CRYPTOSTONE WHITEPAPER v2.8

A Study on Decentralized Digital Gemstone Assets

English Version

CryptoStone Protocol

Abstract

Bitcoin did not directly collateralize physical gold. Nevertheless, through a fixed supply, publicly disclosed mining rules, a decentralized network, and a transaction structure verifiable by anyone, it established a new asset concept known as “digital gold.” The essential significance of Bitcoin lies in demonstrating that digital scarcity and digital ownership can be implemented through code and network consensus, without relying on a specific issuer or centralized authority.

The author seeks to extend this philosophy to the asset concept of gemstones. In the physical world, gemstones are limited by geological availability and mining constraints, and each gemstone derives different degrees of scarcity and value from attributes such as weight, color, clarity, and cut. Even gemstones of the same type may differ materially in value when their individual attributes differ. In this respect, gemstones are inherently non-fungible and are well suited to representation as unique digital assets.

CryptoStone is a decentralized digital gemstone protocol designed to express the mineability, scarcity, grading structure, and collectibility of gemstones through on-chain data, and to enable Gem NFTs to be mined in a digital environment without arbitrary intervention by a central server or operator. Each gemstone is represented as an ERC-721 NFT and records attributes such as stone type, weight, color, clarity, cut, mining timestamp, and originating mining pool on-chain.

This project does not seek to provide ownership, collateral rights, or redemption rights over physical gemstones. What the author proposes in this whitepaper is a research-oriented and experimental attempt to implement, as independent scarce digital assets, the structural properties of physical gemstones: limited supply, mineability, grading, scarcity, and collectibility.

If Bitcoin digitized the scarcity and mineability of gold, CryptoStone seeks to digitize the scarcity and attribute-based value of gemstones in a decentralized manner.

1. Introduction

In the physical world, gemstones have long functioned as stores of value, ornamental assets, collectible assets, and symbolic assets. The value of a gemstone does not arise solely from its physical existence. It is shaped by the difficulty of extraction, limited deposits, precision of processing, grade differentials, collectible demand, and cultural symbolism.

In particular, gemstones such as diamond, ruby, sapphire, and emerald may have significantly different values even within the same gemstone category. A gemstone with greater weight, superior color, higher clarity, and more refined cut has greater scarcity. This structure demonstrates that gemstones are not merely fungible commodities, but non-fungible assets whose value varies according to individual attributes.

Blockchain technology provides a foundation for representing such non-fungible attributes in a digital environment. However, the existing NFT market has largely developed around images, game items, memberships, or access rights to external content. In such cases, the value of the NFT may depend on an external image, a centralized server, a specific platform, or an operating entity.

CryptoStone proposes a different direction. CryptoStone is not an NFT that merely proves ownership over an external image or server-hosted content. Rather, each NFT directly contains gemstone attribute data, and the attributes themselves express scarcity and collectible value as a digital gemstone asset.

Through this whitepaper, the author does not attempt to transfer the physical ownership of gemstones onto a blockchain. Instead, this paper describes how the scarcity and attribute-based value of gemstones can be implemented in a decentralized digital environment.

2. The Simplest Way to Understand CryptoStone

CryptoStone is an on-chain protocol for mining digital gemstones. A user deposits STONE into the gemstone mining pool of their choice, and once a sufficient Proof of Mining, or PoM, value has accumulated over time, the user may claim a Gem NFT. The mined NFT is not merely an image. It is a unique digital gemstone that records stone type, weight, color, clarity, cut, rarity score, and mining timestamp.

Users may choose among 12 gemstone pools, including Diamond, Ruby, Sapphire, and Emerald. Each stone has a distinct supply limit, mining interval, and scarcity schedule. As mining progresses, the remaining supply decreases and the scarcity multiplier increases.

The core experience of CryptoStone is simple.

```
Deposit STONE into a digital mine.
Over time, Mining Power accumulates as Proof of Mining, or PoM.
When the required PoM threshold is reached, claim a Gem NFT.
The gemstone attributes are determined by public probabilities and
verifiable randomness.
```

Accordingly, CryptoStone is not designed as a purchased NFT collection, but as a system for mined digital gemstones. Users do not simply purchase an image; they mine their own digital gemstones under public rules and fixed probability structures.

3. Research Objective

The objective of CryptoStone is not to replicate physical gemstones or to tokenize ownership rights over real-world gemstones. The purpose of this project is to transfer the structural properties of gemstones—mineability, limited supply, grading, scarcity, and collectibility—into a digital environment.

CryptoStone begins with the following question:

> *If Bitcoin could become digital gold without directly collateralizing gold, can the scarcity, grading structure, and collectibility of gemstones also be implemented as independent assets in a decentralized digital environment?*

The author proposes one technical, economic, and philosophical design in response to this question.

Objective	Description
Digitalization of attributes	Structure gemstone weight, color, clarity, and cut as on-chain attributes.

Implementation of mining	Implement the gemstone mining process through smart contracts.
Fixed supply	Predefine the maximum supply and scarcity structure for each stone.
Decentralized participation	Allow anyone to participate in mining pools without a central server.
Prevention of attribute manipulation	Prevent operators from arbitrarily assigning gemstone grades or attributes.
Formation of collectible value	Create a structure in which rare attribute combinations may be recognized as collectible assets.
Long-term extensibility	Establish a foundation for future expansion into an Appchain or Mainnet.

4. Protocol Trust Principles

CryptoStone seeks to avoid reliance on the trustworthiness of a specific founder or operator. The trust foundation of the protocol is intended to arise from public code, fixed supply, immutable probability tables, a No Admin Mint structure, verifiable randomness, and on-chain data that anyone can inspect.

The operator should not be able to arbitrarily allocate rare NFTs to particular users, modify the supply of a stone, or manipulate mining probabilities. The purpose of CryptoStone is to establish a structure in which the scarcity of digital gemstones is determined by protocol rules rather than by human authority.

CryptoStone therefore follows the trust principles below.

Trust Principle	Description
Fixed Supply	The total supply of STONE and the maximum NFT supply for each stone are fixed in advance.
100% Public Circulation	STONE follows a 100% public circulation structure.
No Admin Mint	The operator must not be able to mint Gem NFTs arbitrarily.
Immutable Probability	Gemstone attribute probability tables must be disclosed and immutable after finalization.
Verifiable Randomness	Gemstone attributes must be determined through a verifiable randomness structure.
On-chain Attributes	Core attributes of Gem NFTs must be recorded as on-chain data.
Transparent Pools	Mined supply, remaining supply, and difficulty for each stone pool must be publicly verifiable.
Open Verification	Anyone must be able to verify the contracts and mining rules.

These principles demonstrate that CryptoStone is intended to function not through operator discretion, but through public rules and verifiable code as a decentralized digital gemstone protocol.

5. Basic Concept of the Digital Gemstone Asset

CryptoStone consists of a single STONE token, 12 gemstone mining pools, and a single ERC-721 Gem NFT contract.

Component	Role
STONE Token	A single mining resource required to participate in the digital mines.
12 Gemstone Mining Pools	Independent digital mines for each birthstone.
CryptoStone Gem NFT	A unique ERC-721-based digital asset representing a mined gemstone.
Mining Pool Contract	Manages staking, Mining Power, difficulty, and claim conditions.
Gem NFT Contract	Manages gemstone NFT attributes, supply, and ownership.

STONE is not the gemstone itself. STONE is the source of Mining Power required to participate in digital mining. By staking STONE into a chosen gemstone mining pool, a user obtains Mining Power and accumulates PoM over time.

The mining output is the CryptoStone Gem NFT. Gem NFTs are issued from one unified ERC-721 contract, and each NFT contains on-chain attributes indicating what stone it is and what weight and grade it possesses.

The physical gemstone mining structure may be abstracted as follows.

Physical Gemstone Mining	CryptoStone
Mine	Gemstone Mining Pool
Mining equipment and energy	STONE Token
Mining work	Proof of Mining, PoM
Mining output	ERC-721 Gem NFT
Mine difficulty	Pool Difficulty
Depletion of deposits	Scarcity Multiplier
Gemological appraisal	On-chain Attribute & Rarity Score

6. Representation of Gemstone Attributes

The value of a gemstone is not determined solely by its type. Even within diamonds, value differs according to weight, color, clarity, and cut.

CryptoStone assigns the following four core attributes to each Gem NFT in order to represent these gemstone properties in a digital environment.

Attribute	Meaning
Weight	Gemstone weight.
Color	Gemstone color grade.
Clarity	Gemstone clarity grade.
Cut	Gemstone cut grade.

These four attributes are determined at the time of mining and cannot be modified after minting. This digitally implements a structure analogous to physical gemstones, which are evaluated according to individual attributes after appraisal.

In CryptoStone, each NFT is not simply a token pointing to an image file. It is a digital asset that directly holds gemstone attribute values. Images, 3D models, or visual card formats may serve as user-experience aids, but the essence of the CryptoStone NFT lies in the attribute data recorded on-chain.

7. Digital Implementation of Gemstone Uniqueness

CryptoStone can evaluate various technical approaches for expressing the uniqueness of each gemstone, including fungible token structures, semi-fungible token structures, and hybrid token structures. However, the core requirement is that each gemstone must have its own unique attribute combination and tokenId.

Therefore, CryptoStone gemstones are represented as ERC-721-based NFTs. This choice is not made to emphasize a technical standard for its own sake, but as a result of the functionality required by the protocol.

Implementation Requirement	Reason for ERC-721 Adoption
Each gemstone requires a unique tokenId	ERC-721 is suitable for unique tokenId-based asset representation.
Each gemstone requires distinct attributes	tokenId-specific metadata and on-chain attribute structures are possible.
Ownership transfer history must be recorded	Standard NFT transfer and ownership records are supported.
Multiple stones must coexist within one collection	The stoneType attribute can distinguish the 12 stones.
Rarity and trading history must be traceable	NFT-specific provenance and rarity tracking are possible.

In this sense, ERC-721 is not used merely to create image NFTs. It functions as the technical container for representing the uniqueness and attribute-based asset nature of digital gemstones.

8. One Collection with 12 Coexisting Stones

CryptoStone does not separate the 12 stones into independent NFT collections. All gemstones are issued from a single ERC-721 Gem NFT contract.

Each NFT is distinguished by a `stoneType` attribute.

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

This structure has the following advantages.

Advantage	Description
Unified collection	Maintains the single collection identity of CryptoStone.
Concentrated trading data	Prevents collection value and marketplace trading data from being fragmented.
Easier rarity management	Enables all gemstones to be compared within one rarity ranking system.
Stone-specific identity	The stoneType attribute preserves the independence of each stone.
Supply limit enforcement	The NFT contract can verify max supply by stone internally.

The NFT contract separately manages the issuance amount for each stone.

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

Accordingly, even if a mint request is made from the Diamond Pool, no further Diamond NFTs can be issued once the maximum Diamond supply has been reached.

9. Structure of Digital Mines

In CryptoStone, each stone is treated as an independent digital mine.

Pool	Description
Garnet Pool	Mining of Garnet NFTs.
Amethyst Pool	Mining of Amethyst NFTs.
Aquamarine Pool	Mining of Aquamarine NFTs.
Diamond Pool	Mining of Diamond NFTs.
Emerald Pool	Mining of Emerald NFTs.

Pearl Pool	Mining of Pearl NFTs.
Ruby Pool	Mining of Ruby NFTs.
Spinel Pool	Mining of Spinel NFTs.
Sapphire Pool	Mining of Sapphire NFTs.
Opal Pool	Mining of Opal NFTs.
Topaz Pool	Mining of Topaz NFTs.
Zircon Pool	Mining of Zircon NFTs.

Each mining pool uses the same STONE token, but each pool has distinct mining conditions.

Item	Meaning
Stone Type	The gemstone type mined from the pool.
Max Supply	The maximum issuance amount for that stone.
Base Mining Interval	The base mining interval.
Target Pool Power	The reference Mining Power level.
Current Pool Power	The current accumulated Mining Power in the pool.
Minted Supply	The amount mined to date.
Pool Difficulty	Difficulty based on overall participation.
Scarcity Multiplier	Scarcity multiplier based on halving mechanics.

Just as diamond mines and ruby mines have different geological deposits in the physical world, each stone in CryptoStone has its own supply and mining difficulty. Mining more diamonds does not increase the difficulty of Ruby. Depletion of Ruby does not reduce the supply of Sapphire.

Each stone has its own independent digital reserve and mining structure.

10. Hash Power, Mining Power, and Proof of Mining

In Bitcoin, miners obtain a probability of generating blocks through hash power. Greater hash power increases the probability of discovering a block, but it does not allow a miner to arbitrarily change Bitcoin's issuance rules or difficulty structure. Hash power is not a right to change network rules; it is computational capacity used to obtain more mining opportunities within fixed rules.

CryptoStone abstracts this concept for digital gemstone mining. In CryptoStone, the concept corresponding to hash power is Mining Power, and the work accumulated over time by Mining Power is Proof of Mining, or 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 is not a separately transferable or tradable token. PoM is an on-chain work metric recorded by the contract based on the user's mining participation and elapsed time. PoM is also not a network consensus algorithm. In CryptoStone, PoM is an internal protocol value used to determine whether a user has reached the condition required to claim a Gem NFT from a specific stone pool.

If user `i` stakes `s_{i,j}` STONE into stone pool `j`, and the lock multiplier is `L_i`, the user's Mining Power `P_{i,j}` is defined as follows.

```
P_{i,j} = s_{i,j} × L_i
```

The user's PoM value accumulates over time as follows.

```
PoM_{i,j}(t + Δt) = PoM_{i,j}(t) + P_{i,j} × Δt
```

Here, `PoM_{i,j}(t)` refers to the Proof of Mining value accumulated by user `i` in stone pool `j` up to time `t`.

PoM is accumulated independently for each stone pool. For example, PoM accumulated in the Diamond Pool can be used only to claim Diamond NFTs and cannot be converted into PoM for the Ruby Pool or Sapphire Pool. This structure protects the independence, scarcity, and mining difficulty of each stone pool.

A user with higher Mining Power may reach the required PoM threshold faster, but the user cannot arbitrarily increase the probability of rare attributes or select a particular gemstone grade.

11. Mining Pool Template and Factory Structure

The 12 Mining Pool Contracts are not separately developed contracts with different logic. All pools are deployed from the same audited Mining Pool Template. Each pool uses the same core logic, while only the following parameters differ.

Parameter	Description
stoneType	The stone type mined from that pool.

maxSupply	The maximum issuance amount for that stone.
baseMiningInterval	The base mining interval.
targetPoolPower	The reference Mining Power level.
scarcitySchedule	The halving structure for that stone.
poolAddress	The address authorized by the NFT contract to mint.

CryptoStone may use a Pool Factory structure for this purpose. The Pool Factory deploys the 12 stone-specific pools from the same Mining Pool Template and fixes the core parameters of each pool after deployment.

Advantage	Description
Code consistency	All 12 pools use the same logic.
Audit efficiency	Security auditing can focus on one Pool Template.
Reduced risk	Reduces the probability of exceptional bugs caused by different code per pool.
Parameter transparency	Differences among pools arise only from disclosed fixed parameters.
Extensibility	The same structure can be used for future stone pool expansion.

Accordingly, CryptoStone maintains the economic structure of “12 independent mines,” while improving security and transparency by using the same verifiable smart contract template in development.

12. Limited Supply by Stone

The 12 CryptoStone stones each have different maximum supplies. This structure gives the stone type itself a first layer of scarcity.

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

The maximum supply of all Gem NFTs is as follows.

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

Diamond has the lowest supply, while Zircon has the highest supply. Thus, stone type itself becomes an element of scarcity.

From a global collection perspective, the supply share of a specific stone `j` may be expressed as follows.

```
P_stone,j = N_j ÷ N_total
```

Here, `N_j` is the maximum supply of a specific stone and `N_total` is the maximum supply of the entire Gem NFT collection. This value may be used as a foundational variable in explaining the relative scarcity of each stone in the Probability Rarity Index.

The total Gem NFT supply in CryptoStone does not represent the simple issuance size of a single rare NFT collection. Rather, it represents a long-term digital gemstone asset class composed of 12 stone pools and multi-layered attribute combinations. Scarcity is not determined by total supply alone; it is shaped by stone type, mining timestamp, halving stage, Weight, Color, Clarity, Cut, tokenId, and the Probability Rarity Index.

Therefore, the total supply of 1,980,000 in CryptoStone should be interpreted not as mass issuance for a short-term minting event, but as the total digital reserve of a gemstone ecosystem designed to allow a broad range of participants to mine different stones and attribute combinations over a long period.

13. Design of Mining Intervals

Each stone has a distinct base mining interval.

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
Spinel	140,000 sec
Sapphire	190,000 sec
Opal	130,000 sec
Topaz	120,000 sec
Zircon	110,000 sec

A longer base mining interval makes mining more difficult under the same Mining Power. Therefore, the initial scarcity of each stone is formed by two elements.

Element	Description
Max Supply	Total possible issuance amount of the stone.
Base Mining Interval	Time required to mine one unit under the base mining unit.

For example, Diamond has the lowest supply and the longest base mining interval. This is designed to make Diamond structurally the scarcest stone in the CryptoStone ecosystem.

14. Determination of Initial STONE Supply

CryptoStone does not issue separate tokens for the 12 stones. It uses a single STONE token.

The initial total supply is fixed as follows.

```
STONE Initial Total Supply = 1,200,000,000 STONE
Additional Mint = None
```

The reason for setting the supply at 1,200,000,000 STONE is not merely to increase the token count. CryptoStone seeks to accommodate a structure in which more than 100,000 users may participate in mining pools at various scales. To achieve this, the token unit must naturally support small participants, mid-scale participants, and high Mining Power participants.

With a supply of 1,200,000,000 STONE, a natural participation UX based on several thousand STONE units can be designed even under the assumption of more than 100,000 users. This lowers entry barriers for small participants, provides a meaningful mining participation unit for mid-scale participants, and enables long-term mining strategies for high Mining Power participants.

Accordingly, the issuance of 1.2 billion STONE should be understood not as an indiscriminate increase in supply, but as a unit design intended to accommodate a broad user base and a Proof of Mining structure.

```
Expected Active Mining Ratio = approximately 30% to 40%

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

Under an assumption of 100,000 participants, the average active stake is as follows.

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

Thus, the 1,200,000,000 STONE structure is designed to accommodate a large participant base while allowing small participants to access the mining ecosystem.

15. 100% Public Circulation Structure of STONE

In CryptoStone, STONE is the single mining resource required to participate in digital gemstone mining. The author considers it more consistent with the philosophy of CryptoStone for STONE distribution to follow a public market structure accessible under equal conditions, rather than a structure that grants pre-allocated rights to specific insiders.

Therefore, STONE follows a 100% public circulation structure. This means that STONE is not pre-allocated to specific parties, but is circulated through public DEX liquidity and may be acquired by anyone under the same public market conditions.

Item	Structure
Total Supply	1,200,000,000 STONE
Distribution Principle	100% public circulation
Market Access	Public DEX liquidity
Additional Mint	None
Access Rule	Anyone may acquire STONE under the same public market conditions.
Primary Utility	Participation in mining pools for Gem NFT mining.
Mechanism	Acquire STONE -> stake -> generate Mining Power -> accumulate PoM -> claim Gem NFT.
Supply Trust	Supply, pool structure, probability tables, and claim conditions are contract-verifiable.

Users may acquire STONE from the public market and deposit it into the stone mining pool of their choice. They then generate Mining Power based on their staked STONE and accumulate Proof of Mining, or PoM, over time. Once the accumulated PoM reaches the required threshold of the relevant pool, the user may claim a Gem NFT.

In this structure, the DEX is the public access route to STONE, while the mining pools are the actual use case of STONE. In other words, the purpose of STONE is not simple holding or speculative circulation, but functioning as a protocol resource for participation in digital gemstone mining.

The foundation or early ecosystem contributors may also acquire STONE under the same conditions in the public market, without separate pre-allocation. This approach minimizes privileged acquisition structures and aligns protocol participation with public markets and on-chain rules.

For the 100% public circulation structure to earn trust, the initial liquidity supply method, LP token treatment, contract permissions, and absence of additional minting must be clearly disclosed. Initial liquidity is formed through a public DEX pool, and it is desirable for the treatment of initial LP tokens to be publicly disclosed through long-term locking or burning. This reduces concerns about liquidity removal and strengthens trust in the public market access structure of STONE.

If the foundation or early contributors acquire STONE, such acquisition should be made under the same conditions in the public market rather than through separate pre-allocation. Major holding wallets should preferably be publicly verifiable on-chain. This structure does not deny the existence of a foundation. Rather, it expresses the principle that the foundation must also participate under the same public market rules rather than through privileged allocation outside the protocol.

The trust of CryptoStone is formed not through pre-allocated holdings of specific parties, but through fixed total supply, 100% public circulation, immutable mining rules, verifiable PoM structure, and transparent on-chain data.

16. Base Mining Unit and Small-Scale Participation

The base mining unit of CryptoStone is defined as follows.

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

However, this is not a minimum participation amount. The Base Mining Unit is a reference unit used to calculate mining speed and difficulty.

CryptoStone adopts a PoM accumulation structure so that as many users as possible can participate in mining. Users may participate in a mining pool with less than 100,000 STONE, and their PoM value accumulates in proportion to their staked amount and elapsed time.

A user may claim a Gem NFT once the accumulated PoM value is equal to or greater than the required PoM threshold `R_j` of the relevant pool.

```
PoM_{i,j}(t) >= R_j
```

For example, under initial Diamond Pool conditions where Pool Difficulty and Scarcity Multiplier are both 1x, the estimated mining times are as follows.

Active Stake	Estimated Time to Mine 1 Diamond NFT
100,000 STONE	approximately 2.55 days
10,000 STONE	approximately 25.5 days
5,000 STONE	approximately 51 days
1,000 STONE	approximately 255 days

100 STONE	approximately 6.98 years

This structure gives high Mining Power users faster mining opportunities while allowing small participants to accumulate PoM over time and eventually claim Gem NFTs.

The author considers this structure essential for the expansion of the CryptoStone ecosystem. NFT scarcity should be preserved through total supply, attribute probabilities, and halving mechanics, while user participation should be expanded through low entry barriers and PoM accumulation.

17. Target Pool Power and Long-Term Mining Period

The Target Pool Power of CryptoStone is calculated not based on the total STONE supply, but on the effective staking amount expected to participate in mining.

```
Target Pool Power = 40,000,000 Power per Pool
12 Pools Total Target Power = 480,000,000 Power
```

This reflects the assumption that approximately 40% of the total STONE supply of 1,200,000,000 may participate in the mining ecosystem over the long term.

If the total Mining Power of a specific pool `j` is `P_j` and the Target Pool Power is `P_j^*`, the total pool power is defined as follows.

```
P_j = Σ P_{i,j}

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

Assuming that participants increase by 10,000 users per year, reaching approximately 100,000 participants after 10 years, and that average active stake is approximately 4,800 STONE, it may take approximately 8 to 9 years for around 90% of the total Gem NFT supply to be mined.

Due to the halving structure, mining speed after the 90% level becomes even slower. Therefore, it may take more than 12 years for the entire Gem NFT supply to be fully mined.

This period estimate is not intended to predict any specific return or price. It is a model intended to show that CryptoStone is not a short-term NFT minting event, but a decentralized mining ecosystem in which digital gemstones are gradually mined over an extended period.

18. Interpretation of Parameters and Numerical Values

The stone-specific supply amounts, base mining intervals, Mining Power formula, PoM thresholds, halving multipliers, Weight, Color, Clarity, and Cut probability tables, and Rarity Score formula presented in this whitepaper are not absolute standards that perfectly replicate the physical gemstone ecosystem.

These values are initial reference parameters designed for the following purposes.

Purpose	Description
Digital scarcity representation	Represent gemstone scarcity in an on-chain environment.

Mining difficulty implementation	Implement mining difficulty and supply limits through smart contracts.
Relative scarcity differentiation	Enable comparative scarcity among stones.
Collectible value differentiation	Improve market understanding through rarity and tier structures.
Long-term supply control	Manage supply speed through halving and difficulty increases.
Participation scalability	Accommodate both small participants and large participants.

Accordingly, the numerical values in this whitepaper should not be viewed as fully reflecting all price formation factors, appraisal standards, distribution structures, supply and demand dynamics, cultural values, physical custody costs, or gemological appraisal models of the physical gemstone market.

CryptoStone does not attempt to replicate the physical gemstone market in its entirety. It is a project designed to implement the core properties of gemstones—scarcity, grading, mineability, and collectibility—in a decentralized digital environment.

The author regards the parameters in this whitepaper not as arbitrary figures, but as initial reference values for explaining and experimenting with the concept of decentralized digital gemstones. They may evolve into a more precise model through further research, market response, community review, technical verification, and legal review. However, after official deployment and finalization of the core protocol rules, the fixed core parameters should not be arbitrarily changed by an operator.

19. Calculation of Mining Power

In CryptoStone, Mining Power determines the speed and opportunity with which a user can mine gemstones. Participants who stake more STONE obtain greater Mining Power and may reach claim conditions more frequently.

If user `i` stakes `s_{i,j}`, has lock multiplier `L_i`, and the user's Mining Power is `P_{i,j}`, then Mining Power is calculated as follows.

```
P_{i,j} = s_{i,j} × L_i
```

Mining Power does not directly increase the probability of higher gemstone grades. Mining Power affects only the rate at which PoM accumulates.

This is similar to the Bitcoin mining structure. A participant with more mining equipment obtains more mining opportunities, but cannot change the mining rules themselves. Likewise, in CryptoStone, a participant staking more STONE accumulates PoM faster, but cannot arbitrarily increase the probability of obtaining a better gemstone.

20. Long-Term Participation Adjustment and Flexible Cooldown

A Lock Multiplier may be applied according to staking period in order to recognize long-term participation.

Lock Type	Lock Period	Mining Multiplier `L_i`	Maturity Burn	Returned STONE	Cooldown
Flexible	None	1.00x	0%	100%	7 days
Short Lock	90 days	1.05x	2.5%	97.5%	None
Medium Lock	180 days	1.12x	5%	95%	None
Long Lock	365 days	1.25x	10%	90%	None

Flexible Lock has no depreciation burn, but includes a 7-day cooldown period after an unstake request in order to prevent excessive short-term liquidity inflows and outflows.

Long-term lockups are optional, not mandatory. Users may choose the Flexible option with no depreciation burn, and only users who want higher Mining Power need to select a long-term lockup that involves a certain depreciation burn.

This structure seeks the following balance.

Choice	Benefit	Cost
Flexible	Free participation, no depreciation	7-day return waiting period
90-day Lock	Slightly higher Mining Power	2.5% depreciation
180-day Lock	Moderate Mining Power	5% depreciation
365-day Lock	Highest Mining Power	10% depreciation

The Lock Multiplier is capped at 1.25x. This provides reasonable recognition for long-term participants while preventing any large participant from gaining an excessively dominant advantage.

A user may claim a Gem NFT during the lockup period if the user's PoM value reaches the required threshold. In other words, lockup restricts the timing of STONE withdrawal, but it does not prohibit Gem NFT claiming itself.

21. Accumulation of Proof of Mining, PoM

CryptoStone does not use a simple point or credit system. It uses a Proof of Mining, or PoM, model that abstracts Bitcoin's Proof-of-Work concept into a digital gemstone mining structure.

PoM refers to the amount of mining work accumulated by a user who stakes STONE in a specific stone pool over time. PoM is not a separately transferable or tradable token. It is an on-chain work metric recorded by the contract based on the user's mining participation and elapsed time.

The PoM value of user `i` for stone pool `j` accumulates over time as follows.

```
PoM_{i,j}(t + Δt) = PoM_{i,j}(t) + P_{i,j} × Δt
```

For example, if a user stakes 100,000 STONE into the Diamond Pool under the Flexible condition, the user's Mining Power is as follows.

```
P_{i,Diamond} = 100,000 × 1.00 = 100,000
```

If the user waits for 100,000 seconds, the accumulated PoM value is as follows.

```
PoM = 100,000 × 100,000
PoM = 10,000,000,000
```

A user may claim a Gem NFT once the accumulated PoM value is equal to or greater than the required PoM threshold of the relevant pool.

```
PoM_{i,j}(t) >= R_j
```

When a Gem NFT is claimed, the required threshold `R_j` is deducted from the user's PoM value in that pool.

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

This structure does not unnecessarily extinguish PoM accumulated beyond the threshold. For example, if the required PoM threshold is 22,000,000,000 and the user has 23,000,000,000 PoM at the time of claim, then 1,000,000,000 PoM remains after the claim and continues to apply toward the next mining cycle.

PoM is accumulated independently for each stone pool. PoM accumulated in the Diamond Pool can be used only to claim Diamond NFTs and cannot be converted into PoM for the Ruby Pool or Sapphire Pool. This protects the independence, scarcity, and mining difficulty of each stone pool.

If a user unstakes STONE from a specific pool, the already accumulated PoM may remain recorded in that pool. However, after unstaking, the user's Mining Power in that pool becomes 0, and no additional PoM accumulates. If the user later stakes STONE again into the same pool, new PoM accumulation continues from the previously recorded PoM.

If a user stakes additional STONE into the same pool, existing PoM is preserved and only the Mining Power after the additional staking increases. Conversely, if the user reduces the staked amount, existing PoM is preserved, but the future accumulation speed decreases.

PoM cannot be transferred or traded externally, and it cannot be moved to another stone pool. This is because PoM is not an asset in itself, but a work metric representing the mining participation actually accumulated by a specific user in a specific pool.

22. Required PoM Threshold

The required PoM threshold for mining one gemstone is determined by the Base Mining Unit, the stone-specific base mining interval, Pool Difficulty, and Scarcity Multiplier.

If the base mining interval of stone `j` is `T_j`, the Base Mining Unit is `B`, Pool Difficulty is `D_j`, and Scarcity Multiplier is `S_j`, then the required PoM threshold `R_j` is defined as follows.

```
R_j = B × T_j × D_j × S_j
```

The reference values of CryptoStone are as follows.

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

For example, if the base mining interval of the Diamond Pool is 220,000 seconds and both Pool Difficulty and Scarcity Multiplier are 1x, then:

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

If the Mining Power of user `i` is `P_{i,j}`, the expected time required for the user to claim one NFT of stone `j` can be expressed as follows.

```
E[T_{i,j}] = R_j ÷ P_{i,j}
```

For example, if a user stakes 100,000 STONE into the Diamond Pool under Flexible conditions:

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

Thus, under initial conditions, a user staking 100,000 STONE can claim one Diamond NFT approximately every 2.55 days.

23. Adjustment of Pool Difficulty

If the number of participants increases and total Mining Power rises, gemstones may be mined too quickly. To prevent this, each pool adjusts difficulty according to total Mining Power.

If the total Mining Power of stone pool `j` is `P_j`, the Target Pool Power is `P_j^*`, and Pool Difficulty is `D_j`, then:

```
D_j = max(1, P_j ÷ P_j^*)
```

The reference value of CryptoStone is as follows.

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

The following examples illustrate the calculation.

Target Pool Power	Total Pool Mining Power	Calculation	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

The purpose of the `max(1, ·)` structure is to prevent difficulty from falling below 1.0x even when total Mining Power is lower than the Target Pool Power. This prevents mining speed from becoming excessively fast in early stages with fewer participants.

Conversely, when total Mining Power exceeds Target Pool Power, Pool Difficulty increases proportionally. For example, if total Mining Power in a pool increases to 80,000,000 Power, Pool Difficulty becomes 2.0x. In this case, the time required for the same user to mine one NFT increases by approximately two times.

In smart contract implementation, a BPS-based approach may be used to avoid decimal calculations.

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

Here, `10,000 BPS = 1.0x`.

This structure allows mining difficulty to increase naturally as participation grows, preventing excessive short-term depletion of each stone supply.

24. Halving and Scarcity Multiplier

CryptoStone applies halving independently by stone, rather than across the entire collection.

If the maximum supply of stone `j` is `N_j`, the amount mined to date is `n_j`, and the mining progress ratio is `q_j`, then:

```
q_j = n_j ÷ N_j
```

For example, if the maximum supply of Diamond is 110,000 and 55,000 have been mined:

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

This means that the Diamond Pool has reached the 50% mining stage.

The Scarcity Multiplier `S_j` increases according to the mining progress ratio `q_j`.

Mined Supply Ratio	Remaining Supply	Scarcity Multiplier
0% to 50%	100% to 50%	1x
50% to 75%	50% to 25%	2x
75% to 87.5%	25% to 12.5%	4x
87.5% to 93.75%	12.5% to 6.25%	8x
93.75% to 96.875%	6.25% to 3.125%	16x
96.875% and above	3.125% and below	32x

This may be generalized as follows.

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

For initial stages, `S_j(q_j)` remains at a minimum of 1x. In actual smart contracts, this may be implemented using a disclosed interval table rather than computing the above formula directly.

This formula expresses a structure in which mining difficulty increases geometrically as the remaining supply of each stone decreases. It digitizes the real-world mining concept that extraction costs and difficulty rise as geological deposits are depleted.

25. Nonlinear Structure of Mining Speed and Supply Depletion

The mining structure of CryptoStone is not a simple linear minting model. Each stone has an independent supply, mining interval, Pool Difficulty, and Scarcity Multiplier, and mining speed slows as the mining progress ratio rises due to the Scarcity Multiplier.

If the effective Mining Power of stone pool `j` is `P_eff,j`, it may be expressed as follows.

```
P_eff,j = min(P_j, P_j^*)
```

This means that when total Mining Power is below Target Pool Power, actual participant power affects mining speed; when Target Pool Power is exceeded, difficulty adjustment limits effective mining speed.

The expected mining rate per unit time of stone pool `j`, `lambda_j`, may be conceptually expressed as follows.

```
λ_j = P_eff,j ÷ (B × T_j × S_j)
```

Here, `B` is the Base Mining Unit, `T_j` is the stone-specific Base Mining Interval, and `S_j` is the Scarcity Multiplier.

The time required for a specific stone to reach mining progress ratio `q` may be expressed with the following nonlinear model.

```
Time_j(q) = (N_j × B × T_j ÷ P_eff,j) × ∫₀^q S_j(x) dx
```

This equation shows that the mining structure of CryptoStone is not a linearly depleting model, but a nonlinear mining model that gradually slows as the remaining supply of a stone decreases.

Accordingly, Gem NFTs may be mined relatively actively in early stages, but after the 90% region, mining of the remaining supply slows significantly due to the rising Scarcity Multiplier.

26. Digitalization of the Weight Attribute

All stones use CT, or carat, as the common weight unit. However, each gemstone's weight value is randomly generated.

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

The smart contract does not store decimals directly, but stores weight as an integer unit of 0.01 CT.

Displayed Weight	Contract Stored Value
0.10 CT	10
1.25 CT	125
10.50 CT	1050
200.00 CT	20000

Weight is not generated uniformly. Just as larger carat gemstones are rarer in the physical world, larger weights are generated with lower probability in CryptoStone.

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

27. Digitalization of the Color Attribute

Color represents the gemstone color grade. Higher grades are generated with lower probability.

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. Digitalization of the Clarity Attribute

Clarity represents the clarity grade of the gemstone.

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. Digitalization of the Cut Attribute

Cut represents the cut grade of the gemstone.

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. Attribute Generation and Random Verification

Gemstone attributes are not manually entered by an operator. At the time of mining, the mining contract determines Weight, Color, Clarity, and Cut based on a random value.

The randomness generation method must be verifiable. If the operator could arbitrarily generate high-grade NFTs, the decentralization and scarcity of CryptoStone would be compromised.

Therefore, the randomness generation structure of CryptoStone follows the principles below.

Principle	Description
Unpredictability	Neither operators nor users should know the result in advance.

No result selection	Operators should not be able to select favorable results or reject unfavorable ones.
No retry	Users should not be able to cancel or retry a claim after a randomness request but before result finalization.
No Admin Reroll	Operators should not be able to reroll or replace a particular result.
Public verification	The result generation process must be on-chain or publicly verifiable.
Fixed probability tables	Probability tables must be disclosed before deployment and immutable after finalization.
Immutable after minting	Attributes must not be modifiable after minting.

At initial implementation, a verifiable external VRF structure may be considered. Alternatively, a Commit-then-Reveal structure may be used to separate the randomness request stage from the result finalization stage. Regardless of the method used, users must not be able to cancel or retry a claim before finalization, and operators must not be able to select or reroll specific results.

After a randomness result is requested, the user must not be able to cancel or retry the claim because the result is unfavorable. The operator must also not be able to allocate favorable results to specific users or choose seeds that produce specific attribute combinations. This is a core condition for ensuring that rare gemstone generation is determined by verifiable randomness rather than operator discretion.

After minting, the core attributes of a Gem NFT must be frozen, and core metadata such as Weight, Color, Clarity, Cut, stoneType, minedAt, and minedFromPool must not be modifiable by the operator.

In the initial stage, practically verifiable randomness infrastructure may be used. Over the long term, CryptoStone may evolve toward a structure in which the network itself performs randomness generation and verification.

31. Rarity Score and Probability Rarity Index

CryptoStone uses two indicators to quantify the rarity of each gemstone.

Indicator	Purpose
Rarity Score	A user-friendly 0 to 100 score that is easy to understand.
Probability Rarity Index	A mathematically grounded rarity metric based on actual occurrence probabilities.

31.1 Rarity Score

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

The score allocation is as follows.

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

Stone Scarcity Score is calculated based on the maximum supply of each stone.

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

The reference values are as follows.

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

For example, Diamond has a Max Supply of 110,000 and therefore receives the highest Stone Scarcity Score. Zircon has a Max Supply of 220,000 and therefore receives the lowest Stone Scarcity Score.

31.2 Probability Rarity Index

Whereas Rarity Score is a user-friendly comparison metric, the Probability Rarity Index is a mathematical rarity metric based on the occurrence probability of each attribute.

The probability that a Gem NFT `g` has a particular attribute combination is defined as follows.

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

The probability-based rarity metric is then calculated as follows.

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

This metric indicates how statistically rare a specific Gem NFT combination is.

For example, the following combination is extremely rare.

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

Such a combination receives a high Rarity Score and also a very high Probability Rarity Index.

By using both metrics, CryptoStone provides both a user-friendly score system and a data-based rarity structure that can be verified mathematically.

32. Rarity Tier Structure

A perfect top-tier combination can only be generated with extremely low probability. This is beneficial from a scarcity perspective, but a collectible market also requires multiple upper tiers in order to support diverse trading and collecting behavior.

Accordingly, CryptoStone may apply the following rarity tiers based on Rarity Score and the Probability Rarity Index.

Tier	Example Criteria	Meaning
Common	Mainly ordinary attributes	The most common gemstone group.
Rare	One or more upper attributes	A generally rare gemstone.
Epic	Two or more upper attributes	A gemstone with high collectible value.
Legendary	Three or more upper attributes	A highly rare gemstone.
Genesis	Extreme combination or early mining uniqueness	The highest collectible class.

The Genesis Tier may not be determined solely by score. Early mining timestamp, low tokenId, extreme probability combination, and stone-specific scarcity may be considered together.

This structure is similar to the way rarity grades form collectible value in markets such as Pokemon cards, sports cards, limited-edition figures, artworks, and luxury watches. However, in CryptoStone, rarity is not based on subjective operator judgment. It is calculated from disclosed probability tables and on-chain attribute values.

33. Formation of Collectible Value

Scarcity is an important value-forming factor in collectible markets. Pokemon cards, sports cards, limited-edition figures, artworks, and luxury watches are not valued solely by utility. Price may be formed by series identity, limited supply, rarity grade, preservation condition, market demand, and community perception.

CryptoStone applies this collectible economy logic to digital gemstones.

Element	Description
Stone-specific total supply	Supply differences among Diamond, Ruby, Sapphire, and others.
Pool-specific mining difficulty	Target Power and Difficulty for each pool.
Stone-specific halving	Scarcity Multiplier increases as mining progresses.
Weight probability	Larger carat values occur with lower probability.
Color probability	Higher color grades occur with lower probability.
Clarity probability	Higher clarity grades occur with lower probability.
Cut probability	Higher cut grades occur with lower probability.
Low tokenId	Collectibility of early-mined gemstones.
Mining timestamp	Meaning of specific timing or halving stages.
On-chain trading history	Ownership and provenance record.

This structure allows users to collect unique digital gemstones mined under public probability structures, rather than merely purchasing NFT images.

In CryptoStone, rarity is not a marketing expression. Rarity is formed by fixed supply, probability tables, mining difficulty, and halving structures embedded in the contract.

34. Decentralized Mining Structure

Mining in CryptoStone is not performed by a server on behalf of users. Users stake STONE into the stone pool of their choice and, when their PoM value reaches the required threshold of that pool, directly call a contract function such as `claimGem()` to receive a Gem NFT.

Step	Description
1	The user holds STONE.
2	The user selects a stone pool.
3	The user stakes STONE.
4	Mining Power is generated.
5	PoM accumulates over time.
6	When PoM reaches the required threshold, the user calls `claimGem()`.
7	The contract verifies mining eligibility.
8	Attributes are generated using verifiable randomness.
9	An ERC-721 Gem NFT is minted.

10	The NFT is transferred to the user’s wallet.

In this process, no central server issues gemstones or assigns attributes. Mining conditions and results are determined by code.

A smart contract does not execute itself automatically. However, anyone can call the contract, and the contract verifies and executes the result according to predefined conditions. Therefore, CryptoStone’s mining structure can operate without a central server.

The author considers the critical point not merely that “there is no server,” but that “even without a server, users can directly call the contract and receive mining results under fixed rules.”

35. Mining Cost and STONE Burn Structure

In CryptoStone, STONE is not simply a payment token. It is a mining resource used to participate in digital gemstone mining. Just as physical mining equipment and energy are consumed and mining equipment depreciates over time, STONE deposited into mining pools has a certain digital depreciation structure during mining participation.

The author views the STONE burn structure not as a mechanism designed to guarantee token price appreciation, but as a mechanism expressing the resource consumption and scarcity structure required for digital gemstone mining.

STONE burn in CryptoStone may occur in two primary cases.

Burn Type	Timing	Purpose
Claim Burn	At the time of Gem NFT claim	Representation of mining cost and scarcity.
Maturity Burn	At unstake after lockup maturity	Representation of depreciation of mining resources.

The burn amount generated when claiming a Gem NFT, `B_claim,j`, is calculated as follows.

```
B_{claim,j} = β × S_j
```

Here, `β` is the Base Claim Burn and `S_j` is the Scarcity Multiplier of the relevant stone.

The initial reference value is defined as follows.

```
β = 20 STONE
```

Scarcity Multiplier	Claim Burn
1x	20 STONE
2x	40 STONE
4x	80 STONE
8x	160 STONE

16x	320 STONE
32x	640 STONE

The Base Claim Burn represents a minimal resource consumption structure for mining and is not intended to rapidly reduce total supply. Burned STONE is not paid to the operator or foundation, but permanently removed from circulation. Through this mechanism, STONE functions not as a passively deposited asset, but as a digital mining resource actually used and consumed within the CryptoStone ecosystem.

36. Lockup Depreciation and Return Structure

When a user deposits STONE into a mining pool with a selected lockup period, a portion of the STONE may be burned as depreciation at the time of unstaking after lockup maturity, while the remaining STONE is returned.

Lock Type	Lock Period	Mining Multiplier	Maturity Burn	Returned STONE	Cooldown
Flexible	None	1.00x	0%	100%	7 days
Short Lock	90 days	1.05x	2.5%	97.5%	None
Medium Lock	180 days	1.12x	5%	95%	None
Long Lock	365 days	1.25x	10%	90%	None

If user `i` stakes STONE amount `s_i` and the depreciation rate according to lock period is `δ_i`, the amount of STONE burned at maturity, `M_i`, is defined as follows.

```
M_i = s_i × δ_i
```

The returned STONE amount `R_i` is as follows.

```
R_i = s_i - M_i
```

This structure provides higher Mining Power to long-term participants while also reflecting the cost associated with use of the mining resource. A user may choose a longer lockup to obtain higher mining speed, but must accept higher depreciation burn at the end of the lockup.

Long-term lockup is not mandatory. If users do not want STONE burn exposure, they may choose the Flexible option. Long-term lockup is an optional structure for participants seeking higher Mining Power, and depreciation should be interpreted as the digital resource cost associated with that choice.

The author considers this structure not a simple penalty, but a form of depreciation arising from the use of digital mining equipment. Just as physical mining equipment wears down over time, STONE provides Mining Power while deposited in a mining pool, and a portion may be burned according to the duration of its use.

37. Choice of Development Structure

CryptoStone adopts the following structure.

```
STONE ERC-20
+ ERC-721 CryptoStone Gem NFT
+ 12 Mining Pool Contracts
+ Pool Factory
```

This structure is not a mere list of technical standards. It is a design intended to satisfy the attributes and functions that CryptoStone seeks to implement.

Choice	Reason
STONE ERC-20	Provides a single mining resource and liquidity structure.
ERC-721 Gem NFT	Represents the uniqueness and attributes of each gemstone.
12 Mining Pools	Implements independent mines for each stone.
Pool Factory	Deploys pools from the same verified template.
Unified NFT Contract	Concentrates collection identity and trading data.
Verifiable Randomness	Enables attribute generation without operator manipulation.
Finalize Mechanism	Prevents changes to core rules.

First, the roles of STONE and Gem NFT are separated. STONE is the token for Mining Power, while Gem NFT is the mining output.

Second, gemstone uniqueness is protected. Each Gem NFT has a tokenId and attribute combination, and its attributes cannot be modified after minting.

Third, stone-specific independence is maintained. Each mining pool has an independent supply, mining interval, and halving structure, making it suitable for digitally representing the concept of separate physical mines.

Fourth, the NFT collection remains unified. This concentrates CryptoStone's brand and market data, enabling integrated management of trading and rarity rankings.

Fifth, the structure is highly extensible. CryptoStone may begin with EVM-based smart contracts and later expand into an independent Appchain or Mainnet.

Sixth, centralized dependencies are reduced. Mining and minting are executed by contracts rather than a server, and anyone can verify the conditions.

38. Protocol Finalization Principles

For CryptoStone to pursue decentralized asset characteristics similar to Bitcoin, core rules must not be arbitrarily changed after deployment.

Fixed Item	Description

STONE total supply	1,200,000,000 STONE.
STONE circulation structure	100% public circulation.
Max Supply by stone	Maximum NFT supply for each stone.
Base Mining Interval by stone	Base mining interval.
Target Pool Power	Initial reference value of 40,000,000 Power.
Base Mining Unit	100,000 STONE.
Weight probability table	Weight generation probabilities.
Color probability table	Color grade generation probabilities.
Clarity probability table	Clarity grade generation probabilities.
Cut probability table	Cut grade generation probabilities.
Scarcity Multiplier	Halving-based difficulty multiplier.
Claim Burn formula	Burn formula at claim.
Mining Power formula	Staking-based Mining Power formula.
PoM formula	Proof of Mining accumulation and claim conditions.
Lock Multiplier	Mining multiplier by lockup period.
Maturity Burn formula	Depreciation burn formula at lockup maturity.

After initial configuration, the protocol should be finalized. After finalization, the operator should not be able to arbitrarily increase supply, modify rarity probabilities, or manually mint NFTs for specific users.

The core contracts of CryptoStone should be publicly verified after deployment. Token supply, NFT supply, probability tables, mining formulas, and PoM threshold calculation structure should not be modifiable after finalization.

If limited management functions are necessary before finalization, the list of such functions, their purpose, removal timing, and control mechanism should be clearly disclosed. After finalization, administrator authority related to core supply, probability tables, minting rights, and PoM calculation should be removed or disabled.

Decentralization is not completed merely by deployment on a blockchain. It is formed through rules that an operator cannot change, code that anyone can verify, and structures in which anyone can participate.

39. Balance Between Security Response and Decentralization

CryptoStone adopts No Admin Mint and No Central Server as core principles. However, during early development and deployment, limited management structures may be required for security audits, testing, and vulnerability response.

Stage	Management Structure
Testnet and audit stage	Limited management authority may exist.
Before official deployment	Parameter verification and security review.
After official launch	Removal of core minting, supply, and probability change authority.
After finalization	No Admin Mint, No Supply Change, No Probability Change.

If an emergency pause function exists, it must be used only for limiting security incidents, not for manipulating minting results or supply. Such emergency functionality should be limited through publicly verifiable mechanisms such as timelocks or multi-signature structures, and must not become a means for the operator to alter rarity or issuance.

The main contracts of CryptoStone consist of the token contract, Gem NFT contract, Mining Pool Template, Pool Factory, and randomness generation structure. These contracts should preferably undergo security audits before and after deployment, and audit results and responses to major vulnerabilities should be disclosed.

The core verification elements to be disclosed are as follows.

Verification Item	Description
Contract Source Verification	Disclosure and verification of deployed contract source code.
Audit Report	Audit report for major contracts and randomness structure.
Admin Function List	Existence and removal plan of administrator functions.
Finalize Event	Timing and event record of core parameter finalization.
LP Lock / Burn Proof	Record of initial liquidity LP treatment.
Probability Table Hash	Verification that probability tables match the pre-disclosed values.
Metadata Freeze	Verification that core attributes cannot change after minting.

This structure is intended to balance practical security response with decentralized asset integrity.

40. Position of Images and Metadata

CryptoStone does not reject visual representation. Gem NFTs may be represented as images, 3D models, or visual cards for user experience and collectible convenience.

However, images are not the essence of CryptoStone.

The essence of CryptoStone lies in the following data.

Data	Description
stoneType	Gemstone type.
weight	Weight.
colorGrade	Color grade.
clarityGrade	Clarity grade.
cutGrade	Cut grade.
rarityScore	User-friendly rarity score.
probabilityRarityIndex	Probability-based rarity metric.
minedAt	Mining timestamp.
minedFromPool	Mining pool of origin.
tokenId	NFT unique identifier.

Accordingly, even if an image server is temporarily unavailable, the core attributes of a CryptoStone NFT should remain on-chain. This design helps address the problem of conventional NFTs that rely excessively on external images or centralized servers.

41. Ecosystem Expansion Modules and Gem Refinement

The core protocol of CryptoStone consists of STONE, 12 stone-specific mining pools, Proof of Mining, and ERC-721-based Gem NFTs. However, the CryptoStone ecosystem is not limited to the core mining structure alone. In the future, the ecosystem may be expanded through additional smart contracts or extension modules that interact with already deployed contracts. Such extensions may include Marketplace functions, Arena Game modules, Ranking Systems, Collection Quests, Gem Refinement, and other utility layers.

Gem Refinement is one example of such an ecosystem expansion module. It is an optional post-mining utility structure designed to allow mined Gem NFTs to be used again within the ecosystem. Gem Refinement is not an unlimited additional NFT issuance mechanism. Rather, it is a supply compression mechanism in which two existing Gem NFTs with the same `stoneType` are combined to create one Refined Gem NFT with the same `stoneType`.

```
2 Gem NFTs
+ a small amount of STONE usage or burn
→ Parent Gem NFTs burned
→ 1 Refined Gem NFT minted
```

Each time refinement is executed, two parent Gem NFTs are burned or otherwise rendered permanently unusable, and only one new Refined Gem NFT is minted. As a result, the total circulating NFT supply decreases by one.

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

In the initial model, Gem Refinement should be limited to same-stone refinement. For example, two Diamond Gem NFTs may be refined into one Refined Diamond Gem NFT, and two Ruby Gem NFTs may be refined into one Refined Ruby Gem NFT. Cross-stone refinement is not included in the initial model, as it may unnecessarily complicate the stone-specific supply, scarcity, halving, and mining difficulty structures.

Item	Principle
Required Materials	Two Gem NFTs with the same `stoneType`
Additional Cost	A small amount of STONE usage or burn
Parent NFT Handling	Two parent Gem NFTs are burned or permanently removed from circulation
Output	One Refined Gem NFT with the same `stoneType`
Generation	Recorded as Gen1 or Refined Generation
Supply Effect	Total circulating NFT supply decreases
Minting Authority	Limited to the Refining Contract
Admin Mint	Not allowed
Randomness	Verifiable randomness should be used

The base tier of the Refined Gem NFT may be calculated based on the higher tier of the two parent Gem NFTs.

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

Here, T_1 and T_2 represent the tiers of the two parent Gem NFTs, and T_base represents the base tier used to determine the refinement result.

Tier Level	Tier
1	Common
2	Rare
3	Epic
4	Legendary

The refinement result should be designed so that the probability of maintaining the same tier as the base tier is the highest. The probability of falling by one tier should remain very low. If an upgrade occurs, the increase should generally be limited to one or two tiers. Lower tiers may have relatively higher upgrade probabilities, while higher tiers should have significantly lower upgrade probabilities in order to preserve the scarcity of high-tier Gem NFTs.

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

An example of the base threshold model, assuming no tier gap between the two parent Gem NFTs, is as follows.

Base Tier	-1 Tier	Same Tier	+1 Tier	+2 Tier
Common	None	68.0%	27.0%	5.0%
Rare	1.0%	76.0%	20.0%	3.0%
Epic	1.5%	88.5%	10.0%	None
Legendary	2.0%	98.0%	None	None

The purpose of this structure is to preserve the expectation of refinement while preventing excessive creation of high-tier NFTs. Common and Rare Gem NFTs have relatively higher upgrade potential, which gives lower-tier or duplicate Gem NFTs additional utility. From Epic onward, the probability of upgrading becomes significantly lower. Legendary is treated as the highest tier in this refinement model and does not allow further upward tier progression.

If the two parent Gem NFTs have different tiers, the upgrade probability may be additionally adjusted. The tier gap G is defined as follows.

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

Tier Gap G	Upgrade Modifier	Principle
0	100%	Same-tier refinement. Base probabilities apply.
1	70%	Adjacent-tier refinement. Upgrade probability is partially reduced.
2	35%	Large tier gap. Upgrade probability is significantly reduced.
3 or higher	Restricted	Refinement may be restricted in the initial model.

The adjusted upgrade probability may be calculated as follows.

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

Any upgrade probability reduced by this adjustment is added back to the probability of maintaining the same tier. This prevents repeated attempts to combine one high-tier Gem NFT with a significantly lower-tier Gem NFT in order to generate higher-tier outputs too easily.

The Refining Contract should perform ownership verification, same-stone verification, tier-gap validation, STONE usage or burn, parent NFT burning, randomness request, and the minting request for the resulting Refined Gem NFT. A Refined Gem NFT must not be created through arbitrary operator minting. It should only be created when the Refining Contract verifies that all predefined conditions have been satisfied.

Gem Refinement does not replace the core mining structure of CryptoStone. It is an optional expansion module intended to enhance post-mining utility, collectibility, marketplace demand, and potential game utility for Gem NFTs. In addition to Gem Refinement, CryptoStone may gradually expand its digital gemstone ecosystem through Marketplace functions, Arena Game modules, Ranking Systems, Collection Quests, and other utility extensions.

42. Need for Website, Simulator, and Explorer

The CryptoStone protocol itself operates through smart contracts and on-chain data, but a separate user interface is required for users to understand and participate intuitively.

The CryptoStone ecosystem may therefore require the following web-based tools.

Tool	Role
Mining Simulator	Calculates estimated mining time based on STONE amount, selected pool, and lockup period.
PoM Dashboard	Shows each user’s PoM by pool, required PoM threshold, and claim eligibility.
Pool Dashboard	Shows mined supply, remaining supply, Pool Difficulty, and Scarcity Multiplier by stone pool.
Gem Explorer	Allows lookup of Gem NFT attributes, rarity, tokenId, mining timestamp, and trading history.
Rarity Explorer	Shows rarity and Probability Rarity Index for Weight, Color, Clarity, and Cut combinations.
Protocol Status Page	Verifiably displays key protocol information such as 100% public circulation, No Admin Mint, total supply, probability tables, and pool status.

These tools do not replace the essential trust foundation of the protocol. They serve as interfaces that allow users to interpret on-chain data more easily. In other words, the essence of CryptoStone lies in contracts and on-chain rules; the website and explorer are means of interpreting and visualizing them.

43. Future Direction

CryptoStone should initially begin on an EVM-compatible network with an ERC-20, ERC-721, and Mining Pool Contract structure. At this stage, the focus should be on verifying the core protocol functions: staking, Mining Power calculation, PoM accumulation, stone-specific halving, gemstone attribute generation, and Gem NFT minting.

Thereafter, the ecosystem should expand user-facing tools such as a mining dashboard, Mining Simulator, PoM Dashboard, Gem Explorer, Rarity Explorer, stone-specific trading data, and NFT marketplace features. Since CryptoStone’s value depends on collectible-market understanding and data transparency, a data layer through which anyone can verify gemstone rarity, trading history, stone-specific floor prices, and high-grade gemstone rankings is important.

As the ecosystem grows, CryptoStone may evolve beyond a simple smart contract project into a dedicated Appchain or Rollup. In such a case, STONE may function not merely as a mining token, but as a gas token or native asset of the network, while Gem NFTs may become the base digital assets of the CryptoStone network.

Over the long term, development into an independent CryptoStone Mainnet may also be considered. This would require native validators, open-source nodes, a native mining module, an on-chain randomness module, an internal marketplace, and a public protocol improvement process. However, a mainnet should not be pursued simply because it is technically possible to create a chain. It should be pursued only after sufficient users, liquidity, validators, and developer ecosystem have formed.

The long-term direction of CryptoStone is not to operate a single NFT collection, but to establish a new on-chain asset category known as digital gemstones.

44. Legal and Investment Disclaimers

CryptoStone does not provide ownership, redemption rights, or collateral rights over physical gemstones. CryptoStone Gem NFTs are not claims against real-world gemstones, but digital gemstone assets mined on-chain.

The staking and lockup structures of CryptoStone are not designed to provide fixed returns, interest, dividends, or investment income. Depositing STONE into a mining pool is a form of protocol participation to obtain the opportunity to mine Gem NFTs, and it does not guarantee any specific return or market price increase.

Holding or staking STONE does not guarantee any particular profit, dividend, interest, price appreciation, or NFT resale revenue. Gem NFTs are collectible digital assets, and their market value may vary according to the subjective assessment and demand of external market participants.

PoM is not a separate investment asset, debt instrument, revenue right, point, or tradable token. PoM is an internal protocol metric indicating the amount of mining work accumulated by a user in a specific stone pool. It cannot be transferred between pools or assigned externally.

CryptoStone does not promise any particular return, price appreciation, principal protection, or market liquidity. The value of CryptoStone may be formed by collectible demand, market participants' perception of scarcity, trading activity, and ecosystem expansion.

The numerical values and formulas presented in this whitepaper are initial design values for implementing the concept of decentralized digital gemstones. They do not fully represent all economic, cultural, or gemological factors of the physical gemstone market, and should not be regarded as a complete economic model of the ecosystem.

Risk	Description
Smart contract vulnerability	Possibility of code errors or hacking.
Randomness generation risk	Dependency on randomness infrastructure or implementation error.

Insufficient NFT market demand	Possibility that collectible demand may not be sufficient.
STONE liquidity shortage	Possibility of insufficient DEX or exchange liquidity.
Regulatory changes	Changes in digital asset regulations by jurisdiction.
Mainnet expansion failure	Possibility that the long-term roadmap may not be realized.
Rarity valuation uncertainty	The market may assess rarity differently.
Initial parameter risk	Parameters may operate differently from actual market demand.
Burn burden	Claim Burn and Maturity Burn may impose participation costs.
Early public-market volatility	The 100% public circulation structure may involve high early market price volatility.
LP structure risk	Trust issues may arise concerning initial liquidity supply and LP treatment.

Accordingly, CryptoStone should be implemented carefully after technical, economic, and legal review.

45. Significance of the Project

The significance of CryptoStone may be summarized in three points.

First, CryptoStone proposes that NFTs can move beyond ownership over external content and become attribute-based assets in themselves. While many existing NFTs depend on images or platforms, CryptoStone seeks to reinforce the asset nature of NFTs by recording gemstone attributes directly as on-chain data.

Second, CryptoStone transfers gemstone scarcity and grading structures into a digital environment. Physical gemstone value differs according to weight, color, clarity, and cut. CryptoStone implements this through probability tables, mining difficulty, halving mechanics, and supply limits.

Third, CryptoStone extends the concept of decentralized mining into a new asset domain after Bitcoin. If Bitcoin digitized the scarcity of gold, CryptoStone digitizes the scarcity and collectibility of gemstones.

CryptoStone does not claim to replace physical gemstones. It is a project that reinterprets the asset concept of gemstones in a digital environment.

The author believes that this attempt may contribute to the broader role of blockchain technology beyond financial transactions, enabling the representation of abstract real-world value and attribute-based assets in a digital environment.

46. Conclusion

CryptoStone proposes a new asset concept: digital gemstones.

Just as Bitcoin created the concept of digital gold without physically custodying gold, CryptoStone seeks to implement the core properties of gemstones—scarcity, mineability, grading, and collectibility—in a digital environment without collateralizing ownership over physical gemstones.

The structure of CryptoStone may be summarized as follows.

Core Structure	Details
Single token	STONE ERC-20
Initial supply	1,200,000,000 STONE
Circulation structure	100% public circulation
Access method	Market access through public DEX liquidity
NFT structure	One ERC-721 Gem NFT contract
Mining pools	12 independent gemstone mining pools
Pool implementation	Same Pool Template + Factory structure
Base Mining Unit	100,000 STONE
Target Pool Power	40,000,000 Power
Total Target Power across 12 pools	480,000,000 Power
PoM structure	Accumulated work model based on Proof of Mining
Claim condition	Pool-specific PoM >= Required PoM Threshold
Claim Burn	20 STONE × Scarcity Multiplier
Lock Model	Flexible, 90 days, 180 days, 365 days
Depreciation	Maturity Burn according to lockup period
Rarity	Rarity Score + Probability Rarity Index
Halving	Stone-specific Scarcity Multiplier
Randomness	Initial VRF or Commit-then-Reveal, long-term native randomness module
Hash power abstraction	STONE-based Mining Power
Decentralization	No Admin Mint, No Central Server, finalize structure
Public verification	Source code disclosure, audit report, LP treatment proof, probability table verification
User tools	Mining Simulator, PoM Dashboard, Gem Explorer, Rarity Explorer
Long-term direction	Possible expansion into Appchain or Mainnet
Ecosystem expansion	Marketplace, Gem Refinement, Arena Game, Ranking System, Collection Quest

The author does not consider the goal of CryptoStone to be short-term NFT sales. The goal of CryptoStone is to demonstrate how the asset concept of gemstones can be implemented in a decentralized digital environment.

The trust of CryptoStone is formed not by founder authority, insider allocation, or centralized operational rights, but by fixed supply, a 100% public circulation structure, a verifiable PoM model, immutable probability tables, publicly verifiable contracts, and on-chain data accessible to anyone.

If Bitcoin is digital gold, CryptoStone is decentralized digital gemstone.