**Minemon技术白皮书**

1. **摘要**

比特币的诞生，因其自带金融属性这一特征，第一次以技术手段保证了私有财产神圣不可侵犯，同时比特币系统所采用的技术理论和设计模式开启了一个新的技术行业——区块链技术行业。

比特币诞生12年来，如同诞生了一片去中心化的金融公海，如今各种区块链项目如雨后春笋般涌现，在这片金融公海里畅游，虽然目前整个区块链行业还处在混沌期，但是越来越多的技术人员和各个企业都在进行积极的技术创新与探索，我们也在经过不断地探索后创立了Minemon项目，Minemon创新性的设计让整个网络系统轻能耗，同时也创新性的将“黄金分割比例”定律引入到Minemon系统的token激励算法中，用以平衡Minemon的经济生态，让Minemon项目可持续发展。

1. **行业现状**

以比特币为代表的各种POW（proof of work）共识的区块链项目每天消耗着大量的电力能源，尤其比特币挖矿时大量消耗能源的议题一直备受关注，比特币挖矿预计消耗 130 TWh，约占全球总电力消耗量的 0.6%，大约等同一个发展中国家的全年用电量，在资源有限的情况下，挖矿行业因此被视为污染行业。挖矿与区块链技术可以说是共生的，但区块链就等于污染吗？不，很多技术一直寻求更环保的挖矿办法，例如以太坊提出转用POS（proof of stake）来减少消耗能源，以求达到更环保的目的，但当中就会出现其他问题，更有一些项目利用硬盘的数据空间，使用硬盘挖矿，当然也会被矿工为了利润而不停堆叠，最后亦避免不了污染问题。

人类的发展会因为污染而停止吗？汽车的污染是众所周知的高，飞机亦如是，人类不停想出办法减低污染，用电甚至水作为能源为汽车提供动力，可是能够不产生污染吗？人类只能做到在发展同时和污染取得平衡点。

基于对以上问题的思考和探索，我们创立的Minemon项目使用人性模型，以产出作为抵押物，矿工不一定需要很多矿机，但一定需要很大的参与度，从污染的角度看可能不是完美，但技术层面上，它既公平，又可靠，相对低污染，矿工成本的大比重不再是电费，而是他们对Minemon的参与度，依托矿工广泛的参与度来稳定提升Minemon区块链项目的价值。

1. **什么是**minemon

在区块链领域中，矿工代表着维持运作的主要劳动者，同时亦代表著逐利者，当生态中无利可图将立即离去。项目命名为 Minemon，是 Miner（矿工）和 Mammon （玛门）的结合，项目简写为MAM,同时MAM也是Minemon区块链上的通正（token）激励（即玛门币）。

玛门在新约圣经中用来描绘物质财富或贪婪，犹如矿工的逐利和贪婪一样，MAM就是一个基于区块链生态下的人性测试，旨在保持矿工和贪婪的玛门在去中心化机制下的平衡状态，用数学理论及程序代码来解决矿工对区块链生态带来的影响，以实现MAM项目的可持续发展和MAM通正的价值提升。

1. **设计理念**

如前所述，MAM的设计是一个轻能耗的POW共识项目，同时引入了黄金分割比例参与网络计算，即= ...

黄金比例是属于数学领域的一个专有名词，但是它涵盖的内容不仅与数学领域的研究有关，它也侧重于从数学关系去探讨美的规律，并认为美就是和谐与比例，按照这种比例关系就可以组成美的图案，这其实是一个数字的比例关系，即将一条线分成两部分，较长的一段与较短的一段之比等于全长与较长的一段之比，它们的比例大约是1.618:1，知名的费氏数列也体现了这个数学原则，按此种比例关系组成的任何事物都表现出其内部关系的和谐与均衡，MAM的通正激励也因此将该规律引入到系统计算中来，用以平衡矿工的贪婪对MAM的影响。

此外MAM网络接受矿工挖出的玛门币作为抵押用来提升算力，即质押的币可代替算力来分享挖出的玛门币，因此矿工不需要过多的矿机，只需要适量的矿机和玛门币的抵押就可以获得全额的出块奖励，相反如果没有玛门币作为抵押，即便挖出了当前区块也只能获得较少一部分奖励，没有抵押时的出块奖励为(1-)\*当前区块奖励数量，为上述黄金比例值，即没有抵押挖出块时只能拿到当前区块奖励的38.2%（近似值），当前区块余下的部分奖励自动结转到下一个待挖区块中。因此MAM网络系统的设计鼓励矿工抵押玛门币获取更多的出块token奖励，让矿工不必一味地增加矿机数量，以此来达到整个MAM网络的轻能耗。

1. **MAM分发机制**

* MAM总量为210,000,000个，零预挖，零预留，零募资，全开源，全透明，全挖矿。
* 每分钟产生一个区块，初始每个区块的奖励为100个MAM，每两年（以区块高度为准）区块奖励减半一次。
* 第一个两年最大产出105,120,000，第二个两年最大产出52,560,000，第三个两年最大产出26,280,000，第四个两年最大产出13,140,000 ...

1. **抵押机制**

用户（矿工或持币者）抵押MAM时，需要创建抵押模板地址（由用户钱包地址、挖矿地址、收益发放方式经过加密计算所得的新地址），用户抵押时将MAM转到抵押模板地址，转帐交易上链后抵押才生效，抵押模板地址的花费权限只有用户自己可操作，即抵押模板地址对应的私钥仍然为用户自己钱包地址的私钥。挖矿地址在出块计算奖励时，需要汇总该挖矿地址下关联的所有抵押模板地址的MAM余额，奖励按汇总后的抵押总额进行计算，抵押部分产生的收益根据创建抵押模板时设定的发放方式进行发放，可以自动发送到抵押模板地址进行再抵押，或直接发送到用户的钱包地址用于转账交易。

抵押的MAM可以随时解除抵押（即赎回），解除抵押时需要创建解押模板地址（由用户钱包地址、随机数经过加密计算所得的新地址），解除抵押操作是将抵押模板中的MAM转到解押模板中并锁定144000高度，每天（每1440个高度）解锁1%的MAM，约100天解锁完，解锁后的MAM才行消费转账，解压模板地址中的MAM不会计算收益，同时抵押模板只能向解押模板转账（不能向其它模板地址或钱包地址转账）并且转账时抵押模板和解押模板中包含的钱包地址必须相同。若用户进行多了次解除抵押操作并且在解除抵押时向同一个解押模板进行了多笔转账，以最后一笔转入解押模板的交易为准进行重新锁定计时，即该解押模板地址上所有MAM重新锁定144000高度（即重新锁定100天），每天解锁1%的MAM，约100天解锁完。

1. **挖矿奖励机制**

MAM以SHA256作为挖矿的加密算法，以算力及MAM抵押来分享区块奖励，矿工挖矿时，需要有足够多的MAM作为抵押才能在出块时获得更多的奖励。单个挖矿地址最小抵押量为N，最大抵押量为M,假设当前全网MAM总的流通量为P，则N= ,M= （即100N）,当 < 100时,则N=100，若矿工实际抵押量为D，当D<N时，则不计算抵押量，即此时抵押量按D=0计算，当D>M时，实际抵押量按D=M计算（即挖矿地址超额抵押时，仍按最大抵押量M计算）。假设当前区块奖励的MAM数量为T，上一区块剩余结转的MAM数量为S,则该当前挖矿地址出块时可获得的总奖励数量为R=T\*[\*+1-]+S\*,当D>=M时，R=M+S,即该矿工获得当前区块的全部奖励；当D<N时，矿工只能获得当前区块的少部分奖励（无抵押收益产出），即只能获得T\*(1-)的奖励（约为T\*38.2%），剩余部分继续结转到下一区块中；当N=<D<M时，矿工可获得当前区块抵押收益产出的部分奖励，剩余部分继续结转到下一区块中；转入下一区块的MAM数量为S=T+S-R（赋值运算），则下一个被挖区块中矿工可获得的MAM总奖励数量仍通过公式R=T\*[\*+1-]+S\*进行计算，同上，若D>=M时，矿工获得全部出块奖励，否则剩余的MAM（即T+S-R）继续再转结到下一个区块中，照此持续进行下去。

另外按链上规则约定每100个区块高度内，一个挖矿地址只能出一个块，全网的挖矿地址始终保持不少于100个。持币用户可以委托抵押，即抵押模板地址中的挖矿地址为某个矿工的地址，该矿工出块产生的收益需按各个抵押人的抵押量计算收益，并给抵押人发放收益，抵押人的收益由链上直接发放，保障抵押人的权益，挖矿地址每个块的抵押总收益为R'=T\*[ \*]+S\*，系统自动将总收益按各抵押人在该挖矿地址上的抵押率进行奖励发放。

1. **增强型去中心化**

从上述的抵押机制及挖矿机制可以看出，MAM可以避免算力集中的问题，即便大算力接入，由于受挖矿机制100区块高度现在，大算力在每100个区块高度内只能挖出一个块，同时即便算力很大但在没有MAM作为抵押或抵押很少的情况下，挖矿产出的收益也比较抵。大算力矿工想要获得更高收益，只能购买增持MAM，这样也有益于MAM的经济生态，同时会跟MAM生态绑定在一起成为MAM利益相关者，会更好的服务于MAM生态。

1. **minemon联合挖矿**

minemon联合挖矿（即双挖）是一个有效利用比特币现有算力的特点，由于minemon与比特币采用相同的挖矿算法，minemon提供了相关的接口参数设置，使得比特币矿机在挖比特币的同时也可以对minemon链进行出块，以便获取minemon区块链上的奖励，这样设计可以充分利用比特币矿机的算力，矿工挖比特币的工作量证明即为minemon的工作量证明，即便矿工的算力不满足比特币的出块要求，仍有可能获得minemon的区块奖励，当矿工进行双挖时，通常情况下minemon的出块难度会比比特币的出块难度小很多，因此矿工在没有比特币收益时仍可能获得minemon的收益。此举也正好凸显了minemon轻能耗和可持续发展的设计，因为minemon重复利用了比特币网络系统现有的算力来为minemon网络提供算力保障。

minemon与比特币实现联合双挖的技术设计遵循了Auxiliary Proof-of-Work (AuxPOW)混合挖矿协议，在进行比特币挖矿出块时，当前比特币区块构建的Coinbase交易里包含了minemon当前待计算区块数据（如版本号、上一区块哈希、难度、Merkle Root及时间戳等）的hash，即minemon相关数据的hash值内置于比特币区块链（父链）的Coinbase里，利用父链来为辅链（即minemon区块链）做存在证明。当矿工提交的计算结果符合minemon出块难度时，矿池所在比特币网络节点将比特币区块头及Coinbase相关的数据发送到minemon网络节点，由minemon节点进行验证，minemon验证过程如下：

1. 首先验证比特币的区块头是否确实符合minemon的难度要求，即将比特币区块头信息进行哈希运算，运算结果反应的难度必须符合minemon当前的区块难度。
2. 将minemon区块头数据进行哈希运算，根据运算后的hash值，确认该hash值被包含在Coinbase中。
3. 将Coinbase与相关交易数据进行Merkle哈希运算，再将计算的Merkle Root的值与比特币区块头的Merkle Root进行比较，确认两者是否相等，相等则验证通过。

以上全部验证通过后该区块才会被作为合法区块广播到整个minemon网络，同时比特币相关的区块头信息也会被打包到minemon区块。

1. **风险提示与免责声明**

* **风险提示：**

任何投资项目均存在系统性与非系统性潜在风险，本白皮书中所描述的内容仅为技术可实现的情况及项目发展愿景，并不提供任何投资建议。本文件不构成也不理解为任何买卖行为的要约、请求或推荐，不是任何形式上的合约或承诺。数字资产投资作为一种新型投资模式，尚存在各种潜在风险，MAM 属于数字资产类，价格上下浮动属于正常现象，需要投资者谨慎评估投资风险并具备风险承受能力；区块链技术属于早期阶段，各国对区块链项目的监管态度和监管政策也不一样，不排除项目运营管理方面的变化。

* **免责声明：**

投资者一旦参与了投资，即表示了解并接受本项目风险，并愿意承担相应的结果。MAM团队不承担任何参与MAM项目造成的直接或间接的资产损失。资本市场不可预测，投资有风险，入市需谨。

**参考文献**

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” www.bitcoin.org, p. 9, 2008.