达摩（DMCH）公链——隐私、高性能、可扩展的区块链去中心化金融解决方案
项目白皮书

序

乌托邦（Utopia）本意是“没有的地方”或者“好地方”，延伸为还有理想化、不可能完成的好事情。达摩（DMCH）是一个真正的、基于隐私底层的、并能创建智能合约发行隐私稳定币的金融世界，通过原子交换、Oracle 预言机，实现隐私稳定币与 DMCH 进行价值交换，让新的金融世界与现实世界完成价值交换，我们称之为 DMCH 乌托邦。

目录

第 1 章 引言

1.1 项目背景

自中本聪发行比特币白皮书，比特币为整个区块链世界奠定了区块链世界的原则：安全、透明、去中心化，所有的规则在链上运行，没有人可以作恶，没有人可以擅自改变规则，所有的法律都是由机器运行，不能人为干预，区块链的准则给了我们实现乌托邦的愿景，我们离光明并不是那么遥远。

基于 CryptoNote 协议的字节币（ByteCoin）和门罗（Monero）极大程度上解决了比特币支付系统的匿名性问题。然而世界除了需要去中心化的支付系统，还需要更多复杂的去中心化匿名应用。不幸的是，字节币和门罗诸如吞吐率低、等待时间长、不支持智能合约、预言机等问题阻碍了去中心化应用的进一步发展。由于去中心化的原因，要完美解决上述问题需要全球共识的改变，其代价已经远超运行一个新的项目。

此外，生活在这个时代，我们的命运被操控在他人手中，大多数人还并没有发现，更多的人发现了也无力挣脱。无现金社会正在悄然袭来，移动支付越来越普遍，让人享受便利的同时窥视和监管也愈发严重，未来的世界，可能纸钞和现金将被取缔，因为纸钞和现金不利于监管和流通，强流通、强监管的无现金社会正在慢慢取代旧的现金流世界。

但是对于隐私来说，这是梦魇，你将生活在楚门的世界，从出生开始，你的衣食住行都将围绕钱展开，同样你也会因为钱而被监视，你的兴趣爱好将会被大数据整理并以商业广告的形式反馈给你，以此继续培养你的兴趣爱好。因为个人隐私数据存储在中心化的服务器上，个人隐私的泄露愈加的频繁。中心化的官僚组织可以随时暂停你使用钱的权利，这是可怕的，在金钱编织的规则面前，人会变得赤裸裸并且没有任何的隐私，甚至个人的人权也会受到侵害。

1.2 项目意义

互联网基于中心化架构的应用服务（包括金融服务）不断以各种理由收集各类用户信息以谋求业务的扩大，但却忽视了隐私保护，这一不能促进营业额显著增长的基础工作。然而，这类应用服务一旦发生用户信息泄露事故，直接导致数亿级别用户信息的泄露。这些泄露的信息，被用于黑客用于精准诈骗甚至是身份盗用，给用户带来无法预计的无妄之灾。

如今社会迫切需要以不以人的意志为转移的技术保证的隐私保护措施，保护

个人隐私是最基本的人权。

达摩（DMCH）公链项目旨在成为基于门罗（Monero）的隐私、高性能、可扩展的区块链去中心化金融解决方案。达摩（DMCH）采用 Block DAG 区块结构，并在门罗（Monero）的隐私框架上集成了私有地址，私有智能合约，DeFi、DEX，引入不受节点限制的去中心化分布式 PPoS，旨在通过扩展 PPoS 节点来实现高速私有全球 SDWAN，建立一个分散的分布式隐私社区生态系统。达摩（DMCH）不仅继承门罗（Monero）成为加密货币，而且要进一步成为去中心化的专用互联网，保护个人隐私。

1.3 实现方式

区块链行业经过十多年发展，已经涌现数以万计的项目，大多数项目在比特币、字节币和以太坊的基础上进行了改进和优化，并逐渐呈现了螺旋式上升的进化体系。达摩（DMCH）公链项目将由来自于密码学、经济学、计算机科学、软件工程学等领域并致力于保护隐私的团队成员按照“学习、研究、集成、优化”和“市场、需求、资金”两个循环迭代的原则完成区块链技术发展十年以来技术的整合和提升，并最终交付给社区一个隐私、高性能、可扩展的区块链去中心化金融解决方案的具体实践。达摩（DMCH）公链项目的目标是在特定领域形成垄断性优势并为去中心化的理念不断努力、创新。

第 2 章 达摩（DMCH）公链项目技术方案

目前行业内公链项目的核心模块结构分解基本如图 2.1 所示，整个体系已经相对成熟，系统持续运行和不断出现的业务需求会促使公链技术不断迭代，这种迭代还会因为技术的颠覆（如量子计算、硬件突破等）发生跳跃性的变化。然而，技术更新不会改变区块链技术的体系架构而是不断优化体系架构下的核心模块，因此在区块链体系架构的框架之下部署隐私、高性能、可扩展的区块链去中心化金融解决方案具有稳定的体系结构。达摩（DMCH）公链项目作为去中心化匿名系统解决方案的基础公链，将不断整合业内项目的优点、融合行业最新技术、并在此基础上完成优化工作，以确保公链的稳定性、先进性和实用性。

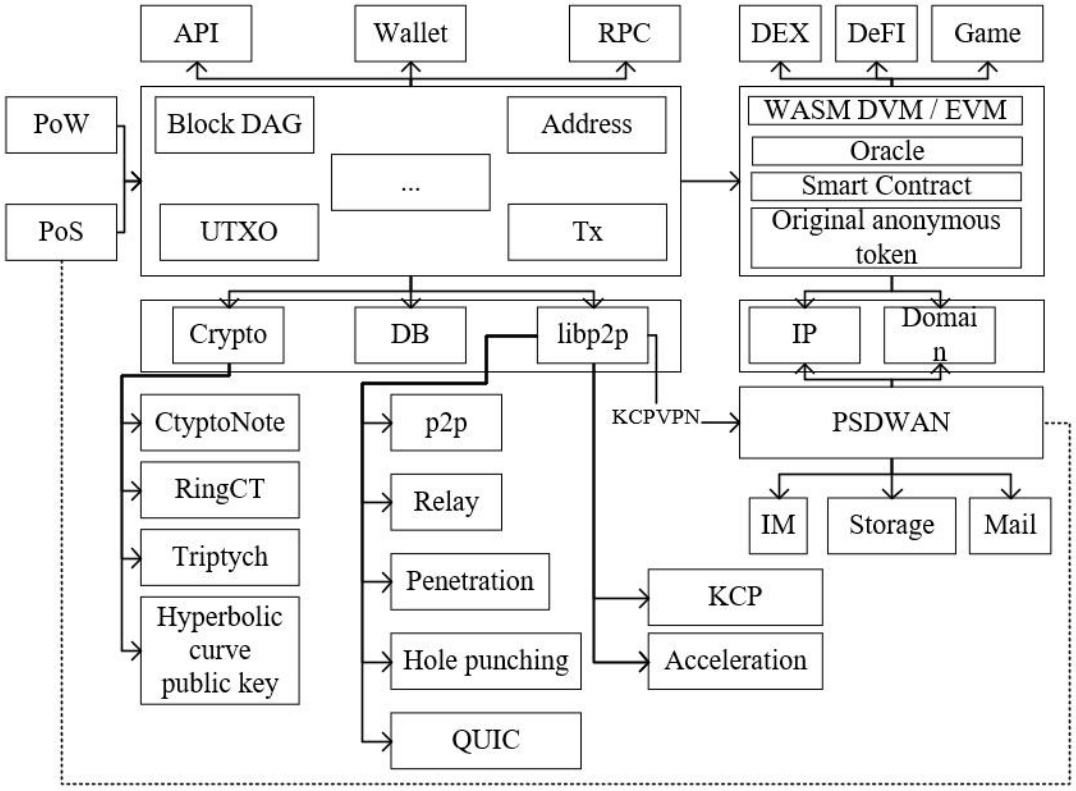

图 2.1 达摩（DMCH）公链项目技术方案系统图

2.1 libp2p

区块链去中心化的概念已经深入人心，但是实际上区块链是一个分布式点对点去中心化网络。大部分人对点对点的概念是很模糊的，点对点网络实际上是参与者(称为对等点或节点)在或多或少“平等”的基础上彼此直接通信的网络。这并不一定意味着所有对等点都是相同的；有些对等点可能在整个网络中扮演不同

的角色。然而，对等网络的定义特征之一是它们不需要一组行为 “客户端”完全不同的特权“服务器”，比如客户端/服务器模型。因为对等网络的定义相当宽泛，所以已经建立了许多不同类型的系统，它们都属于“对等”的范畴。大家比较熟悉的是 BitTorrent 这样的文件共享网络，而区块链网络（比特币、以太坊、DMCH）也是点对点网络。然而目前的互联网，是相当脆弱的，并且存在许多设计问题，这些问题大多源于位置寻址。解决方案是内容寻址，它是弹性更强的分布式点对点网络模型。但是要实现内容寻址，有很多来自于传统互联网的阻力，主要体现为 NAT，防火墙，网络延迟，网络可靠性，漫游，监管，不同设备的不同标准，技术迭代的缓慢等各种因素。

（DMCH）公链项目的 p2p 模块将使用 libp2p 框架解决上述问题，libp2p 原本是协议实验室（protocol lab）IPFS 项目的网络层，后来因为其具有颠覆传统互联网架构的能力被独立成一个单独的项目。简单来说，libp2p 就是帮助链接节点的一个库，任意两个节点，不管在哪里，不管处于什么环境，不管运行什么操作系统，不管是不是在 NAT 之后，只要他们有物理上链接的可能性，那么 libp2p 就会帮你完成这个链接。值得一提的是 libp2p 采用的 QUIC 不一定能解决全球网络穿透问题，DMCH 将整合 KCP 技术，KCP 已经被无国界的广泛使用，而基于 KCPVPN+BGP routing 形成的区块链互联网正是 DMCH 隐私、高性能、可扩展的区块链去中心化金融解决方案的重要生态。

2.2 Block-DAG

从本质上说，区块链的本质是个账本。像任何其他数据库一样，它包含有关各方之间交易的信息。但是，如果您希望此数据库不易受到攻击，并且最重要的是同时保持在许多设备上的相同状态，则它会很棘手。

传统的金融支付系统，能够每秒处理几千到几万笔交易，相较而言，比特币的交易处理性能相差了几个数量级，各种著名的区块链项目的交易处理性能如下表 2-1 所示：

表 2-1. 不同区块链项目的交易处理性能

名称	TPS	出块时间
BTC	7	10min
BCH	24	10min
LTC	7~28	2.5min
ETH	20~40	15s

注：以上数据来自于互联网公开数据

比特币采用著名的链式结构组织区块，每个区块能够包含的交易是有限的，如果有多个矿工挖矿，当同时有多个区块被发现时，需要根据最长链原则选择一条“最佳链”而临时丢弃其它区块，之所以是“临时”，是因为被丢弃的区块继续延伸并满足最长链原则，则会再临时丢弃之前的最佳链，自己成为最佳链。在区块链的顶端，不断来回地选择、丢弃、收敛，这称之为“选择最佳链”。举一个简单例子，如果在同一高度，同时有 10 个矿工广播了 10 个区块，每个区块中有 100 笔交易，那么只有一个区块会被在最佳链上延长，其余 9 个区块将被丢弃，被丢弃的 900 笔交易将陆续在后面的区块中被打包确认。是的，如果这 10 个区块能够被同时确认，那么处理性能将提升 10 倍。

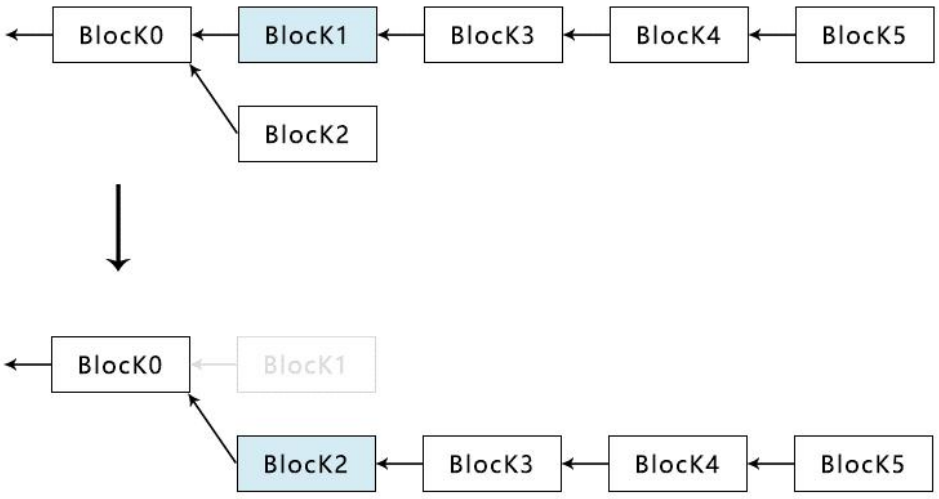

图 2.2：比特币最佳链选择

选择最佳链还会带来另一个重要的安全性问题：51%算力攻击。如前所述，在算力上拥有控制力的矿工，事实上可以人为操纵“最佳链”的选择，用自己精心构造的区块覆盖掉之前的区块。如何防止 51%算力攻击，提高区块链的安全性，也成为比特币的一个热门话题。

2.2.1 Block-DAG 概念

Block-DAG 就是采用有向无环图(DAG)来组织区块，有向无环图指的是一个无回路的有向图。如果有一个非有向无环图，且 A 点出发向 B 经 C 可回到 A，形成一个环。将从 C 到 A 的边方向改为从 A 到 C，则变成有向无环图。换句话来说，就是 Block-DAG 采用“图”，而非“链”的方式来组织区块，这样，就从根本上避免了比特币的“最佳链切换”的性能和安全性问题。用一句话来简单形

像地描述 Block-DAG 与传统比特币的区别就是，“比特币的区块处理是单核单线程，而 Block-DAG 是多核多线程”。

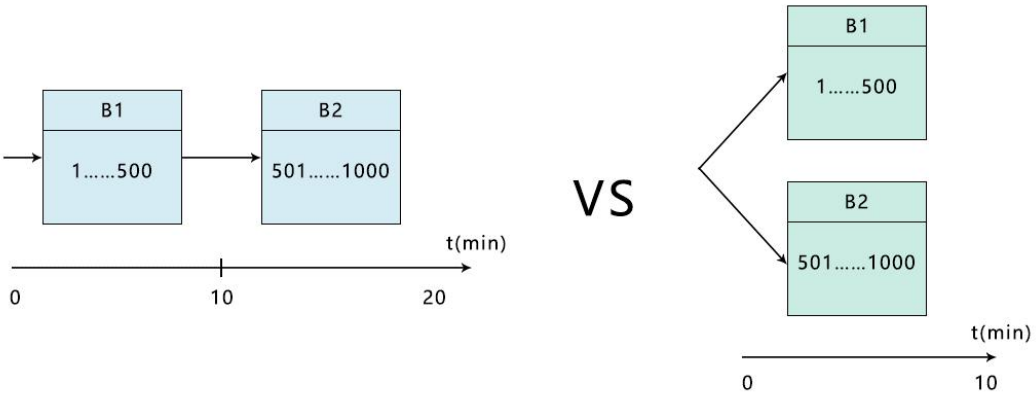

图 2.3：交易的并发处理

基于 Block-DAG 的区块链，不再是单一的链式结构，整个区块呈网状结构，如下图所示：

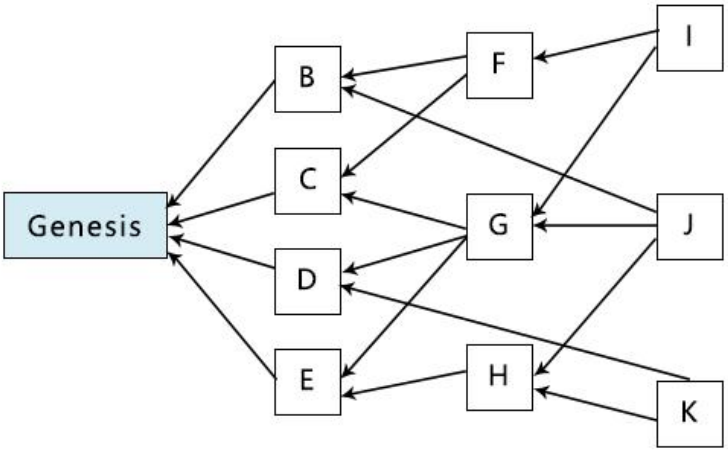

图 2.4：Block-DAG 的区块组织

我们知道，在区块链中，区块都是由低向高不断延伸的，在 Block-DAG 中，如果一个区块，在其后没有新的区块延伸，即其处于“顶端”位置，这样的区块，

被称为“Tip”。从每个 Tip 出发，都可以单向追溯到创世块。Tip 将被新的区块所引用，一个新区块可以同时引用多个 Tip，结合上图，我们来看看 Block-DAG 的区块是如何延伸的：

（1）：在最开始的时候，整个区块链只有创世块一个区块，即只有 1 个 Tip，假设有 4 个矿工同时挖矿，在同一个 Tip 上向后延伸了 4 个区块{B、C、D、E}。

（2）：我们假设因为挖矿速度和网络传输原因，矿工甲和矿工乙收到了{B、C}，矿工丙有{C、D、E}，矿工丁只有自己挖出的{E}，这样，他们分别以{B、C}、{C、D、E}、{E}为 Tip 继续挖矿。是的，他们无需继续等待所有节点区块一致，或者在{B、C、D、E}中切换选择最佳链。

（3）：以{B、C、D、E}为 Tip 分为三组：{B、C}、{C、D、E}、{E}，产生了新的区块{F、H、I}，矿工们又以它们为 Tip，继续挖矿，以此类推。

在 Block-DAG 的区块中，一个 Tip 被下一个区块引用后，称为“父边”，类似于比特币中的“父块”的概念，“边”是 DAG 算法的概念，这里不做进一步阐述。正如你所看到的，基于各种不可预料的因素，不是每一个 Tip 都有机会成为“父边”而继续向后延伸，对于这种区块，在 DMCH 中，将被视为孤块丢弃掉。

另一个值得注意的问题是，当一个新的区块出现时，最多允许引用的 Tip 数量。考虑最极端的情况，如果允许新块引用所有它能看见的 Tip，那么意味着相同高度将会有更多的并行区块，这将带来最高的交易处理性能，但是副作用也非常明显：如果矿工足够多，区块将无限膨胀。所以，在允许新块引用 Tip 的最大数量方面，需要一个折衷的权衡，目前，DMCH 允许新块引用的最大 Tip 数量是 3 个。在 DMCH v3 版本这个值可以动态调整并和交易分片整合实现了 TPS 的巨大提升。

2.2.2 Block-DAG 的排序

对于 Block-DAG 的区块排序，不是必须的，但是在绝大多数应用场景下，排序都显得非常重要。这是因为在交易之间，大多数时候都存在着某种基于顺序的关联性，最典型的代表是智能合约：一个交易中某个条件的发生，以另一个交易中某个条件的执行结果为基础。所以，DMCH 需要在图状的区块中，根据算法“计算”出一条“逻辑顺序”的链出来。这样做为两个目的：

（1） 决定交易的顺序性，满足上层业务的需要；

（2） 孤块将被丢弃；

这个逻辑顺序与传统比特币的链式结构非常相似，但也有本质的区别：比特

币是通过“父块的 Hash”来实现这种顺序性，而“逻辑顺序”只是一种逻辑概念，区块间并不存在这种物理联系。

排序后的区块集合，被称为“full order”，每一个在 full order 中的区块，都拥有一个唯一递增的拓朴高度（Topo Height），这也是为什么在块浏览器上，可以看到每一个区块同时拥有两个高度，Block Height 和 Topo Height。前者是区块在链上的高度，它总是在其最大的 Tip 的 Block Height 基础上加 1，以保证链高度不停地递增。同一个 Block-DAG 下面，可能会有多个矿工同时挖出的块。

针对 Block-DAG 的排序，有多个项目或团队提出了各自的解决方案，这些方案各有优缺点，我们来看 DMCH 是怎么实现的：

（1）：收到矿工广播新块，进行合法性检查，例如双花检测，交易有效性检查，PoW 校验，PoS 签名检查等等，检查合格的区块，将会被放入区块集合。

（2）：根据共识算法，找到本次排序的起点，假设为 Base，最初 Base 就是创世块，随着区块链的延伸，它也会跟着延伸。被选做 Base 的区块是已经稳定的区块（而且是没有 Side Block 的块，V2 版本主要在优化处理这个），其在 full order 中的顺序不会再因为排序而改变。

（3）：从 Base 开始，其后的所有区块的交易暂时标记为无效。

（4）：获取当前最新的 Tip 的集合，最新加入的区块也在这个集合中，根据共识算法选择一个最佳的区块，称为 Best。DMCH 采用了“累计难度和”来决定最佳 Tip 的选取，所谓累积难度和，就是从创世块开始，到当前块的所有经过的区块的难度和。

（5）：从 Best 出发，不断地向前递归追溯其 Tip，最终取得[Base，Best]区间内的所有可到达的区块，根据它们各自的累积难度进行排序，得到最终排序后的区块集合。很明显，集合中的其它 Tip，并不在[Base，Best]之中(因为它们也是顶点，且区块间不存在环路)，将被临时抛弃，甚至它们递归向前的父边，如果没有再被另外的区块引用，也会被同时抛弃。临时抛弃是 Blokc-DAG 的正常收敛过程，将在后文进一步阐述。

（6）：根据排序后的区块顺序（Topo Height），重新计算该区间内所有区块的交易，重复的交易，将自动被标注为无效。天然避免了双花，所有的交易有了顺序，这个为智能协议的运行提供了基础支撑。 在同一高度里，难度最大的块为主块，其他块为 Side Block。

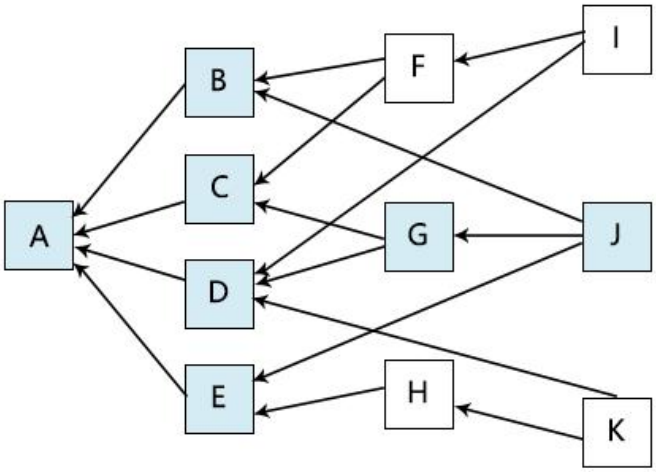

图 2.5 Block-DAG 的排序(1)

如上图，候选的 Tip 集合为{I,J,K}，假设 J 是最优的(即 Best)，A 为 Base 起点（A 没有 Side Block），那么在[A，J]之间的所有区块{A,B,C,D,E,G,J}将被选中排序，而{F,I,H,K}将会被临时抛弃。

在 Block-DAG 的排序过程中，有两点是值得特别注意的：

（1）在 Block-DAG 末端，总是存在一组待收敛排序的区块，DMCH 将这个最小值设为 8 个链高度，并一直往前找到 Base 起点为止，V3 版本正在优化该算法，减少确认时间。它们是不稳定的，称之为“不稳定”，因为区块可能被丢弃掉，那么交易也是不可靠的，这与比特币的未确认区块非常相似。在 DMCH 中，可以通过 getinfo 接口获取当前的“稳定高度”，即可以区分稳定和不稳定的区块。

（2）在谈到“临时抛弃”的时候，假设当前链有 10 个候选的 Tip，仅选择了其中 1 个区块，剩下的 9 个区块不一定会被丢弃，或者说绝大多数时候不会。这是因为下一个新的区块，在选择“父边”的时候，会根据共识算法选择它们中最优的几个（当前允许最多选择 3 个），这样，当下一个新的区块被选择为 Best 时，它们就自然有效了，因为这些区块属于[Base，Best]区间内向前追溯可到达的区块。依次类推，区块在不停地向后延伸，不停地收敛和排序，绝大多数区块都将被视为有效。如上例，一旦有新的块 L 产生，引用了{I,J,K}，那么从 L 向前追溯，所有的区块都将有效。

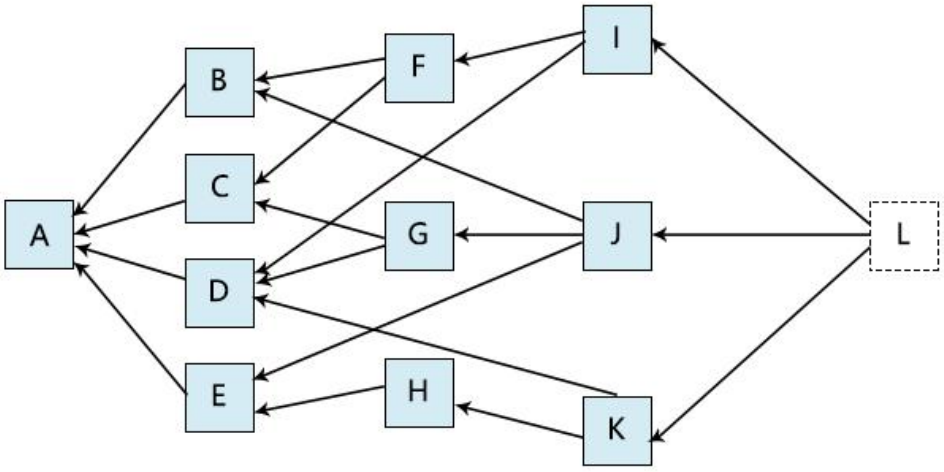

图 2.6 Block-DAG 的排序(2)

Block-DAG 是一种优秀的链上扩容解决方案，它有效地解决了比特币交易处理能力低下的问题。DMCH 的 Block-DAG 技术，与其它类似闪电网络的链下扩容方案是不冲突且有效互补的，结合其它扩容技术，DMCH 的交易处理能力还将进一步大幅提升。同时，DMCH 快速简单的区块收敛排序算法也会下一步的智能合约应用打下了坚实的基础。

2.3 匿名技术

DMCH 是基于门罗的分叉项目，两个项目都起源于 CryptoNote 协议。CryptoNote 最初的白皮书于 2012 年出现并在 Tor 上发表，原始白皮书的作者使用笔名 Nicolas Van Saberhagen。在不到一年后，以相同的笔名发布了第二版白皮书后，作者的身份仍然未知。CryptoNote 协议主要解决两个问题：一是不可追溯。不可追溯性是指对于所有传入交易，所有可能的发件人都可能为来源方，但是不知道是谁发送的；二是不可链接，不可链接性是指无法证明任何两个外向交易是发送给同一个人的；当然 CryptoNote 协议还解决了一些其他问题，详情参阅 https://cryptonote.org/standards/。

2.3.1 环签名

不可追溯的特性采用了环签名技术（注意，这个技术解决的是交易发送方的匿名问题）。环签名技术是基于 David Chaum and E.van Heyst 提出的群组签名概念（具体论文见：https://www.chaum.com/publications/Group_Signatures.pdf），环形签名使用混合在一起的多个公共密钥来混淆交易的真实签名者，这个动作不会影响验证交易有效的能力。值得注意的是环签名技术后来被证明在某些情况下可以被追溯（具体论文见：https://eprint.iacr.org/2006/389.pdf），这个问题由门罗提出的环机密交易（Ring Confidential Transactions，RingCTs)）解决。

2.3.2 一次性密钥

不可链接的特性采用了一次性密钥技术（注意，这个技术解决的是交易接收方的匿名问题）。由于在换签名的时候需要使用公钥，导致可以在区块链上观察到公钥地址的所有传入交易，因此容易暴露交易各方，为此通过改良的迪菲-赫尔曼密钥交换技术（Diffie-Hellman Key Exchange）形成一次性密钥，保护交易各方。大致原理是交易的发送者使用其自己的数据对接收者的公共密钥进行哈希处理，从而为该交易创建唯一的一次性密钥。达到的效果是只有接收者可以生成交易的私有部分。CryptoNote 协议是一个了不起的协议，更多信息请参阅 https://cryptonote.org/inside。

2.3.3 匿名过程

在实现匿名的过程中，单个用户有两个私钥、两个公钥来完成整个加密过程。环签名技术（Ring Signatures）解决交易发起方的匿名问题、一次性地址技术（Stealth Address）解决交易接收方的匿名问题、环机密交易（RingCTs）解决交易内容的匿名问题。

2.3.4 子地址

DMCH 支持子地址，相比于比特币钱包的子地址功能采取每一个地址一对公私钥的方案（相当于一个钱包文件里面，有无数个“小钱包”），DMCH 仍旧是一个钱包，一对公私钥，这在性能、可维护性上会优于比特币方案。

2.3.5 匿名技术优化

为持续保持 DMCH 匿名技术的领先性，Monero 研究实验室（MRL）和加密学最新技术都将是使 DMCH 项目持续优化匿名技术的有力理论依据。例如，MRL 发布了 Triptych，并提出不信任对数大小的环签名。Triptych 相对于目前环签使用的 MLSAG 是一种新的环签名结构，Triptych 将 MLSAG 并且和 Pedersen、Confidential transaction 技术整合成新的 RingCTs，这可以使匿名性提高十倍以上。Triptych 的主要创新在于使环签名的字节大小与诱饵的数量成对数关系，而不是线性关系，这样环尺寸可以显著增加但不会出现大的性能问题。DMCH 项目将持续关注诸如此类的技术革新，就 Triptych 而言，DMCH 项目将从 MLSAG 升级为 CLSAG，并最终过渡至 Triptych。

2.4 共识机制

共识机制可以分为经典分布式共识机制和区块链共识机制。共识机制的研究从 1975 年计算机领域提出的“两军问题”开始。国外学者提出了研究在可能存在故障节点或恶意攻击的情况下，非故障节点如何对特定数据达成一致的“拜占庭将军问题”，该问题是共识机制研究的基础。2008 年，中本聪提出比特币，共识机制进入区块链共识时代。目前区块链共识可以分为两大类，一类是授权共识机制，需要完成身份认证后才能参与后续共识机制；另一类是以比特币为代表的非授权共识机制，即节点随时加入和退出，节点数量动态变化且不可预知，并通过特定算法完成出块者选举、区块生成和节点验证更新区块链等过程。

区块链目前最成功的共识机制还是 PoW。以比特币为首的市值前 10 的公链，基本上使用的都是 PoW 共识机制。出现这种现象的情况一是共识的形成需要时间，当所有人都认为 PoW 是可靠的共识机制后，即使有更好的共识机制出现，也需要很长一段时间完成变更。二是 PoW 确实通过了加密方法和经济激励方法有效解决了拜占庭将军问题，也正因为如此，PoW 公平、公正、去中心化的概念深入人心。随着比特币诞生至今 10 年过去了，我们不得不承认比特币的 PoW 机制在十年后的今天，或多或少出现了一些衍生问题。

区块链共识主要通过安全性、交易吞吐量、可扩展性、交易确认时间、去中心化、资源占用六个方面来评价。DMCH 的共识机制主要经历三个阶段 PoW, PoW+PPoS, PPoS, 演化思路与以太坊保持一致，本质上是基于 PoW 的改进以解决 PoW 运转十年来出现的问题。DMCH 是基于门罗项目的分叉，因此其安全性、交易吞吐量、可扩展性、交易确认时间均继承了门罗的能力，此外在 DMCH 通过 BLOCK-DAG 技术、引入最新加密技术等方法进一步提升了安全性（抗 51% 双花攻击）、吞吐量（TPS 提升至 70）、交易确认时间（约 2 分钟）。

2.4.1 PoW 共识机制的问题

PoW 共识机制发展至今在资源占用和去中心化这两个问题上存在一些问题。一是资源浪费严重：目前比特币挖矿需要投入专业的挖矿设备（ASIC）以及消耗大量的电力，全球比特币一年挖矿消耗的电量相当于一个中小型国家全年的耗电量，且消耗这些电能的专业设备仅仅在做简单的记账工作。用一个国家的全年用电量和相应的算力去产出价格浮动剧烈的比特币，无论从什么角度来说都是一种巨大的资源浪费。二是逐渐中心化：中本聪在创立比特币的时候说过一句话“one cpu one vote”，然而这个美好的愿望随着人们的逐利驱动已经渐行渐远。我们可以观察到比特币全球算力已经出现几个大矿池逐渐垄断的情况，这种中心

化趋势一定会越来越严重。

2.4.2 PoW+PPoS

DMCH 的 PoW+PPoS 是指矿工挖出的块需要经过 PoS 节点签名验证后才被认为是有效的块，这个块的 DMCH 奖励 5%给 PoW 矿工，95%给 PoS 节点和代币持币人。其中 PPoS 这个名词是 DMCH 项目的创新点，意思是分布式 PoS 节点，简单来说就是不同于 EOS 超级节点导致中心化投票的弊端，DMCH 每一个节点都是平等的，在机制上更加去中心化。PoW+PPoS 阶段主要解决以下问题：

（1）绿色环保。当一个块的 DMCH 奖励只有 5%分给矿工的时候，这就意味着激励机制不鼓励 PoW 挖矿，这将大大减少比特币的趋利机制所导致的大规模计算资源和电力的投入，并进一步转化为鼓励支持者持币质押生息，这在本质上减少了计算和电能的浪费，是真正意义上的绿色环保机制。

（2）去中心化。当一个块 95%的奖励给与 PPoS 节点和持币质押用户的时候，人们会因为这个激励机制改变他们的行为。不难想象比特币的 PoW 激励机制形成的局面是“矿池+矿机”的生态，而 DMCH 的 PoW+PPos 激励机制形成的局面是“PPoS 节点+持币质押”的生态。我们可以理解为矿池转变成了 PPoS 节点，而矿机转变成了持币质押。这种形态上一致的生态大概率可以形成去中心化局面。首先是易用性，PoW 矿池和矿机需要一定的 IT 技术能力才能正常运转，但是 PPoS 节点却只要下载软件就能运行，其次是 PPoS 节点建设激励制度，所有的 PPoS 节点除了在出块的时候获得奖励（类似于矿池手续费），还有集体权重奖励，也就是说 PPoS 节点运营者除了手续费的收益还有维护节点的奖励，这就意味着会激励很多人去架设节点，而架设节点就是完成去中心化的过程。DMCH 项目将根据去中心化的程度对激励制度进行调整，其目的是进一步快速推进去中心化网络的建设。

2.5 智能合约

DMCH 智能合约基于 WASM、使用 PLONK 零知识证明、提供完整的 C/C++语言和 GO 语言编译环境、支持“匿名”合约且非常容易移植以太坊的智能合约到 DMCH 智能合约平台。

2.5.1 智能合约概述

智能合约是一种无需中介、自我验证、自动执行合约条款的计算机交易协议，近年来随着区块链技术的日益普及而备受关注。区块链上的智能合约具有去中心化、去信任、可编程、不可篡改等特性，可灵活嵌入各种数据和资产，帮助实现安全高效的信息交换、价值转移和资产管理，最终有望深入变革传统商业模式和社会生产关系，为构建可编程资产、系统和社会奠定基础。智能合约一般具有值和状态两个属性, 代码中用 If-Then 和 What-If 语句预置了合约条款的相应触发场景和响应规则, 智能合约经多方共同协定、各自签署后随用户发起的交易(Transaction, Txn)提交, 经 P2P 网络传播、矿工验证后存储在区块链特定区块中, 用户得到返回的合约地址及合约接口等信息后即可通过发起交易来调用合约。矿工受系统预设的激励机制激励, 将贡献自身算力来验证交易, 矿工收到合约创建或调用交易后在本地沙箱执行环境(如以太坊虚拟机)中创建合约或执行合约代码, 合约代码根据可信外部数据源(也称为预言机, Oracles)和世界状态的检查信息自动判断当前所处场景是否满足合约触发条件以严格执行响应规则并更新世界状态。交易验证有效后被打包进新的数据区块, 新区块经共识算法认证后链接到区块链主链, 所有更新生效。

以太坊的开发者社区很大，许多加密货币开发者都熟悉以太坊虚拟机（EVM）。以太坊从一开始就开发了以 EVM 为目标的语言 Solidity，将其用作智能合约的主要语言。尽管与 Go、Rust 等通用语言相比，Solidity 具有明显的局限性，但它目前是链上应用最广泛的开发工具。

DMCH 使用 Web Assembly 虚拟机（WASM），这是在加密技术和更广泛的技术世界中日益流行的技术。大多数加密货币领域都正朝着这个方向发展，诸如 ETH2，Polkadot 等更多项目都已决定使用 WASM。

尽管 Web Assembly 必将取得成功，但有必要兼顾开发人员的过渡适应期，使得 EVM 可以在 DMCH 上运行。为此，达摩（DMCH）将 EVM 虚拟机集成到了 DMCH 中，DMCH 将同时支持 WASM 虚拟机和 EVM 虚拟机。由于大多数以太坊工具依赖于 web3.js，因此我们实现了自定义的 web3 提供程序，该提供程序允许通过 web3 库中熟悉的接口直接与以太坊合约进行通信。

2.5.2 DMCH 隐私智能合约

区块链行业“隐私”智能合约的发展过程主要经历了三个阶段：

（1）比特币是一个完全公开透明的公链项目，只需知道钱包地址，就能知道比特币的进出，这样很容易查出帐户与帐户之间的关系，将比特币钱包地址和现实中的使用者关联起来，就能让人重新成为互联网时代的“透明人”，毫无隐私性可言。为了解决比特币隐私性问题，开发者们提出了以混币原理为核心的解决

方案，混币原理就是由许多人参与比特币的转入和转出，但是很难在转入和转出中找到一一对应的映射关系，转入和转出是被割裂的，无法从一端找出另一端的，从而保护了使用者的隐私问题。

（2）一些开发者为了从根本解决隐私问题，开发了从原理上直接支持隐私保护的公链项目，市面上主流的保护隐私的公链可以分为四类：混币器类、环签类、零知识证明类和 MimbleWimble 系，各自的代表项目分别是 Dash、Monero、Zcash 和 Grin/Beam。但这些注重隐私保护的公链本身都不支持智能合约，只是单纯作为数字资产工具使用。

（3）2018 年后，开发者们开始意识到对智能合约进行隐私保护的需求在不断增加，于是作为协议层的隐私层项目开始活跃在各种场景中，也就是在公链之上的智能合约提供隐私保护，注意隐私层协议可以建立在第一阶段的公链之上，也可以建立在第二阶段的公链之上。同第二阶段保护隐私的公链项目不同，隐私层项目可以结合各个公链的体系就行跨链操作，相对来说更加灵活，而且可以满足用户和开发者特定的隐私需求，这就是所谓的隐私智能合约了。

目前在以太坊（ETH）上著名的隐私智能合约项目有 NuCypher，Aztec Protocol 和 Zether。那么在门罗系（XMR）项目上的隐私智能合约项目就是 DMCH 了。DMCH 对智能合约的定位非常清晰，那就是在门罗的基础上对标以太坊做出易用、安全、隐私、高效的智能合约平台，以服务于 DMCH 的生态业务发展。

2.5.3 DMCH 的 UTXO 模型与以太坊账户模型的适配

以太坊在整体上可看作是一个基于交易的状态机:起始于一个创世(Genesis)状态, 然后随着交易的执行, 状态逐步改变一直到最终状态, 这个最终状态就是以太坊世界的权威版本。以太坊中引入了账户的概念以取代比特币未花费交易输出(Unspent transaction output, UTXO)模型, 账户分为外部账户和合约账户两类, 两类账户都具有与之关联的账户状态和账户地址, 都可以存储以太坊专用加密货币以太币, 区别在于外部账户由用户私钥控制, 没有代码与之关联, 合约账户由合约代码控制, 有代码与之关联。

用户只能通过外部账户在以太坊中发起交易, 交易可以包含二进制交易负载数据(Payload)和以太币, 交易执行过程中可能产生一系列消息调用。当交易或消息调用的接收者为以太坊指定地址Ø时, 创建合约。新合约账户地址由合约创建者的地址和该地址发出过的交易数量 Nonce 计算得到, 创建合约交易的 Payload 被编译为 EVM 字节码执行, 执行的输出作为合约代码被永久存储。当接收者为合约账户时, 合约账户内代码被激发在本地 EVM 中执行, Payload 作为合

约的输入参数, 可信数据源则为合约提供必要外部世界信息。所有执行结束后, 返回执行结果, 完整交易经矿工广播验证后和新的世界状态一起存入区块链。

考虑到以太坊交易伴随带宽消耗, 存储消耗, 计算消耗等, 为了激励全球算力的投入和合理分配使用权, 避免系统因恶意程序走向失控, 以太坊中所有程序的执行都需要支付费用。各种操作费用以 Gas 为单位计算, 任意的程序片段都可以根据规则计算出消耗的燃料数量, 完整交易的发起者需支付所有执行费用。交易完成后, 剩余的燃料以购买时的价格退回到交易发送者账户, 未退回的费用作为挖出包含此交易区块的矿工的奖励.若交易执行过程中发生燃料不足(Out of Gas, OOG)、堆栈溢出、无效指令等异常而中止, 交易将成为无效交易, 已消耗 Gas 仍作为矿工贡献其计算资源的奖励。

为了支持智能合约的账户模型，DMCH 引入了“匿名账户模型抽像层”设计。因为抽像层的存在，对于普通的 UTXO 账户和智能合约，变化是透明的：即从普通的交易视角来讲，智能合约的创建和调用只是一种类型不同的匿名交易，没有账户模型的概念，而从智能合约开发者的角度，使用的是账户模型，也感知不到 UTXO 账户的存在。假如 A 用户要通过合约 B 向 C 用户转账，则：

（1）A 用户构建一笔到合约地址 B 的合约交易，合约交易的功能是调用 B 的转账函数，为该函数传入 C 用户的接收地址和转账金额，通常是 C 的子地址；

（2）合约 B 收到交易后，执行合约代码，完成 C 的子地址到合约账户的映射，并触发转账流程；

（3）对于合约账户，意味着两笔交易，A 账户的支出和 B 账户的收入，同时 B 的支出和 C 的收入，合约代码将更新合约账户余额；

（4）合约代码运行结束，自动触发一笔到 C 的子地址的普通转账；

这样，从 UTXO 账户模型的角度来讲，有两笔匿名交易，A 到 B 和 B 到 C 的交易。从智能合约内部，则完全是三个合约账户的余额更新。

简单来说，DMCH 将子地址映射成一个合约账户，从而完成了 UTXO 到账户模型合约的转变。因此 DMCH 的智能合约与以太坊智能合约的运行机制完全一样。

2.5.4 DMCH 匿名智能合约的设计

当 DMCH 使用子地址映射方式实现账户模型后，实际上可以将 DMCH 的智能合约直接理解为以太坊（ETH）智能合约， DMCH 项目在实际大规模运行过程中定义了以下几种场景：

（1）合约内容透明、透明 DRC20-TOKEN（ETH 的合约币是 ERC20，DMCH 的合约币是 DRC20）；

（2）合约内容透明、匿名 Dmni-TOKEN（Omni 在 BTC 上透明资产，Dmni 在 DMCH 上匿名资产）；

（3）合约内容匿名 （通过 PLONK 实现，由于全匿名，无所谓其中代币是用哪种）；

上述三种情形，涵盖了智能合约应用的大部分场景，DMCH 提供了用户根据实际情况选择智能合约的种类。实际上追求合约内容匿名可以使用同态加密（FHE）技术，但目前的计算能力不足以支持其计算量。大部分情况下隐私、匿名合约要保护的不是合约的全部内容，而是参与者和资产。简单来说，DMCH 智能合约是可选匿名智能合约，第一种“合约内容透明+透明 DRC20-TOKEN”模式与以太坊合约完全一样，属于所有信息全透明，这使得 DMCH 智能合约具有潜在的庞大的用户基础；第二种“合约内容透明+匿名 Dmni-TOKEN”模式在第一种模式的基础上实现了参与方的保护，也就是合约资产受到底层匿名技术的保护。第三种“合约内容匿名”实现了合约内容的完全匿名，由于使用了 Merkel 树及零知识证明，这种合约隐私保护方案计算量极大、Gas 成本很高，一个块里不能容纳太多的这种交易，仅供特定场景下的使用。

2.5.5 基于比特币 Omni 的 Dmni 方案

Omni 协议是一种基于比特币区块链的数字资产方案（最早是 Master Coin Protocol, 见下图）。其核心原理是，将资产类的相关操作信息（如资产发行、转账等操作），附加到比特币协议中的 OP_RETURN 信息中。原生比特币协议中，OP_RETURN 信息可以是任意内容，并受比特币区块链保护，不可篡改。Omni 协议层附加在比特币区块链上运行，并维护一个本地数据库。Omni 协议分析所有比特币交易中的 OP_RETURN 信息，若符合其协议定义，便会执行其中的操作，更改本地数据库中记录的资产信息。Omni 协议本质上是一种染色币（Colored Coin）方案，也可以认为是最成功的染色币方案。Omni 协议最成功的应用是 Omni-USDT。

DMCH 利用现有的匿名技术框架（环签、一次性地址、RingCT），抽像了一套类 Omni 技术框架，这意味着，可以在 DMCH 上轻松发行自己的匿名数字资产，而不用发行自己的主链或智能合约，甚至不需要编写一行代码。

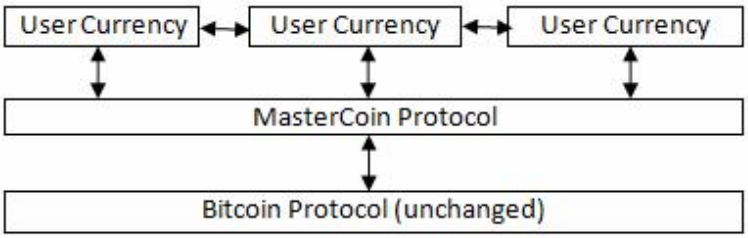

图 2.7 Omni 协议

2.5.6 DRC-20 方案

DRC-20 Token 是一类遵循 DRC-20 标准的 DMCH 智能合约。DRC-20 标准中定义了一系列数字资产操作常用的接口，并便于 DMCH 的 C 语言和 GO 语言（基于 WASM）实现。请注意，DRC-20 只是一系列接口定义，并不包含具体实现。换句话说，数字资产开发者需要自己编写智能合约程现 DRC-20 标准中规定的方法。与其他一般智能合约一样，DRC-20 Token 的最终执行，本质上是 DMCH 虚拟机（DVM）中运行一段智能合约程序。DMCH 协议本身并不关心合约的业务逻辑，因此一个具体的 DRC-20 Token 的表现，完全依赖于其开发者的编程水平。

2.6 其他

DMCH 项目技术方案按照“学习、研究、集成、优化”和“市场、需求、资金”两个循环迭代的原则在图 2.1 达摩（DMCH）公链项目技术方案系统图上不断优化升级。安全性、交易吞吐量、可扩展性、交易确认时间、去中心化、资源占用六个方面是评估技术升级的主要考虑因素，除上述章节外，正处于试验性阶段的技术有 VRF 技术与 Block-DAG 技术结合；MLSAG、CLSAG、Triptych 技术之间的过渡；数据库优化选型等。

第 3 章 达摩（DMCH）公链项目核心生态

一个隐私、高性能、可扩展的区块链去中心化金融解决方案的具体实践需要相对闭环的生态体系（内循环）和相对完善的行业生态体系（外循环）。目前去中心化的行业生态体系已经相对完善，而闭环生态体系在以太坊上比较成功，但是以太坊生态的持续发展已经受限于以太坊技术缺陷而影响生态的持续高速发

展。基于 DMCH 的闭环生态体系有效补充了当前以太坊生态体系不足以满足市场需求的现状，同时解决了市场对隐私和高性能公链的强烈需求。

达摩（DMCH）公链项目将自建“即时通讯 IM”和“分布式私有互联网”核心生态和 DeFi/DEX 金融平台，交付给社区一个集金融支付、安全通讯、小型私有网络的最小生态集合，并期待社区能将达摩（DMCH）生态发展甚至超越以太坊生态。

3.1 达摩（DMCH）金融平台

世界上 80%的财富掌握在 20%的人的手里，这已经是所有人都能感受到的社会现象，我们称之为“二八分化”或者“马太效应”。马太效应，反映了现实社会的两极分化，富的更富，穷的更穷。20%的人是规则的制定者，是既得利益的获得者。世界上大部分的人都是另外那 80%里的一份子，大部分的人都想成为 20%的人。有趣的是，即使有下阶层的人变身成为上阶层的人，这种平衡也不会打破，上阶层的人会制定相应的规则保护自己的既得利益，即少数派会一直处于统治地位。

“马太效应”在金融领域尤为突出，在中心化的金融世界中，金融的力量是集中的，大多数人被排除在获得资金的决策之外，只能从项目中获得一小部分利润。闭锁的金融世界是阻挠经济进一步发展的桎梏，规则保证了少部分人的利益，把大部分人排除在外。

3.1.1 中心化金融(CeFi)的问题

中心化金融系统是不健康的金融系统，是 20%的上层收割 80%下层羊毛的工具。权利的高度集中导致中心化的金融机构完全可以标记、追踪并封锁你的个人资产。银行是中心化金融机构的化身，普通人将自己的资产的控制权交给银行或者信托公司，这些金融中介机构可以便利的利用市场上的资金进行投资，当他们获得高额回报的时候会给与他们给资金委托人承诺的利润。但是，历史上金融次贷危机不断重复发生，中心化的金融机构却不能预见这种风险，甚至更容易犯错误，这种风险会在中心化的系统中造成的危害巨大。中心化的金融世界中，完成金融事件的参与是有门槛存在的，比如股票私募，风险投资，融资并购都是由私募基金和金融大鳄来参与的，普通的投资人穷其一生也无法逾越资本的鸿沟，这造成大部分的优质项目机会都会被上层把控，哪怕你能洞悉未来的行业发展趋势也会因为自身资金实力不够而被拒之门外。

3.1.2 达摩（DMCH）去中心化金融（DeFi）

我们将会越来越经常听到的去中心化金融、分布式金融、可编程金融都可以和 DeFi 等价。DeFi 有几个突出的特点：

（1）基于区块链技术；

（2）资产由个人掌控；

（3）清结算都是实时通过智能合约完成；

（4）通过对信任的最小化依赖，降低个体与个体间的信任成本；

去中心化金融（DeFi）是一种开源技术，旨在通过引入去中心化层来去中介化，消除寻租中间人，从而在各个方面改善目前的金融体系。达摩（DMCH）期望每个人都是自己的主人，每个人都可以自由的调度自己的资产，不会被中心化的机构窥视、监管、封查。达摩（DMCH）会在去中心化、隐私、公平的基础上构建达摩（DMCH）乌托邦世界，保证金融安全，保证每个投资者金融参与的公平性，对抗现实世界中的资产审查与监管，剥离中心化金融的危害，构建真正的、去中心化的金融世界。

乌托邦（Utopia）本意是“没有的地方”或者“好地方”，延伸为还有理想化、不可能完成的好事情。一个真正的、基于隐私底层的、并能创建智能合约发行隐私稳定币的金融世界，通过原子交换、Oracle 预言机，实现隐私稳定币与 达摩（DMCH）进行价值交换，让新的金融世界与现实世界完成价值交换，我们称之为 DMCH 乌托邦。

3.1.3 DeFi/DEX 设计逻辑

以下为达摩（DMCH）DeFi/DEX 的设计逻辑：

（1）发布基于以太坊的 DMSwap，详见 3.1.4 基于以太坊的 DMSwap。

（2）发行 DSC（Darma Cash Stable Coins）：

- Maker 是以太坊上的智能合约体系，提供了第一个去中心化的基础稳定货币 Dai（可简单理解成以太坊上的美元）和衍生金融体系。Dai 是通过数字资产足额抵押担保发行，1 Dai = 1 美元。自 2017 年上线以来，Dai 始终和美元保持锚定，DMCH 将会采用相同的协议发行 DMCH 的稳定币 DSC。
- DSC 之所以可以成为稳定币的原理与 Dai 类似。DSC 始终是超额抵押的，也就是说 DSC 的背后始终有足额的资产。如果资产价格上升，那么 DSC 的担保将更充足。如果资产下跌到一定值（原 CDP 开启者没有追加保证金或偿还 DSC），合约会自动启动清算。任何用户都

可以清算抵押不足的资产，并且获得 3%的无风险收益。这将激励很多市场参与者扮演 Maker 中的 Keeper 角色，他们不仅可以从系统中获益，同时也保护了 DSC 的偿付性。

- 流动性和可兑付性是 DMCH 成功的重要基础设施，DMCH 将会将整体排放的 20% 用于分发给为 DMCH/DSC 提供流动性的 LP。

3.1.4 基于以太坊的 DMSwap

2020 基于 DeFi 概念的 AMM DEX 呈现爆发式增长，以太坊受益于此次 AMM Pool 的流行，其生态得到进一步发展。理论上，基于达摩（DMCH）的 DeFi/DEX 平台相比于以太坊拥有更高的 TPS、更低的 GAS 且支持隐私保护，相比以太坊具有更大潜力。考虑到流动性挖矿已经形成虹吸效应并使得以太坊呈现一家独大局面，达摩（DMCH）将启动基于以太坊的 DMSwap 项目。DMSwap 的设计理念来自于 Uniswap 和 SushiSwap，但与 Uniswap、SushiSwap 等项目不同，DMSwap 除了有用户推荐激励、项目推荐激励、交易激励、代币回购等各种激励机制外，还有匿名公链达摩（DMCH）作为其另一维度的价值支撑，DMSwap 最终将平移回达摩（DMCH）的 DEX 体系中。我们基于达摩（DMCH）主链项目的整体规划，设计了 DMSwap 项目，主要目的如下：

（1）验证基于达摩（DMCH） DEX 和 DeFi 平台的商业模式的可行性；

（2）借助以太坊 AMM DEX 为达摩（DMCH）提供更高的流动性；

（3）在基于达摩（DMCH） DEX 和 DeFi 平台上线前抢占和锁定部分市场份额；

（4）切入 ETH 生态圈，让 ETH 生态圈更多的了解、关注达摩（DMCH）；

相对于 Uniswap 和 SushiSwap，DMSwap 主要在两个方面进行了创新：

（1） 实现用户激励计划（推荐关系），加入了 GAS 成本的考虑；

（2） 创建交易分红手续费；

（3） 交易对创建者可以灵活定义手续费；

（4） 兑换过程可以指定第三方地址；

（5） 参与交易可获得 DMS（DMS 是 DMSwap 的平台币）；

（6） 20%的交易手续费用于回购 DMS；

（7） 实现项目激励计划，设计了一个双令牌激励机制，这意味着如果 A 在 DMSwap 上为 B 做 LP，A 不仅可以获得 DMS，还可以获得 B 项目本身的激励令牌。

3.1.4.1 DMS

DMS（DMCH Swap）是DMSwap协议的代币。持有DMS意味着享有DMSwap平台的所有权益，并对 DMSwap 的发展有投票权。所有 DMS 持有者都可以对 DMSwap 的重大决定进行投票。目前 DMS 可以通过推荐用户使用 DMSwap、推荐项目使用 DMSwap、成为 DMSwap 的 LP、以及在 DMSwap 中交易四种方式获得。DMSwap 的部分手续费还会用于回购 DMS。

3.1.4.2 DMCHE

DMCHE 是托管在以太区块链上的 ERC20 令牌，并由等量的原生 DMCH(在 Darma Cash 区块链上)为依托。一个 DMCHE 与一个本地 DMCH 的价值相同并且可以通过 DMCHBridge 随时在 DMCH 和 DMCHE 之间来回转换。

3.2 达摩（DMCH）即时通讯 IM 生态

即时通讯 IM 是属于社交网络的一部分，社交网络作为互联网最大的基础设施和开放平台，极大幅度提高了社交的效率和速度。基于达摩（DMCH）网络开发的即使通讯 IM 将会是一款基于区块链技术的次世代社交平台，结合 DeFi 后将是基于区块链搭建的首个落地社交金融应用，它能使得所有达摩（DMCH）的用户有属于一个群体的归属感，并进行社交。

3.3 达摩（DMCH）分布式私有网络生态

分布式私有网络可以理解为 WEB 3.0 的一个具体形式，基于达摩（DMCH）分布式的私有网络具有抗 DDoS、抗封锁、高速、稳定等相比于当前互联网基础设施的巨大优势。达摩（DMCH）的 PPoS 节点依靠其经济激励机制形成全球分布式网络（见下图），当 DMCH 的 PPoS 节点足够多的时候，一个去中心化的分布式小世界网络就形成了，这将实现任意两个客户端之间的最短路径都只有 2-3 跳，为 DMCH 的去中心化应用生态提供最完善的区块链基础设施。在此基础上，基于 DMCH 的分布式私有网络可以运营一切当前互联网的所有资源，IP 资源、域名资源、内容资源等等，在这个全新的小世界网络里，达摩（DMCH）重新定义了一个崭新的互联网世界。

第 4 章 达摩（DMCH）释放机制

4.1 规格参数

总量：4.6 亿
共识：PoW + PPoS
算法：CNR
出块时间：15S
确认时间：90S
块大小：1.5M
预挖：3%，约 0.144 亿（私募），已经全部捐赠给 DMCH 社区

4.2 挖矿释放

早期一部分 DMCH 通过 PoW 挖矿完成早期的分发；PPoS(可以理解为 DPoS)上线后，DMCH 采用 PoW+PPoS 挖矿模型，大部分的 DMCH 将由 PPoS 挖矿产生。

4.3 释放曲线

DMCH V1 版本为第一阶段，采用 PoW 共识，初始每个块释放 589DMCH，每月减半一次，累计挖矿 8 个月。

DMCH V2 版本为第二阶段，采用 PoW + PPoS 共识，初始每个块释放 7.4 个 DMCH，其中 5%分给 PoW 矿工，65%分给 PPoS 节点及委托人，30%前期作为 PPoS 节点的运营奖励预留，后期减少到 10%，20%将作为 DMCH 的流动性服务奖励。区块奖励释放数量逐块递减，至第 2 年减至一半，降低到 1%左右以后，每隔 4 年减半并按照社区投票来决定减产周期。DMCH V3 版本将采用 PPoS 共识。

4.4 释放原则

DMCH 的释放、分配机制可能会根据实际情况进行变更。变更的原则是有利于项目进一步的发展。

第 5 章 达摩（DMCH）路线图

Time		Plan
2018	Q1	DMCH 网络研发
2018	Q2	Block-DAG 技术研发
2018	Q3	CryptoNote 协议优化
2018	Q4	环签名优化
2019	Q1	防弹协议优化
2019	Q2	
2019	Q3	
2019	Q4	DMCH 主网上线 DMCH 区块浏览器上线 DMCH 移动钱包上线
2020	Q1	DMCH 从 PoW 切换为 PoW+PPoS
2020	Q2	DMCH EVM 研发
2020	Q3	匿名合约研发 预言机优化 原子交换技术研发
2020	Q4	VRF+PPoS 研发 匿名代币研发 优化智能合约
2021	Q1	VDF+VRF+PPoS 研发
2021	Q2	SDWAN 研发
2021	Q3	IM 研发
2021	Q4	