BYTOM

Bytom 2.0

新太阳时代

前言

基于 PoW（工作量证明）的 区块链（如比特币），节点（矿工）是付出价格高昂的硬件与电力成本来解决数学难题，从而铸造新币，并处理交易。矿工通过维护网络安全性来获得增发的新币和交易费。PoW 的去中心化在创造巨大价值的同时，也会带来极高的成本。比原链 1.0 的解决方案是主链采用 PoW，负责资产发行，侧链采用 PoS，负责交易效率。但是这带来了新的问题，需要为两条链的节点运行支付成本，每年大约需要向主链矿工付出 8000 万 BTM 和向侧链节点付出 1000 万 BTM 的经济激励，这给 BTM 生态带来沉重的经济负担。

相比之下，在 PoS 区块链中，验证者通过锁定代币来为网络提供安全性，从而铸造新的代币，并处理交易。那么实际上，验证者提供的安全性取决于网络本身的价值。如果有验证者作恶，其锁定的代币就会被 罚没 ，罚没机制会激励验证者遵守协议规则。通过经济模型的设计，可以让验证者成为一致利益人，使得网络获得不亚于 PoW 的安全性。

PoS 之所以具有较高的安全性，一个很大的原因是 PoW 系统容易遭受“蹲点（spawn camping）”攻击。如果作恶者所掌握的挖矿硬件足以攻击比特币等 PoW 区块链，比特币便无力阻止后续攻击，因为网络会不断发生 重组/分叉，然后又会被同一帮挖矿硬件攻击，如此无休止地循环下去。相比之下，PoS 抵御蹲点攻击的能力要强得多 —— 可以分叉并罚没攻击者的押金。

PoS 架构的经济安全性和经济高效性也为开展 DeFi 等上层生态带来极大的便利性，更有利于 MOV 发挥自身最大的潜力和前瞻性。技术架构的大融合也必然会给引入更加通用的智能合约体系和开发者生态带来极大的灵活性，是塑造开放生态的必由之路。

基于此，我们提出比原链 2.0 的架构理念，将一主一侧的架构合并为统一平台，并在统一平台上集成多元资产 DeFi 协议，优化资产流动效率，连通比特世界与原子世界，更好的服务资产上链这一宏大愿景。为“流浪地球”计划点缀“浩瀚星途”。

新愿景

基于 Vapor 侧链架构和 MOV 开放金融平台的多年运行实施，比原链 Bytom 在 2.0 迭代关口选择重新审视自身历史定位，并决定开启一个意义非凡的 2.0 新时代——

- 由 PoW 比原链转向 PoS 比原链；
- 建立以 Vapor 为技术根基的 PoS 新比原链，从一主一侧变成唯一的“统一平台”；
- 致力于构建通缩的经济模型，使真正的 BTM 持有人参与公链底层建设，凝聚共识；
- 更好地集中精力兼容外部生态和合约体系，提高效率，服务开放金融战略 MOV；
- 从根本上为 BTM 实现价值捕获使命。

第一阶段“行星发动机”

比原链 2.0 需要完成作为一条独立大公链的全部安全属性和底层功能建设，成为支撑新比原链浩瀚星途的“行星发动机”。

“行星发动机”的初期“骨架”具体包括：

- 基于更大规模的质押保障 PoS 经济安全，加强提升共识验证效率，完善社区参与 PoS 建设的配套设施；
- 引入资产发行和 GAS 机制；
- 完成对 MOV 平台的兼容性改造，包括钱包、跨链网关系统 OFMF、磁力兑换、闪电兑换、超导兑换、MOV 借贷；
- 完善智能合约体系，建立更为通用和开放的开发者平台；
- 提升跨链互操作的效率和经济安全性。

第二阶段“停止自转”

在未来某个时间通道内，将开启 2.0 新旧交替进程，BTM 原生通证从 PoW 比原链（称之为“历史 PoW 比原链”）不可逆 1:1 映射到 PoS 新比原链（称之为“比原链 2.0”）。映射到比原链 2.0 的 BTM 通证为真正意义上的比原链原生价值载体，一如既往地为各大交易平台承认并流通；如何处理对待历史 PoW 比原链以及其上的历史通证——

（1） 如果历史 PoW 比原链存在后续的接管方（可以为任何社区或者矿工利益集团），将由接管方自主决定 PoW 比原链的未来走向和规划，以及留存

BTM 后续的流通和定价，建议取名为“比原链经典 Bytom Classic”；

（2） 如果社区以及利益集团都达成一致，赞同 2.0 进程，共同从 PoW 比原链转移到 PoS 比原链 2.0，不存在后续接管方，则 PoW 比原链以及留存 BTM 将彻底退出历史舞台。

本阶段具体实施步骤包含如下：

- 处理好市场工作、投资者关系、交易所对接、社区工作，让所有人知悉、处理并解决异议；
- 在未来某一个日期开启 BTM 映射通道；
- 最后，历史 PoW 比原链在截止日后将成为一颗“自由的行星”，比原链官方将不再对其进行运维和背书。

第三阶段“驶出太阳系”

- 全面启动 PoS 比原链的质押运行和交易共识；
- 为了更好地践行 MOV 开放金融战略，发展更为多样性的 MOV 协议簇，获得 DeFi 发展红利对 BTM 通证的价值捕获；
- 比原链 2.0 会从根本上改革自身智能合约系统和开发者生态，引入或者兼容以太坊合约体系，方便其上项目和开发者便捷迁移；
- 落地更为强大的交叉跨链体系，使 MOV 可以被比原链外生态所广泛认同。

这一前所未有的 2.0 进程共分成了三大阶段逐步实施开展，也必将从如下“新经济”、“新共识”、“新平台”、“新 MOV”四个方面为新比原链和新 BTM 带来深远影响。

新经济

新经济，是新的经济模型，也是新的经济价值。

比原链将从 PoW 转向 PoS，从一主一侧两条链聚变为“统一平台”，最直接的影响莫过于将从根本上改变比原链底层经济模型和 BTM 价值体系。

现存的 PoW 比原链上承载着 21 亿 BTM 的庞大总量，且其中有超过 4 亿 BTM 有待矿工在未来逐步挖出，进而造成一个每年约 8000 万新增 BTM 的通胀现象。同时随着比原链将生态战略聚焦在 MOV 和 Vapor 侧链，PoW 比原链主链对生态建设和 BTM 价值捕获的作用越来越边缘化。

除此之外，为了兼顾 Vapor 侧链的同时运转，其上运行的 PoS 奖励机制也会带来每年约 1000 万新增 BTM 的通胀率。双重增发每年近一个亿的 BTM 给价值捕获带来了巨大挑战。

比原链 2.0 将彻底改革经济模型，从通缩经济模型的基本角度出发，凝聚新共识，提高价值捕获效率，具体体现在如下四个方面——

（1） **总量缩减**——从历史 PoW 比原链转向 PoS 比原链 2.0 后，将不再出现未来每年约 8000 万 BTM 的挖矿奖励，新 BTM 总量将从 21 亿缩减到约 15.66 亿 BTM。

（2） **流通总量缩减**——假设这 15.66 亿已流通 BTM 全部或者绝大多数映射到比原链 2.0，由于新比原链采取 PoS 机制，为了达到足够的系统安全边界，需要验证人集团携数量庞大的 BTM 参与长期锁定质押，以满足高质押率，因此这 15.66 亿总量中很大一部分将不会流通（其数量将远超过现在 Vapor 验证质押量）。PoS 的成功实行将会进一步减少 BTM 市场流通总量。

（3） **年增发规模变小**——比原链 2.0 虽然缩减了理论总量并真正意义上减少了可自由流通总量，但也并非意味着没有增发，为了维护 PoS 持续运转，验证人群体依然需要一定的 BTM 增发量来作为奖励，需要维持一个恰当的年化收益。但比原链 2.0 保证 BTM 的年增发量将远远小于现阶段约 9000 万的增发量，上限为 3000 万。验证人集团更与公链生态的集体利益保持一致，是最为坚实的底层通证的做多力量。

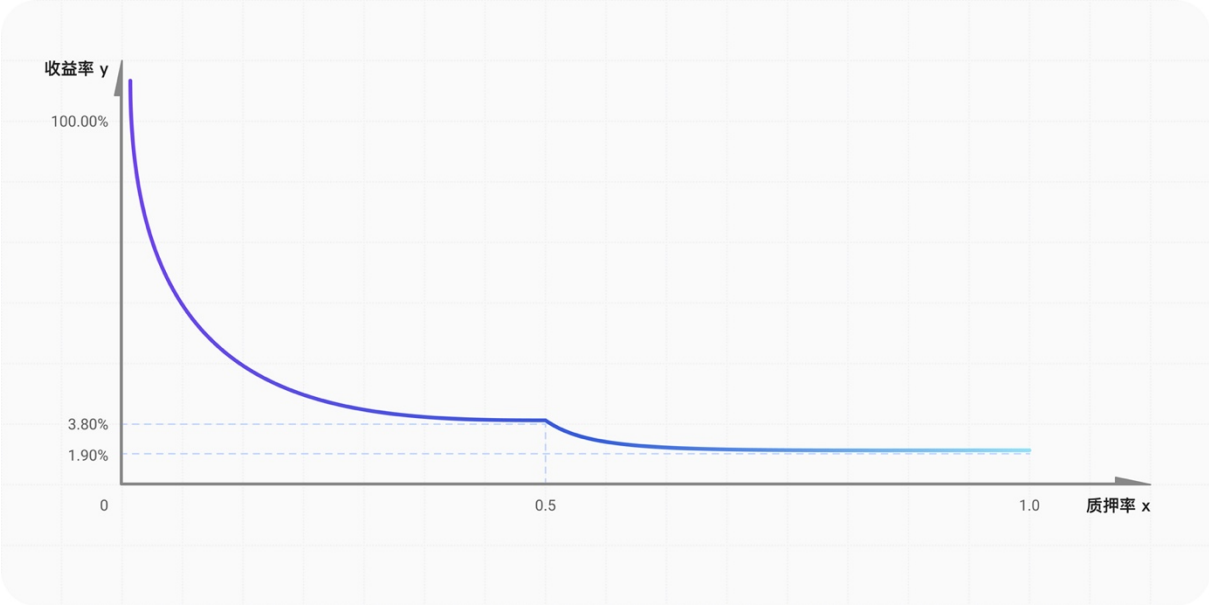
具体增发量关系如下：

当 0< x<=0.5 $y = (x + 0.5) * \frac{0.3}{x*z}$

当 0.5< x<=0.5 $y = \frac{0.3}{x*z}$

其中 x 为质押比例，z 为发行总量，y 为质押收益率。

z 的初始值约为 15.66 亿，带入上述公式后绘制出收益率曲线如下图所示：



注：假定每年增发 3000 万个 BTM 用于 DPOS 的激励，根据不同的抵押率设定不同的收益率，激励出现剩余时剩余部分归入基金会，用于项目运营。

（4） 用户将同时拥有两种 BTM，但团队只持有一种。BTM 的升级将采取在某个区块快照映射的方式，由于原链（Bytom Classic，以下简称 BTMC）的矿工可能会继续维持挖矿，原链可在去中心化的算力支持下继续存在。团队将在升级后永久销毁所有的 BTMC，而只持有新 BTM。 但用户在升级后可能同时拥有两种 token。

最后，如果公链生态业务获得了飞速发展，PoS 系统甚至可以做到理论通缩。首先，由于权益证明避免了高电耗和硬件产业成本，因此在奖励增发方面的数量会远远小于 PoW，便可满足验证人群体正常运行。然后，随着交易量的飞跃，GAS 机制的捕捉，底层通证作为交易手续费会被不断“烧毁”，供应量随之减少。

此外，BTM 的使用场景将考虑不断拓展，比如包括但不限于以下方面：

- 投票治理。BTM 持有者可以使用BTM 进行投票，参与 Bytom 2.0 公链层面的重要事项的治理。
- 购买基础类服务。外部项目请求使用比原链上预言机等基础类服务时，需使用

BTM 进行付费。预言机节点等服务相关方需抵押一定数量的 BTM 以防止作恶。

- 共识节点竞选。持有一定数量 BTM 以上的用户可以参与共识节点竞选，所有的 BTM 持币人可以对备选节点进行投票。
- 参与其它公链的挖矿。与其它项目合作，BTM 通过跨链参与以太坊等其它公链项目的挖矿
- 空投。BYTOM 生态中发行新通证时考虑对持有一定数量 BTM 的用户或者一定时期内参与过 BYTOM 相关产品的用户进行空投。
- 锁仓挖矿。BYTOM 生态中发行新币时考虑对参与 BTM 锁仓的用户分发部分新币，即锁仓挖矿
- 手续费折扣。根据用户在 Bycoin 和 Byone 中持有 BTM 的数量提供 MOV 中各类产品不同等级的交易手续费折扣优惠
- 抵押借贷。BTM 可作为 MOV 稳定币和借贷产品的抵押资产，借出稳定币或其它资产。

新共识

新共识，是新的共识机制，也是新的品牌共识，更是对新 BTM 的共识。

以 Vapor 根基全面建设 PoS 经济系统，使之成为新 BTM 更为坚实可靠的共识体系。一方面需要对现有的 Vapor 共识算法 DPoS+BFT 进行经济质押层面的加固和完善，另一方面还需要引入更细致的奖励和惩罚机制，对合法行为和作恶行为进行定量定性奖惩。此外，DPoS+BFT 的混合共识模型可以更好地兼顾可用性和一致性，也能够迅速完成对新 PoS 系统的升级支持。同时得益于 Vapor 多年的成熟运行，新共识的建立进程也必将顺利。

PoW 链以及 PoW 比原链都会面临矿工集团垄断的局面，理论上的物理去中心化往往以卡特尔式矿池集团为唯一共识。不但抑制着比原链/BTM 的价值捕获、底层链升级迭代的迅速进行，而且不利于形成社区（真正的 BTM 利益持有者）参与共识的有利局面。导致当下真正关心 BTM 利益的社区群体只能去参与到更为上层的协议建设和治理（如 MOV），然而相比于底层链本身对 BTM 价值捕获的显著效应，上层应用需要更为漫长的时间和更为庞大的外生态用户群体增长。

比原链 2.0 可以从底层链共识层面改变既往格局，让真正的 BTM 利益持有人享受底层链共识建设的权益，形成 BTM 价值同盟，更能建立起长期的信念，社区也会更好地参与到自下而上全生态的建设。社区往往是一个公链生态和底层通证最为重要的支撑体，如果社区不能很好地参与到共识建设，这股最为重要的支撑力量也终究不会变为价值捕获的中坚力量。因此，新共识的本质是让社区、交易平台乃至原有的矿工集团都对以 Vapor 为根基建设的 PoS 比原链 2.0 达成共识，能够积极携 BTM 参与到共识验证群体，获取可观的年化收益率，同时享受底层链集体建设的权益。相信，独立公链级别的 PoS 会带来新一轮 BTM 锁定质押，长期利好。

从安全层面，PoS 系统引入的“经济终局性”可以更加抵御对底层链的超级攻击，即便是遭遇了 51% 攻击，相比于 PoW，PoS 也能尽快恢复正常，且作恶集团所付出的成本和所收获的利益远远不对等，实际操作层面不可行。

比原链 2.0 较之历史 PoW 比原链，会在去中心化、安全、可扩展性（效率、升级）三方面有所超越，能够更好地服务 MOV 战略的实施，支撑起更优质的应用和资产。

回到 Vapor 的升级改造和新品牌共识上。自比原链 2.0 正式启动后，Vapor 将不再作为 Layer-2 概念存在，而是彻底升级蜕变为一条完全自主独立的大公链结构，并成为代表比原链 2.0 的新品牌。从此以后，比原链将只有比原链 2.0 这一条链结构，所有配套设施，包括官方钱包、浏览器、插件、开发者工具、跨链系统 OFMF 等，都将重新定向到比原链 2.0。

Vapor 将维持现有的 DPoS+BFT 共识主结构不变，为了提升公链级别的安全，将会扩大验证人集体，并能够灵活地支持动态加入、选举、退出等 PoS 属性。通过 DPoS 保障共识群体的去中心化和不可串谋，通过 BFT 保障每一轮共识的最终确定性（被超过⅔*N+1 不同的验证人所确认），防止分叉攻击，同时提高共识效率和跨链效率。此外会不断完善升级经济惩罚机制，对所有验证人行为进行约束，例如双重签名和节点不稳定性等拜占庭行为。

现有的 Vapor 需要具备资产发行能力，因此目前 PoW 比原链唯一的资产发行职责会顺利交接给升级后的 Vapor。对以后用户和开发者开展 MOV 应用建设节省了成本，提高了效率。团队的开发力量也会更加集中，提高产品交付效率。

新共识的建立离不开对新 BTM 价值共识的建立。比原链 2.0 网络安全在很大程度上依赖于新 BTM 的价格。新 BTM 的价格可能会出现大幅度的波动，而 2.0 网络是否有足够的弹性维持经济稳定性和安全性，避免攻击者迅速扩大攻击能力，也是 2.0 建设过程中需要重点设计的地方。

新平台

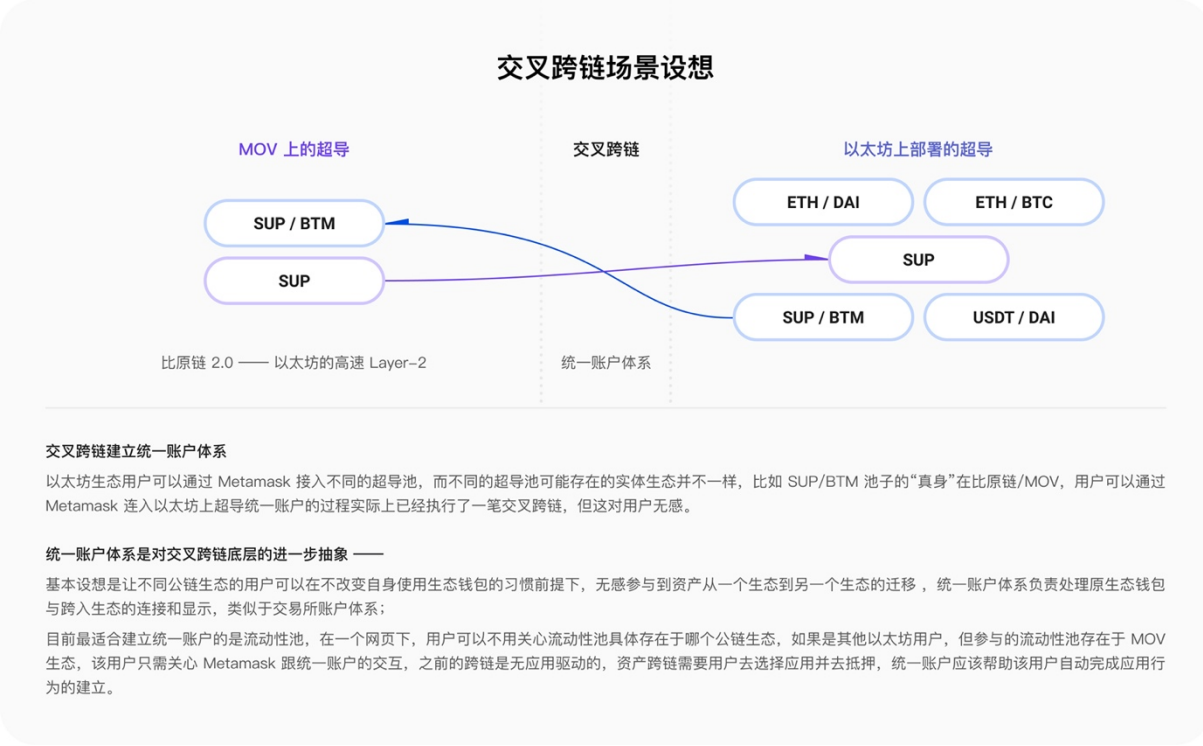
新平台，是新的智能合约平台，也是新的开发者生态平台

比原链 2.0 要走向成功，除了要打造成功的经济模型和共识模型，从内因上重塑 BTM 价值，还要建设出更为通用的智能合约平台以及与以太坊等主流生态无缝衔接的开发者与应用生态，才能彻底盘活 MOV，让 MOV 带着 BTM 的价值走出去，真正意义上从流通的本质实现 BTM 价值共识，才是长久之计。

因此，比原链 2.0 的意义更是一种全新的平台战略，是对以往自身开发生态的深度反思与改革。当从双链聚变为“统一平台”后，新比原链为开发者和应用方除去了以往的多道门槛，也更能友好地对待新加入的开发者，降低学习成本；在与其他公链生态实现互操作的过程中，底层架构也更为简洁，操作效率也更为高效。比原链 2.0 的核心使命之一便是如何更好地对待开发者群体和与外部生态的合作互通，只有共同建设 MOV，MOV 才能成为国产开放金融平台的扛鼎之作，使 MOV 很多超前的设计为全世界 DeFi 生态所熟知和引用。

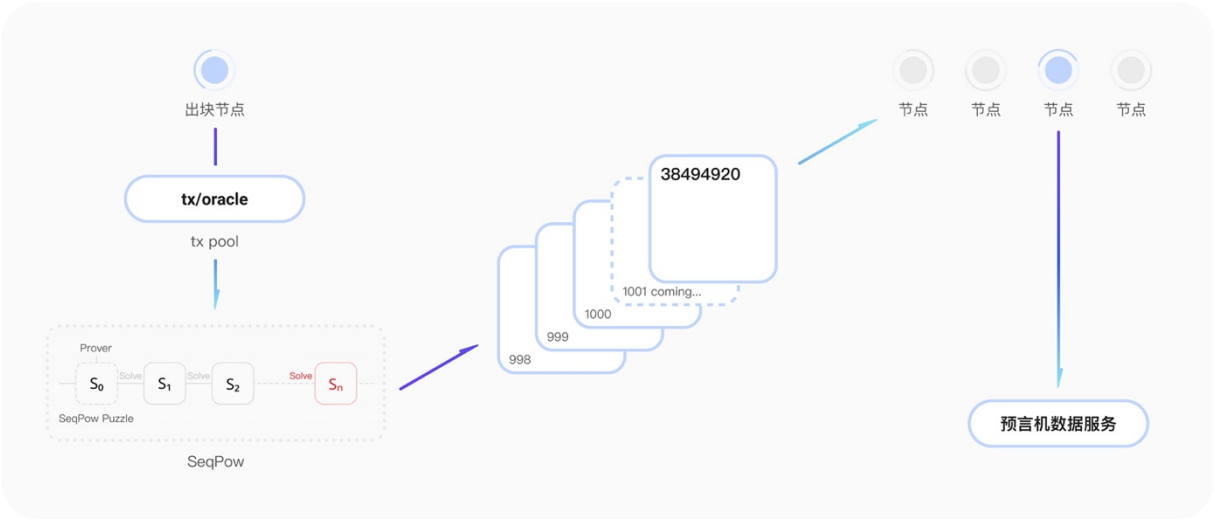
在具体的路线图中，基于 MOV 战略实行以来对自身智能合约开发提出了很高的要求，因此提升 Vapor 和比原链 2.0 的智能合约成熟度以更好地支撑 DeFi 等应用的开发是 2.0 路线图中非常重点的一环。在 Vapor 现有智能合约的基础上，会不断完善使之可以方便地开发出 MOV 提出的所有产品线和协议簇，以便在 2.0 运行早期便可以允许自身社区内的开发者进驻，共同建设开放式的 MOV 生态。

在之后的路线中，还会建设更为强大的综合性合约系统，能够兼容以太坊合约体系，在 UTXO 账户模型的基础上实现 EVM/eWASM 等主流虚拟机架构，使得大多数以太坊上 DeFi 应用、生态系统组件和工具将与比原链 2.0 兼容，不需要修改或只需要很小的更改，带动两个生态上的开发者和协议应用实行双向互通，才能真正将 MOV 提出的交叉跨链生态设想变为现实（如下为比原链/MOV 很早提出的一种设想，但其对底层链提出了非常高的要求，相信比原链 2.0 有能力将之变为现实）。



新的平台还应当是一个健全的平台，包括——

- 引入和完善对 DeFi 建设具有重大意义的基础机制，如开放资产发行、GAS 机制等；
- 跨链系统也能够具备更强大的可扩展性，可以迅速添加其他生态和通证，在见证检验不同链上跨链事件的效率上也能够提升一个数量级，建立更为强大的跨链网关节点群体，加强 MPC/门限签名的进一步落实和对外输出，不再局限于比原链内部生态的服务，例如可以在以太坊上轻松实现 RenVM/renBTC 的功能定位，或者向以太坊 DeFi 生态输出 BBTC（从比原链 2.0 映射过去的 BTC）；
- 建立健全比原链 2.0 随机数与预言机体系。基于 SeqPow 机制建设一种优于 VRF 的随机数发生机制，借助比原链 2.0 的共识结构，所有 PoS 验证人都可以参与到去中心化的随机数生成过程，并可以基于随机数机制选举成为 2.0 生态的预言机服务节点，向 MOV 以及外部 DeFi 生态提供去中心化的预言机服务，获得额外收益（如下图）。


出块节点
tx/oracle
tx pool
Prover
S0
Solve
S1
Solve
S2
Solve
Sn
SeqPow Puzzle
SeqPow
998
999
1000
1001 coming...
38494920
节点
节点
节点
节点
预言机数据服务

新 MOV

新 MOV，是比原链 2.0 的 MOV，也是走向外生态的 MOV。

新平台的强大足以让 MOV 获得新的活力，而新的 MOV 不仅是比原链 2.0 的 MOV，也将是其他生态上的 MOV，走出去的 MOV 会更为强大。MOV 走出去，BTM 也终将走出去。

比原链 2.0 也依然将 MOV 战略视为永恒不变的第一定位，过去几年所有 MOV 建设不仅没有白费，还将焕发更强大的活力——

- **更强大的互操作性**：比原链 2.0 会重新建立跨链网关系统，使得外部公链生态可以与 MOV 直接互通，不必再经由 PoW 比原链中间过渡，极大地提高了互操作效率，促进交叉跨链真正落地。因此比原链 2.0 将会具有更强大的与以太坊生态跨链互操作性，也兼任起以太坊 Layer-2 的功能定位，积极拥抱以太坊外溢的 DeFi 项目，如可以对接 MetaMask 的自定义网络 API，将比原链 2.0 网络添加到用户网络列表中，作为以太坊 Layer-2 呈现在用户面前。
- **更强大的可组合性**：MOV 超导和 MOV 借贷，以及之后的 MOV 稳定币，在比原链 2.0 的支持下，都将能实现更好的组合互通性，BTM 也能更顺畅地参与到每一个协议的质押和费用支付，进一步促进基础通证 BTM 的实用价值，提高各种资产的资本利用效率。
- **更强大的开放性**：现阶段的 MOV 尚在早期阶段，且受制于底层基础设施的束缚和技术力量的分散，不能很好的践行 DeFi 的开放性特征，在吸引主流资产、新资产、官方外应用、开发者上都处于劣势，纵使 MOV 理念再超前，也无法跟以太坊生态比拼速度和网络效应。因此，在比原链 2.0 和新 MOV 阶段，强大的开放性将成为核心要素，在做到强大的跨链互操作性和可组合性后，开放性将变为现实，资产会多起来、用户会参与起来、其他生态的应用会迁移过来。

新 MOV 会坚持建设完毕兑换、借贷和稳定币三大 DeFi 基础设施，并将三大服务以接口和可组合的方式开放给比原链 2.0 生态开发者以及以太坊等外部生态上的应用，使得社区可以基于官方提供的三大基础设施，在其上开展更为精彩的去中心化金融场景，带来如结构性金融、去中心化期货期权池等衍生创新。

也许我们可以做一个大胆的设想：区块链，或者一条公链，要获得价值证明，可能恰恰不是之前所固化的思维——即一定要深入实体产业去落地、去作用国计民生，相反，

如果一条公链能够从区块链原教旨理念/机制出发将自身的全方面建设给做好、做完美，那么它的原生通证就是有价值的，它的社区共识和社区生态也是有价值的，也终究会被人们所广泛认同。

最后，比原链 2.0 携“五新”即将来临。流浪地球，浩瀚星途，建设新家园！