CRYPTOSTONE WHITEPAPER v2.8

关于去中心化环境下数字宝石资产的研究

Chinese Version

目录

CRYPTOSTONE WHITEPAPER v2.8

CRYPTOSTONE WHITEPAPER v2.8

关于去中心化环境下数字宝石资产的研究

摘要

比特币并未直接以现实世界中的黄金作为担保，但它通过有限的供应量、公开的挖矿规则、去中心化网络，以及任何人都可以验证的交易结构，形成了“ 数字黄金 ”这一全新的资产概念。比特币的本质意义在于，它证明了即使不依赖特定发行者或中央机构的信用，也可以仅通过代码和网络实现数字资产的稀缺性与所有权。

笔者希望将这一哲学扩展至“ 宝石 ”这一资产概念。现实世界中的宝石具有有限的开采量，每一颗宝石都会根据重量、颜色、净度、切工等属性，形成不同的稀缺性与价值。即使是同一种宝石，只要个体属性不同，其价值也会不同。因此，宝石本质上具有非同质化特征，非常适合在数字环境中被表达为独立的唯一性资产。

CryptoStone 是一个去中心化数字宝石协议，旨在将宝石的可开采性、稀缺性、等级性和收藏性表达为链上数据，并使数字环境中的宝石 NFT 能够在没有中央服务器或运营方任意干预的情况下被挖掘出来。每一颗宝石都以 ERC-721 标准的 NFT 形式表示，并将宝石类型、重量、颜色、净度、切工、挖掘时间、挖掘来源矿池等属性记录在链上。

本项目并不旨在提供现实宝石的所有权、抵押权或兑换权。笔者在本白皮书中提出的是一项研究与实验：即如何将现实宝石所具有的结构性属性——有限性、可开采性、等级性、稀缺性和收藏性——在数字环境中实现为独立的稀缺资产。

如果说比特币将黄金的稀缺性和可开采性数字化，那么 CryptoStone 则试图以去中心化方式，将宝石的稀缺性与属性价值数字化。

1. 引言

在现实世界中，宝石长期以来一直作为价值储存手段、装饰资产、收藏资产和象征性资产而存在。宝石的价值并不仅仅来源于其物理存在本身。宝石的价值由开采难度、储量限制、加工精度、等级差异、收藏需求以及文化象征性共同形成。

尤其是钻石、红宝石、蓝宝石、祖母绿等宝石，即使属于同一种类，也会因个体属性不同而拥有完全不同的价值。重量更大、颜色更优、净度更高、切工更精细的宝石，通常具有更高的稀缺性。这一结构说明，宝石并不是可完全替代的商品，而是会根据个体属性产生价值差异的非同质化资产。

区块链技术为在数字环境中表达这种非同质化属性提供了基础。然而，现有 NFT 市场大多围绕图像、游戏道具、会员权益、外部内容的所有权或访问权展开。在这种情况下，NFT 的价值可能依赖于外部图像、中央服务器、特定平台或运营主体。

CryptoStone 提出了一种不同方向。CryptoStone 并不是用于证明外部图像或中央服务器内容的 NFT，而是 NFT 本身直接持有宝石属性数据，并通过这些属性本身表达稀缺性与收藏价值的数字宝石资产。

笔者在本白皮书中并非试图将现实宝石的物理所有权转移至区块链，而是希望阐述：宝石所具有的稀缺性与属性价值，如何能够在数字环境中以去中心化方式实现。

2. 理解 CryptoStone 最简单的方式

CryptoStone 是一个用于挖掘数字宝石的链上协议。用户将 STONE 投入自己选择的宝石挖矿池中，随着时间推移，Proof of Mining（PoM）数值不断累积，当 PoM 达到足够阈值后，用户便可以 claim Gem NFT。被挖掘出的 NFT 并不是单纯的图片，而是记录了宝石类型、重量、颜色、净度、切工、稀有度分数和挖掘时间的唯一数字宝石。

用户可以在钻石、红宝石、蓝宝石、祖母绿等 12 个宝石矿池中选择想要参与的矿池。每一种宝石都具有不同的供应量、挖矿周期和减半结构。随着挖矿进展，剩余供应量会减少，稀缺性倍率会提高。

CryptoStone 的核心体验非常简单。

> 将 STONE 投入数字矿山。
> 随着时间推移，Mining Power 会累积为 Proof of Mining，即 PoM。
> 当达到所需 PoM 阈值时，可以 claim Gem NFT。
> 会生成哪种宝石，由公开概率和可验证随机性决定。

也就是说，CryptoStone 并不追求“ 购买 NFT ”，而是追求“ 被挖掘出的数字宝石 ”。用户不是简单购买一张图片，而是在公开规则与固定概率结构下，挖掘属于自己的数字宝石。

3. 研究目的

CryptoStone 的目的并不是复制现实宝石，也不是将实物宝石所有权数字化。本项目的目的在于，将现实宝石所具有的结构性属性，即可开采性、有限性、等级性、稀缺性和收藏性，迁移到数字环境中。

CryptoStone 从以下问题出发：

> 如果比特币可以在不直接以黄金作担保的情况下成为数字黄金，
> 那么宝石的稀缺性、等级性和收藏性，是否也能够在去中心化数字环境中作为独立资产被实现？

笔者在本白皮书中提出的，正是对这一问题的一种技术性、经济性和哲学性设计。

目的	说明
属性数字化	将宝石的重量、颜色、净度、切工结构化为链上属性。
挖掘过程实现	基于智能合约实现宝石挖掘过程。
供应量固定	预先固定各宝石的最大发行量与稀缺性结构。
去中心化参与	让任何人无需中央服务器即可参与挖矿池。
防止属性操纵	防止运营方任意操纵宝石等级或属性。
收藏价值形成	通过稀有属性组合形成可被收藏市场识别的价值结构。
长期扩展性	为未来扩展至 Appchain 或 Mainnet 奠定基础。

4. 协议信任原则

CryptoStone 追求一种不依赖特定创始人或运营方信用的结构。本协议的信任基础不在于创始人的身份，而在于公开代码、固定发行量、不可更改的概率表、No Admin Mint 结构、可验证随机性，以及任何人都可以确认的链上数据。

运营方不应能够向特定用户任意分配稀有 NFT，也不应能够修改各宝石供应量或操纵挖矿概率。CryptoStone 的目的在于，让数字宝石的稀缺性由协议规则形成，而不是由人的权威决定。

信任原则	说明
Fixed Supply	STONE 总发行量和各宝石 NFT 最大发行量预先固定。
100% Public Circulation	STONE 采用 100% 公开流通结构。
No Admin Mint	运营方不得任意发行 Gem NFT。
Immutable Probability	宝石属性概率表公开，并在 finalize 后不得更改。
Verifiable Randomness	宝石属性必须由可验证随机结构决定。
On-chain Attributes	Gem NFT 的核心属性必须作为链上数据记录。
Transparent Pools	各宝石矿池的挖掘量、剩余数量、难度应可公开查询。
Open Verification	任何人都可以验证合约和挖矿规则。

这一结构表明，CryptoStone 是一个由公开规则和可验证代码驱动的去中心化数字宝石协议，而非依赖特定运营方裁量的项目。

5. 数字宝石资产的基本概念

CryptoStone 由一个 STONE 代币、12 个宝石挖矿池和一个 ERC-721 Gem NFT 合约组成。

组成要素	作用
STONE Token	参与数字矿山所需的单一挖矿资源
12 Gemstone Mining Pools	用于挖掘各诞生石的独立数字矿山
CryptoStone Gem NFT	表示被挖掘出的数字宝石的 ERC-721 唯一资产
Mining Pool Contract	管理质押、Mining Power、难度和 claim 条件
Gem NFT Contract	管理宝石 NFT 的属性、发行量和所有权

STONE 并不是宝石本身。STONE 是参与数字矿山并产生 Mining Power 的资源。用户将 STONE 质押到自己选择的宝石挖矿池中，从而获得 Mining Power，并随着时间累积 PoM。

挖掘结果物是 CryptoStone Gem NFT。Gem NFT 由一个统一的 ERC-721 合约发行，每个 NFT 都以链上属性记录自己属于哪一种宝石、拥有怎样的重量和等级。

现实宝石挖掘结构可以抽象如下。

现实宝石挖掘	CryptoStone
矿山	Gemstone Mining Pool
挖矿设备与能源	STONE Token
挖矿工作量	Proof of Mining, PoM
挖掘结果物	ERC-721 Gem NFT
矿山难度	Pool Difficulty
储量减少	Scarcity Multiplier

现实宝石挖掘	CryptoStone
宝石鉴定	On-chain Attribute & Rarity Score

6. 宝石属性的表达

宝石的价值并不单纯由种类决定。即使同为钻石，也会因重量、颜色、净度、切工而在市场上形成不同价值。

CryptoStone 为了在数字环境中表达这些宝石属性，会为每一个 Gem NFT 赋予以下四个核心属性。

属性	含义
Weight	宝石重量
Color	宝石颜色等级
Clarity	宝石净度等级
Cut	宝石切工等级

这四个属性在挖掘时确定，且在 mint 后不可更改。这相当于以数字方式实现了现实宝石在鉴定后根据个体属性进行评估的结构。

在 CryptoStone 中，每个 NFT 并不是简单指向“图片文件的代币”，而是直接持有宝石属性值的数字资产。图像、3D 模型或卡片形式的视觉表达可以作为用户体验的辅助元素，但 CryptoStone NFT 的本质在于记录于链上的属性数据。

7. 宝石唯一性的数字实现

CryptoStone 可以为了表达每一颗宝石的唯一性而评估多种技术选择。可替代代币结构、半可替代代币结构、复合代币结构等多种方式均有可能，但 CryptoStone 希望实现的核心在于：每一颗宝石都拥有唯一的属性组合和 tokenId。

因此，CryptoStone 的宝石以 ERC-721 NFT 表示。该选择并不是为了强调某个技术标准，而是为了实现以下功能。

实现需求	采用 ERC-721 的理由
每颗宝石需要唯一 tokenId	ERC-721 适合表达基于唯一 tokenId 的资产。
每颗宝石需要保存不同属性	可通过 tokenId 级 metadata 与 on-chain attribute 结构实现。
需要记录所有权转移	支持标准 NFT 转账和所有权记录。
一个集合中表达多种宝石	可通过 stoneType 属性区分 12 种宝石。
追踪稀有度与交易历史	可实现 NFT 级 provenance 与 rarity tracking。

也就是说，CryptoStone 中的 ERC-721 并不是为了制作图片 NFT，而是作为表达数字宝石唯一性和属性资产性的技术容器。

8. 单一集合与 12 种宝石的共存

CryptoStone 不会将 12 种宝石分别拆分为不同 NFT 集合。所有宝石都由一个 ERC-721 Gem NFT 合约发行。

不过，每个 NFT 会通过 stoneType 属性区分自己属于哪一种宝石。

Token ID	Stone Type	Weight	Color	Clarity	Cut
#10291	Diamond	3.42 CT	D	VVS1	6 Star
#58102	Ruby	8.13 CT	G	VS2	4 Star
#77410	Sapphire	1.25 CT	E	IF	5 Star

这种结构具有以下优点。

优点	说明
集合统一	维持 CryptoStone 作为一个集合的统一身份。
交易数据集中	防止 marketplace 中集合价值和交易数据分散。
稀有度管理方便	可在一个 rarity ranking 体系中比较所有宝石。
保持宝石独立性	通过 stoneType 属性表达各宝石的独立性。
可限制供应量	NFT 合约内部可验证各宝石 max supply。

NFT 合约会单独管理各宝石的发行量。

```
maxSupplyByStone[Diamond] = 110,000
mintedByStone[Diamond] < maxSupplyByStone[Diamond]
```

因此，即使 Diamond Pool 发出 mint 请求，如果 Diamond 已达到最大发行量，也不会再发行 Diamond NFT。

9. 数字矿山的组成

在 CryptoStone 中，每一种宝石都被视为一个独立的数字矿山。

Pool	说明
Garnet Pool	挖掘 Garnet NFT
Amethyst Pool	挖掘 Amethyst NFT
Aquamarine Pool	挖掘 Aquamarine NFT
Diamond Pool	挖掘 Diamond NFT
Emerald Pool	挖掘 Emerald NFT
Pearl Pool	挖掘 Pearl NFT
Ruby Pool	挖掘 Ruby NFT
Spinel Pool	挖掘 Spinel NFT
Sapphire Pool	挖掘 Sapphire NFT
Opal Pool	挖掘 Opal NFT
Topaz Pool	挖掘 Topaz NFT
Zircon Pool	挖掘 Zircon NFT

各挖矿池都使用同一个 STONE 代币，但具有不同的挖矿条件。

项目	含义
Stone Type	该矿池中被挖掘的宝石类型
Max Supply	该宝石的最大发行量
Base Mining Interval	基础挖矿周期
Target Pool Power	基准 Mining Power
Current Pool Power	当前矿池累计 Mining Power
Minted Supply	目前已挖掘数量
Pool Difficulty	根据整体参与度调整的难度
Scarcity Multiplier	基于减半结构的稀缺性倍率

就像现实中钻石矿山和红宝石矿山的储量不同一样，在 CryptoStone 中，每种宝石也拥有不同的总量和挖掘难度。Diamond 被大量挖出并不会导致 Ruby 的难度上升。Ruby 即将枯竭，也不会减少 Sapphire 的供应量。

每种宝石都拥有独立的数字储量与挖掘结构。

10. Hash Power、Mining Power 与 Proof of Mining

在比特币中，矿工通过 Hash Power 获得生成区块的概率。Hash Power 越高，发现区块的可能性越高，但矿工不能任意更改比特币的整体发行规则或难度结构。换言之，Hash Power 并不是改变网络规则的权力，而是在既定规则下获得更多挖矿机会的计算资源。

CryptoStone 将这一概念抽象到数字宝石挖掘结构中。在 CryptoStone 中，对应 Hash Power 的概念是 Mining Power，而 Mining Power 随时间累积形成的工作量就是 Proof of Mining，即 PoM。

Bitcoin	CryptoStone
Hash Power	Mining Power
Proof of Work	Proof of Mining, PoM
ASIC / Mining Equipment	Staked STONE
Block Reward	Gem NFT
Network Difficulty	Pool Difficulty
Halving	Scarcity Multiplier
BTC Issuance	Gem NFT Minting
Miner	STONE Staker / Gem Miner

PoM 不是可以单独转移或交易的代币。PoM 是合约记录用户挖矿参与和时间经过的链上工作量指标。PoM 也不是网络共识算法。CryptoStone 的 PoM 是协议内部用于判断用户在特定宝石矿池中是否达到 claim Gem NFT 条件的数值。

用户 i 在特定宝石矿池 j 中质押的 STONE 数量为 s_{i,j}，锁仓周期对应的倍率为 L_i 时，用户的 Mining Power P_{i,j} 定义如下。

$$P_{i,j} = s_{i,j} \times L_i$$

用户的 PoM 值会随着时间按照以下方式累积。

$$PoM_{i,j}(t + \Delta t) = PoM_{i,j}(t) + P_{i,j} \times \Delta t$$

其中 $PoM_{i,j}(t)$ 表示用户 i 在宝石矿池 j 中截至时间 t 所累积的 Proof of Mining 值。

PoM 按宝石矿池独立累积。例如，在 Diamond Pool 中累积的 PoM 只能用于 claim Diamond NFT，不能转换为 Ruby Pool 或 Sapphire Pool 的 PoM。该结构保护了各宝石矿池的独立性、稀缺性和挖掘难度。

Mining Power 较高的用户可以更快达到所需 PoM 阈值，但不能任意提高宝石稀有等级出现概率，也不能选择特定等级的宝石。

11. Mining Pool Template 与 Factory 结构

12 个 Mining Pool Contract 并不是使用不同逻辑分别开发的合约。所有矿池都基于同一个经过审计的 Mining Pool Template 部署。每个矿池使用相同核心逻辑，只在以下参数上有所不同。

参数	说明
stoneType	该矿池中挖掘的宝石类型
maxSupply	该宝石的最大发行量
baseMiningInterval	基础挖矿周期
targetPoolPower	基准 Mining Power
scarcitySchedule	各宝石的减半结构
poolAddress	NFT 合约允许 mint 的矿池权限地址

因此，CryptoStone 可以采用 Pool Factory 结构。Pool Factory 基于同一个 Mining Pool Template 生成 12 个宝石矿池，并在部署后固定各矿池核心参数。

优点	说明
代码一致性	12 个矿池使用同一逻辑。
审计效率	可围绕一个 Pool Template 进行安全审计。
降低风险	减少每个矿池使用不同代码导致的异常 bug 可能性。
参数透明性	各矿池差异仅由公开固定参数产生。
扩展性	未来新增宝石矿池时可复用同一结构。

因此，CryptoStone 在保持“ 12 个独立矿山 ”经济结构的同时，也能通过统一且可验证的智能合约模板提升安全性和透明度。

12. 各宝石的限定供应量

CryptoStone 的 12 种宝石各自拥有不同的总发行量。该结构为宝石类型本身赋予第一层稀缺性。

Month	Stone	Meaning	Max Supply
January	Garnet	Friendship	160,000
February	Amethyst	Sincerity	170,000

Month	Stone	Meaning	Max Supply
March	Aquamarine	Happiness	180,000
April	Diamond	Love	110,000
May	Emerald	Luck	120,000
June	Pearl	Wealth	150,000
July	Ruby	Peace	130,000
August	Spinel	Wisdom	190,000
September	Sapphire	Truth	140,000
October	Opal	Hope	200,000
November	Topaz	Health	210,000
December	Zircon	Victory	220,000

Gem NFT 的总最大发行量如下。

```
Total Gem NFT Max Supply = 1,980,000
```

Diamond 的供应量最少，Zircon 的供应量最多。因此，宝石类型本身就是稀缺性的一个要素。

从全局集合角度来看，特定宝石 j 的供应占比可以表示为：

```
P_stone,j = N_j ÷ N_total
```

其中 N_j 为特定宝石的最大发行量， N_total 为所有 Gem NFT 的最大发行量。该值可用于后文概率型稀有度指标中，解释宝石类型的相对稀缺性。

CryptoStone 的 Gem NFT 总供应量并不代表单一稀有 NFT 集合的简单发行数量。它代表的是由 12 个宝石矿池和多层属性组合构成的长期挖矿型数字宝石资产群。稀缺性并不只由总数量决定，而是由宝石类型、挖掘时间、减半区间、Weight、Color、Clarity、Cut、tokenId 和 Probability Rarity Index 共同作用。

因此，CryptoStone 中 1,980,000 个总供应量不应被理解为短期 mint 活动的大规模发行结构，而应被理解为一个数字宝石生态系统的总储量，该系统允许大量参与者在长期内挖掘不同宝石和属性组合。

13. 挖矿周期的设计

每种宝石具有不同的基础挖矿周期。

Stone	Base Mining Interval
Garnet	170,000 sec
Amethyst	160,000 sec
Aquamarine	150,000 sec
Diamond	220,000 sec
Emerald	210,000 sec
Pearl	180,000 sec
Ruby	200,000 sec

Stone	Base Mining Interval
Spinel	140,000 sec
Sapphire	190,000 sec
Opal	130,000 sec
Topaz	120,000 sec
Zircon	110,000 sec

基础挖矿周期越长，在相同 Mining Power 下挖掘越困难。因此，各宝石的稀缺性首先由以下两个因素形成。

因素	说明
Max Supply	该宝石可发行的总数量
Base Mining Interval	以基准挖矿单位挖出 1 个所需时间

例如，Diamond 的供应量最少，基础挖矿周期也最长。这意味着 Diamond 在 CryptoStone 生态中被设计为具有最高结构性稀缺性的宝石。

14. STONE 初始发行量的设定

CryptoStone 不会为 12 种宝石分别发行不同代币，而是使用一个统一的 STONE 代币。

初始总发行量设定如下。

```
STONE Initial Total Supply = 1,200,000,000 STONE
Additional Mint = 无
```

将 STONE 设置为 1,200,000,000 个，并不是为了单纯扩大代币数量。CryptoStone 目标是未来让 100,000 名以上用户以不同规模参与挖矿池。因此，需要一种能够让小额参与者、中等规模参与者和高 Mining Power 参与者都能自然参与的单位结构。

在 1,200,000,000 STONE 的结构下，即使假设未来有 100,000 名以上参与者，也可以设计出以数千 STONE 为单位的自然参与体验。这降低了小额参与者的进入门槛，为中等规模参与者提供实际挖矿参与单位，也使高 Mining Power 参与者能够制定长期挖矿策略。

因此，12 亿枚发行量并不是无节制扩大供应，而是为了容纳更广泛用户基础和 Proof of Mining 结构而设计的单位体系。

```
Expected Active Mining Ratio = 约 30% ~ 40%

1,200,000,000 STONE × 40%
= 480,000,000 Active Mining STONE
```

以 100,000 名参与者为基准，平均 active stake 如下。

```
480,000,000 STONE ÷ 100,000 users
= 4,800 STONE per user
```

也就是说，1,200,000,000 STONE 结构既能容纳大规模参与者基础，也能使小额参与者进入挖矿生态。

15. STONE 的 100% 公开流通结构

在 CryptoStone 中，STONE 是参与数字宝石挖掘的单一挖矿资源。笔者认为，相较于向特定内部人士预先分配权利的方式，STONE 的分发结构更应遵循任何人都能以同等条件接触的公开市场结构，这更符合 CryptoStone 的理念。

因此，STONE 采用 100% 公开流通结构。这意味着 STONE 不通过向特定主体预先分配的方式进入市场，而是通过公开 DEX 流动性流通，任何人都可以在同一公开市场条件下取得 STONE。

项目	结构
Total Supply	1,200,000,000 STONE
Distribution Principle	100% 公开流通
Market Access	公开 DEX 流动性
Additional Mint	无
Access Rule	任何人可在同一公开市场条件下取得
Primary Utility	用于参与 Gem NFT 挖矿池
Mechanism	取得 STONE → 质押 → 生成 Mining Power → 累积 PoM → claim Gem NFT
Supply Trust	发行量、矿池结构、概率表、claim 条件可由合约验证

用户在公开市场取得 STONE 后，可以将其投入自己选择的宝石挖矿池。随后，用户基于所质押的 STONE 生成 Mining Power，并随着时间累积 Proof of Mining，即 PoM。当累积的 PoM 达到相应矿池所需阈值时，用户便可以 claim Gem NFT。

在这一结构中，DEX 是进入 STONE 的公开入口，而挖矿池是 STONE 的实际使用场景。也就是说，STONE 的目的并不是单纯持有或投机流通，而是作为参与数字宝石挖掘的协议资源。

基金会或早期生态贡献者也不应通过单独预分配取得 STONE，而是可以在公开市场以同等条件取得 STONE。该方式旨在最小化特定主体的优先占有结构，并将协议参与标准建立在公开市场和链上规则之上。

为了使 100% 公开流通结构获得信任，初始流动性供应方式、LP 处理方式、合约权限、是否无法追加发行等信息必须明确公开。初始流动性通过公开 DEX 池形成，初始 LP 代币的处理方式最好通过长期锁定或销毁方式公开。这有助于减少对流动性被撤回的担忧，并增强对 STONE 公开市场准入结构的信任。

CryptoStone 的信任并不来自特定主体的预分配份额，而是来自固定总发行量、100% 公开流通结构、不可更改的挖矿规则、可验证的 PoM 结构以及链上数据透明性。

16. Base Mining Unit 与小额参与结构

CryptoStone 的基准挖矿单位设定如下。

```
Base Mining Unit = 100,000 STONE
```

但这并不是最低参与数量。Base Mining Unit 是用于计算挖矿速度和难度的基准单位。

CryptoStone 采用 PoM 累积结构，以便尽可能让更多用户参与挖矿。用户即使持有少于 100,000 STONE 的数量，也可以参与挖矿池，并按照质押数量与时间比例累积 PoM。

当用户累积的 PoM 值达到相应矿池所需 PoM 阈值 R_j 以上时，即可 claim Gem NFT。

$$PoM_{i,j}(t) \geq R_j$$

例如，在 Diamond Pool 初始条件下，假设 Pool Difficulty 和 Scarcity Multiplier 均为 1x，则如下。

Active Stake	预计挖出 1 个 Diamond NFT 所需时间
100,000 STONE	约 2.55 天
10,000 STONE	约 25.5 天
5,000 STONE	约 51 天
1,000 STONE	约 255 天
100 STONE	约 6.98 年

该结构既能让高 Mining Power 用户获得较快挖掘机会，也能让小额参与者通过长期累积 PoM 最终 claim Gem NFT。

笔者认为，这一结构对 CryptoStone 生态扩展非常重要。NFT 的稀缺性应通过总发行量、属性概率和减半结构维持，而用户参与性则应通过低进入门槛和 PoM 累积结构扩大。

17. Target Pool Power 与长期挖矿周期

CryptoStone 的 Target Pool Power 并不是以 STONE 总供应量为基准，而是以预计实际参与挖矿的有效质押量为基准进行估算。

$$\text{Target Pool Power} = 40{,}000{,}000 \text{ Power per Pool}$$
$$\text{12 Pools Total Target Power} = 480{,}000{,}000 \text{ Power}$$

这反映了一个假设：在 1,200,000,000 STONE 总供应量中，约 40% 可能长期参与挖矿生态。

特定矿池 j 的总 Mining Power 为 P_j，Target Pool Power 为 P_j^* 时，矿池总算力定义如下。

$$P_j = \Sigma\ P_{i,j}$$

$$P_j^* = 40{,}000{,}000$$

如果参与者每年增加 10,000 人，10 年后约有 100,000 人参与，平均 active stake 约为 4,800 STONE，则整个 Gem NFT 供应量中约 90% 被挖出可能需要约 8~9 年。

由于减半结构的影响，90% 之后的挖矿速度会进一步放缓。因此，全部 Gem NFT 100% 被挖出可能需要约 12 年以上。

这种时间估算并不是为了预测特定收益率或价格，而是为了说明 CryptoStone 并不是短期 NFT mint 活动，而是一个长期逐步挖掘数字宝石的去中心化挖矿生态。

18. 对数值和参数的解释

本白皮书中提出的各宝石供应量、基础挖矿周期、Mining Power 公式、PoM 阈值、减半倍率、Weight · Color · Clarity · Cut 概率表和 Rarity Score 公式，并不是对现实宝石生态的绝对完整复制。

这些数值是为以下目的设计的初始基准参数。

目的	说明
表达数字稀缺性	在链上环境中表达宝石稀缺性
实现挖矿难度	通过智能合约实现挖矿难度和供应限制
区分相对稀缺性	设计可比较的宝石稀缺性差异
区分收藏价值	通过稀有度和等级结构增强收藏市场理解
控制长期供应	通过减半和难度上升管理供应速度
扩展参与性	同时容纳小额参与者和大规模参与者

因此，本白皮书中的数值并不能被视为完全反映现实宝石市场的所有价格形成因素、鉴定标准、流通结构、供需关系、文化价值、实物保管成本和鉴定机构评估模型。

CryptoStone 并不是试图完全复制现实宝石市场，而是一个尝试在数字环境中以去中心化方式实现宝石核心属性——稀缺性、等级性、可开采性和收藏性——的项目。

笔者认为，本白皮书中的数值并非单纯任意值，而是用于说明和实验“ 去中心化数字宝石 ”这一概念的初始基准值。未来可根据研究、市场反馈、社区讨论、技术验证和法律审查进一步发展为更精细的模型。但在协议正式部署并核心规则确定之后，已确认的核心数值不应被运营方任意更改。

19. Mining Power 的计算

在 CryptoStone 中，Mining Power 决定用户挖掘宝石的速度和机会。质押更多 STONE 的参与者会获得更多 Mining Power，并更频繁地达到 claim 条件。

用户 i 的质押数量为 $s_{i,j}$，锁仓倍率为 L_i，用户 Mining Power 为 $P_{i,j}$ 时，计算如下。

$$P_{i,j} = s_{i,j} \times L_i$$

Mining Power 并不会直接提高宝石等级概率。Mining Power 只影响 PoM 累积速度。

这类似比特币挖矿结构。拥有更多挖矿设备的参与者可以获得更多挖矿机会，但不能更改挖矿规则本身。在 CryptoStone 中，质押更多 STONE 的参与者可以更快累积 PoM，但不能任意提高获得更好宝石的概率。

20. 长期参与补正与 Flexible Cooldown

为了奖励长期参与者，可以根据质押周期适用 Lock Multiplier。

Lock Type	Lock Period	Mining Multiplier L_i	Maturity Burn	Returned STONE	Cooldown
Flexible	无	1.00x	0%	100%	7 days
Short Lock	90 天	1.05x	2.5%	97.5%	无
Medium Lock	180 天	1.12x	5%	95%	无
Long Lock	365 天	1.25x	10%	90%	无

Flexible Lock 没有折旧销毁，但为了防止短期流动性过快进出，在 unstake 请求后设置 7 天 cooldown。

长期锁仓不是强制条件，而是选择项。用户可以选择没有折旧销毁的 Flexible 模式；如果希望获得更高 Mining Power，则可以选择伴随一定折旧的长期锁仓。

锁仓倍率最高限制为 1.25 倍。这是为了在合理奖励长期参与者的同时，避免特定大型参与者获得过度优势。

即使在锁仓期间，只要用户的 PoM 值达到所需阈值，也可以 claim Gem NFT。换言之，锁仓限制的是 STONE 可返还时间，而不是禁止 Gem NFT claim。

21. Proof of Mining, PoM 的累积

CryptoStone 并不采用简单的积分或信用点方式，而是使用将比特币 Proof-of-Work 概念抽象到数字宝石挖掘结构中的 Proof of Mining，即 PoM 模型。

PoM 表示用户将 STONE 质押到特定宝石矿池后，随时间累积的挖矿工作量。PoM 不是单独可转移或交易的代币，而是合约记录用户挖矿参与和时间经过的链上工作量指标。

用户 i 对特定宝石矿池 j 的 PoM 值随时间按如下方式累积。

$$PoM_{i,j}(t + \Delta t) = PoM_{i,j}(t) + P_{i,j} \times \Delta t$$

例如，用户以 Flexible 条件在 Diamond Pool 质押 100,000 STONE，其 Mining Power 为：

$$P_{i,Diamond} = 100,000 \times 1.00 = 100,000$$

如果该用户等待 100,000 秒，则累积的 PoM 为：

$$PoM = 100,000 \times 100,000$$
$$PoM = 10,000,000,000$$

当用户累计 PoM 达到对应矿池所需 PoM 阈值以上时，可以 claim Gem NFT。

$$PoM_{i,j}(t) \geq R_j$$

Gem NFT 被 claim 后，用户在该矿池的 PoM 值会扣除所需阈值 R_j。

$$PoM_{i,j,new} = PoM_{i,j,old} - R_j$$

该结构不会无谓消除用户超过阈值的 PoM。例如，所需 PoM 阈值为 22,000,000,000，而用户持有 23,000,000,000 PoM 时 claim Gem NFT，则 claim 后剩余 1,000,000,000 PoM 会继续保留，用于下一次挖掘。

PoM 按各宝石矿池独立累积。Diamond Pool 中累积的 PoM 只能用于 claim Diamond NFT，不能转换为 Ruby Pool 或 Sapphire Pool 的 PoM。该结构保护了各宝石矿池的独立性、稀缺性和挖矿难度。

如果用户从特定矿池 unstake STONE，已累积的 PoM 可继续记录在该矿池中。但 unstake 后，用户在该矿池的 Mining Power 变为 0，因此不会继续累积新的 PoM。若用户再次在同一矿池质押 STONE，则会在既有 PoM 基础上继续累积新的 PoM。

PoM 不可对外转让或交易，也不可转移到其他宝石矿池。这是因为 PoM 不是资产本身，而是在特定矿池中，特定用户通过实际挖矿参与累积的工作量指标。

22. 所需 PoM 阈值

挖掘 1 个宝石所需的 PoM 阈值由 Base Mining Unit、各宝石基础挖矿周期、矿池难度和稀缺性倍率决定。

宝石 j 的基础挖矿周期为 T_j，Base Mining Unit 为 B，矿池难度为 D_j，稀缺性倍率为 S_j 时，所需 PoM 阈值 R_j 定义如下。

$$R_j = B \times T_j \times D_j \times S_j$$

CryptoStone 的基准值如下。

```
B = 100,000 STONE
Target Pool Power = 40,000,000 Power
```

例如，Diamond Pool 的基础挖矿周期为 220,000 秒，Pool Difficulty 和 Scarcity Multiplier 均为 1x 时：

```
R_Diamond = 100,000 × 220,000 × 1 × 1
R_Diamond = 22,000,000,000 PoM
```

当用户 i 的 Mining Power 为 P_{i,j} 时，该用户挖出 1 个宝石 j 所需的预计时间可表示为：

```
E[T_{i,j}] = R_j ÷ P_{i,j}
```

例如，用户以 Flexible 条件在 Diamond Pool 中质押 100,000 STONE 时：

```
E[T_{i,Diamond}] = 22,000,000,000 ÷ 100,000
= 220,000 秒
≈ 2.55 天
```

也就是说，在初始条件下，质押 100,000 STONE 的用户约每 2.55 天可以 claim 1 个 Diamond NFT。

23. 矿池难度调整

当参与者增多、总 Mining Power 增加时，宝石可能被过快挖出。为了防止这一点，各矿池会根据整体 Mining Power 调整难度。

宝石矿池 j 的总 Mining Power 为 P_j，Target Pool Power 为 P_j^*，矿池难度为 D_j 时，计算如下。

```
D_j = max(1, P_j ÷ P_j^*)
```

CryptoStone 的基准值如下。

```
P_j^* = 40,000,000 Power
```

示例如下。

Target Pool Power	Total Pool Mining Power	计算	Pool Difficulty
40,000,000	20,000,000	20,000,000 ÷ 40,000,000 = 0.5 → max(1, 0.5)	1.0x
40,000,000	40,000,000	40,000,000 ÷ 40,000,000 = 1.0	1.0x
40,000,000	80,000,000	80,000,000 ÷ 40,000,000 = 2.0	2.0x
40,000,000	200,000,000	200,000,000 ÷ 40,000,000 = 5.0	5.0x

公式中应用 max(1, ·) 的原因是，即使总 Mining Power 低于 Target Pool Power，难度也不会低于 1.0x。也就是说，即使在早期参与者较少的阶段，也要防止挖矿速度过度快于基准。

相反，如果总 Mining Power 超过 Target Pool Power，Pool Difficulty 会按比例上升。例如，某矿池总 Mining Power 增至 80,000,000 Power，则 Pool Difficulty 为 2.0x。在这种情况下，同一用户挖出 1 个 NFT 所需时间也约增加至 2 倍。

在智能合约实现中，可使用 BPS 方式避免小数计算。

```
D_{j,BPS} = max(10,000, P_j × 10,000 ÷ P_j^*)
```

其中 10,000 BPS = 1.0x。

这一结构使参与者增加时整体挖矿速度自然调整，并防止各宝石供应在短时间内过度枯竭。

24. 减半与稀缺性倍率

CryptoStone 的减半并不是以整个集合为基准，而是对每种宝石独立适用。

宝石 j 的最大发行量为 N_j，当前已挖掘数量为 n_j，挖掘进度为 q_j 时，计算如下。

```
q_j = n_j ÷ N_j
```

例如，Diamond 的最大发行量为 110,000 个，目前已挖出 55,000 个，则：

```
q_Diamond = 55,000 ÷ 110,000 = 0.5
```

也就是说，Diamond Pool 已达到 50% 挖掘阶段。

各宝石稀缺性倍率 S_j 根据挖掘进度 q_j 上升。

Mined Supply Ratio	Remaining Supply	Scarcity Multiplier
0% ~ 50%	100% ~ 50%	1x
50% ~ 75%	50% ~ 25%	2x
75% ~ 87.5%	25% ~ 12.5%	4x
87.5% ~ 93.75%	12.5% ~ 6.25%	8x
93.75% ~ 96.875%	6.25% ~ 3.125%	16x
96.875% 以上	3.125% 以下	32x

可将其一般化为如下公式。

```
S_j(q_j) = 2^min(5, floor(log2(1 ÷ (1 - q_j))))
```

但当 q_j 处于初始区间时， S_j(q_j) 至少保持 1x。实际智能合约中可不直接计算上述公式，而是使用预先公开的区间表实现。

该公式表达了随着各宝石剩余供应量减少，挖掘难度会以指数方式上升的结构。这将现实矿山中储量减少导致开采成本和难度上升的结构迁移到了数字环境中。

25. 挖矿速度与供应枯竭的非线性结构

CryptoStone 的挖矿结构并不是简单线性 mint 模型。每种宝石拥有独立的供应量、挖矿周期、矿池难度和稀缺性倍率，随着挖掘进度上升，稀缺性倍率会使挖掘速度放缓。

宝石矿池 j 的有效 Mining Power 为 P_{eff,j} 时，可表示为：

```
P_{eff,j} = min(P_j, P_j^*)
```

这意味着当总 Mining Power 低于 Target Pool Power 时，实际参与算力影响挖矿速度；当总 Mining Power 超过 Target Pool Power 时，难度上升会限制有效挖矿速度。

宝石矿池 j 单位时间内的预计挖掘量 λ_j 可概念性表示如下。

```
λ_j = P_{eff,j} ÷ (B × T_j × S_j)
```

其中 B 为 Base Mining Unit， T_j 为各宝石 Base Mining Interval， S_j 为 Scarcity Multiplier。

某宝石达到挖掘进度 q 所需时间可用如下非线性模型表示。

$$Time_j(q) = (N_j \times B \times T_j \div P_{eff,j}) \times \int_0^q S_j(x)\,dx$$

该公式表明，CryptoStone 的挖矿结构并不是线性枯竭模型，而是随着宝石剩余供应减少而逐渐放缓的非线性挖矿模型。

因此，早期阶段 Gem NFT 会相对活跃地被挖出，但在 90% 之后，Scarcity Multiplier 会上升，剩余供应量的挖掘速度会显著放缓。

26. Weight 属性的数字化

重量是所有宝石共同使用的 CT，即克拉单位。但每颗宝石的重量值是随机生成的。

```
Minimum Weight = 0.10 CT
Maximum Weight = 200.00 CT
Storage Unit = 0.01 CT
```

智能合约不直接存储小数，而是以 0.01 CT 为单位的整数存储。

显示重量	合约存储值
0.10 CT	10
1.25 CT	125
10.50 CT	1050
200.00 CT	20000

重量并非均匀概率生成。正如现实宝石中克拉越大的宝石越稀有，在 CryptoStone 中，重量越大的宝石出现概率也越低。

Weight Range	Probability	Rarity Tier	Score
0.10 ~ 0.99 CT	50.00%	Common	2
1.00 ~ 1.99 CT	25.00%	Uncommon	5
2.00 ~ 4.99 CT	15.00%	Rare	9
5.00 ~ 9.99 CT	6.00%	Epic	13
10.00 ~ 19.99 CT	2.50%	Legendary	17
20.00 ~ 49.99 CT	1.00%	Mythic	20
50.00 ~ 99.99 CT	0.40%	Ancient	23
100.00 ~ 200.00 CT	0.10%	Genesis	25

27. Color 属性的数字化

Color 表示宝石的颜色等级。等级越高，生成概率越低。

Color Grade	Probability	Score
D	1%	15
E	2%	13
F	4%	11
G	8%	8
H	15%	5
I	20%	3
J	25%	1
K	25%	1

28. Clarity 属性的数字化

Clarity 表示宝石的净度等级。

Clarity Grade	Probability	Score
FL	0.5%	20
IF	1.0%	18
VVS1	2.0%	16
VVS2	4.0%	13
VS1	8.0%	10
VS2	14.0%	7
SI1	25.0%	4
SI2	45.5%	1

29. Cut 属性的数字化

Cut 表示宝石的切工等级。

Cut Grade	Probability	Score
6 Star	1%	20
5 Star	4%	16
4 Star	10%	12
3 Star	20%	8
2 Star	30%	4
1 Star	35%	1

30. 属性生成与随机验证

宝石属性不是由运营方手动输入的。在挖掘时，挖矿合约会基于随机值决定 Weight、Color、Clarity、Cut。

关键在于随机生成方式必须可验证。如果运营方能够任意生成高等级 NFT，CryptoStone 的去中心化和稀缺性将被破坏。

因此，CryptoStone 的随机生成方式遵循以下原则。

原则	说明
不可预先预测	运营方和用户均不得提前知道结果。
不可选择结果	运营方不得只选择有利结果或拒绝不利结果。
防止重试	随机请求后、结果确定前，用户不得取消 claim 或重试。
禁止 Admin Reroll	运营方不得对特定结果重新抽取或替换。
公开验证	结果生成过程必须能以链上或公开方式验证。
概率表固定	属性概率表在部署前公开，并在 finalize 后不可更改。
Mint 后不变	Mint 后属性不得更改。

初期实现可优先考虑可验证的外部 VRF 结构，也可使用 Commit-then-Reveal 等方式，将随机请求时间点与结果确定时间点分离。无论采用何种方式，用户都不得在结果确定前取消 claim 或重试，运营方也不得选择或重抽特定结果。

随机结果请求后，用户不得因结果不利而取消或重试 claim。运营方也不得向特定用户分配有利结果，或选择 seed 以获得特定属性组合。这是确保稀有宝石由可验证随机结构决定，而非运营方裁量决定的核心条件。

Mint 后，Gem NFT 的核心属性应被冻结，Weight、Color、Clarity、Cut、stoneType、minedAt、minedFromPool 等核心 metadata 不应被运营方更改。

31. Rarity Score 与 Probability Rarity Index

CryptoStone 使用两个指标对每颗宝石的稀有度进行数值化。

指标	目的
Rarity Score	用户可以直观理解的 0~100 分数
Probability Rarity Index	基于实际发生概率的数学稀有度指标

31.1 Rarity Score

```
Rarity Score
= Stone Scarcity Score
+ Weight Score
+ Color Score
+ Clarity Score
+ Cut Score
```

分数分配如下。

Attribute	Max Score
Stone Scarcity	20
Weight	25
Color	15
Clarity	20
Cut	20
Total	100

Stone Scarcity Score 基于各宝石总发行量计算。

```
Stone Scarcity Score
= 20 × (MaxCollectionSupply - StoneMaxSupply)
÷ (MaxCollectionSupply - MinCollectionSupply)
```

基准值如下。

```
MaxCollectionSupply = 220,000
MinCollectionSupply = 110,000
```

例如，Diamond 的 Max Supply 为 110,000 个，因此具有最高 Stone Scarcity Score。Zircon 的 Max Supply 为 220,000 个，因此具有最低 Stone Scarcity Score。

31.2 Probability Rarity Index

如果 Rarity Score 是用户友好的比较指标，那么 Probability Rarity Index 则是基于各属性发生概率的数学稀有度指标。

Gem NFT g 的属性组合发生概率 P(g) 定义如下。

```
P(g) = P_stone × P_weight × P_color × P_clarity × P_cut
```

基于该概率，计算概率型稀有度指标。

```
Probability Rarity Index = -log10(P(g))
```

该指标显示某个 Gem NFT 的属性组合在概率上有多稀有。

例如，以下组合极其稀有。

```
Diamond
+ 100.00 CT 以上
+ D Color
+ FL Clarity
+ 6 Star Cut
```

这样的组合不仅会在 Rarity Score 中获得高分，也会在 Probability Rarity Index 中表现出极高稀有度。

CryptoStone 同时使用这两个指标，使收藏者能够获得直观可理解的分数体系，同时也能获得基于数据验证的稀有度体系。

32. 稀有度等级结构

完全顶级组合只会以极低概率生成。这在稀缺性方面是优点，但在收藏市场中，也需要形成多个不同的高等级层级，以促进交易和收藏活动。

因此，CryptoStone 可以基于 Rarity Score 和 Probability Rarity Index 适用以下稀有度等级结构。

Tier	示例标准	含义
Common	以普通属性为主	最常见的宝石群
Rare	至少 1 个上位属性	普通稀有宝石
Epic	至少 2 个上位属性	具有较高收藏价值的宝石
Legendary	至少 3 个上位属性	非常稀有的宝石
Genesis	极端组合或早期挖掘唯一性	顶级收藏资产

Genesis Tier 不一定只由分数决定。早期挖掘时间、较低 tokenId、极端概率组合、特定宝石稀缺性等都可能被综合考虑。

该结构类似于宝可梦卡、体育卡、限量收藏品市场中由稀有等级形成收藏价值的方式。但在 CryptoStone 中，稀有度并非由运营方主观判断，而是由公开概率表和链上属性值计算得出。

33. 收藏价值的形成

在收藏市场中，稀缺性是重要的价值形成因素。宝可梦卡、体育卡、限量手办、艺术品、高级手表等并不只因使用价值形成价格。特定系列、限定数量、稀有等级、保存状态、市场需求、社区认知共同作用，最终形成价格。

CryptoStone 将这种收藏经济原理应用于数字宝石。

因素	说明
各宝石总发行量	Diamond、Ruby、Sapphire 等宝石供应差异
各矿池挖矿难度	各矿池的 Target Power 与 Difficulty
各宝石减半结构	挖掘量增加带来的 Scarcity Multiplier 上升
Weight 概率	克拉越大，概率越低
Color 概率	颜色等级越高，概率越低
Clarity 概率	净度等级越高，概率越低
Cut 概率	切工等级越高，概率越低
较低 tokenId	早期挖掘宝石的收藏性
挖掘时间	特定时期或减半前后的意义
链上交易历史	所有权与 provenance 记录

这一结构使用户不是简单购买 NFT 图片，而是在公开概率结构中收藏被挖掘出的唯一数字宝石。

在 CryptoStone 中，稀缺性不是营销文案。稀缺性由合约中固定的数量、概率表、挖矿难度和减半结构共同形成。

34. 去中心化挖矿结构

CryptoStone 中的挖矿不是由服务器代替执行的方式。用户将 STONE 质押到自己选择的宝石矿池中，随着时间推移，当 PoM 达到相应矿池所需阈值后，用户可以直接调用 claimGem() 等合约函数领取 Gem NFT。

步骤	说明
1	用户持有 STONE。
2	选择希望参与的宝石矿池。
3	质押 STONE。
4	产生 Mining Power。
5	随时间累积 PoM。
6	PoM 达到所需阈值后调用 claimGem()。
7	合约验证是否可挖掘。
8	使用可验证随机值生成属性。
9	Mint ERC-721 Gem NFT。
10	NFT 转入用户钱包。

在该过程中，中央服务器不会发行宝石，也不会指定属性。挖矿条件和结果由代码决定。

智能合约不会自行自动执行。但任何人都可以调用合约，合约会根据预先定义的条件验证并执行结果。因此，CryptoStone 的挖矿结构可以在没有中央服务器的情况下运行。

笔者认为，在这一结构中，重要的并不是“ 没有服务器 ”这一事实本身，而是“ 即使没有服务器，用户也可以直接调用合约，并根据既定规则获得挖矿结果 ”这一点。

35. 挖矿成本与 STONE 销毁结构

在 CryptoStone 中，STONE 不只是支付工具，而是参与数字宝石挖矿的挖矿资源。正如现实矿山中使用挖矿设备和能源，而设备会随时间磨损一样，在 CryptoStone 中，投入挖矿池的 STONE 也具有一定的数字折旧结构。

笔者认为，STONE 销毁结构并不是为了保证代币价格上涨，而是用于表达数字宝石挖矿所需的资源消耗与稀缺性结构。

CryptoStone 的 STONE 销毁主要可能发生在两种情况下。

销毁类型	发生时间	目的
Claim Burn	claim Gem NFT 时	表达挖矿成本与稀缺性
Maturity Burn	锁仓结束后 unstake 时	表达挖矿资源折旧

claim Gem NFT 时发生的销毁量 B_{claim,j} 通过以下公式计算。

$$B_{claim,j} = \beta \times S_j$$

其中 β 为 Base Claim Burn， S_j 为该宝石的 Scarcity Multiplier。

初始基准值如下。

$$\beta = 20 \text{ STONE}$$

Scarcity Multiplier	Claim Burn
1x	20 STONE
2x	40 STONE
4x	80 STONE
8x	160 STONE
16x	320 STONE
32x	640 STONE

Base Claim Burn 是表达挖矿成本的最低消耗结构，并不是为了急剧减少总供应量的装置。被销毁的 STONE 不会支付给运营方或基金会，而是永久从流通量中移除。由此，STONE 不只是被存入的资产，而是在 CryptoStone 生态中实际被使用和消耗的数字挖矿资源。

36. 锁仓折旧与返还结构

当用户选择锁仓周期并将 STONE 投入挖矿池时，在锁仓结束后的 unstake 阶段，一部分 STONE 会根据锁仓周期进行折旧销毁，其余 STONE 会返还。

Lock Type	Lock Period	Mining Multiplier	Maturity Burn	Returned STONE	Cooldown
Flexible	无	1.00x	0%	100%	7 days
Short Lock	90 天	1.05x	2.5%	97.5%	无
Medium Lock	180 天	1.12x	5%	95%	无
Long Lock	365 天	1.25x	10%	90%	无

用户 i 所质押的 STONE 数量为 s_i，锁仓周期对应折旧率为 δ_i 时，到期销毁的 STONE 数量 M_i 定义如下。

$$M_i = s_i \times \delta_i$$

返还的 STONE 数量 R_i 如下。

$$R_i = s_i - M_i$$

该结构为长期参与者提供更高 Mining Power，同时反映挖矿资源使用带来的成本。也就是说，用户可以选择更长期锁仓获得更高挖矿速度，但在锁仓结束时需要承担更高折旧销毁。

长期锁仓不是强制条件。若用户不愿承担 STONE 销毁负担，可以选择 Flexible 模式。长期锁仓是为希望获得更高 Mining Power 的参与者提供的选择型结构，折旧则是该选择所伴随的数字挖矿资源使用成本。

笔者认为，这一结构不应被视为单纯惩罚，而应被解释为“数字挖矿设备使用带来的折旧”。正如现实挖矿设备会因使用时间而磨损，CryptoStone 中的 STONE 在投入挖矿池期间提供 Mining Power，并根据使用周期销毁一部分。

37. 开发结构的选择

CryptoStone 采用以下结构。

STONE ERC-20
+ ERC-721 CryptoStone Gem NFT
+ 12 个 Mining Pool Contract
+ Pool Factory

该结构并不是单纯罗列技术标准，而是为了满足 CryptoStone 希望实现的属性和功能。

选择	理由
STONE ERC-20	提供单一挖矿资源与流动性结构。
ERC-721 Gem NFT	表达每颗宝石的唯一性和属性。
12 Mining Pools	实现各宝石独立矿山结构。
Pool Factory	通过同一验证模板部署矿池。
Unified NFT Contract	集中一个集合身份与交易数据。
Verifiable Randomness	实现无运营方操纵的属性生成。
Finalize Mechanism	防止核心规则更改。

第一，分离 STONE 与 Gem NFT 的作用。STONE 是用于 Mining Power 的代币，Gem NFT 是挖掘结果物。

第二，保护宝石唯一性。每个 Gem NFT 拥有 tokenId 和属性组合，并且 mint 后属性不可更改。

第三，保持各宝石独立性。各挖矿池具有独立供应量、挖矿周期和减半结构，因此适合数字化表达现实中的独立矿山概念。

第四，NFT 集合保持统一。这有助于集中 CryptoStone 的品牌和市场数据，并统一管理交易和稀有度排名。

第五，未来扩展性较高。初期可从 EVM 智能合约开始，长期可扩展为独立 Appchain 或 Mainnet。

第六，减少中心化依赖。挖矿和 mint 由合约执行，而不是服务器执行，任何人都可以验证条件。

38. 协议固定原则

CryptoStone 若要追求类似比特币的去中心化资产属性，部署后核心规则不得被任意更改。

固定项目	说明
STONE 总发行量	1,200,000,000 STONE
STONE 流通结构	100% 公开流通
各宝石 Max Supply	各宝石 NFT 最大发行量
各宝石 Base Mining Interval	基础挖矿周期
Target Pool Power	初始基准值 40,000,000 Power
Base Mining Unit	100,000 STONE
Weight 概率表	重量生成概率
Color 概率表	颜色等级生成概率
Clarity 概率表	净度等级生成概率
Cut 概率表	切工等级生成概率

固定项目	说明
Scarcity Multiplier	基于减半的难度倍率
Claim Burn 公式	claim 时销毁公式
Mining Power 公式	基于质押的 Mining Power 公式
PoM 公式	Proof of Mining 累积与 claim 条件
Lock Multiplier	各锁仓周期 Mining Power 倍率
Maturity Burn 公式	锁仓结束时折旧销毁公式

初始设置完成后，协议应被 finalize。此后，运营方不得任意增加发行量、修改稀有度概率，或手动向特定用户 mint NFT。

CryptoStone 的核心合约部署后应公开验证源码，代币发行量、NFT 供应量、概率表、挖矿公式、PoM 阈值计算结构在 finalize 后不得更改。

如果 finalize 前存在必要的有限管理功能，则该功能列表、目的、移除时间和控制方式必须明确公开。finalize 后，与核心发行量、概率表、mint 权限、PoM 计算方式相关的管理员权限应被移除或停用。

去中心化并不会仅因部署在区块链上而自动完成。去中心化形成于运营方无法更改的规则、任何人都可验证的代码，以及任何人都能参与的结构之中。

39. 安全应对与去中心化的平衡

CryptoStone 将 No Admin Mint 和 No Central Server 作为核心原则。但在初期开发和部署阶段，可能需要用于安全审计、测试和漏洞应对的有限管理结构。

阶段	管理结构
测试网与审计阶段	可能存在有限管理权限
正式部署前	参数验证与安全检查
正式上线后	移除核心 mint、供应、概率修改权限
finalize 后	No Admin Mint, No Supply Change, No Probability Change

如果存在紧急暂停功能，该功能不应被用于操纵 mint 结果或修改供应量，而只能作为防止安全事故的有限功能使用。此外，紧急功能应通过 timelock 或 multisig 等公开可验证方式进行限制，不得成为运营方任意修改稀有度或发行量的手段。

CryptoStone 的主要合约包括代币合约、Gem NFT 合约、Mining Pool Template、Pool Factory 和随机生成结构。这些合约在部署前后最好接受安全审计，审计结果与主要漏洞应对内容应公开。

应公开的核心验证要素如下。

验证项目	说明
Contract Source Verification	公开并验证已部署合约源码
Audit Report	主要合约与随机结构审计报告
Admin Function List	管理员函数存在与否及移除计划

验证项目	说明
Finalize Event	核心参数固定时间点与事件记录
LP Lock / Burn Proof	初始流动性相关 LP 处理记录
Probability Table Hash	验证概率表是否与部署前公开值一致
Metadata Freeze	mint 后核心属性是否不可更改

该结构旨在平衡实际安全应对与去中心化资产属性。

40. 图像与元数据的位置

CryptoStone 并不否定视觉表达。宝石 NFT 可以通过图像、3D 模型、视觉卡片形式呈现，以提升用户体验和收藏便利性。

但图像并不是 CryptoStone 的本质。

CryptoStone 的本质在于以下数据。

数据	说明
stoneType	宝石类型
weight	重量
colorGrade	颜色等级
clarityGrade	净度等级
cutGrade	切工等级
rarityScore	用户友好的稀有度分数
probabilityRarityIndex	概率型稀有度指标
minedAt	挖掘时间
minedFromPool	挖掘来源矿池
tokenId	NFT 唯一标识符

因此，即使图像服务器暂时中断，CryptoStone NFT 的核心属性也应保留在链上。这一设计旨在弥补现有 NFT 过度依赖外部图像或中央服务器的问题。

41. 生态扩展模块与 Gem Refinement

CryptoStone 的核心协议由 STONE、12 个宝石挖矿池、Proof of Mining，以及基于 ERC-721 的 Gem NFT 组成。但 CryptoStone 生态并不限于核心挖矿结构，未来可以通过增加额外智能合约，或开发与已部署合约联动的扩展模块，扩展出多种使用功能。这些扩展功能可能包括 Marketplace、Arena Game、Ranking System、Collection Quest、Gem Refinement 等。

Gem Refinement，即宝石精炼，是这些生态扩展模块之一。它是一种选择型的挖矿后实用功能结构，旨在让已挖掘的 Gem NFT 能够再次在生态中被使用。Gem Refinement 并不是额外的无限 NFT 发行结构，而是将两个具有相同 stoneType 的 Gem NFT 结合，生成一个同样 stoneType 的 Refined Gem NFT 的供应压缩机制。

```
Gem NFT 2 个
+ 少量 STONE 使用或销毁
→ Parent Gem NFTs Burned
→ Refined Gem NFT 1 个 Minted
```

每执行一次精炼，两个父级 Gem NFT 会被销毁或以不可回收方式处理，只生成一个新的 Refined Gem NFT。因此，总流通 NFT 数量减少 1 个。

```
2 Gem NFTs Burned → 1 Refined Gem NFT Minted
Net Circulating NFT Supply = -1
```

初期 Gem Refinement 最好只允许相同宝石之间的精炼。例如，两个 Diamond Gem NFT 可以精炼为一个 Refined Diamond Gem NFT，两个 Ruby Gem NFT 可以精炼为一个 Refined Ruby Gem NFT。不同宝石之间的精炼可能会使各宝石供应量、稀缺性、减半和挖矿难度结构复杂化，因此在初期模型中排除更为合适。

项目	原则
所需材料	两个相同 stoneType 的 Gem NFT
额外成本	少量 STONE 使用或销毁
父 NFT 处理	两个父级 Gem NFT 被销毁或不可回收处理
结果物	一个相同 stoneType 的 Refined Gem NFT
世代信息	记录为 Gen1 或 Refined Generation
供应效果	总流通 NFT 数量减少
Mint 权限	限定于 Refining Contract
Admin Mint	无
随机性	使用可验证随机结构

Refined Gem NFT 的基础等级可以根据两个父级 Gem NFT 中较高的等级计算。

```
T_base = max(T_1, T_2)
```

其中 T_1 、 T_2 分别表示两个父级 Gem NFT 的等级， T_{base} 表示用于确定精炼结果的基础等级。

等级结构可以简化如下。

Tier Level	Tier
1	Common
2	Rare
3	Epic
4	Legendary

精炼结果应被设计为：与基础等级相同的结果出现概率最高。下降一级的概率应保持非常低。如果发生升级，通常应限制在上升 1 至 2 个等级之内。较低等级可以拥有相对更高的升级概率，而较高等级的升级概率应显著降低，以保护高等级 Gem NFT 的稀缺性。

可以采用基于 BPS 的阈值模型，使用从 0 到 9,999 的随机值 U 。

```
U ∈ [0, 9,999]
10,000 BPS = 100%
```

在两个父级 Gem NFT 没有等级差的情况下，基础阈值模型示例如下。

Base Tier	-1 Tier	Same Tier	+1 Tier	+2 Tier
Common	无	68.0%	27.0%	5.0%
Rare	1.0%	76.0%	20.0%	3.0%
Epic	1.5%	88.5%	10.0%	无
Legendary	2.0%	98.0%	无	无

该结构的目的，是在保持精炼期待感的同时，防止高等级 NFT 被过度生成。Common 和 Rare Gem NFT 具有相对更高的升级可能性，从而为低等级或重复 Gem NFT 赋予额外用途。从 Epic 开始，升级概率显著降低。Legendary 在该精炼模型中被视为最高等级，不允许进一步向上提升。

如果两个父级 Gem NFT 具有不同等级，则升级概率可以进一步调整。等级差 G 定义如下。

```
G = |T_1 - T_2|
```

Tier Gap G	Upgrade Modifier	原则
0	100%	同等级精炼，适用基础概率。
1	70%	相邻等级精炼，升级概率部分降低。
2	35%	较大等级差，升级概率显著降低。
3 或以上	限制	初期模型中可限制精炼。

调整后的升级概率可计算如下。

```
Adjusted Upgrade Probability
= Base Upgrade Probability × Upgrade Modifier
```

因该调整而减少的升级概率，会加回到维持同等级的概率中。这可以防止用户反复将一个高等级 Gem NFT 与明显低等级 Gem NFT 结合，以过于容易地生成更高等级输出。

Refining Contract 应执行所有权验证、相同宝石验证、等级差验证、STONE 使用或销毁、父 NFT 销毁、随机值请求，以及结果 Refined Gem NFT 的 mint 请求。Refined Gem NFT 不得通过运营方任意 mint 创建。它只能在 Refining Contract 验证所有预定义条件均满足后生成。

Gem Refinement 并不替代 CryptoStone 的核心挖矿结构。它是一种选择型扩展模块，旨在增强 Gem NFT 在挖矿后的使用性、收藏性、市场需求和潜在游戏用途。除 Gem Refinement 外，CryptoStone 也可以通过 Marketplace、Arena Game、Ranking System、Collection Quest 等多种扩展模块，逐步扩展其数字宝石生态。

42. 网站、模拟器与浏览器的必要性

CryptoStone 协议本身由智能合约与链上数据运行，但为了让用户能够直观理解并参与其中，需要独立的用户界面。

因此，CryptoStone 生态中可能需要以下基于网页的工具。

工具	作用
Mining Simulator	根据用户持有的 STONE 数量、选择的矿池和锁仓周期计算预计挖矿时间。
PoM Dashboard	显示用户各矿池 PoM 值、所需 PoM 阈值和 claim 可能性。

工具	作用
Pool Dashboard	显示各宝石矿池的挖掘量、剩余数量、Pool Difficulty、Scarcity Multiplier。
Gem Explorer	查询已挖出 Gem NFT 的属性、稀有度、tokenId、挖掘时间、交易历史。
Rarity Explorer	查看 Weight、Color、Clarity、Cut 组合对应的稀有度与 Probability Rarity Index。
Protocol Status Page	可验证地展示 100% 公开流通、No Admin Mint、总发行量、概率表、矿池状态等核心协议信息。

这些工具并不替代协议的核心信任基础，而是帮助用户更容易理解链上数据的界面。也就是说，CryptoStone 的本质在于合约和链上规则，而网站与浏览器只是解释和可视化这些规则的工具。

43. 未来推进方向

CryptoStone 初期最好基于 EVM 兼容网络，以 ERC-20、ERC-721 和 Mining Pool Contract 结构启动。在该阶段，应重点验证协议核心功能，包括质押、Mining Power 计算、PoM 累积、各宝石减半、宝石属性生成和 Gem NFT mint 结构。

随后，为了让用户更容易参与，需要扩展挖矿仪表盘、Mining Simulator、PoM Dashboard、Gem Explorer、Rarity Explorer、各宝石交易数据和 NFT marketplace 功能。CryptoStone 的价值来自收藏市场理解和数据透明性，因此每颗宝石的稀有度、交易历史、各宝石 floor price、高等级宝石排名等数据层非常重要。

随着生态成长，CryptoStone 可以从单纯智能合约项目扩展为专用 Appchain 或 Rollup。在这种情况下，STONE 可以不仅作为挖矿代币，还可以作为网络 gas token 或原生资产，Gem NFT 则可以成为 CryptoStone 网络的基础数字资产。

长期来看，也可以考虑发展为独立的 CryptoStone Mainnet。在这种情况下，需要独立验证者、开源节点、原生挖矿模块、链上随机模块、自有 marketplace 和公开的协议改进程序。但 Mainnet 并不只是技术上创建一条链，而应在形成足够用户、流动性、验证者和开发者生态后推进。

CryptoStone 的长期方向并不是运营一个 NFT 集合，而是形成“ 数字宝石 ”这一新的链上资产类别。

44. 法律与投资性注意事项

CryptoStone 不提供现实宝石的所有权、兑换权或抵押权。CryptoStone Gem NFT 不是对现实宝石的请求权，而是在链上被挖掘出的数字宝石资产。

CryptoStone 的质押与锁仓结构并不是为了提供固定收益、利息、分红或投资收益。将 STONE 投入挖矿池的行为，是为了获得 Gem NFT 挖矿机会而进行的协议参与行为，并不保证特定收益率或市场价格上涨。

持有或质押 STONE 不保证任何特定收益、分红、利息、价格上涨或 NFT 销售收益。Gem NFT 是收藏型数字资产，其市场价值会根据外部市场参与者的主观评价和需求而变化。

PoM 不是单独的投资资产、债权、收益权、积分或可交易代币。PoM 是用于表示用户在特定宝石矿池中是否累积了挖矿工作量的协议内部指标，不能在矿池之间转换，也不能对外转让。

此外，CryptoStone 不承诺任何特定收益率、价格上涨、本金保证或市场流动性。CryptoStone 的价值可能由市场参与者的收藏需求、对稀缺性的认知、交易活跃度和生态扩展性形成。

本白皮书中提出的数值和公式，是为了实现“ 去中心化数字宝石 ”概念而设计的初始参数。这并不代表现实宝石市场的所有经济、文化或宝石鉴定学因素已被完整表达，也不能被断定为生态系统的完整经济模型。

风险	说明
智能合约漏洞	代码错误或被黑客攻击的可能性
随机生成风险	随机基础设施依赖或实现错误
NFT 市场需求不足	收藏需求可能不足
STONE 流动性不足	交易所和 DEX 流动性可能不足
监管环境变化	各国数字资产监管可能变化
Mainnet 扩展失败	长期路线图可能无法实现
稀缺性评价不确定性	市场可能以不同方式评价稀缺性
初始参数风险	数值可能与实际市场需求不匹配
销毁负担	Claim Burn 和 Maturity Burn 可能成为参与者负担
公开流通初期波动性	100% 公开流通结构下，初期市场价格波动可能较大
LP 结构风险	初始流动性供应和 LP 处理方式可能引发信任问题

因此，CryptoStone 必须经过技术、经济和法律层面的审慎审查后实施。

45. 项目的意义

CryptoStone 的意义可以总结为三点。

第一，CryptoStone 提出 NFT 的概念可以从外部内容所有权中脱离出来，NFT 本身也可以成为属性型资产。现有 NFT 往往依赖图像或平台，而 CryptoStone 试图通过让宝石属性直接成为链上数据，强化 NFT 本身的资产属性。

第二，CryptoStone 将宝石的稀缺性和等级结构迁移到数字环境。现实宝石会根据重量、颜色、净度、切工形成不同价值。CryptoStone 通过概率表、挖矿难度、减半结构和供应限制来实现这一点。

第三，CryptoStone 将去中心化挖矿概念扩展到比特币之后的新资产领域。如果说比特币将黄金稀缺性数字化，那么 CryptoStone 则将宝石的稀缺性与收藏性数字化。

CryptoStone 并不主张取代现实宝石。CryptoStone 是一个在数字环境中重新解释“ 宝石 ”这一资产概念的项目。

笔者认为，这样的尝试未来可以帮助区块链技术超越单纯金融交易，在数字环境中表达现实世界中的抽象价值与属性型资产。

46. 结论

CryptoStone 提出了“ 数字宝石 ”这一新的资产概念。

正如比特币不需要直接保管现实黄金，也能创造数字黄金的概念一样，CryptoStone 即使不担保现实宝石所有权，也试图在数字环境中实现宝石的核心属性：稀缺性、可开采性、等级性和收藏性。

CryptoStone 的结构可总结如下。

核心结构	内容
单一代币	STONE ERC-20
初始发行量	1,200,000,000 STONE
流通结构	100% 公开流通
访问方式	通过公开 DEX 流动性进入市场
NFT 结构	一个 ERC-721 Gem NFT 合约
挖矿池	12 个独立宝石挖矿池
矿池实现	同一 Pool Template + Factory 结构
Base Mining Unit	100,000 STONE
Target Pool Power	40,000,000 Power
12 个矿池整体 Target Power	480,000,000 Power
PoM 结构	基于 Proof of Mining 的累积工作量模型
Claim 条件	各矿池 PoM ≥ Required PoM Threshold
Claim Burn	20 STONE × Scarcity Multiplier
Lock Model	Flexible、90 天、180 天、365 天
折旧	根据锁仓周期产生 Maturity Burn
稀有度	Rarity Score + Probability Rarity Index
减半	各宝石 Scarcity Multiplier
随机性	初期 VRF 或 Commit-then-Reveal，长期原生随机模块
对应 Hash Power 的概念	基于 STONE 的 Mining Power
去中心化	No Admin Mint、No Central Server、finalize 结构
公开验证	源码公开、审计报告、LP 处理记录、概率表验证
生态扩展	Marketplace、Gem Refinement、Arena Game、Ranking System、Collection Quest
用户工具	Mining Simulator、PoM Dashboard、Gem Explorer、Rarity Explorer
长期方向	可扩展至 Appchain 或 Mainnet

笔者认为，CryptoStone 的目标并不是短期 NFT 销售。CryptoStone 的目标是证明：在数字环境中，“ 宝石 ” 这一资产概念如何能够以去中心化方式被实现。

CryptoStone 的信任不来自创始人权威、内部配额或中央运营权限，而来自固定发行量、100% 公开流通结构、可验证 PoM 模型、不可更改概率表、可公开验证的合约，以及任何人都可以确认的链上数据。

如果比特币是数字黄金， 那么 CryptoStone 就是去中心化数字宝石。