德尔塔（Delta）白皮书

引言

一种名为比特币的去中心化加密数字货币的诞生，标志着人类社会正在逐步迈向去中心化的超主权数字货币时代。公平、安全、保值、快速、绿色的新型数字货币成为日常支付货币是世界人民的民心所向。

我们的使命是建立一个让每个普通人都能自由参与铸造和运营的数字货币及去中心化应用程序平台。

我们的愿景是与全世界的每一个人一起，创造一种公平、安全、快速、绿色且无通货膨胀的超主权数字货币。我们致力于建立一个相对自由的点对点生态系统和在线应用环境，让每个人都能自由地参与其中，共同推动德尔塔的发展和应用。

1. 主权货币问题简述

1.1 充当世界货币的主权货币发行国能够获得巨额的国际铸币税和国际通货膨胀税收益，这种单一的世界货币格局是一种不公平的结构。
1.2 国际货币支付手段职能的前提是货币发行国强大的信用保证，但是特里芬难题使主权货币发行国面临着两难选择，单一的世界货币格局是一种不稳定的结构。
1.3 货币价值尺度的二重性决定了国际市场上只能有一种货币执行世界货币的职能，多极世界货币格局会导致货币发行国之间的摩擦，对世界经济和平发展不利。
1.4 政府为了刺激经济和增加财政收入而集中的货币发行权，可能会导致货币严重超发并形成高通货膨胀，这会严重影响普通人口袋里现有货币的价值，增加了生存的经济压力。

2. 当前加密货币的现状与弊端

比特币是最早的加密货币，概念最初由中本聪在 2008 年 11 月 1 日提出，并于 2009 年 1 月 3 日正式诞生。根据中本聪的思路设计发布的开源软件以及建构其上的 P2P 网络。比特币是一种 P2P 形式的数字货币。比特币的交易记录公开透明。点对点的传输意味着一个去中心化的支付系统。与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生。人类后续发明的一些加密数字货币产品也基本参考了比特币的模式与技术。

这样的模式与技术方案具有许多优秀的好处，并为后来数字货币的发展带来了诸多启发。

比如：
去中心化、不可篡改——这些特性确保了人们所持有的资金不受任何第三方控制和监管，同时让人们感受到了完全的拥有感。持有者不必担心资金被冻结或被抹去，这让人感到安心。
独立性、公平性——加密货币不受任何国家、银行或金融机构的控制，它们基于的是一个去中心化的网络。从理论上一定程度上避免了各国在追求货币政策和金融体系的优势时所引发的竞争和冲突。

但是，同时也带来了许多方面的现实问题，以下面对相关问题展开论述。

2.1 安全性

按以上原理设计的加密货币安全性问题主要有两个方面：

①私钥破解——比特币私钥破解理论上的难度等于破解一个 256 位的密钥。换句话说，攻击者最多需要穷举大约 10^{77} 次。虽然这个几率非常渺小，但是没有人能够保证碰撞成功的事件一定会发生在最后一次。同时，随着量子计算机的出现和发展，将给持有者带来更大的担忧。

②私钥丢失或被窃取——保管基于密码学加密货币的私钥是持有者面临的一个重要问题。无论选择使用冷钱包、纸钱包还是脑钱包，都有可能发生私钥丢失或被窃取的情况，这让人感到十分焦虑。世界上每个人都有物品丢失或被盗的经历，也可能会忘记重要信息。因此，没有人能够保证这种情况不会发生在管理私钥或助记词方面。最糟糕的是，一旦丢失或被窃取，无法通过任何一种方式找回或重置，这给持有者带来了巨大的风险。

2.2 公平性

同样以比特币为例，虽然其去中心化的特性使得任何人都可以参与验证交易和挖掘区块，但在早期，只有少数人致力于此，并因此获得了大量的比特币。随着比特币网络的兴起，大量的算力集中在了少数矿场手中，使得比特币的生产和财富分配出现了大规模的集中化。目前，87%的比特币由网络中 1%的人拥有，这使得大多数普通人很难有机会参与其中。后期希望拥有比特币的人们只能高价在二级市场购买或投入巨资购买算力，这样的情况让大多数普通人很难有信心和实力加入其中。因此，在比特币等加密货币网络中，公平性是一个值得思考的问题。

2.3 能耗与环境问题

根据剑桥大学替代金融中心[ii]（Cambridge Centre for Alternative Finance）发布的实时比特币电力消耗指数（CBECI）数据，全球比特币挖矿的能源消耗量惊人。目前，这一

数字约为 131.73 TWh，与阿根廷或荷兰等国家的年度电力消耗相当。此外，比特币挖矿还产生了大量的碳排放，占全球总排放量的 0.10%左右。这加剧了全球环境问题，特别是气候变化和环境污染。

随着比特币和类似网络挖矿的规模不断扩大，能源消耗量和碳排放量也在持续增长。然而，尽管这些挖矿的能源消耗和碳排放问题备受关注，但这也推动了人们对更环保、更高效的加密技术的研发和应用。

2.4 POS 困境

POS（Proof of Stake）机制的出现确实在一定程度上解决了比特币等加密货币在能耗和交易速度方面的问题。然而，POS 机制也存在一些困境。其中最主要的问题是，在 POS 机制中，质押代币最多的验证者能够更快地获得验证资格并获得奖励。这种机制可能会导致“富者更富，穷者更穷”，从而引发分配公平性的问题。这进一步阻碍了加密货币的流通和普及。

在 POS 机制下，拥有大量代币的验证者能够获得更多的奖励，这使得富有的验证者更加富裕，而贫穷的验证者则更加贫困。这种模式可能会加剧社会贫富差距，降低普通人的参与度，进而阻碍加密货币的普及和发展。

此外，POS 机制还存在一些其他的问题。例如，质押代币可能会产生风险，如果代币价格下跌，验证者可能会遭受损失。此外，POS 机制中的验证者可能会被攻击者恶意攻击，从而影响整个网络的安全性和稳定性。

因此，虽然 POS 机制在一定程度上解决了比特币等加密货币在能耗和交易速度方面的问题，但是它也带来了一些新的问题和挑战。为了解决这些问题，需要进一步研究和探索更加公平、安全和有效的共识机制。

当然，除了上述提到的安全性、公平性、能耗和 POS 问题之外，现有的各种加密货币还存在着其他一些问题。例如，交易速度慢、交易成本高、价格波动大、缺乏应用场景以及兑换鸿沟等问题。这些问题在此暂不展开论述，后续的德尔塔设计说明章节中将会探讨如何通过一些有效的方法和策略来解决与避免这些问题。

3. 德尔塔（Delta）更理想的数字货币系统

为了设计和开发更理想的数字货币，我们站在前人的肩膀上，吸取他们的优点，避免重蹈覆辙。同时，结合当前的社会状况和技术基础，我们以人本货币为基本理念，致力于设计和构建在未来社会中理想的数字货币系统。

3.1 名词与定义

为了更方便阐述和阅读本文档，我们将一些必要的名词和定义的解释写在前面。

- **DTC**：这是 Delta Coin 的缩写，也是该数字货币的代码。
- **DTCT**：这是 Delta Credit 的缩写，表示未被激活释放的 DTC。
- δ：这是 Delta Coin 的货币符号，例如 10δ、100δ、1000δ等。
- **挖矿**： 在 Delta 应用中，通过特定的分配规则和模式，用户通过点击操作获取 DTCT 的行为。

角色与职能：

角色与职能构成货币铸造、共识建设、系统安全的有机整体。在德尔塔系统中，有三个核心角色：矿工、大使和验证者。

- **矿工（Miner）**：德尔塔系统的参与者，在首次进行采矿操作时将获得矿工身份。其主要职能是在德尔塔的移动应用上进行挖矿操作以生成 DTC。这种设计非常有趣且实用，因为它没有额外的电力消耗，对环境友好，同时也不会引发时间焦虑，影响个人健康。在德尔塔共识的建设过程中，矿工是主要的力量。
- **大使（Ambassador）**：任何矿工都可以通过使用自己的 DID（数字身份标识）推荐身边的人加入德尔塔，并构建出一个微社区网络。成功推荐他人加入者将自动获得大使身份。大使的职责是教授新成员如何进行挖矿操作，并帮助他们了解德尔塔的运作机制。因此，大使是 Delta 共识建设的关键力量。
- **验证者（Validator）**：德尔塔系统的独特设计使得它成为一个无需密码、无需私钥、无需助记词的数字货币系统。在这个系统中，验证者的角色是通过验证终端为不特定的用户提供账户身份验证服务。任何矿工都有机会通过竞选程序成为验证者，他们在保障系统安全方面发挥着重要作用。

3.2 移动手机挖矿

在加密货币中引入挖矿概念，有助于解决货币发行中分配公平性的问题。Pi Network[iii] 开创了移动挖矿这一创新设计，它绿色环保，有效规避了能耗问题，无需占用设备的算力和额外网络。在移动电话高度普及的今天，让普通人参与数字货币挖矿成为了可能。德尔塔继承了这一设计。需要说明的是，**挖矿的本质在于分配，而非计算。**中本聪在比特币设计中利用参与者算力计算数学难题来争夺记账权并奖励比特币。由此可见，算力只是用于争夺记账权游戏，它与记账并无直接关联。从计算机工作过原理来看，它只是将数据写入磁盘的过程，这个过程能耗极低。所以，摒弃算力挖矿在现有技术背景下是完全合理和可行的。

3.3 Proof of People（POP）

如果我们把通过计算机工作算力的多少来证明对网络的贡献叫做 POW 挖矿（Proof of Work），把质押货币的多少来证明对网络的贡献叫做 POS 挖掘（Proof of Stake），那么我们就可以把通过以人本身的真实性来证明对网络的贡献叫做 POP 挖矿（Proof of People）。当我们启用手机上的 Delta 程序来进行挖矿时，这并非手机本身在进行挖矿过程，而是手机作为载体，用于对个人的真实性校验。因此，Delta 的本质是将铸币权交给人民，是一种人本货币的理念。

3.4 3-No-Verification（三无验证）

创意的设计让德尔塔成为一个无需密码，无需私钥的加密货币系统，

通过 **3-No-Verification 是用户进入 Delta 系统的唯一方法，**为了解决 2.1 章节 提到的加密货币安全性问题，我们在德尔塔账户身份验证设计中提出并使用三无验证。含义即：

- 无密码
- 无私钥
- 无助记词

我们无需密码、私钥、助记词的原因在于，如果系统仍采用账户+密码的形式设计，那么将需要通过电子邮件或短信方式进行密码保护，这将导致去中心化程度和服务的持续性受到严重质疑。具体来说，邮箱认证需要一个专门的发件箱地址，短信验证则需要一个在电信公司申请的短信接入号码或发送端口。这些资源不仅需要持续维护，还需要付费。这些工作需要由中心化的人为操作执行，这会引发用户的不信任感，与去中心化应用的核心理念相悖。

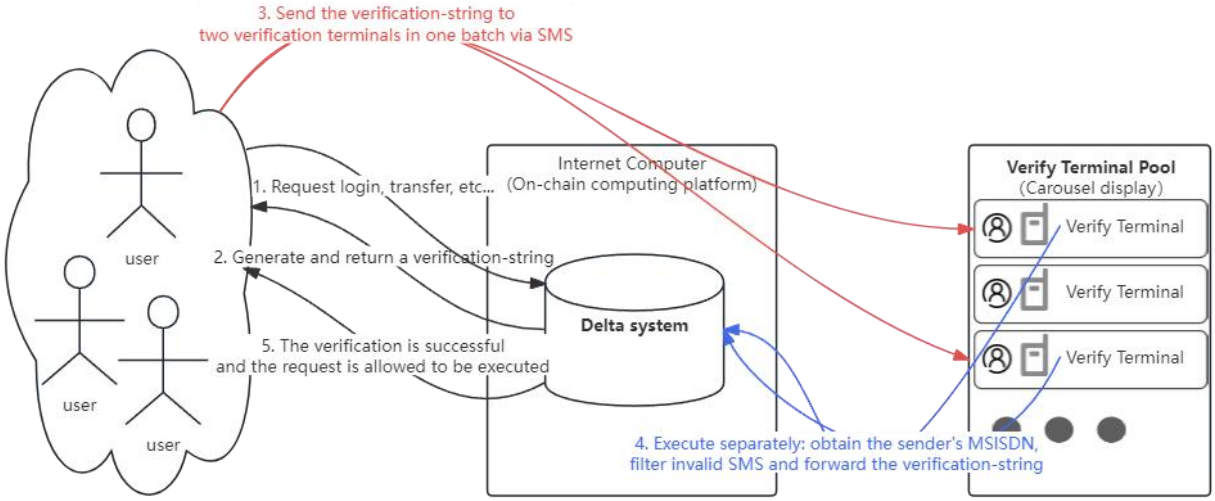
比特币诞生后，非对称私钥被用作于权限认证手段，这是一种完全去中心化的认证方案。后来，为了便于用户记忆和管理，开发者们衍生出了助记词的解决方案并在去中心化应用中广泛使用。然而，这些方案都存在私钥或助记词丢失、忘记、被盗用等风险，并且让用户产生一定的焦虑情绪。因此，我们需要一种更加安全、便捷的认证方式来替代传统的密码、私钥和助记词。

由于密码、私钥和助记词存在被破解、丢失和忘记的风险，因此摒弃这三种验证方式实现去中心化账户验证并非不可能。德尔塔成功实现了三无验证，这主要得益于基于区块链的 Internet Computer 的强大功能和全球高度成熟的移动通信网络。MSISDN 是移动通信网络中唯一能识别移动用户的号码，因此三无验证又被称为去中心化短信认证。德尔塔开发者设计了一套《去中心化短信认证的协议》框架，这是一套完全可靠且去中心化的方案。有关 Internet Computer 的技术背景和更详细说明将在后续的技术方案章节中进行介绍。

3.3.1 验证的流程和规则，验证的流程和规则的概述如下：首先，我们允许满足特定条件的用户申请校验终端权限成为验证者。验证者可以利用闲置的 MSISDN（即移动电话号码）和智能手机，下载并安装德尔塔校验应用。使用 MSISDN 作为接入号码，接收和转发验证字符串。验证者只需确保手机电力和网络连接稳定，验证处理过程将完全由德尔塔系统自动完成。当有大量用户申请并成为验证者时，将形成一个验证终端池。之后，当有用户进行注册、登录或转账等需要身份验证的操作时，德尔塔系统将生成一个验证字符串。用户将从验证终端池中选择一个运行良好的终端，并将该验证字符串以短信形式发送到该终端的接入号码。验证终端在收到验证字符串后，同时提取发送者号码，然后转发到德尔塔系统。最后，德尔塔系统执行验证比对，合法用户的请求将被允许通过。有关更详细的信息，请参阅《去中心化短信验证协议》[iv]框架。

另外，需要额外说明的是：一是在系统尚未形成足够多的验证终端的早期阶段，将由开发者接入一个全球通用的虚拟接入号码，为早期用户提供验证接入。一旦验证者数量能够满足基本需求，这个虚拟接入号码将被移除。二是为了避免用户产生较高的国际短信费用，系统将为需要验证的用户优先显示本国验证接入号码。

图表 1（验证原理图示）



3.3.2 验证者规则部分，我们的设计包括以下几项：

(1) 人数规则：允许每个区域（按照 E.164[v]国家代码分区）的验证者数量上限为总注册人口的万分之一，同时允许最低下限人数为 1000 人。

(2) 质押竞选：要成为验证者，必须通过质押竞选。竞选者需将一定数量的 Delta Coin 投入竞选池，并下载德尔塔验证终端，确保与德尔塔系统连接正常。根据竞选规则，系统将在每个竞选周期（一天）内自动从竞选池中筛选出一定数量的获胜者成为验证者。每个周期最多选出 30 人，同时，筛选出的总人数不能超过区域规定的上限。成功胜出的验证者将获得 90 天的工作周期。

(3) 离线罚没：在工作周期（90 天）内，验证者不得因任何原因离线超过 1 小时，否则其质押资金将被罚没，并重新转入社区挖矿资金池。

(4) 攻击惩罚：对于企图通过攻击行为（如抓包、篡改等）获取他人权限的验证者，系统将罚没其质押资金，并标记为不诚信用户。

(5) 竞选续约：在 90 天工作期满后，验证者可以选择继续参加质押竞选以保持验证服务。质押金额可以与当前服务期内的金额叠加计算。

此外，为诚信验证者提供奖励机制，有关奖励的详细措施将在经济模型部分进行阐述。

3.5 安全圈

在引入 3-No Authentication（三无验证）这一安全验证模型后，数字资产的使用和管理将变得更为安全和便捷。然而，特殊情况下，这种单一验证机制可能会失去其安全性。例如，当移动设备丢失或被他人盗用时，对方可能完全掌握设备的控制权，包括发送验证短信。为了防止这种情况发生后，并保护账户资产的安全，我们在系统的设计中加入了安全圈功能，为账户提供二次身份验证，以增强账户的安全性。

安全圈是基于用户社会关系的验证模型，该功能是完全去中心化的。是通过用户的

社会关系圈帮助其实现安全验证，安全圈功能能够有效地增加恶意攻击的难度，并降低账户被他人获取的风险。

安全圈的工作原理如下：首先，用户可以将可信任的人（一般是亲朋好友）加入到自己的安全圈成员列表，通常为 3-5 人。当账户需要进行安全圈验证时，Delta 智能合约程序将随机从安全圈成员列表中选取一位成员，协助当前用户通过提供安全码的方式进行身份确认。当当前使用者向该成员询问安全码时，被选中的安全圈成员将能够帮助确认用户是否是本人。同时，程序将提示：“如果不是亲友本人的情况下拒绝提供安全码”，以保护账户安全。因此，任何 Delta 用户都应确保安全圈成员列表中的人员是可信任的。

什么情况下需要用到安全圈呢？

①当有用户安装有 Delta 程序的手机丢失时，用户应该需要使用一台新的设备来强制登录 Delta 应用。在这种情况下，用户需要使用安全圈验证来确保其账户的安全性。由于手机丢失，原有的验证状态已经失效，用户需要通过安全圈成员提供的帮助来验证其身份并登录应用。

②当账户进行敏感操作时，如更换手机号码或更新安全圈成员等，为了防止这些操作被他人执行，因此，也需要启用安全圈验证。

3.6 经济模型

在 2.2 章节中提及了现有加密货币在分配上存在的公平性问题，因此德尔塔分配规则的设计需要避免类似比特币的分配方式，即将大部分币量分配给早期参与者。这种分配方式可能导致后期参与者需要以高昂的价格购买，从而使其沦为投机工具。这不仅阻碍了人类货币共识的形成，还可能导致流通价值无法实现。因此，德尔塔分配规则需要采用更加合理的方式来实现。

首先，我们将 Delta Coin 的初始总量定义为 3000 亿枚，相对于其他加密货币，Delta 采用这样庞大的总量设计旨在方便日常生活中的流通和使用。（例如，我们希望将一盒 250 毫升的牛奶定价为 0.3 δ，而不希望 0.0000003 δ 这样，小数点后面过多的零会让人感到困惑）

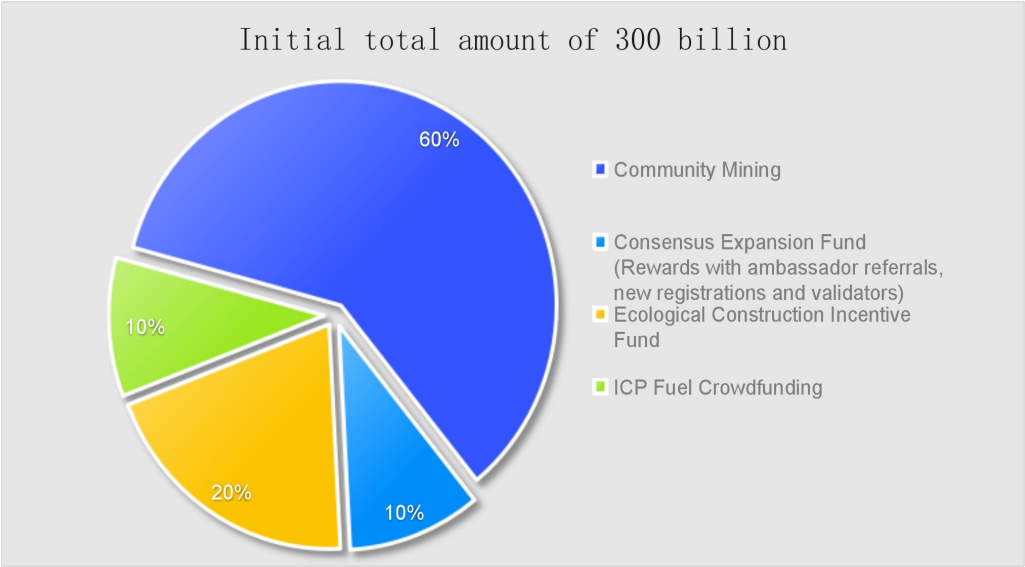
然后，我们将这 3000 亿枚分为四个部分，每个部分发挥不同的作用：

第一部分：社区挖矿——60%

第二部分：共识拓展基金（用于大使推荐、新注册和验证者奖励）——10%

第三部分：生态建设奖励基金——20%

第四部分：ICP 燃料众筹——10%



将币量分为多个部分进行分发的目的在于同步推动社区共识和生态建设的发展，并旨在刺激社区初期生态建设的积极性和确保长期系统运行的可靠性。

关于分配方案的一些额外说明如下：

1. 初始总量和当前的分配方案是在“临时治理模式”下执行的。显然要作为全球共识货币这些总量是不够的。之后可在 DAO 模式下可由 Delta 全员选举的“治理委员会”根据发展的需要商议提出增发提案。

2. 初始的 3000 亿枚货币并不代表它们在之后全部都可以成为可流通的 DTC。这 3000 亿是 Delta Credit（DTCT）的总量，表示在未通过 KYC 激活和释放之前的有效数量。经过 KYC 筛查后，一般来说最终可流通的 DTC 数量通常会小于 DTCT。

3. Delta 以人本货币为理念，理论上应该将所有币量通过社区挖矿和共识拓展方式分配，而其他部分应该通过捐助或手续费的方式筹集。然而，在项目早期，生态建设的需求和工作量非常大，为了确保项目的成功和让生态建设者更有信心，我们实行了预留分配。同样，燃料众筹部分也是为了提供更可靠的运行机制。

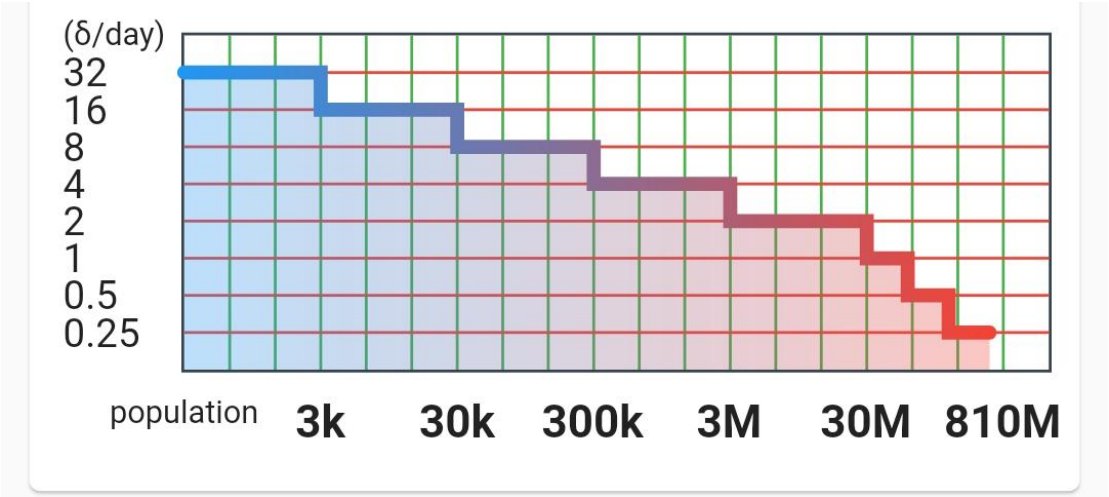
3.6.1 社区挖矿

社区挖矿的总量为 1800 亿枚，等于总量 3000 亿枚的 60%。我们通过用户真人每日签到贡献关注度的方式来分配这些币量。这种方式经过长时间进行后就可以形成共识。其原理是用户通过贡献关注度，将无形的虚拟数字转化为货币共识，这种共识度反过来促进它作为货币的价值。在挖矿基础速率方面，为了在早期激励性和长期公平性之间找到平衡，我们采用了两阶段倍减方案设计。

第一阶段：当参与人数为 1 到 3000 万之间时，1 人到 3000 人之间该速率为 32δ/天，以此作为起步基准。每当人数增加 10 倍时，该速率减半，直到参与人数达到 3000 万时速率降致 2δ/天后进入下一阶段。

第二阶段：当参与人数达到 3000 万及以上后，每当人数增加 3 倍时，该基础速率减半，直到最后挖完停产。

图表 2，（基础速率减半图表解析）



3.6.2 注册与推荐奖励

为了促进德尔塔网络更快的发展，我们专门设置了推荐奖励计划。在成为矿工之后，任何人都可以成为一名推广大使，通过推荐他人来获取这些奖励。

- 推荐固定奖励：为了邀请亲朋好友加入德尔塔，推荐者只需通过二维码或链接分享自己的数字 DID。当对方在注册时填写推荐者的数字 DID 时，双方都将获得 1 δ 的奖励。如果推荐注册发生在社区挖矿停止之后，奖励将会减半，各获得 0.5 δ 。这部分奖励将从 300 亿“共识拓展基金”的总量中分配。
- 直接推荐奖励：大使每直接推荐一人，当被推荐者在处于挖矿状态时，其挖矿速率将提高基础速率的 1/3。另外，当大使的上级推荐人处于挖矿状态时，也将按照此比例计算到直接推荐奖励中。

假设当前基础速率为 16δ/天， 大使已推荐人数为 n，并处于挖矿状态，那么当天这部分提升收益计算公式如下：$16\times \frac{1}{3}\times(n+1)=x$（δ/day）

- 间接推荐奖励：推荐大使直接推荐团队中的每一个人他们再推荐的每一个人都代表大使的间接推荐用户。当一个间接推荐用户处于挖矿状态时，推荐大使的挖矿速率将额外提升基础速率的 1/10。

假设基础速率同上，间接推荐并处于挖矿的人数为 n_2，那么当天这部分提升收益计算公式如下：$16\times \frac{1}{10}\times n_2=x$（δ/day）。直接推荐和间接推荐这两部分奖励将叠加计算，并在 1800 亿社区挖矿总额资金中支配。

3.6.3 验证者奖励

在 3.4 章节中阐述了三无验证的基本原理和流程，为了实现这样的验证程序，系统

需要一部分用户申请成为验证者，同时我们也需要设计一定的奖励来激励这些为此付出的人。验证者的奖励方式和金额是分为两种情况的。

① 首先，当共识拓展基金的 10%还未用完时，验证者的奖励将使用这部分基金来支付，每次完成验证的奖励的具体金额为当前挖矿基础速率的 1/3。

② 另外，当共识拓展基金已经用尽时，验证的费用将由需要验证的用户支付，这个费用将在验证过程完成后自动扣除。这时验证的费用将按日常转账手续费的 3 倍计算。

3.6.4 生态建设奖励基金

为促进德尔塔生态多方面的建设和发展，该基金将面向多个生态建设方面的奖励计划，其中包括：

1. 生态 dApp 开发者奖励计划：旨在激励早期生态开发，对德尔塔生态的贡献以及优质生态项目开发者。更多详情请参阅 dApp 广场章节。
2. 形象及知名度宣传奖励计划：旨在奖励对 Delta 形象及知名度宣传有特别贡献的个人或团队。
3. 早期交易奖励计划：用于奖励在 Delta 应用中参与早期各类交易行为的用户。

在早期“临时治理模式”下，该基金由 Delta 核心团队托管和规划使用。其目标是促进 Delta 各方面生态建设的繁荣和发展。具体用途和规则将根据实际需求进行设计和调整，并在相关用途计划中明确说明。

之后，一旦进入“DAO 治理模式”，核心团队将把剩余的基金转交给 DAO 进行托管。后续的使用决策将由 DAO 做出。

3.6.5 ICP 燃料众筹

这方面的资金分配方式将在燃料机制章节阐述。

3.6.6 手续费

在交易时产生一定的手续费的好处之一是为了防止恶意小额转账而产生大量垃圾记账数据的攻击行为，以保护 Delta 系统的健康运行。另外，Delta 系统的手续费将采用燃烧模式，交易消耗的手续费将直接转入一个空地址中。

在“临时治理模式”下，每笔交易燃烧的手续费为 1‰，同时限制最低为 0.01δ，最高为 0.3δ。在这一模式下，为确保权力不被滥用，不得以任何理由增发新币，相当于在这一模式下是一种通缩机制。

之后，在“DAO 治理模式”下，DAO 可以根据实际需要通过提案的方式实现增发机制，增发的货币可以弥补手续费燃烧部分，阻止进一步通缩。增发的货币用途的第一部分将是支

付 Delta 运行的燃料”cycles”。其他部分可用于治理参与奖励资金和其它有利于生态良性发展的事宜。另外，在长期的 DAO 治理模式下，可通过年度提案来重新确定交易手续的具体额度或规则。

3.7 KYC 验证

KYC（Know Your Customer/Client）验证是一个重要的过程，旨在确认用户的身份，并防止虚假账户的创建。在 Delta 系统中，由于其挖矿机制是基于社交网络和完全去中心化的，因此 KYC 验证尤为重要。为了确保公平分配和杜绝虚假身份挖矿，我们计划采用 AI 识别和社区 KYC 市场结合的方式进行。用户可以通过 KYC 市场实现社区成员匿名交叉互相认证，并设立一定的奖罚机制。这些措施将确保 Delta 系统的公平性和生态健康发展，同时提高用户对系统的信任度和参与度。

首先，AI 识别技术可以用于身份验证过程中，通过深度学习和图像识别技术，对用户提供的身份证明文件进行自动化识别和比对。这样可以大大提高身份验证的效率和准确性，减少人为错误和欺诈行为。

其次，社区 KYC 市场是一种基于去中心化思想的市场机制，通过人为检查和判断防止“人皮面具”和“数字换脸”等行为，可以有效阻止等针对 AI 的欺诈和攻击的发生。用户可以通过这个市场实现社区成员匿名交叉互相认证和确认。在社区 KYC 市场中，用户可以发布自己的身份证明信息，并设置有一定的奖惩机制，鼓励其他用户进行验证和交叉认证。通过这种方式，我们可以建立一个互相监督和信任的机制，确保每个账户的真实性和可信度。

同时，在 KYC 市场人工检查认证过程中，我们采取选择性披露的方式进行。在认证中，选择性披露是指在保证个人信息不泄露的情况下，只向验证者展示验证所需的必要信息，对个人真实性进行验证的过程。 采用这种方式的优点是可以在确保被验证者隐私不被泄露的情况下，能有效地对必要的信息进行验证。Delta 在处理个人信息资料时采用了碎片化分布式存储的方式，这为选择性披露身份认证提供了技术基础。

此外，为了防止恶意行为和虚假账户的创建，Delta 系统还将建立一套严格的监管机制。如果发现可疑行为或违规操作，系统将立即采取相应的措施，如暂停或标记相关账户，阻止流程向下继续执行。

通过以上措施，Delta 系统可以有效地防止虚假账户的创建和恶意行为的发生，确保系统的公平性和可靠性。同时，KYC 验证也可以提高用户对 Delta 系统的信任度和参与度，推动 Delta 生态的健康发展。

之后，当用户获得 KYC 认证后，系统将立刻为该用户释放第一笔 DTC，具体的释放规则参见 3.12 释放机制章节。

3.8 非 KYC 账户

在 Delta 系统中，任何人都没有权限删除或冻结任何账户。应为，早期在编写 Delta 程序时，并没有设计这样的功能或接口，这样更符合去中心化和用户自主的理念。因此，非 KYC 账户是被允许长期存在于系统之中的，并且可以参与交易或互动。然而，通过 KYC 认证的账户会获得特定的标记，未标记 KYC 的账户会被限制某些权利，例如参与 DTCT 资金释放行动、成为交易卖方等。由于未标记 KYC 可能被视为不可信，可能会被某些系统生态子应用或交易对手拒绝。

3.9 燃料机制

首先，所有计算机程序的运行都需要支出电费和硬件成本。例如，对于传统的 Web2 程序，需要在如 Amazon AWS 之类的平台上托管服务并支付资源使用费。区块链也不例外，比特币矿工需要购买昂贵的 ASIC 矿机和支付高昂的电费，他们的这些运行成本就以挖矿奖励和转账手续费的方式反馈给矿工。因此，像比特币这样的加密货币的转账手续费是相当昂贵的。其他的 POS 模式的区块链降低了挖矿（游戏式的算力计算）成本，所以转账手续费也相对下降了，但该模式的治理成本依然很高，最后手续费用仍然较高。

德尔塔也需要运行成本。德尔塔完全运行在由 Dfinity 研发的 Internet Computer 的加密空间(Cypherspace)内。互联网计算机的架构设计对于传统区块链更为先进，运行成本更低。根据官方公布的数据，存储方面的费用大约为 5 美元/GB/年，而且互联网计算机并非使用主权货币计费。相反，它需要一种名为“cycles”的燃料来支持计算操作和存储[vi]。这种“cycles”是通过 Internet Computer （ICP）实用代币的转换生成的。因此，德尔塔需要 ICP 这个实用代币来作为运行成本。

因此，德尔塔需要一种燃料机制来确保其程序的长期运行。根据德尔塔的发展，我们将燃料来源分为 3 个阶段，即启动阶段、共识建设阶段和共识形成阶段。

① 启动阶段——就是在德尔塔部署到无用户的早期阶段，核心开发者将一次性注入 30 ICP 代币到 Internet Computer 智能罐（关于智能罐将在运行环境章节详细说明），以确保程序正常运行，并为即将加入的用户提供服务保证。

② 共识建设阶段——是指从开始运行到还未产生流通价值之前的阶段。在这个阶段，我们在德尔塔的应用广场启动一个“ICP 燃料众筹”子程序，以筹集德尔塔运行所需要的“cycles”燃料。任何用户都可以通过这个子程序为德尔塔筹集转换“cycles”燃料所需的 ICP 代币，程序将根据设定的算法，奖励给参与者对应数量的 Delta Credit 作为对其支持的奖金。这些可奖励的 ICP 代币是总量分配的第四部分（ICP 燃料众筹），共计 300 亿 δ，全部发放完毕后将自动停止众筹。所有众筹到的 ICP 代币将存储到一个没有绑定 MSISDN 的虚拟 DID 中（意味着任何人没有权限操作这个虚拟 DID），德尔塔燃料管理程序会自动监控智能罐中的“cycles”余额，当“cycles”低于 3000 billion 时会自动将虚拟账户中 ICP 的其中 10 枚兑换为 cycles。众筹兑换率的计算结果主要由总用户量和已发放量这两个参数决定的，具体算法公式如下：

定义：

R = 注册量

D = 已发放 Delta Credit 金额

Ex_rate = 当前众筹兑换率

$$a = \log 10(R)$$

$$\mathrm{Ex\_}rate = a \times \log(D, 13 - a) \times 0.0001$$

其中 13 和 0.0001 是一个固定常数。
假设，现在已注册量 R=100000，众筹已发放奖励金额 D=330000 枚，
那么，当前兑换率如下计算：

$$a = \log(\mathrm{R},10) = \log(100000,10) = 5$$

$$\mathrm{Ex\_rate} = a \times \log(\mathrm{D},13-a) \times 0.0001$$

$$= 5 \times \log(330000,13-5) \times 0.0001$$

=0.00305535
即当前：1 *ICP* 可兑换 1/0.00305535 = 327δ (结果采取近似取整)

③ 共识形成阶段——是指完成大规模 KYC 验证并进入“DAO 治理模式”后， DAO 可以根据增发提案，增发一定量的 Delta Coin 弥补交易手续费燃烧，并将增发额度的一部分优先用于兑换燃料”cycles”。

3.10 dApp 广场

dApp 广场是德尔塔的去中心化应用市场，是德尔塔在线生态建设的平台，是面向未来的 Web3 应用中心。任何具备开发能力的用户都可以开发德尔塔应用并入驻，经过社区广泛讨论和投票后，将起草并发布《Delta 应用生态白皮书》。该白皮书将确定开发者奖励政策、道德行为、用户隐私和用户数据自主策略等方面的设计和规范。

3.11 USDT 双币挖矿

USDT[vii]双币挖矿，其含义就是 DTC 与 USDT 两种数字货币同时挖掘。

其目的是在 Delta 生态还没有形成和繁荣的早期阶段，为矿工提供一定的有效收入；同时，也为开发者提供一定的经费支持，确保开发者能够持续长期的提供开发服务，最终能够实现 Delta 规划和愿景；也为广告商提供一种有效的推广渠道，促进共识正向发展。

其原理是利用 Delta 社区庞大的用户群体实现流量变现，为广告商、Delta 核心开发者和矿工提供多方受益。

其方法是接入现有成熟的广告平台，用户可以通过 USCT 挖矿模块的一个“播放按钮”展示激励广告并获取变现收益。

分配机制与结算周期等相关细节可参见 Delta App “USCT 挖矿模块”页面。

3.12 激活与释放机制

在以太坊智能合约出现之后，市场发行了各种五花八门的代币，这些代币的发行大多都有释放激活机制，它们的方式一般是要求用户承诺（或者规定）将代币按一定比例、一定时间周期进行质押，后再按质押周期进行一次或多次释放，释放后的代币可获得自由流动的权利。

这样的设计目的是保障代币价格的稳定和向上，防止代币因大量抛售而造成价值坍塌。其原理是通过时间的延长来获得生态与共识的发展。这样做对早期共识建设和稳定价格的确有一定的帮助，但其作用并不强。因为，这样做会在系统内形成大量的僵尸用户，这些僵尸用户它们什么都不做只是等待时间的到来和价格的暴涨，这样的情况对共识生态的长期建设没有任何帮助。

为此，Delta 重新定义了释放机制，我们将周期与社区行为相结合，即在一个设定周期内并满足一定行为的条件将获得 DTC 释放，我们把这种释放机制称为行为性周期释放。

我们的具体设计方案如下：将账户 DTC 的释放设定为 100 个周期进行，每个周期最少为 7 天，每个周期等额释放，共计 100 期释放完毕。账户在一个周期内完成对应的易货行为后，即可获得释放权利。

具体来说，首先，在大规模 KYC 之前，我们将在 dApp 广场建立一个“跳蚤市场”应用。该应用允许任何 Delta 用户在上面发布和买卖闲置商品。在这个应用上的交易行为将与 DTC 释放程序有机结合。当用户在“跳蚤市场”应用上产生购买或销售的行为时，该行为将自动传导到 DTC 释放程序。符合规则的买卖行为将立即触发释放机制，并完成周期内应有的 DTC 释放。

第一次 DTC 释放将在用户完成 KYC 后立即执行，并释放总额的 1/100。之后，每 7 天，如果用户在“跳蚤市场”应用上发生有效的交易行为，将触发 DTC 释放。每个周期的释放量依次为总量的 1/99、1/98、1/97，直到最后 1/1 释放完毕。

同时，有效的行为需要满足的条件是，不能长期进行单向的买或卖。程序设计中最多连续 3 次单向行为，超出后将不会释放本期金额，直到改变交易方向后恢复。

在周期性方面，实际的程序设计中我们按照连续 14 天内最多 2 次判定为有效释放行动。这样做有助于用户灵活地安排交易时间。在可释放交易行为之外，用户可以参与更多的交易行为，这完全是自由的，并有助于更好的共识建设。

3.13 DID 数字身份

在用户通过三无验证进入 Delta 应用时，系统会为其生成一个全局唯一的 13 位字符串，作为数字身份 DID（去中心化标识符），作为数字身份 DID 不但承载着个人资料和信用值，并且可以管理、接收和发送资产。结合 KYC 的实施，使得用户和 DID 数字身份之间形成唯一、真实可信的绑定关系。

在未来，用户通过 Delta 数字身份 DID 授权和管理其他第三方应用或元宇宙中的数字孪生成为可能。

3.14 隐私保护和可追溯性

如果个人的财产状况被完全公开在交易账本中，可能会引起焦虑、不安、尴尬或羞愧。无论财产是多或少，暴露财产状况都可能会对个人造成不良影响。因此，保护个人隐私的权利不可忽视。

同时，可追溯性在提高数据安全和信任度方面发挥着积极的作用。交易数据的公开透明和可追溯性增加了人们对资产的信任和安全感，使人们不用担心数据被篡改或暗箱操作。

因此，隐私保护和可追溯性同等重要。我们需要一个合理的方法来解决这两个看似冲突的问题。Delta 采用记账地址与 DID 数字身份分离设计，以及 DID 数字身份与记账地址单向关联的措施来解决这个问题。记账地址采用 18 到 19 位基于 Base58 编码的密码学地址，这是一种比特币地址算法的变种，其目的是便于人们与比特币地址区分开来，并节省存储资源。这样，所有的资金和交易都记录在记账地址上，任何人都可以通过 Delta 浏览器查看和追踪交易，但无法查找到记账地址所对应的 DID 数字身份。一个 DID 数字身份下可以创建多个记账地址（为了防止滥用，在一个 DID 数字身份下面创建超过一个地址时，每创建一个地址将会产生一笔交易手续费），并且可以设置一个默认收款地址。用户可以使用任何一个地址收款，同时也可以直接使用 DID 数字身份或手机号码收款。使用 DID 或手机号码收款的金额将自动转入默认地址。这样，用户可以根据使用场景在隐私和便捷性方面任意选择。

3.15 去中心化多链钱包

去中心化多链钱包是 Delta 系统中内置的核心功能之一。Delta 多链钱包使用户能够与其他区块链之间的资产流转、信息互通和应用协同成为可能。它可以方便地接收和发送其他公链资产，当用户管理这些资产时，完全不需要任何私钥、助记词或密码。这种方便易用并安全的特性，主要得益于 Delta 的三无验证协议和基于 Internet Computer 的 ECDSA 门限签名（Threshold ECDSA signatures）技术。ECDSA 门限签名技术允许人们在没有掌握私钥的情况下创建第三方区块链的地址并执行转账。这使得在 Delta 多链钱包中托管的资产非常安全和值得信赖。

互联网计算机实现了一种新颖的门限 ECDSA 协议作为其链密钥签名工具箱的一部分。在此协议中，私有 ECDSA 密钥仅作为指定方持有的秘密共享方片段式存在，即 IC 上支持门限 ECDSA 的子网的副本，并且使用这些秘密共享计算签名，而无需重建私钥。此类子网的每个副本都拥有一个密钥共享片段，该共享片段本身不提供任何信息（事实上，任何达到三分之一门限的共享片段集都无法与一组随机字符串区分开来）。至少三分之一的副本需要使用它们各自的密钥片段来生成门限签名。除了实际的门限签名协议之外，链密钥 ECDSA 还包括安全密钥分布式密钥生成和定期密钥重新共享协议，它们是协议的关键部分。这使得链密钥 ECDSA 签名比任何现成的门限 ECDSA 协议更强大。

互联网计算机的任何子网上的每个容器都可以控制唯一的 ECDSA 公钥，并且可以请求计算此公钥的签名。签名仅颁发给符合条件的容器，即该 ECDSA 密钥的合法持有者。每个容器只能获取其自己的 ECDSA 密钥的签名。请注意，容器本身不持有任何 ECDSA 私钥或密钥共享片段。门限加密技术可以帮助实现区块链信任模型中的功能，而这些功能是单独使用传统加密技术无法实现的。[viii]

3.16 技术方案与实现

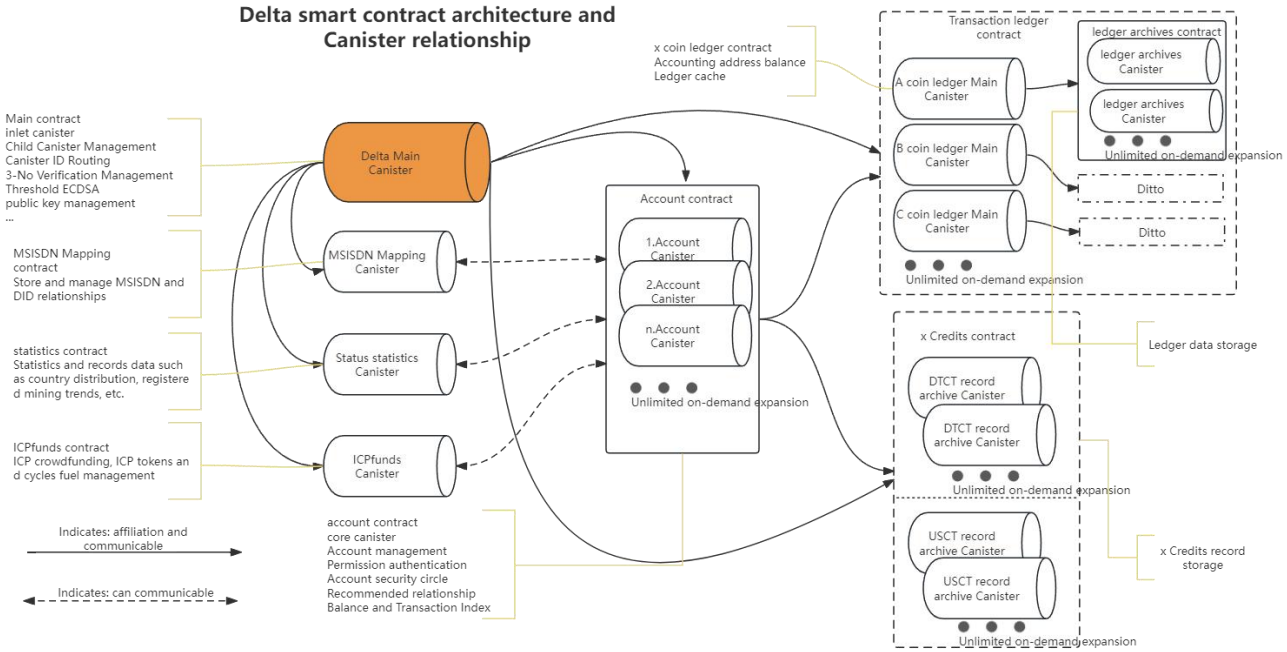
Delta 选择 Internet Computer（IC）作为基础运行环境，并使用 Motoko 编程语言来实现其服务端编码。Delta 系统完善和复杂的功能得以实现，得益于 IC 提供的强大可编程能力和高速、低成本的运营环境。

Internet Computer（IC）是目前世界上最先进的智能合约容器运行平台。这一成果归功于 DFINITY 基金会的创始人兼首席科学家 Dominic Williams，是他带领一大批顶尖的计算机和密码学专家进行了多年研究的成果，为 Delta 的实现提供了强大可靠的基础。

Internet Computer（以下简称 IC）实现了世界计算机的愿景——一个开放和安全的基于区块链的网络，可以以智能合约的形式托管程序和数据，以安全可靠的方式在智能合约上执行计算，并无限扩展。IC 智能合约是在去中心化区块链上运行的可组合且自治的软件部件，这使得它们无法被篡改和停止。IC 摆脱了智能合约在传统区块链上的速度、存储成本和计算能力方面的限制，使智能合约的全部潜力得以释放。IC 允许智能合约第一次实现完全的去中心化。

关于 Motoko 编程语言，它是一种新的、现代的、类型安全的语言，适用于构建下一代分布式应用程序的智能合约，以便在 Internet Computer 区块链网络上运行。Motoko 被专门设计用于支持 Internet Computer 的独特功能，并提供用户熟悉的强大编程环境和能力。

Delta 系统架构图：（该架构会随着功能的增加和变化而调整）



注：canister 是在 IC 中的运行容器和基本单元

3.17 标志与货币符号

- 符号：δ，如 10δ、100δ、1000δ。
- 货币代码：DTC，来源于"Delta Coin"
- 标志图标：一个金色的莱洛三角形轮廓，中央为一个由δ符号抽象而来的绿芽。这个标志象征着财富、稳定、流畅、安全、可靠和希望。
- 节日：为了丰富精神生活，促进 Delta 的交流和发展，我们需要定义一个节日。从 2023 年开始，每年的 3 月 3 日将被定义为 Delta 的节日。同时，当天产生的所有 Delta 交易将完全免除手续费。这个免交易手续费的机制将在开发之初就被设定在程序之中。

4. 未来

4.1 稳定币

无可置疑，主权货币是目前最普及的货币，我们期待德尔塔成为全球未来主流的超主权数字货币。稳定币ix是一种始终与主权货币价格保持一致的加密数字货币。这意味着，从价值层面上讲，在当前法币交易的场景中，它可以直接替换使用。可靠的稳定币是衔接非主权货币与主权货币的桥梁，我们计划设计一种让每个普通老百姓都能参与铸造和运营的普惠化稳定币，这将彻底引发未来非主权数字货币的盛行。我们将在后续的社区讨论和意见征集过程中，争取在 Delta 的基础上建立这样的稳定币。

4.2 开源方式

为了确保系统的透明度、公正性和公开性，并得到更广大社区的支持，成为全人类共同的货币系统，Delta 的开源将势在必行。整个 Delta 系统需要由多个部分和多个软件项目组成，这些部分需要在不同的环境中运行，例如以服务端的形式运行在 Internet Computer 上，以客户端的形式运行在安卓或 IOS 设备上，或以 WEB 形式。为了保护 Delta 生态并防止源码被滥用，我们将根据发展的需要逐步开源部分软件项目。预计在用户总量达到世界人口总量的 1/30 时，我们将完全开源。

4.3 治理与升级

为了建立一个持久的治理模型，并在效率与公正方面找到平衡，Delta 将采取两个阶段的计划。

4.3.1 临时治理模式

在系统开源之前，将采用一种“临时治理模式”，类似于当前主流的“链下”治理模式。在这种模式下，核心开发者在系统开发和发展方向方面发挥着非常重要的作用。Delta

将首先启用一个“路线图”子程序，开发者会先将已经完成的部分、正在进行的部分和计划开发的部分发布在“路线图”中。此外，“路线图”子程序还将具备建议和投票的功能，任何 Delta 社区的成员都可以通过这个功能来反馈意见和提出建议。最后，核心开发者将根据这些意见和建议进一步更新路线图。这种模式可以保证效率和公开性，但在公正和持久方面非常依赖于核心开发者。

4.3.2 DAO 模式

在系统完全开源后，将采取“去中心化自治组织（DAO）模式”。在 DAO 模式下，Delta 将根据用户全员投票选举的方式成立一个“治理委员会”和一个“开发者委员会”，并依赖于一个服务神经系统（SNS）。治理委员会成员将通过这个 SNS 系统发布和投票提案，最终投票通过的提案将由“开发者委员会”成员接手并实现该提案的开发。实现完成后，再交由“开发者委员会”评审并投票，投票通过后将由 SNS 执行新版本的程序发布。这个过程的执行流程将由 SNS 控制。另外，将成立一个“治理和开发者奖励基金”，以奖励为 Delta 投入时间和精力的治理者和开发者。“治理和开发者奖励基金”的费用主要来源于交易手续费燃烧后从新增发额度的一部分和原始“生态建设奖励基金”的剩余部分。

在形式上，为了提高人们对每次升级的重视程度和表达每次升级的重要性，Delta 将采取与全球河流相关的命名方式来为每个重大版本升级命名。具体来说，Delta 将使用全球河流长度排名前 100 的河流名称，按照顺序依次作为每个重大升级的版本名称。这一计划的采用源于“Delta”一词在地理名词中的含义，它恰好指的是大型河流下游入海口的冲击三角形平原地带。

根据《维基百科》数据目前河流长度排名列表，前 100 名为尼罗河、亚马逊河、长江.....托坎廷斯河。

4.3.3 提案类型

在 DAO 模式下主要通过提案的方式来改善系统的运行参数和升级，我们把提案主类型分为年度提案和日常提案。

年度提案：代表着一项一年只能修改和执行一次的提案。为了赋予这一过程更多的仪式感，我们决定在 Delta 的节日（3 月 3 日）执行年度提案。通常，年度提案涉及的是影响广泛的系统参数的修改，例如交易手续费的修改等。

日常提案：其它提案都可为日常提案。

最后：

Delta 的设计与创建并非空穴来风，Delta 是站在无数货币变革者和呐喊者的肩上取其智慧，总结其经验的结果。 Delta 的灵感主要来源于《货币的非国家化》、“比特币”、“以太坊”、“Internet Computer”、《Pi 白皮书》等相关书籍、文献、和项目。在此对 “弗

里德里希·哈耶克”、“中本聪”、“维塔利克·布特林”、“多米尼克·威廉姆斯”、“尼古拉·科卡利斯 和 范成道 夫妇”等作者表示鸣谢。同时，也感谢所有在区块链和非主权货币领域行动和付出的每一个人，感谢大家。

Haida 于 2023 年

参考文献：

[i] Triffin Dilemma：https://en.wikipedia.org/wiki/Triffin_dilemma

[ii] Cambridge Centre for Alternative Finance：https://ccaf.io/cbnsi/cbeci

[iii] Pi Network：https://github.com/pi-apps

[iv] Decentralized SMS Verification : https://github.com/delta-kim/document/blob/main/DecentralizedSMSVerification%20protocol_en.md

[v] E.164: https://en.wikipedia.org/wiki/E.164

[vi] Gas and cycles cost of IC: https://internetcomputer.org/docs/current/developer-docs/gas-cost/

[vii] USDT: https://en.wikipedia.org/wiki/Tether_(cryptocurrency)

[viii] Threshold ECDSA signatures: https://internetcomputer.org/docs/current/developer-docs/integrations/t-ecdsa/

[ix] Stablecoin: https://en.wikipedia.org/wiki/Stablecoin

[x] List of global river length rankings：https://en.wikipedia.org/wiki/List_of_river_systems_by_length