CyberMiles DPoS 协议

免责声明

Cybermiles Foundation Limited（“CyberMiles”）是一家在香港注册的基金会，本文包含了对 CyberMiles 的信念的前瞻性陈述，以及 CyberMiles 的一些假设和 CyberMiles 所获得的信息。对于任何计划、未来预测、前景的完成及合理性，任何人概不提供任何陈述或保证。当 CyberMiles 平台完成时，可能与本文所述有所不同。

此外，关于本文所述的信息、陈述、意见或其他事项的准确性或完整性，任何人不做任何声明和保证。本文中的任何内容都不应被视为对未来或投资建议的承诺或陈述。在适用法律允许的最大范围内，即便有任何疏忽、违约或疏于护理，任何因本文引起的任何损失或损害(无论是否可预见)的所有责任，或其任何方面，均应免责。在责任可以受到限制但未能完全免除的情况下，将在适用法律允许的最大范围内免责。

本文所表达的观点和意见仅是 CyberMiles 的观点和意见。这些观点和意见不是建议，也不是任何形式的要约或恳求，也不应出于被任何目的而被依赖。CMT 和 CyberMiles 平台没有意向在任何司法管辖范围内发行或构成证券或任何其他受监管的产品。请获取必要的专业意见。

I. CyberMiles 的愿景是什么?

CyberMiles 致力于建立一个类似以太坊，但为促进电商交易进行了显著优化的智能合约平台。CyberMiles 区块链能够让人们创建并执行由计算机代码实施的商务合约。我们的目标是建立一个网络时代原生的电商生态系统：

- 没有热衷寻租的中心化垄断；
- 更公平地分配网络产生的奖励;
- 通过经济激励来强化网络效应。

CyberMiles 将是新一代的电商网络，该网络对买家来说更实惠（包括商品价格和融资选择），对卖家来说可以获得更多的收益流（如数据变现、供应链融资和消费者贷款）。

II. 什么是 PoS 机制?

中本聪发明比特币时，一个重要的观点就是要建立这样一个经济体系：“加入并建设网络”比“攻击网络”更有利可图。在比特币系统中，用来抵御攻击的一种机制称为工作量证明（Proof-of-Work）或 **PoW** 共识。然而，多年来，PoW 共识机制的问题愈发明显，它不仅效率低下，同时浪费了太多能源。

为了解决 PoW 的问题，提出了一种名为权益证明（Proof-of-Stake）或 **PoS** 的新共识机制。PoS 系统允许每个 token 持有者对每个新的区块进行投票。新区块的提议者是随机选择的。每个账户的投票权重占比与其 token 持有量成正比。这一设计是为了激励 token 持有者，尤其是持有大量 token 的人，参与投票，以确保网络安全。有了投票，区块链可以用最少的计算量验证区块。新区块被接受后，其提议者可获得区块链的加密货币作为奖励。这个过程被称为“**铸造**”新的加密货币，而不是 PoW 的“**挖矿**”。PoS 系统通常比 PoW 系统性能更高。

然而，传统的 PoS 系统也存在两个显著问题，第一个问题仍然是性能。所有 token 持有者都可以运行区块链节点来进行提议及投票处理区块，但大多数 token 持有者没有专业知识或足够的预算，无法达到运行高性能节点所需的计算机硬件和软件要求。因此，区块链网络速度取决于其系统中最慢的节点。第二个是“无成本权益投票”的问题，即 token 持有者可以通过同时投票给两个存在竞争关系的新区块来作弊。

III. 什么是 DPoS 机制?

授权股份证明机制（DPoS）是对 PoS 机制的改进，类似于人类社会中土地拥有者的代议制民主。在 DPoS 机制中，token 持有者投票选出几个代表，即“**验证人**”，来代表所有 token 持有者运营网络。验证人运行**超级节点**，也就是专业运行的网络服务器，来保证区块链网络的安全和性能。这就解决了 PoS 的性能问题。

投票以投 token 的形式进行。权益投票（以下简称“投票”）的 token 会被网络锁定。当验证人有不当行为时，权益投票的 token 可能被削减。权益投票的 token 不会转移给他们投票的验证人，仅作为投票权的证明，并激励 token 持有者选择负责任且有能力的验证人来维护区块链。潜在的惩罚解决了“无成本投票”的问题。

CyberMiles 相信 DPoS 机制是高性能且安全的区块链共识的未来。

IV. CyberMiles 的 DPoS 如何运行

授权股份证明机制（DPoS）是 CyberMiles 区块链网络中至关重要的经济机制，用于奖励帮助维护网络协议安全和公正的 token 持有者。CyberMiles 的 DPoS 协议中有两个角色：**权益投票人**和**验证人**。

A. 权益投票人和验证人

选择成为权益投票人的 CMT 持有者可以通过投票机制锁定，也就是说**权益投票** CMT，参与到区块链网络治理中。权益投票的 CMT 必须由网络保管，不能交易或转让，因为当治理失误的情况出现时，这部分的 CMT 将会被削减。作为回报，网络每产生一个新区块，权益投票人就可以获得因系统性增发和网络新产生的每个区块的交易费而新铸造的 CMT。 这些 CMT 称为**区块奖励**。

权益投票人自己通常没有能力或者不愿意运行真正为区块链网络提供动力的计算机服务器。因此，权益投票人通过将 CMT 投票给特定的验证人候选人，即**雇佣**，也就是说**选举**其他 CMT 持有者或**验证人**来完成此项工作。验证人负责维护重要网络基础设施，并代表他们的权益投票人做规则变更和治理决策。由于 CyberMiles 系统中只有 19 个验证人，因此验证人必须通过竞争获取权益投票人的选票（即权益投票的 CMT）。这些竞争包括提供能够运行最新软件的安全服务器，提供足够的计算能力和网络带宽，为 CyberMiles 的全球性区块链网络提供动力。

权益投票人将他们的区块奖励中的一部分支付给验证人。 每个验证人在区块奖励中的份额

称为**验证人报酬**。验证人在宣布竞选时就要宣布其默认报酬率。默认报酬率是所有权益投票人必须为此验证人支付的最高报酬率。 但是，一旦权益投票人投票给了验证人，验证人可以选择自愿降低该权益投票人的报酬率。 验证人的这一行为是对社区做出重大贡献的权益投票人的认可。

如果验证人有不当行为并试图损害网络时，网络可能会削减其投票的 CMT，那么就导致其权益投票人遭受损失。这样可以激励权益投票人只投票给声誉良好且值得信赖的验证人，从而提高整个网络的安全性。

在 CyberMiles 协议中，一个验证人的所有 CMT 投票中的 10%必须是验证人自己持有的 CMT。此举是为了确保每个验证人自身也承担风险，因为验证人自己的 CMT 也存在被削减的风险。因此，验证人同时也是自己的权益投票人。

除这 19 个验证人外，CyberMiles 区块链还有 5 个**备用验证人**，以防验证人卸任、被黑客入侵或由于其他原因被削减后不能继续当验证人。备用验证人同样由选举他们的权益投票人支付报酬。验证人的报酬和自我投票概念都适用于此。CyberMiles DPoS 协议将所有的区块奖励分为两部分：验证人及其权益投票人共获得总区块奖励的 90%；备用验证人及其权益投票人共获得 10%。权益投票人能够根据验证人和备用验证人之间 CMT 得票状况找出平衡点 。我们预计备用验证人的合计投票数量占比会超过总权益投票数量的 10%，这意味着，相对验证人来说，备用验证人及其权益投票人投票的每个 CMT 收益相对较低。这是因为备用验证人承担的削减风险较低。

下表展示了验证人和权益投票人通过 DPoS 机制参与网络治理的责任、风险和回报。

	奖励	责任和风险
权益投票人	通过在网络中投票 CMT 获得区块奖励。	无法交易权益投票的 CMT。如果其投票的验证人行为不当，存在一定被削减的风险（最多为投票量的 1.2%）。
验证人	通过验证区块，从权益投票人的区块奖励和自身投票的 CMT 区块奖励中获得验证人的报酬。 参与网络治理。	无法交易自我权益投票的 CMT。 负责精密的 IT 系统运营，存在被黑客攻击和因作恶被削减的风险。
备用验证人	从权益投票人的区块奖励中获得验证人报酬，并获得自我权益投票的 CMT 区块奖励。	负责精密的 IT 系统运营，作为验证人的替补。

A1. 投票权

区块奖励根据投票权分配给权益投票人和验证人。权益投票人的每个权益投票(stake)都有一定的投票权（voting power)。每个验证人的投票权(voting power)是其当前所有权益投票（stake）的投票权（voting power）的总和，整个系统的投票权（voting power）是所有验证人投票权（voting power）的总和。

定义集 1:

- $S_{ij}(t)$ 是权益投票人 j 在时间 t 将投票给验证人 i 的 CMT 数量。 当前时间是 t = 0，而 t = x 对应过去的 x 天。验证人 i 有 n 个权益投票人，包括验证人自己。
- $S_{ij}(t)$ 是权益投票人 j 在时间 t 权益投票给验证人 i 的调整后数量。下表中展示了是如何计算的。
- $S(t)$ 是在时间 t 权益投票给所有验证人的 CMT 的总量。它也可以表示为 $\sum_{i=1}^{m}\sum_{j=1}^{n} S_{ij}(t)$。$S(0)$是当前时间用于投票的 CMT 总量。
- T_{ij} 是权益投票人 j 从当前时间算起一直投票支持验证人 i 的加权时间。如果权益投票人保持或者增加其权益以投票，随着经过的时间增加。但是，如果权益投票人撤销其部分权益投票，，T_{ij}作为 S_{ij}的一部分按照相对于撤销投票的数量按比例被降低。
- T_i是从验证人 i 宣布参与竞选并投票自己宣布票数的 10%之后，经过的时间。

CyberMiles 协议不鼓励任何验证人规模过于庞大。如果单一的验证人的权益投票增加到 c 超过整个权益投票网络的 12%，该验证人会导致网络不稳定。因此，网络协议将该验证人的 $S_{ij}(t)$ 往低调整到 $S'_{ij}(t)$. T 这个限制激励有大量 CMT 的持币人将投票多样化并权益投票给多个验证人，这还会激励验证人限制他们可接受的最大投票总量。

$$S'_{ij}(t) = \min\left(S_{ij}(t),\ S_{ij}(t) \cdot \frac{12\%}{\sum_{j=1}^{n} S_{ij}(t)/S(t)}\right)$$

验证人 i 的权益投票人 j 的当前投票权表示为 V_{ij}。通常，投票权随着当前权益投票的 CMT 数量的增加而增长。 但投票权也取决于该权益投票人的投票历史。

$$V_{ij} = \left(\frac{\int_{t=0}^{10\ days} \sum_{j=1}^{n} S_{ij}(t) \cdot dt}{\max\left(\left\{\sum_{j=1}^{n} S_{ij}(t) : t = 0, \ldots, 90\ days\right\}\right) \cdot 10}\right)^2 \cdot \log_2\left(\frac{T_{ij} \cdot [T_{ij} < 180\ days]}{180\ days} + 1\right) \cdot \left(1 - \frac{1}{4n+1}\right)^2 \cdot S_{ij}(0)$$

等式右侧（RHS）的第一个因式是奖励验证人层面权益投票数量的增长。如果验证人在过去 10 天内增加了总权益投票量（total stake），那么她的所有权益投票人都将获得投票权(voting power)增长。但是，如果验证人的总权益投票量在过去 10 天内下降，她的所有权益投票人投票权相对下降。验证人层面因式收到权益投票人的集体博弈策略影响，但是不由任何单个的权益投票人决定。

RHS 的第二个因式是奖励忠诚度。一个全新的权益投票人获得零投票权。随着时间的推移，权益投票人如果不撤销投票，将逐渐获得更多的投票权。验证人自我投票的 CMT 在此因式中可获得最高的投票权。当权益投票到 180 天时，第二个因式达到最大值 1，不再增长.

RHS 中的第三个因式基于验证人的权益投票人数量来影响投票权。验证人的权益投票人数量越多，则投票权越高。这样促使投票可以来自不同的权益投票人。权重在 0 到 1 之间。

- 若 n = 1，权重为 0.64;
- 若 n = 5，权重为 0.91;
- 若 n = 10，权重为 0.95;
- 若 n = 20，权重为 0.97;
- 若 n = 40，权重为 0.98

RHS 的最后一个因式是投票数量。投票权，权益投票人的区块奖励和验证人从中得到的报酬都与 CMT 的投票数量成正比。投票数量越多，获得的奖励就越多。当然，个人的实际投票权取决于系统中其他人的行为，因为前三个因式都是全球性范围因式。

A2. 区块奖励份额

任何权益投票人和验证人的区块奖励份额取决于当前的总投票权，为正式和备用验证人保留的奖励池，以及每位权益投票人的验证人报酬率。下一组方程式解释了分配给权益投票人和验证人的区块奖励的份额。

定义集 2:

- C_{ij} 是验证人 i 的权益投票人 j 的报酬率。 正如我们所提到的，验证人可以调整其权益投票池中各个权益投票人的报酬率。
- $R_r(i)$ 是区块奖励池中保留给 i 这类的验证人的部分。 例如，验证人为 0.9，备用验证人为 0.1。

在每个区块中，每个验证人和权益投票人得到的区块奖励份额如下.

$$验证人i的区块奖励份额 = \frac{\sum_{j=1}^{n}(V_{ij} \cdot C_{ij})}{\sum_{i=1}^{m}\sum_{j=1}^{n} V_{ij}} \cdot R_r(i)$$

$$验证人i的权益投票人j的区块奖励份额 = \frac{V_{ij} \cdot (1 - C_{ij})}{\sum_{i=1}^{m}\sum_{j=1}^{n} V_{ij}} \cdot R_r(i)$$

区块奖励的来源是验证人投票决定的通胀率（每年最高可达 8%）和从区块交易中收取的 gas 费。在实际操作中，我们可能会选择以小时甚至以天为单位计算和分配区块奖励。

A3. 推论

该计算投票权的公式，就验证人和权益投票人潜在报酬，可以得出下列推论。

推论 1：验证人能够在自我权益投票之外吸引越多的权益投票，验证人得到的报酬越多。

推论 2：如果验证人有多个权益投票人，并且每人权益投票数量比较少，验证人得到报酬越多。

推论 3：如果验证人分时间增加其总权益投票数量，那么验证人及其权益投票人都可以获得更多的报酬。

推论 4：如果权益投票不中断，权益投票人及其验证人获得的报酬会每天增加，增长到第

180 天到达最大值不再增加。

基于权益投票机制的工程设计，验证人可以通过改变单个权益投票人的验证人报酬率来激励某些权益投票人的行为。

这种投票权算法可能会受到 Sybil 攻击的影响。权益投票人和验证人会发现，小规模的权益投票能够创造更多的利润和虚假增长。因此，一个权益投票人可能拆分成许多小账户并分时间进行权益投票。CMT Cube 能够减轻 Sybil 攻击，下文 D 小节有讨论。一旦区块链网络达到运营稳定，Sybil 攻击的难度将显著增加。

A4. 验证人和权益投票人报酬示例

详细计算验证人和权益投票人的报酬是非常复杂的，并且取决于许多外部因素，例如其他人的权益投票行为。然而，在本节中，我们将通过研究简化的场景来说明潜在的 ROI。我们的假设包括以下内容：

- 系统已经达到平衡状态
    - 所有的权益投票至少持续 180 天，并拥有完全投票权
    - 对所有的验证人来说，没有增加新的权益投票
- 每一个验证人有相同数量的权益投票人
- 所有的权益投票人+验证人组，有相同的验证人报酬率
- 交易中的交易费可忽略不计

定义集 3:

- $Total(t)$是在时间 t 的 CMT 总数量。$Total(0)$ 是当前 CMT 的总数量。
- I 是系统年通胀率。
- C是整个系统的验证人报酬率。
- SSR是验证人自我投票比率。
- $R_s(i)$ 是给验证人 i 的类型（正式或备选）的权益投票数量，占所有权益投票数量的百分比。由于块奖励仅分配给参加权益投票的 CMT，因此需要这一数值。

以下公式计算了在不同情况下验证人和权益投票人的自己账户中投票的每个 CMT 的年收益。

$$\textit{验证人收入/CMT} = \frac{I \cdot Total(0)}{S(0)} \cdot \left(1 + \left(\frac{1}{SSR} - 1\right) \cdot C\right) \cdot \frac{R_r(i)}{R_s(i)}$$

$$\textit{权益投票人收入/CMT} = \frac{I \cdot Total(0)}{S(0)} \cdot (1 - C) \cdot \frac{R_r(i)}{R_s(i)}$$

下表展示了如何在不同情况下应用上述公式来计算权益投票人的区块奖励和验证人的报酬。表中列出是每年每投票 100CMT，验证人和权益投票人的收入。简单起见，表格中假定$\frac{R_r}{R_s} = 1$，这意味着备用验证人获得总投票 CMT 的 10%，这种情况下备用验证人的收入与正式验证人相同。

验证人报酬占区块奖励的百分比（C）		如果是 50%		如果是 20%	
投票比率(全部/S)	验证人自我投票的比例（SSR）	验证人(CMT)	权益投票人(CMT)	验证人(CMT)	权益投票人(CMT)
25%	10%	176	16	90	26
25%	20%	96	16	58	26
25%	40%	56	16	42	26
50%	10%	88	8	45	13
50%	20%	48	8	29	13
50%	40%	28	8	21	13
75%	10%	59	5	30	9
75%	20%	32	5	19	9
75%	40%	19	5	14	9

注释：

1. 第一列“投票比例”是指 DPoS 权益投票占总 CMT 供应量的百分比。例如，最初 CMT 总量为 10 亿，因此 25%意味着 CMT 持有者参与 DPoS 机制权益投票的总量为 2.5 亿 CMT。
2. 我们假设系统的年通胀率是 8%，这是区块奖励的来源。
3. 验证人收入=验证人报酬+自我投票产生的 CMT 区块奖励
4. 权益投票人收入=权益投票的 CMT 产生的区块奖励 - 验证人报酬
5. 验证人投票比例不得超过“全网总权益投票 CMT”的 12%。 如果验证人超过这个限制，验证人与权益投票人的收入都会下降。存在这个限制的原因，参见 B4。

当权益投票 CMT 的人减少时， 8%的通货膨胀奖励在更少的主体之间分配，验证人和权益投票人的收入都会增加。当验证人自我投票更少 CMT 并从其他权益投票人的投票中获得报酬时，其自我投票的每个 CMT 收入则会上升。但是，正如前文提及，每个验证人自己的权益投票量至少占其权益投票总量的 10%。

接下来，计算在有风险溢价时，验证人可获得相对于备用验证人的收入。在下表中，我们假设验证人的报酬率（C）为 20%，总投票 CMT 的 30%用于备用验证人（Rs）。回想一下，备用验证人及其权益投票人共获得总区块奖励（Rr）的 20%。30%的投票比率意味着每个投票给备用验证人的 CMT 将比每个投票给验证人的 CMT 产生更少的收入。权益投票人投给备用验证人，是因为备用验证人被削减风险较低。

投票比例（全部/S）	验证人自我投票的比例（SSR）	验证人（CMT）	权益投票人(CMT)	备用验证人（CMT）	备用权益投票人（CMT）
25%	10%	103	30	60	17
25%	20%	66	30	39	17
25%	40%	48	30	28	17
50%	10%	51	15	30	9
50%	20%	33	15	19	9
50%	40%	24	15	14	9
75%	10%	34	10	20	6
75%	20%	22	10	13	6
75%	40%	16	10	9	6

B. 持续的验证人选举

一旦网络（主链）启动并且开始运行，验证人就可以当选或者落选，实时进行。任何情况下，获得最多“投票权”（用获得权益投票的CMT数量衡量）的前19位验证人候选人，视为由权益投票人“雇佣”为验证人。排在第19名到24名的验证人候选人被选为备用验证人。

B1. 宣布参选

验证人候选人向网络社区宣布参与竞选。宣布竞选时需要给出以下 3 条信息：

1. 运营和资质的详细信息，包括司法辖区，数据中心位置，安全部署和技术部署。CyberMiles 基金会将评估所有验证人候选人，并公示符合基金会标准（即信息准确性，技术能力和硬件/网络设置）的候选人。 然而，token 持有者可以自由地权益投票给参与任何候选人，无论候选人是否符合基金会标准。
2. 愿意接受权益投票 CMT 的最大数量。为了防止任何单个验证人规模变得过大以至于产生垄断风险，网络协议会惩罚规模过大的验证人和其权益投票人。（参阅“B4.区块奖励和验证人报酬”部分）
3. 验证人向其权益投票人要求的报酬比例。例如，约定 40%意味着权益投票人赚取的所有区块奖励的 40%会支付给验证人作为报酬。

B2. 候选人接受资格

在新候选人宣布竞选时，网络会立即从候选人账户中抽出其宣布的最高权益投票额度的10%，作为自我投票。

如果候选人没有权益投票最高额度的 10%，则会参选失败。当然，验证人可以在之后增加自己 CMT 的投票数量。

CyberMiles 基金会将审查候选人的信息。如果基金会验证了其信息的准确性，则在链上标明该候选人是“已验证的”。CMT 持有者可以投票给任何他们喜欢的候选人，包括未经验证的候选人，但是经过基金会验证的候选人，更能赢得 CMT 持有者的权益投票。

B3. 权益投票和解除权益投票

验证人候选人在社区中进行宣传活动，并要求持币人参与权益投票（即持币人雇佣验证人候选人成为验证人）

CMT 持有者（权益投票人）将他们的 CMT 投票给验证人候选人。需要注意的是，权益投票的 CMT 不能交易，并且一旦投票，权益投票人之后想要再次交易，必须申请解除投票，并等待一周。

设置一周等待期是为了防范"长距离双花攻击"

注释：

在网络运行的第一年，所有的权益投票人都必须通过专门的硬件设备（也叫 CMT Cube）来投票 CMT。这是为了在网络启动的关键时期保证网络稳定和资金安全。CMT Cube 将是免费的，区块链权益投票协议也将在第一年后向所有人开放。想要了解更多参见本文最后一章。

B4. 区块奖励和验证人报酬率

一旦验证人候选人获得的权益投票进入了前 19 名，他就会成为验证人，并且其所有的权益投票人都将开始获得区块奖励（约每 10 秒出块）。该奖励包含两部分：

1. 系统的年通货膨胀率为 8%。通货膨胀新铸造的 CMT 分配给权益投票人。
2. 权益投票人还将得到区块链中重度用户支付的交易费用。

首先将系统总区块奖励按照权益投票人投票比例分配给每位权益投票人。然后，系统根据验证人的报酬率自动向验证人和权益投票人分发区块奖励。这些奖励会默认添加到权益投票中。当权益投票人和验证人取回 CMT 进行交易时，他们需要申请解除权益投票并等待一周。

验证人可以随时放弃其验证人资格。一旦某个验证人退出，权益投票 CMT 数量排名紧随其后的候选人将成为验证人。当验证人退出时，所有权益投票给他的 CMT 将在一周等待期后自动解锁。在整个权益投票期间，权益投票人 CMT 的所有权没有转移。

B5. 削减和惩罚

当验证人变得不可用或产生与其他验证人不同的结果时，系统将在每个区块（每 10 秒）中削减并燃烧其全部权益投票的 0.1%（即验证人和所有权益投票人都将损失 CMT）。连续削减 12 次后，系统将移除验证人，并会选出下一个验证人候选人。也就是说，在验证人行为不当的情况下，权益投票人最多被惩罚权益投票的 1.2%。

被移除的验证人不会再遭受削减的损失，但其权益投票人也不会获得任何区块奖励。其权益投票人可以要求解除权益投票，然后在一周等待期后重新投票他们的 CMT。

C. 初始验证人选举

当 CyberMiles 主链上线时，需要从 19 个验证人开始，这些验证人也被称为创世验证人。然而，类似“鸡和蛋”的问题是，在主链上线之前没有办法进行权益投票。

为了解决这个问题，在主链发布前，CyberMiles 基金会将根据每个验证人候选人预计的投票权力和其对社区的贡献与社区一起选举创始验证人。选举过程将公开透明并采用公开的评分机制。评分标准包括：

- 候选人愿意权益投票的 CMT 初始数量（至少为其宣布的最大值的 10% —— 见下文）
- 要求从权益投票人处获得的验证人报酬率
- 来自社区的权益投票口头承诺
- 运营实体（entity）的声誉
    - 官网
    - 公司信息（团队简介、主要员工列表及照片以及相关背景资质）
- 社区的规模和活动（例如，Twitter, Telegram, Medium 等关注量和互动量）
- 验证人的地缘政治多样性（没有被充分代表的国家的候选人将获得更高的权重）
- 承诺会根据基金会设定的技术标准来运行验证人节点（总开支和技术计划;硬件扩展计划）
- 社区发展计划（验证人候选人的价值路线图，社区项目时间表，财务状况，透明度或其他任何候选人认为重要的主题。）

- 测试链上可操作的节点，以用于社区参与测试网络

要参与创世验证人选举，每个候选人必须：

- 宣布其接受的 CMT 权益投票数量上限
- 将最大限额的百分之十存储在自己的账户中，在创世时刻作为对自己的权益投票
- 宣布验证人的报酬率
- 披露组织或个人的详细信息

一旦 CMT Cube 设备分配给了 CMT 持有者，则持续的验证人选举开始。CMT 持有者将使用 CMT Cube 为他们想“雇佣”的验证人投票。

D. 关于 CMT Cube

CMT Cube 是一个家庭使用的设备，在 CyberMiles 网络运行的第一年，专门为促进 CyberMiles 验证人选举设计。这是一个硬件设备，同时扮演着 CMT 钱包(即存储和管理一个 CMT 帐户)，以及权益投票 CMT 以选择验证人（验证节点）的角色。用户界面（UI）非常容易使用，显示最新的收益(权益投票人的区块奖励)。家用硬件钱包比基于网络或基于手机的软件钱包要安全许多，因此它是持有和存储大量 CMT 的理想选择。

CMT Cube 硬件由一个用于管理关联帐户中的 CMT 的 LED 触摸屏，存储私钥信息的安全芯片和运行定制版 Android 的移动计算机组成。它使用的电力很少，并且只有当用户要对帐户进行更改时才需要打开(例如，检查帐户余额、存储和取出 CMT、投票或撤销投票给验证人等)。

从长远来看，任何 CMT 持有者都可以通过网络提供的开放式软件 API 来投票他或她的 CMT。但是，在网络启动期的关键时期，网络很容易受到攻击，CyberMiles 基金会必须发挥积极作用，确保验证人选举不受攻击和欺诈。对硬件设备的要求为验证人选举过程创建了额外的安全措施。例如，由于 Cube 具有预付成本（将在一年内全部返还因而最终免费），并每台容纳的 CMT 具有上限（100,000 个 CMT），持有大量 token 的人很难将 token 分散进数百个 CMT 帐户以暗中操纵选举。该设备必须持有并投票的下限是 1000 CMT，以防止 DDoS 攻击或者 Sybil 攻击（参见第 A3 节），即使用少量投票去滥用系统。

分发给权益投票人的区块奖励将自动显示在 CMT　Cube 用户界面上。由于 CMT Cube 是参与验证人权益投票的唯一方式，因此它是目前 CMT 持有者获得权益投票人奖励的唯一方式。

如“验证人和权益投票人报酬”表中所示，每个 CMT Cube 的预期收入（权益投票人的收入）与 CMT 权益投票数量成正比，并且与多种非线性因式例如全网总权益投票 CMT 和验证人报酬率，权益投票人的多样性，最近增长以及权益投票人的忠诚度相关。我们通常预计权益投票人的收入将高于系统通货膨胀率（目前每年为 8%）。

CMT Cube 将仅在 cybermiles.io 网站上销售，并用 CMT 定价。

第二种 CMT Cube 称为“CMT Enterprise Cube”。是为大型权益投票人权益投票专门设计的通用计算设备。每个权益投票人帐户中权益投票的下限是 100 万 CMT，并且可以权益投票给多个验证人。

V. 关键参数

术语	值	描述
年通胀率	最多 8%	系统将“新”CMT 的数量作为权益投票人和验证人的区块奖励。 实际通胀率由验证人投票决定，但不应超过每年 8%。
最低自我投票比率	10%	验证人所有得票的 CMT 数量中必须来自自我投票的部分。
验证人规模限额	12%	在系统减少单个验证人及其权益投票人的区块奖励之前，单个验证人可以获得全部网络权益投票的限额（软顶）。
验证人数量	19	得票数量最多的前 19 名候选人成为验证人。 他们的权益投票人会得到区块奖励。
备用验证人数量	5	CMT 权益得票数量排名在第 20 至 24 之间的候选人。他们的权益投票人获得区块奖励。
验证人与备用验证人的区块奖池分配	9:1	验证人及其权益投票人共同获得总区块奖励的 90%;备用验证人及其权益投票人获得总区块奖励的 10%。
区块时间	10 秒	产生一个新区块所需的时间。一旦一个区块产

		生，区块中所有交易都确认且敲定
削减	每 12 个区块，削减投票量的 0.1%（最多为权益投票的 1.2%）	当验证人行为不当时，系统会削减并燃烧验证人的权益投票（包括所有参与其中的权益投票人）。
取消权益投票等待时间	7 天	权益投票人在取消对某个验证人的投票并收回 CMT 时，必须等待的时间。
CMT Cube 上限	100,000 CMT	单个 CMT Cube 设备可以容纳和投票的 CMT 的最大数量。
CMT Cube 下限	1,000 CMT	单个 CMT Cube 设备可以容纳和投票的 CMT 的最小数量。
CMT Enterprise Cube 上限	无	单个 CMT Enterprise Cube 账户可以容纳和投票的 CMT 的最大数量。
CMT Enterprise Cube 下限	1,000,000 CMTs	单个 CMT Enterprise Cube 账户可以容纳和投票的 CMT 的最小数量。