证作为一种支付单位具有不可逆的功能，将被用于 MAI 网络参与者的转账交易中。引入 MAI TOKEN 通证的目的是为生态系统中的网络参与者提供一个便捷安全的支付结算模式。MAI TOKEN 通证并不代表任何股权、参与权、投票权、职位、以及 MAI 基金会的收益。基金会及其分支机构，或其他公司、企事业单位不会给通证持有者承诺任何利润以及投资回报，也不会在新加坡或任何相关管辖区内构成有价证券。MAI TOKEN 通证只能在 MAI 网络上使用，并且通证持有者没有被授予任何明示或暗示的权利，除了正确使用 MAI TOKEN 通证以促进 MAI 网络和谐发展。

关于 MAI TOKEN 通证，需特别注意：

（a）基金会及其任何附属机构没有对通证进行退款或者变现（或者替换成等值的其他虚拟货）或者其他任何支付方式的义务；

（ b）通证不会使通证持有者获得基金会（及其任何附属机构）任何形式的权利、收益或资产，包括但不限于基金会有权获得的未来收益，股票，股权或股份，证券，任何投票、分配、赎回、清算、产权（包括所有形式的知识产权），或者与其他金融、法律同等的权利，或者与 MAI 网络参与者、基金会、服务供应商有关的任何知识产权。

（c）MAI TOKEN 通证并不是一种货币（包括电子货币），有价证券，商品，债券，债务或其他任何一种金融工具或投资；

（d）MAI TOKEN 通证不是基金会或其任何附属机构的贷款，也并不是基金会或其任何附属机构所欠债务，且没有任何预期的利润；

（e）基金会及其任何附属机构不会授予 MAI TOKEN 通证持有者任何权利或者收益。

8 MAI 驱动的生态系统

一个区块链智能合约自由搭建的基础公链 ，基于 MAI 公链将具有无限的可扩展性。

案例 1. 防伪区块链合约

目前，国内防伪企业约有 3000 家。绝大多数产品采用的是低技术含量的防伪手段，很容易被复制，而传统的数字防伪成本极高，防伪麻烦难推广，特别是对于低值、高消费的产品。

通过 MAI 防伪，品牌商可以根据智能合约模板或自身的需求快速创建智能合约，生成一个新的基于 MAI 系统的区块链系统，并生成仅使用防伪和点数的品牌令牌。这个令牌是品牌管理人员使用的，需要在每次执行合同时使用。品牌所有者通过生成数字令牌来完成防伪工作。每个用户可以使用 MAI DAPP 对基于 MAI 系统，生成令牌的品牌商家的产品执行一键扫描码防伪。此代码只能扫描一次。扫描代码将保存在区块链中，不能更改。因此，只有能领取数字令牌的商品才是真正的商品，防伪技术不可篡改，不可复制，真正做到了低成本高效防伪的目的。

案例 2. 飞机晚点保险合约

传统的保险行业三分之一的钱用于销售人员，三分之一的钱用于管理和运营支出，经营成本过高且效率低下。

现在通过 MAI 公链我们以航空晚点为例，创建一个保险的智能合约，乘客只要通过智能合约指定地址下单，当系统同步信息航班出现合约中规定的晚点条约一旦达成，合约系统会自动履行合约付款给乘客。省去了人工售险运行成本，提升了保险的处理效率，达到降本高效运营的目的。

案例 3. 彩票智能合约

现有的模式是，彩票通过实体门店销售，或者网络销售，1.彩民对中奖诚信有些质疑；2.你是有听过某某人中了大奖因遗忘错过领奖机会；3.是大额现场领奖隐私得不到保护。

采用 MAI 公链创建售彩智能合约，彩民通过彩票智能合约向合约发布方购彩，当彩票中奖时系统自动将彩金支付给中奖彩民，高效、透明、无遗漏，彩民隐私得到保护。

案例 4.　无人驾驶汽车系统

比如行使在高速上无人驾驶汽车，如果发出指令给前车要求他们保持一定的安全距离，不要紧急刹车，注意保存车距，有可能会出现前车没有收到信息或者延迟的情况，会导致安全事故。

采用 MAI 公链创建无人驾驶智能合约系统，通过智能合约一致性记账机制，智能合约汽车之间会同时执行相同的命令，规避信息不同步的风险发生，智能合约技术的广泛应用，将提升无人驾驶领域的安全系数。

MAI 公链就像是手机安卓系统一样，开发者可以任意基于安卓系统开发符合法规机制的 DAPP，均可在安卓系统上运行。所以 MAI 公链是一个可以无限延伸扩展的智能合约开发创建公链，可以广泛应用于：共享经济领域，智能家居领域，智能制造领域，金融领域，旅游领域，信息化数据领域，物联网智能领域，征信智能管理领域，食品安全，医疗安全领域，智能电商领域，产品溯源，产品防伪领域，智能导航，无人驾驶领域等等几乎覆盖了所有领域，人工智能与区块链的强强结合是大势所趋。

物联网时代智能产品之间的互通互联而产生的数据信息与人身安全一样重要，而个人信息包括手机号、照片、视频等被泄漏及公开的恶性事件屡屡发生，

这些数据安全事故已经给我们敲响了警钟。区块链能够保证物联网能够安全、有灵活的可拓展性、高效。高效随之带来的是成本的降低。鉴于此，区块链的技术可以为未来物联网的发展起到极大的推动作用。

MAI 公链通过对节点赋予人工智能后，人工智能对公链上新增的节点智能合约进行识别合法性与合理性，对不符合人性及非法要求的智能合约，不予启用，同时会对系统现有适合的智能合约进行推荐。对新增先进的智能合约，人工智能会自我驯化学习，提升对智能合约思考判断推荐能力，从而让人工智能实现自我学习驯化进化的能力，节点将通过不断的驯化学习，让 MAI 公链系统成长的越来越强大，越来越人性化，MAI 未来将大力推动防伪、共享经济领域、物联网智能科技、征信领域、金融保险领域、医疗安全、产品溯源、智能合约领域的快速发展，在未来商业化运营中 MAI 公链将体现它非凡的价值和实力。

9 潜在研究方向

MAI 团队目前致力于如下研究方向：

面向隐私保护的计算：

这里列出在这一技术方向上我们正在积极探索的几个领域：

区块链上一组节点如何进行面向隐私保护的计算

在合约内容加密的情况下由虚拟机执行面向隐私保护的智能合约。尽管全同态加密[8]以及不可区分的代码混淆技术[4]在理论上能够实现面向隐私保护的智能合约，最近提出的基于零知识证明的方案例如 Hawk[5]为面向隐私保护的智能合约在实际系统中落地提供了解决方案。

进一步减少 MAI 的区块链隐私保护技术所需的算量与存储需求。

针对 MAI 目前使用的隐私保护技术研究后量子版本，例如后量子环签名技术

1) 状态裁剪与转移

因为许多设备处理信息的能力有限，我们正在评估不同的方法来安全地裁剪存储在子链上的信息，以减少存储内容。对块和交易信息的压缩并非难事。此外，以一种高效和隐私保护的方式将信息从子链转移到主链（因为后者在存储方面更强）上也是一个有趣的话题。

2) 区块链治理与自我修正

虽然 MAI 区块链为维持其帐本共识的支持者们提供奖励，但到目前为止还没有一种链上机制可以精确修正治理协议的规则并对协议的发展提供奖励。我们将进一步研究区块链治理与自我修正机制以解决此问题。

3) 树状架构的区块链

目前 MAI 系统为两层式区块链架构，在将来它可以利用 Plasma 和 Cosms 的技术扩展成树状结构。我们计划进一步评估现有方案旨在将 MAI 打造成为可以支持复杂层次化结构的区块链项目。

结论

在白皮书中，我们介绍了一种可扩展的、注重隐私保护并具有延展性的 AI 区块链，并且介绍了它的架构以及如下核心技术：

1) 运用链中链基础架构最优的优化其扩展性和隐私性;
2) 运用轻量级秘密地址的使用、环签名方式（无需可信启动）以及避弹衣机制保护交易隐私；
3) 运用可证明或者验证的随机函数以及权益证明，实现高速共识机制其中最为重要的前提就是 AI 的应用；
4) 构建灵活的轻量级 MAI 系统架构。

特别鸣谢

在此感谢在此白皮书撰写过程中给予我们及时反馈并提出宝贵意见的各位导师、顾问，以及许多致力于 AI、密码学、虚拟货币领域的专家和伙伴。

参考目录

Blockchain Size.https://blockchain.info/charts/blocks-size.

VitalikButerin.Light Clients and Proof of Stake. https: //bloq. ethereum. org/2015/01/10/light-clients-proof-stake/.

EOS.https://eos.io/.

Sanjam Garg et al.Candidate indistinguishability obfuscation and functional encryption for all circuits.In:SIAM Journal on Computing45.3(2016)，pp.882-929.

Ahmed Kosba et al.Hawk:The blockchain model of cryptography and priMAIy-preserving smart contracts.In:Security and PriMAIy(SP)，2016 IEEE Sym-posium on.IEEE.2016，pp.839-858.

Lisk.https://lisk.io/.

Raiden Network，https://raiden.network/.

Ronald L Rivest，Len Adleman，and Michael L Dertouzos.On data banks and priMAIy homomorphisms.In:Foundations of secure computation4.11(1978)，pp.169-180.

Nicolas van Saberhagen.Cryptonotev2.0.2013.

Stellar， https://www.stellar.org/.

Tendermint.https://tendermint.com/.

Tendermint Ecosystem.https://tendermint.readthedocs.io/en/master/ecosystem.html.

WebAssembly.http://webassembly.org/.

Zilliqa.https://vwvw.zilliqa.com/.

MAI 技术框架

白皮书技术补充

作者：MAI 基金会

完成日期：2018 年 12 月 17 日

1. MAI 的定义

在传统的区块链世界中，系统会在一段时间内（可能是十分钟，也可能是一秒钟），选出其中记账最快最好的一个节点，让他在这段时间里记账。他会把这段时间内数据的变化记录在一个数据区块中。在记完账以后，该节点就会把这一页的账本发给其他节点。其他节点会核实这一页账本是否无误，如果没有问题就放入到自己的账本中。而在这里，比特币是人为设定的区块产生的时间，以太坊是设置了每个区块的 GAS 值，当 GAS 值满了的时候一个区块就打包成功，随之到网络上公布。在这里以太坊前期使用的也是 POW 的方式，后期才采用 POS 的机制。在 MAI 中，我们重新定义和制定了一套规则，结合 POW、POS 以及我们所定义的 POD 来进行的一套共识机制来让整个网络的记账速度提高，而这一切的控制和分配都是通过 AI 来进行的。这里需要特别强调的是，我们还采用了分片式技术来保证用户的数据入链速率大幅度提升。而 MAI 则一开始就定义了不止是转账和用户消费信息的数据进行实时的打包，而且我们不定义区块的大小。我们认为最佳区块大小必须是动态的，适应网络交易的需求，尽可能保持它的最佳状态。

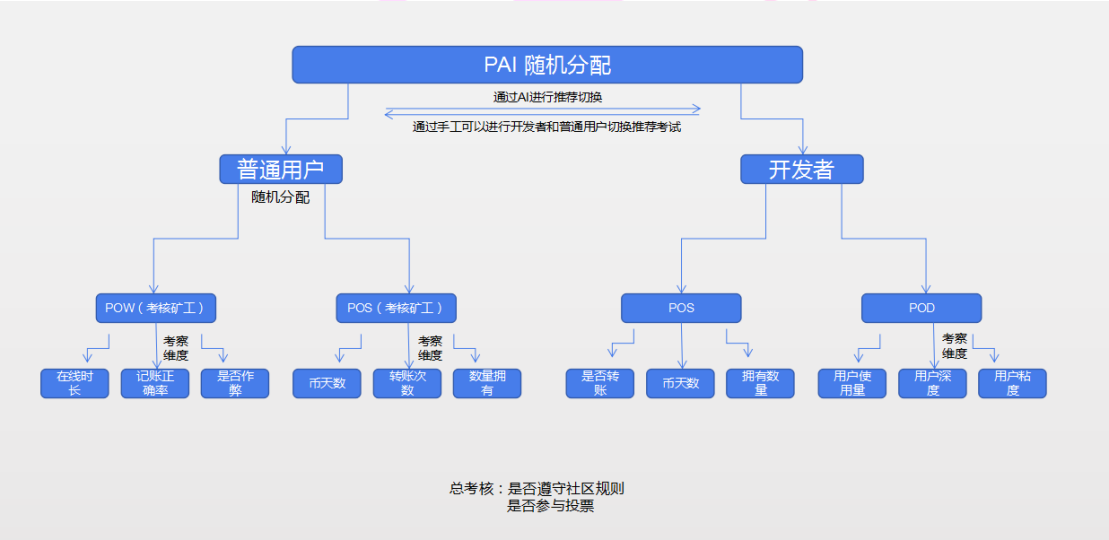
2. 技术体系

2.1 共识机制

2.1.1 我们的共识机制是什么？

我们采用 PAI 共识机制，但是在这里的 PAI 共识机制包含了 POW、POS 以及 POD。权益证明（POS）机制是一种 SHA256 的替代方法，从根本上解决了工作量计算浪费的问题，他不要求证明者完成一定数量的计算工作，而是要求证明者对某些数量的钱展示所有权，通过每一笔交易摧毁的币天数来实现，币天数代表一个特定的币距离最后一次在网络上交易的时间。在既定的时间内，只存在有限的币天数，他们在那些长期持有大量货币结余的人手里持续增加。所以币天数可被视为在网络中权益的代表。简单来说我们就是把 POW 由算力决定记账权变成由持有币数以及持有的时间来决定记账权。在 POW 中，是按照算力占有总算力的百分

比从而决定你获得本次记账权的概率。但是在我们这个体系中的 POW 是检验和考察普通矿工的在线时长，记账正确率以及矿工有没有“作弊”，通过这几个维度来确定矿工有没有可信度。如果矿工通过了“考核”那么他就进入到下一个层面通过 POS 来进行的分配记账。这里有一个核心的思路，如果在 POS 机制里面矿工没有做到合理的记账我们会采用末尾淘汰机制，如果矿工在 pos 机制里面没有遵守社区规则并且表现很差，我们将会让这 10%的矿工重回 POW 进行“考核”。这里我就要阐述我们的另一个共识机制 POD 共识机制。POD 共识机制就是要解决开发者奖励的问题。这里我来阐述我们的解决方案。POD 采用的是根据开发者维度其中包括：1. 使用频率 2. 使用时长 3. 使用人数 4. 用户活跃程度 5. 用户深度 6. 智能合约被调用的次数，这六个开发者维度来进行分析；除此之外我们还会使用 POS 共识机制来考核开发者。这里来补充一点，我们会使用 AI 来做一些关于智能合约的分析，分别是：1. 完整性 2. 潜在漏洞指数 3. 人性 4. 可拓展性，从这四个方面给出综合分析来解决现在频频发生的智能合约问题，从而提高安全性，避免因为智能合约漏洞所导致的一系列问题。



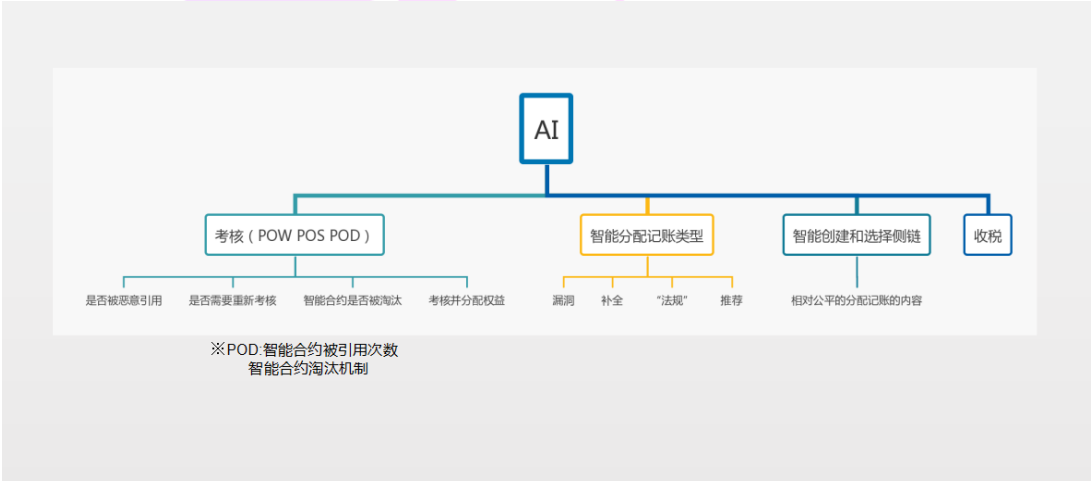
2.1.2 PAI 的特性和功能是什么？

PAI 所采用的是 AI 进行的分配和管理，这里只是 AI 的一部分使用场景，接下来的章节我会讲解哪些部分使用了 AI。当有需要入链的数据进来的时候我们先通过 AI 的方式进行分配，在这里我们分为两个属性，一种就是普通矿工，另外一种是开发者矿工。首先我们对于普通矿工进行阐述：所有的普通矿工都需要

先通过 POW 的考试，考试合格以后才可以进入到 POS。进入到 POS 以后我们会通过 1. 币天数 2. 转账次数 3. 拥有的数量来进行对于矿工的审核和评定。符合要求的就会有多的记账权。接下来我们需要讨论的就是开发者矿工，开发者矿工有两点核心的共识机制，一点是 POS，另外一点是 POD 共识机制。POS 的共识机制的考察内容和普通矿工是一致的。

但是这里要着重讲的是 POD 共识机制。这里我们需要通过几个维度进行考察开发者的智能合约或者 DAPP 的使用情况；POD 采用的是根据开发者维度其中包括：1. 使用频率 2. 使用时长 3. 使用人数 4. 用户活跃程度 5. 用户深度 6. 智能合约被调用的次数，这六个开发者维度来进行分析。这几种维度会综合权益比进行调控。这就是我们所提出来的 POD 共识机制。

这里要进行补充的是开发者模式和普通矿工模式可以进行切换，当一个开发者获得收益的和记账权的概率还不如普通矿工的时候系统会提示他，让他进入到普通矿工模式。而且我们也可以通过手动的模式来进行普通矿工和开发者矿工的切换。对于开发者来讲，AI 会通过学习的模型给予开发者所开发的智能合约一定的建议，同时把好的智能合约收录到库中，当智能合约被引用的次数较高的情况下同样也会是一个很高的权重对于开发者矿工来讲。对于普通矿工来讲，你也很好很快的可以拥有自己的智能合约，体验一把当开发者的快感。



2.2 TPS 的相关问题

2.2.1 区块链中 TPS 是什么？

系统中系统的吞吐量决定了系统每单位时间成功传输数据的次数。应用在区块链中，TPS 指的是每秒系统处理交易的数量。假如 TPS 每秒并发太低，很容易造成网络拥堵严重，从而使得区块链在高价值的高并发业务领域无法落地。比如，由于 TPS 每秒并发太低，比特币和以太坊都存在交易费用高、确认时间长、扩展性差的问题，比特币社区因此产生分裂，硬分叉成为常态。

那么，区块是如何产生的呢

节点运行共识：节点实时监听系统，同时共识算法开始运行，比如 PoW 共识算法是根据区块头和 nonce 进行哈希运算。 广播并验证的时间：当一个节点完成计算后，提交给网络中的 peers，验证后加入到区块链上，继续广播，直到网络中的节点均达成共识。

x 个 confirmation 之后被认为是安全的：为了防止区块链受到攻击，通常可以在几次甚至几十次确认之后使用转移的令牌，例如，一些交换需要 12 次确认。这里 x 的数量，确认是来自包含目标事物的块的数量，并且有 x 个块连续地链接到区块链。x 越大，区块链越长，攻破就越难。

这三步是有前后次序的，不能并发。实际上，区块生成的时间只是第一步和第二步。

2.2.2 我们对 TPS 问题的相关解决方案

1）分片是数据库中的常用方法，即并行计算。区块链本质上是一种存储数据的方式，因此使用数据库优化是一个好主意。Internet 数据库的碎片意味着数据库（可以想象为 excel 表单）被切割成多个部分。每当您运行一些基本操作（如搜索）时，您都可以操作多个链并发执行，从而链接搜索。树查找中的时间复杂度从 o（n）减少到 o（logn）。

假设网络中有1000个节点，则网络自动分为10个分量片（每片100个节点）。各分片能同时进行交易验证。如果单组件平板电脑可以在一定时间内验证100笔交易，那么10组件平板电脑可以同时验证1000笔交易。

具体一点，我们所采用的分片技术是通过PAI共识机制把节点进行合理的分配，让1000个节点分为每100个节点一个分片，每次进行分配记账的时候让每个分片的100个节点选出1个节点进行记账，让其他节点进行验算，当验算成功时这个分片内的节点进行同步。同时这个节点把同步的信息发送给主链上的数据同步节点，让主链上的同步节点把信息进行同步和记录。这里的主链上的同步节点不进行任何的挖矿操作，只负责同步每个分片发送过来的信息，确保节点信息的同步性。这种设计模型使用了“三权分立”的设计模型，让信息的分配、处理以及同步变得公平和有效。区块浏览器所查的所有信息都来自于同步节点，同步节点的收益来自于社区的反哺。

2）将所有人工智能节点直接连接成一个单独的区块链是不现实的。除了不同的智能合约应用程序需要不同的区块链属性设置之外，在单个区块中，承载过多的节点对其规模和算力的要求直线上升，对人工智能来说计算量级过重。相反，职责分离可确保每个区块链与特定组别的人工智能节点进行互动，在有需求时才与其他区块链进行互动。这与互联网的构架相似，异构设备首先形成一个内部连接的组，即内部网络。较小的内部网络进而构成一个更大的内部网络，最终连接到互联网中心并相互通信。职责分离通常会创建一个均衡的系统，最大限度地提高效率和保护隐私。

3）如前文所述，区块链生态中充满了异构系统和节点，它们的算力、存储容量和功耗各不相同。由于强节点可轻易完成弱节点能够完成的操作，因此应该以弱节点为设计目标优化区块链操作。例如，操作需以轻量级为目标，从而节省算力、存储空间和能源等相关资源。

4）MAI是由许多分层排列的区块链组成的网络，这些区块链在保持互操作性的前提下共同运行。 在MAI生态中，主链(root blockchain)管理着许多独立的区块链或侧链(subchain)。侧链与AI计算出的具有相似性的智能合约相连接，这包括功能的相同性、应用场景或级别相似性。如果一条侧链在遭受攻击或遇到DAPP错误时无法正常运行，主链完全不受影响。此外，也可以进行跨区块链交

易，将价值和数据从侧链转移到主链，或者通过主链从一条侧链转移到另一条侧链。

主区块链是任何人都可以访问的公共链，它有三个主要目标：

1.以保护隐私的方式在侧链之间传递数值和数据，以实现侧链间的互操作性；

2.监督侧链，例如通过没收定金(bond confiscation)惩罚侧链上的运营方(bonded operators)；

3.计算和确定支付，建立侧链信任。

有了具体目标，主链将专注发展其可扩展性，稳固性，隐私保护功能和协调侧链的能力。

侧链具有成为私有区块链的可能，并且依赖于主链作为中间站与其他侧链进行交互。侧链需具备灵活性和延展性以适应智能合约应用的多样化需求。侧链很可能由在主链上存有定金的运营商运营。在另一种方案中，系统允许运营商提名一个或多个运营商在有/无特别绑定的前提下为其运作。运营商像主链上的轻量级客户端，作为侧链上的完整节点来打包新区块。

2.3 挖矿机制

在说挖矿机制以前要先介绍一下费用机制和区块大小机制。MAI 在费用设计上不同于其他虚拟货币的预设式设计模型。MAI 采用的是更加友好和高效的——动态区块，这样就会产生一个动态的费用。所谓动态区块或者是动态费用就是指，MAI 的费用是根据网络的使用情况（区块奖励和区块大小）来进行动态调整的，并且费用会随着使用者增多而逐渐减少。具体的动态费用计算公式如下：

费用 = (F/F0) * (S0/S) * P0

F：区块奖励

F0：参考区块奖励（设置为 10 个 MAI）

S：区块大小上限

S0：最小区块大小上限（300kb）

P0：0.002 个 MAI

我们会根据 MAI 的发行曲线进行逐步的减少我们的区块奖励，这就造成我们公式中的第一项会逐渐减小。同时，随着使用人数的增多，MAI 的区块大小上限会逐步增加，导致公式中的第二项会逐渐减小。如此一来，随着时间增加，使用人数的增加，MAI 的交易费用会稳步下降。MAI 这种动态费用设计，就是为了避免比特币和以太坊在使用人数急剧增加，币值急剧上升情况下交易费用也急剧上升。在良性发展的情况下，MAI 费用设计不但保证了矿工可以得到应有的收益，同时保证了用户的交易费用不会被矿工所绑架。也保证了区块的大小最符合效率和费用的平衡，通过这样的方式让整个生态网络趋于平衡和稳定的发展。

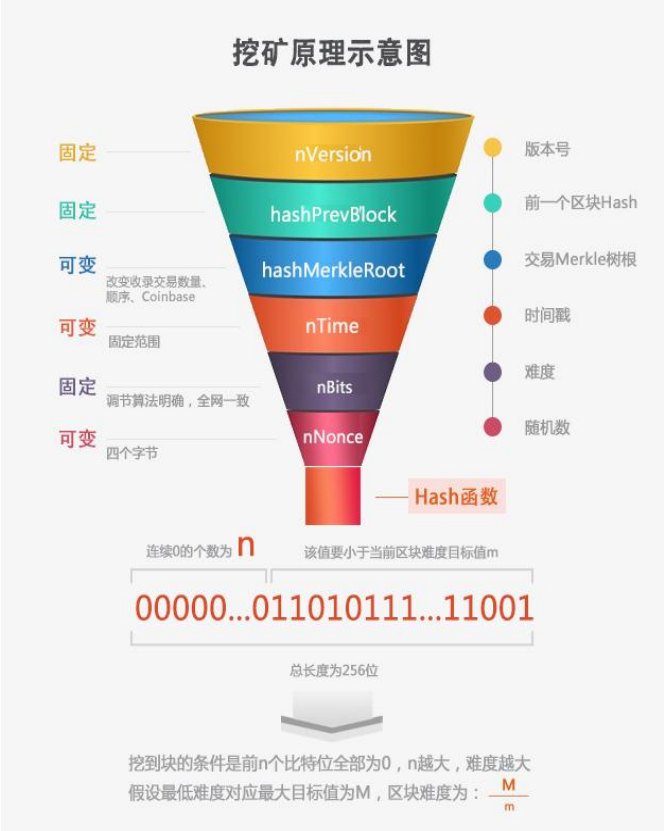
2.3.1 挖矿概率比

我们通过 PAI 共识机制可以为普通矿工和开发者做一个预设的获得记账权的概率比。这也是 PAI 共识机制的一个创新。对于区分开发者矿工和普通矿工来讲是很好区分的，每一个钱包地址都是一个唯一的 HASH 值，这个 HASH 值所生成的智能合约都会和他的 HASH 值关联，智能合约的使用情况跟智能合约有关联，这就形成了一条关联的链条。而普通用户是没有关联的智能合约的。根据这个维度我们进行相关的区分。MAI 把挖矿的对比做了五个等级。

我们就可以看到不同的综合评分所对应的不同的记账权概率，这也是对开发者友好的一种行为。

2.3.2 挖矿原理

我们的挖矿原理是运用的融合式挖矿，挖矿过程可以总结为几个过程，如图所示：



1. 根据钱包地址验证身份，判断用户是开发者矿工还是普通矿工然后进行打包交易，检索待确认交易内存池，选择包含进区块的交易。矿工可以任意选择，但是不能无限选择。对于矿工来说，最合理的策略是首先根据手续费对待确认交易集进行排序，然后由高到低尽量纳入最多的交易。

2. 构造 Coinbase，确定了包含进区块的交易集后，就可以统计本区块手续费总额，结合产出规则，矿工可以计算自己本区块的收益。

3. 构造 hashMerkleRoot，对所有交易构造 Merkle 数。

4. 填充其他字段，获得完整区块头。

5. Hash 运算，对区块头进行 SHA256D 运算。

6. 验证结果，如果符合难度，则广播到全网，挖下一个块;不符合难度则根据一定策略改变以上某个字段后再进行 Hash 运算并验证。

合格的区块条件如下：

SHA256D(Blockherder) < F(nMAIs)

其中，SHA256D(Blockherder)就是挖矿结果，F(nMAIs)是难度对应的目标值，两者都是 256 位，都当成大整数处理，直接对比大小以判断是否符合难度要求。

为了节约区块链存储空间，将 256 位的目标值通过一定变换无损压缩保存在 32 位的 nMAIs 字段里。具体变换方法为拆分利用 nMAIs 的 4 个字节，第 1 个字节代表右移的位数，用 V1 表示，后 3 个字节记录值，用 V3 表示，则有：

此外难度有最低限制，也就是说 有个最大值，最低难度取值 nMAIs=0x1d00ffff，对应的最大目标值为：

0x00000000FFFF0000000000000000000000000000000000000000000000000000

2.4 友好的挖矿机制

为了让普通的用户可以参与到整个 MAI 生态环境中来，我们对于挖矿客户端做了一定的改进和补充。我们采用了一些现在很成熟的技术来保证普通矿工在电脑闲时的挖矿和在使用电脑时的挖矿都不会造成使用电脑时的感受不佳的情况，智能分配电脑和网络资源，让挖矿这件事对普通矿工更加友好。这里我们采用了网络分配技术、内存智能分配技术和 CPU 智能分配技术，他们分别是：

1）QoS（质量服务）是一项非常复杂的技术，但应用广泛。可实现的主要功能包括流量监管（对进入接口的，超出限制速率的报文进行丢弃）、流量整形（对接口发送的，超出限制速率的报文先进行缓存，等待流量不超出速率时发送）、拥塞避免（在出现网络拥塞时对符合条件的报文进行丢弃）、拥塞管理（在出现网络拥塞时采用队列调度的方法对符合条件的队列中的报文优先发送）、流策略（可根据不同的流分类实现诸如禁止/允许通过，重标记报文优先级、重标记报文 VLAN 标签、重定向流量、过滤报文、流量镜像、启用流量统计功能等行为）。QoS（Quality ofService，服务质量）是一种可以为不同类型业务流提供差分（即“不同”）服务等级的技术。通过 QoS 可以给那些对带宽、时延、时延抖动、丢包率等敏感的业务流提供更加优先的服务等级，使业务能满足用户正常、高性能使用的需求。

2）malloc 的全称是 memory allocation，中文叫动态内存分配，用于申请一块连续的指定大小的内存块区域以 void*类型返回分配的内存区域地址，当无法知道内存具体位置的时候，想要绑定真正的内存空间，就需要用到动态的分配内存。

3）智能线程分配技术。①detectCores() 此函数能够检测出计算机或集群所有能够使用的核数。②makeCluster(x) 此函数能创建一个使用的核集 cls，x 为你想创建的核集的数量 ，不能大于函数 detectCores 所检测到的核的数量。③clusterExport(cls,x) 此函数是将变量 x 传给 cls 核集中的所有核的 cache ④clusterApply() 方法的使用雷同于 apply 函数，只不过多了个 cls 参数来指引核集罢了，是真正执行并行计算的主要函数，静态分配任务块 ⑤ clusterApplyLB() 功能与 clusterApply 相同，动态分配任务块。

2.5 收税体系

为了保证为生态环境所付出的每个普通矿工的权益，我们采用智能收税的方式来平衡整个生态网络。针对于大节点和一些大的矿场收取较高比重的税金来补贴一些符合规则和勤恳的普通矿工。我们暂时的税收体系参照的是美国的税收体制，目前还在研究更好的税收体制来完善我们的生态环境。税收的具体情况以及税金的用途将在下一版白皮书中进行补充。

2.6 安全体系

理论上区块链去中心化和所有节点同步记账的特点足以保证网络的安全，但是智能合约、挖矿记账的算力却是认为操控的，如果不加以管控，则可能造成野蛮式的发展，但是任何一项技术走向成熟的过程中，都会经历这样一个从野蛮的成长期逐步走向成熟的阶段，如果不加以管理，那么随时都可能形成一颗定时炸弹，一旦被引爆，后果将不堪设想。比如，一个矿场无限制的扩大，那么去中心化的网络将会再次被中心化从而引发信息被篡改的风险，再者，假如开发者在发布一些智能合约的时候植入一些病毒算法，那么一旦上链，可能会自动执行一些不安全的操作让使用该智能合约的用户蒙受损失。

而 MAI 公链则将安全体系交给人工智能来进行管理，通过中心化的 AI 大数据分析，从根本性入手，在发布智能合约时，对智能合约的代码进行严格审核过滤，如果检测到非法代码则进行修复或拒绝发布。而共识机制部分，PAI 将会通过多维度的算法对节点记账的权重进行综合评估，如此一来算力并不是唯一的维度，从而全方位的对 MAI 公链进行体系化的管理。

3. MAI 解决了什么现实问题

3.1 解决了公链的什么问题

3.1.1 吞吐量带来的瓶颈问题

目前区块链中的公链都面临的一个很尴尬的局面就是区块链共识协议，这个协议限制着区块链的发展：网络中的节点对于信息的处理；网络中的节点都要对数据进行同步。因此区块链现在所处理信息的能力不能超过单节点处理信息的能力。现阶段，随着节点数的增加区块链变得更加孱弱了，因为节点间的延迟会随着每个新增节点呈对数性增长。吞吐量的限制也是造成这个问题的一个很主要的方面，通过我们独创的 PAI 共识方式，能并行进行记账和通知，这样一来区块链网络的并发瓶颈问题就不复存在，DAPP 的普及化和易开发性会得到很好的解决。

3.1.2 算力集中引起的再中心化

EOS 的创始人与以太坊的拥护者进行过一场激烈的辩论，他们就以下问题进行过辩论和讨论，从中我们可以看出现在区块链公链所面临的一些风险如下：

1. EOS 通过设置 21 个超级节点来进行信息的处理无疑是对公平的一种挑战，虽然 EOS 解决了部分 TPS 的问题，但是还是牺牲了很大一部分的公平性；

2. EOS 同时指出了以太坊目前也是由 7-8 个矿池所控制的，中心化程度相较于 EOS 其实是有过之而无不及的。综合事实，他的反驳也不无道理。其实权利一直都在少数人手中的这件事已经很久了，人们期望区块链可以解决这个问题，对区块链抱有很强的期望，但就目前来看，还是有一定的距离的；

目前是比特币基于算力来分配权利，如果不考量在算法上或者在其他方面进行升级的话会成为按财富分配权利的等价形式。以为允许任何人使用和接入就是公平，不考虑底层如何进行权利分配结果，这是对公平的一个曲解。而 MAI 的理念就是既避免权力的集中化又保证了记账的公平性。

反 ASIC 机制

我们所采用的机制是通过反 ASIC 机制来进行的。ASIC 是一件对于整个生态网络不公平的机制，也是对于资源的一种浪费，所以我们致力于改善这个生态环境，我们必须要做到反 ASIC 算法。我们所采用的机制是挖矿的算法每 7 天会改变一次加密模式，如果想用 ASIC 模式改变挖矿的收益是一件非常麻烦的事情，所以我们每 7 天改变一次加密模式让厂家的生产设计模式跟不上密码模式从而达到反 ASIC。这就是我们的反 ASCI 设计模型。

3.1.3 安全性的问题

公链在大家的认知内就是一个自由的世界，不可以被治理，是一个法外世界。因此对于治理有一种抵抗情绪，似乎认为公链上的智能合约应当是一切人类文明成果当中的一个法外圣地，在这里要排除掉其他的干扰和影响。这已经带来一系列的问题，争议缺乏协商解决以及管理机制，最后只能诉诸于丛林法则，这就距离公正、公道更加远了。表面上一切由代码来定义，由一开始设定的规则来规定，暗地里却可以使出各种底线之外的手段方式来施加影响，而 MAI 则是把治理的手段交给人工智能，依靠在智能合约层面进行人工智能的把控审核，使得进入公链的合约在规范化、安全性和合理合法化方面得到了极大的保证。

3.2 解决了开发者的什么问题

3.2.1 高安全性

自动化的筛选优质的智能合约推荐，使用神经网络和累积的数据，在特定时间内选择与特定用户最相关的智能合约推荐，从而为获得所需的智能合约应用场景提供最大的效率和安全性。区块链+人工智能技术的应用使得 MAI 可以让智能合约的编写更加智能，让公平性和使用率得到最大的发挥。

3.2.2 高便捷性

通过人性化的汉化处理能力，大大地减少开发者的学习门槛。通过规范化的API 语法和尽可能的降低代码的冗余度来减少开发者的开发周期。从而提高开发者的热情，提高 DAPP 的使用频次和黏度。

3.2.3 高易用性

MAI 社区将同步成立开发者研究中心和开设应用服务商店，能为中小企业和个人开发者提供大量的开源项目和各分类 API 接口服务能力，大大减少中小企业再项目开发中的投入。

3.2.4 严格的审核机制

通过 PAI 共识机制为开发者提供便利，PAI 通过对比智能合约使用频次、编写频次、安全性、合法性的相关信息得出谁拥有记账的可能性，从而提升 DAO 的整体性能、规范和使用频率从而衍生出更多好的 DAPP。

3.2.5 声誉评级体系

建立多层次的平台参与者声誉评价体系，建立针对开发者和用户的评级系统，开发者和用户的全部运营历史记录将存储在区块链中，以防止欺诈并形成最符合法律的生态环境。

3.2.6 完善的商业体系

商家和开发者可以在公链上共享用户数据，方便快捷的对自己的产品进行高效有针对性的推广。

3.3 解决了普通用户什么问题

3.3.1 用户的隐私问题

MAI 会把用户的行为资料打包储存在链上，极大地保证用户的隐私。用户不但可以高效便捷的使用公链上的 DAPP，而且可以快速便捷的得到自己想要的智能推荐。这一切都是基于用户的隐私保证。

3.3.2 便捷的操作方式

用户在使用 MAI DAPP 应用时，并不能明显的感知到这是一款中心化的应用还是去中心化的应用，用户操作无门槛化也极大的增加了便捷性和易用性。

3.3.3 清晰的价值体系

用户可以通过在公链上累计自己的操作行为来获取商家提供的报酬，并且用户可以决定商家是否可以换取自己的数据。MAI 真正的把用户行为变成了实实在在的价值从而体现出来，并且把决定权交给了用户自己。