

CRYPTOSTONE WHITEPAPER v2.8

탈중앙 환경에서의 디지털 보석 자산에 관한 연구

CryptoStone 탈중앙 디지털 보석 프로토콜

목차

CRYPTOSTONE WHITEPAPER v2.8

1. 서론
2. CryptoStone을 이해하는 가장 단순한 방식
3. 연구 목적
4. 프로토콜 신뢰 원칙
5. 디지털 보석 자산의 기본 개념
6. 보석의 속성 표현
7. 보석 고유성의 디지털 구현
8. 단일 컬렉션과 12개 스톤의 공존
9. 디지털 광산의 구성
10. 해시파워, 마이닝 파워, Proof of Mining
11. Mining Pool Template과 Factory 구조
12. 스톤별 한정 공급량
13. 채굴 주기의 설계
14. STONE 초기 발행량의 산정
15. STONE의 100% 공개유통 구조
16. Base Mining Unit과 소액 참여 구조
17. Target Pool Power와 장기 채굴 기간
18. 수치와 파라미터에 대한 해석
19. 마이닝 파워의 계산
20. 장기 참여 보정과 Flexible Cooldown
21. Proof of Mining, PoM의 누적
22. 필요 PoM 임계값
23. 풀 난이도의 조정
24. 반감기와 희소성 배수
25. 채굴 속도와 공급 고갈의 비선형 구조
26. Weight 속성의 디지털화
27. Color 속성의 디지털화
28. Clarity 속성의 디지털화
29. Cut 속성의 디지털화
30. 속성 생성과 랜덤 검증
31. Rarity Score와 Probability Rarity Index
32. 희귀도 티어 구조
33. 수집 가치의 형성
34. 탈중앙 채굴 구조
35. 채굴 비용과 STONE 조각 구조
36. 락업 감가상각 및 반환 구조
37. 개발 구조의 선택
38. 프로토콜 고정 원칙
39. 보안 대응과 탈중앙성의 균형
40. 이미지와 메타데이터의 위치
41. 생태계 확장 모듈과 Gem Refinement
42. 홈페이지, 시뮬레이터 및 익스플로러의 필요성
43. 향후 추진 방향
44. 법률 및 투자성 유의사항
45. 프로젝트의 의의
46. 결론

초록

비트코인은 현실의 금을 직접 담보하지 않았음에도 불구하고, 한정된 공급량, 공개된 채굴 규칙, 탈중앙네트워크, 누구나 검증 가능한 거래 구조를 통해 “디지털 금”이라는 새로운 자산 개념을 형성하였다. 비트코인의 본질적 의미는 특정 발행자나 중앙 기관의 신뢰 없이도, 코드와 네트워크만으로 디지털 자산의 희소성과 소유권을 구현할 수 있음을 증명한 데있다.

필자는 이러한 철학을 보석이라는 자산 개념으로 확장하고자 한다. 현실 세계의 보석은 채굴량이 제한되어 있으며, 각각의 보석은 무게, 색상, 투명도, 컷팅과 같은 속성에 따라 서로 다른 희소성과 가치를 갖는다. 같은 종류의 보석이라도 각개체의 속성이 다르다면 그 가치는 달라진다. 이러한 점에서 보석은 본질적으로 비대체적이며, 디지털 환경에서 고유 자산으로 표현하기에 적합한 특성을 가진다.

CryptoStone은 보석의 채굴성, 희소성, 등급성, 수집성을 온체인 데이터로 표현하고, 중앙 서버나 운영자의 임의 개입없이 디지털 환경에서 보석 NFT가 채굴될 수 있도록 설계된 탈중앙 디지털 보석 프로토콜이다. 각 보석은 ERC-721 기반 NFT로 표현되며, 스톤 종류, 무게, 색상, 투명도, 컷팅, 채굴 시점, 채굴된마이닝 풀 등의 속성을 온체인에 기록한다.

본 프로젝트는 실제 보석의 소유권, 담보권 또는 교환권을 제공하는 것을 목적으로 하지 않는다. 필자가본 백서에서 제안하는 것은 현실 보석이 가진 구조적 속성, 즉 한정성, 채굴성, 등급성, 희소성, 수집성을 디지털 환경에서 독립적인 희소자산으로 구현하려는 연구이자 실험이다.

비트코인이 금의 희소성과 채굴성을 디지털화하였다면, CryptoStone은 보석의 희소성과 속성 기반 가치를 탈중앙 방식으로 디지털화하고자 한다.

1. 서론

현실 세계에서 보석은 오랜 기간 동안 가치 저장 수단, 장식 자산, 수집 자산, 상징 자산으로 기능해왔다.

보석의 가치는 단순한 물리적 존재에서만 발생하지 않는다. 보석은 채굴의 어려움, 매장량의 제한, 가공의 정교함, 등급의 차이, 수집 수요, 문화적 상징성에 의해 가치가 형성된다.

특히 다이아몬드, 루비, 사파이어, 에메랄드와 같은 보석은 동일한 종류의 보석이라 하더라도 개별 보석의 속성에 따라 전혀 다른 가치를 갖는다. 무게가 크고, 색상이 우수하며, 투명도가 높고, 컷팅이 정교한 보석은 더 높은 희소성을 가진다.

이러한 구조는 보석이 대체 가능한 상품이 아니라, 개별 속성에 따라 가치가 달라지는 비대체적 자산임을 보여준다.

블록체인 기술은 이러한 비대체적 속성을 디지털 환경에서 표현할 수 있는 기반을 제공한다. 그러나 기존 NFT 시장은 대부분 이미지, 게임 아이템, 멤버십, 외부 콘텐츠의 소유권 또는 접근권을 표현하는 방식으로 발전해왔다. 이 경우 NFT의 가치는 외부 이미지, 중앙 서버, 특정 플랫폼, 운영 주체에 종속될 수 있다.

CryptoStone은 이와 다른 방향을 제안한다. CryptoStone은 외부 이미지나 중앙 서버의 콘텐츠를 증명하기 위한 NFT가 아니라, NFT 자체가 보석의 속성 데이터를 보유하고, 그 속성 자체로 희소성과 수집 가치를 표현하는 디지털 보석 자산이다.

필자는 본 백서를 통해 현실 보석의 물리적 소유권을 블록체인으로 이전하려는 것이 아니라, 보석이 가진 희소성과 속성기반 가치를 디지털 환경에서 어떻게 탈중앙적으로 구현할 수 있는지에 대해 서술하고자한다.

2. CryptoStone을 이해하는 가장 단순한 방식

CryptoStone은 디지털 보석을 채굴하는 온체인 프로토콜이다. 사용자는 STONE을 원하는 보석 마인딩풀에 투입하고, 시간이 지나 Proof of Mining, PoM 값이 충분히 누적되면 Gem NFT를 claim 할 수 있다. 채굴된 NFT는 단순 이미지

가 아니라, 스톤 종류, 무게, 색상, 투명도, 컷팅, 희귀도 점수, 채굴 시점이 기록된 고유한 디지털 보석이다.

사용자는 다이아몬드, 루비, 사파이어, 에메랄드 등 12개 스톤 풀 중 원하는 풀을 선택할 수 있다. 각 스톤은 서로 다른 공급량, 채굴 주기, 반감기 구조를 가지며, 채굴이 진행될수록 남은 공급량은 줄어들고 희소성 배수는 상승한다.

CryptoStone의 핵심 경험은 단순하다.

STONE을 디지털 광산에 투입한다.

시간이 지나 Mining Power가 Proof of Mining, PoM으로 누적된다.

필요 PoM 임계값에 도달하면 Gem NFT를 claim한다.

어떤 보석이 나올지는 공개된 확률과 검증 가능한 랜덤성에 의해 결정된다.

즉, CryptoStone은 “구매하는 NFT”가 아니라 “채굴되는 디지털 보석”을 지향한다. 사용자는 단순히 이미지를 구매하는 것이 아니라, 공개된 규칙과 고정된 확률 구조 안에서 자신만의 디지털 보석을 채굴한다.

3. 연구 목적

CryptoStone의 목적은 현실 보석을 그대로 복제하거나 실물 보석의 소유권을 디지털화하는 데 있지 않다. 본 프로젝트의 목적은 현실 보석이 가진 구조적 속성, 즉 채굴성, 한정성, 등급성, 희소성, 수집성을 디지털 환경으로 옮기는 데 있다.

CryptoStone은 다음 질문에서 출발한다.

비트코인이 금을 직접 담보하지 않고도 디지털 금이 될 수 있었다면, 보석의 희소성, 등급성, 수집성도 탈중앙 디지털 환경에서 독립적인 자산으로 구현될 수 있는가? 필자는 이 질문에 대한 하나의 기

술적, 경제적, 철학적 설계를 본 백서에서 제안한다.

속성의 디지털화 보석의 무게, 색상, 투명도, 커팅을 온체인 속성으로 구조화한다.

채굴 과정의 구현 보석 채굴 과정을 스마트컨트랙트 기반으로 구현한다.

공급량 고정 스톤별 최대 발행량과 희소성 구조를 사전에 고정한다.

탈중앙 참여 중앙 서버 없이 누구나 마이닝 풀에 참여할 수 있도록 한다.

속성 조작 방지 운영자가 보석의 등급이나 속성을 임의로 조작할 수 없도록 한다.

수집 가치 형성 희귀한 속성 조합이 수집 시장에서 가치로 인식될 수 있는 구조를 만든다.

장기 확장성 향후 Appchain 또는 Mainnet으로 확장 가능한 기반을 마련한다.

4. 프로토콜 신뢰 원칙

CryptoStone은 특정 창립자나 운영자의 신뢰에 의존하지 않는 구조를 지향한다. 본 프로토콜의 신뢰는 창립자의 신원보다 공개된 코드, 고정된 발행량, 변경 불가능한 확률표, No Admin Mint 구조, 검증 가능한 랜덤성, 그리고 누구나 확인할 수 있는 온체인 데이터에 기반한다.

운영자는 특정 사용자에게 희귀 NFT를 임의로 배정하거나, 스톤별 공급량을 변경하거나, 채굴 확률을 조작할 수 없어야 한다. CryptoStone의 목적은 사람의 권위가 아니라 프로토콜의 규칙에 의해 디지털 보석의 희소성이 형성되는 구조를 만드는 데 있다.

따라서 CryptoStone은 다음 신뢰 원칙을 따른다.

Fixed Supply STONE 총 발행량과 스톤별 NFT 최대 발행량은 사전에 고정된다.

100% Public Circulation STONE은 100% 공개유통 구조를 따른다.

No Admin Mint 운영자는 임의로 Gem NFT를 발행할 수 없어야 한다.

Immutable Probability 보석 속성 확률표는 공개되고, finalize 이후 변경될 수 없어야 한다.

Verifiable Randomness 보석 속성은 검증 가능한 랜덤 구조에 의해 결정되어야 한다.

On-chain Attributes Gem NFT의 핵심 속성은 온체인 데이터로 기록되어야 한다.

Transparent Pools 각 스톤 풀의 채굴량, 잔여 수량, 난이도는 공개적으로 확인 가능해야 한다.

Open Verification 누구나 컨트랙트와 채굴 규칙을 검증할 수 있어야 한다.

이러한 구조는 CryptoStone이 특정 운영자의 재량이 아니라, 공개된 규칙과 검증 가능한 코드에 의해 작동하는 탈중앙 디지털 보석 프로토콜임을 보여준다.

5. 디지털 보석 자산의 기본 개념

CryptoStone은 하나의 STONE 토큰, 12개의 보석 마이닝 풀, 하나의 ERC-721 Gem NFT 컨트랙트로구성된다.

STONE Token 디지털 광산에 참여하기 위한 단일 마이닝 자원 12 Gemstone Mining Pools 각 탄생석을 채굴하는 독립 디지털 광산 CryptoStone Gem NFT 채굴된 디지털 보석을 표현하는 ERC-721 기반고유 자산 Mining Pool Contract 스테이킹, 마이닝 파워, 난이도, claim 조건을 관리 Gem NFT Contract 보석 NFT의 속성, 발행량, 소유권을 관리 STONE은 보석 그 자체가 아니다. STONE은 디지털광산에 참여하기 위한 마이닝 파워의 원천이다. 사용자는 STONE을 원하는 보석 마이닝 풀에 스테이킹함으로써 마이닝 파워를 획득하고, 시간이 지남에 따라 PoM을 누적한다.

채굴 결과물은 CryptoStone Gem NFT이다. Gem NFT는 하나의 통합 ERC-721 컨트랙트에서 발행되며, 각 NFT는 자신이 어떤 스톤인지, 어떤 무게와 등급을 갖는지 온체인 속성으로 보유한다.

현실 보석 채굴 구조를 추상화하면 다음과 같다.

현실 보석 채굴 CryptoStone

광산 Gemstone Mining Pool

채굴 장비 및 에너지 STONE Token

채굴 작업량 Proof of Mining, PoM

채굴 결과물 ERC-721 Gem NFT

광산 난이도 Pool Difficulty

매장량 감소 Scarcity Multiplier

보석 감정 On-chain Attribute & Rarity Score

6. 보석의 속성 표현

보석의 가치는 단순히 종류만으로 결정되지 않는다. 같은 다이아몬드라도 무게, 색상, 투명도, 커팅에 따라 시장에서 다른 가치를 갖는다.

CryptoStone은 이러한 보석의 속성을 디지털 환경에서 표현하기 위해 각 Gem NFT에 다음 네 가지 핵심 속성을 부여한다.

Weight 보석의 무게

Color 보석의 색상 등급

Clarity 보석의 투명도 등급

Cut 보석의 커팅 등급

이 네 가지 속성은 채굴 시점에 결정되며, 민팅 이후 변경될 수 없다. 이는 현실 보석이 감정 이후 개별 속성을 기준으로 평가되는 것과 유사한 구조를 디지털 방식으로 구현한 것이다.

CryptoStone에서 각 NFT는 단순히 “이미지 파일을 가리키는 토큰”이 아니라, 보석의 속성값을 직접 보유하는 디지털자산이다. 이미지, 3D 모델, 카드 형태의 시각적 표현은 사용자 경험을 위한 보조 요소일수 있지만, CryptoStone NFT의 본질은 온체인에 기록된 속성 데이터에 있다.

7. 보석 고유성의 디지털 구현

CryptoStone은 각 보석의 고유성을 표현하기 위해 다양한 기술적 선택지를 검토할 수 있다. 대체 가능한토큰 구조, 반대체 토큰 구조, 복합 토큰 구조 등 여러 방식이 가능하지만, CryptoStone이 구현하려는 핵심은 각 보석이 고유한 속성조합과 tokenId를 갖는 것이다.

따라서 CryptoStone의 보석은 ERC-721 기반 NFT로 표현된다. 이 선택은 특정 기술 표준을 강조하기 위한 것이 아니라, 다음 기능을 구현하기 위한 결과다.

각 보석의 고유 tokenId 필요 ERC-721은 고유 tokenId 기반 자산 표현에 적합하다.

보석마다 다른 속성 저장 tokenId별 metadata 및 on-chain attribute 구조가 가능하다.

소유권 이전 기록 필요 표준 NFT 전송 및 소유권 기록이 가능하다.

하나의 컬렉션 안에 여러 스톤 표현 stoneType 속성으로 12개 스톤을 구분할 수 있다.

희귀도와 거래 이력 추적 NFT별 provenance 및 rarity tracking이 가능하다.

즉, CryptoStone에서 ERC-721은 이미지 NFT를 만들기 위한 수단이 아니라, 디지털 보석의 고유성과속성 기반 자산성을 표현하기 위한 기술적 컨테이너다.

8. 단일 컬렉션과 12개 스톤의 공존

CryptoStone은 12개의 스톤을 각각 별도 NFT 컬렉션으로 분리하지 않는다. 모든 보석은 하나의 ERC-721 Gem NFT 컨트랙트에서 발행된다.

다만 각 NFT는 stoneType 속성을 통해 자신이 어떤 보석인지 구분된다.

Token ID Stone Type Weight Color Clarity Cut #10291Diamond 3.42 CTD VVS1 6 Star
#58102Ruby 8.13 CTG VS2 4 Star #77410Sapphire 1.25 CTE IF 5 Star 이 구조는 다음 장점을 가진다.

컬렉션 통합 CryptoStone이라는 하나의 컬렉션 정체성을 유지한다.

거래 데이터 집중 마켓플레이스에서 컬렉션 가치와 거래 데이터가 분산되는 것을 방지한다.

희귀도 관리 용이 모든 보석을 하나의 rarity ranking 체계로 비교할 수 있다.

스톤별 개별성 유지 stoneType 속성으로 각 보석의 독립성을 표현한다.

공급량 제한 가능 NFT 컨트랙트 내부에서 스톤별 max supply를 검증할 수 있다.

NFT 컨트랙트는 스톤별 발행량을 별도로 관리한다.

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

$\text{mintedByStone}[\text{Diamond}] < \text{maxSupplyByStone}[\text{Diamond}]$ 따라서 Diamond Pool에서 민팅 요청이 들어오더라도 Diamond의 최대 발행량에 도달하면 더 이상 Diamond NFT는 발행되지 않는다.

9. 디지털 광산의 구성

CryptoStone에서 각 스톤은 하나의 독립된 디지털 광산으로 간주된다.

Garnet Pool Garnet NFT 채굴

Amethyst Pool Amethyst NFT 채굴 Aquamarine Pool Aquamarine NFT 채굴 Diamond Pool Diamond NFT 채굴 Emerald Pool Emerald NFT 채굴 Pearl Pool Pearl NFT 채굴 Ruby Pool Ruby NFT 채굴 Spinel Pool Spinel NFT 채굴 Sapphire Pool Sapphire NFT 채굴 Opal Pool Opal NFT 채굴 Topaz Pool Topaz NFT 채굴 Zircon Pool Zircon NFT 채굴 각 마이닝 풀은 동일한 STONE 토큰을 사용하지만, 서로 다른 채굴 조건을 가진다.

Stone Type 해당 풀에서 채굴되는 보석 종류

Max Supply 해당 스톤의 최대 발행량

Base Mining Interval 기본 채굴 주기 Target Pool Power 기준 마이닝 파워 Current Pool Power 현재풀에 누적된 마이닝 파워 Minted Supply 현재까지 채굴된 수량 Pool Difficulty 전체 참여도에 따른 난이도 Scarcity Multiplier 반감기 기반 희소성 배수현실에서 다이아몬드 광산과 루비 광산의 매장량이 다르듯, CryptoStone에서도 각 스톤은 서로 다른 총수량과 채굴 난이도를 가진다. Diamond가 많이 채굴되었다고 해서 Ruby의 난이도가 상승하지 않는다. Ruby가 고갈되어 간다고 해서 Sapphire의 공급량이 줄어들지 않는다.

각 스톤은 독립적인 디지털 매장량과 채굴 구조를 가진다.

10. 해시파워, 마이닝 파워, Proof of Mining

비트코인에서 채굴자는 해시파워를 통해 블록을 생성할 확률을 얻는다. 해시파워가 높을수록 블록을 발견할 가능성은 높아지지만, 비트코인의 전체 발행 규칙이나 난이도 구조를 임의로 변경할 수는 없다. 즉, 해시파워는 네트워크 규칙을 바꾸는 권한이 아니라, 정해진 규칙 안에서 더 많은 채굴 기회를 얻기 위한 연산 자원이다.

CryptoStone은 이 개념을 디지털 보석 채굴 구조에 맞게 추상화한다. CryptoStone에서 해시파워에 대응되는 개념은 Mining Power이며, Mining Power가 시간에 따라 누적된 작업량이 Proof of Mining, PoM이다.

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 PoM은 별도로 전송되거나 거래되는 토큰이 아니다. PoM은 사용자의 채굴 참여와 시간 경과를 컨트랙트가 기록하는 온체인 작업량 지표이다. 또한 PoM은 네트워크 합의 알고리즘을 의미하지 않는다. CryptoStone의 PoM은 특정 스톤 풀

에서 사용자가 Gem NFT를 claim할 수 있는 조건에 도달했는지를 판단하기 위한 프로토콜 내부 값이다.

사용자 i 가 특정 스톤 풀 j 에 스테이킹한 STONE 수량을 $s_{\{i,j\}}$, 락업 기간에 따른 배수를 L_i 라고 할 때, 사용자의 마이닝

파워 $P_{\{i,j\}}$ 는 다음과 같이 정의된다.

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

사용자의 PoM 값은 시간에 따라 다음과 같이 누적된다.

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

여기서 $PoM_{\{i,j\}}(t)$ 는 사용자 i 가 스톤 풀 j 에서 시점 t 까지 누적한 Proof of Mining 값이다.

PoM은 스톤 풀별로 독립적으로 누적된다. 예를 들어 Diamond Pool에서 누적된 PoM은 Diamond NFT claim에만 사용할 수 있으며, Ruby Pool 또는 Sapphire Pool의 PoM으로 전환될 수 없다. 이 구조는 각 스톤 풀의 독립성, 희소

성, 채굴 난이도를 보호한다.

마이닝 파워가 높은 사용자는 더 빠르게 필요한 PoM 임계값에 도달할 수 있지만, 보석의 희귀도 확률을 임의로 높이거나 특정 등급의 보석을 선택할 수 없다.

11. Mining Pool Template과 Factory 구조

12개의 Mining Pool Contract는 서로 다른 로직을 가진 별도 개발물이 아니다. 모든 풀은 동일하게 감사된 Mining Pool Template을 기반으로 배포된다. 각 풀은 동일한 핵심 로직을 사용하되, 다음 파라미터만 다르게 설정된다.

stoneType 해당 풀에서 채굴되는 스톤 종류

maxSupply 해당 스톤의 최대 발행량

baseMiningInterval 기본 채굴 주기

targetPoolPower 기준 마이닝 파워

scarcitySchedule 스톤별 반감기 구조

poolAddress NFT 컨트랙트가 허용하는 민팅 권한 주소이를 위해 CryptoStone은 Pool Factory 구조를 사용할 수 있다. Pool Factory는 동일한 Mining Pool Template을 기반으로 12개 스톤별 풀을 생성하고, 배포 이후 각 풀의 핵심 파라미터를 고정한다.

코드 일관성 12개 풀이 동일한 로직을 사용한다.

감사 효율성 하나의 Pool Template을 중심으로 보안 감사가 가능하다.

리스크 감소 풀마다 다른 코드로 인한 예외적 버그 가능성을 축소한다.

파라미터 투명성 각 풀의 차이는 공개된 고정값으로만 발생한다.

확장성 향후 새로운 스톤 풀 확장 시 동일한 구조를 활용할 수 있다.

따라서 CryptoStone은 “12개의 독립 광산”이라는 경제적 구조를 유지하면서도, 개발상으로는 동일하고 검증 가능한 스마트 컨트랙트 템플릿을 사용하여 안정성과 투명성을 높인다.

12. 스톤별 한정 공급량

CryptoStone의 12개 스톤은 각각 다른 총 발행량을 가진다. 이 구조는 스톤 종류 자체에 1차적 희소성을 부여한다.

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
Month Stone Meaning Max Supply
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
총 Gem NFT의 최대 발행량은 다음과 같다.

Total Gem NFT Max Supply = 1,980,000

Diamond는 가장 적은 공급량을 가지며, Zircon은 가장 많은 공급량을 가진다. 따라서 스톤 종류 자체가 희소성의 한 요소가 된다.

글로벌 컬렉션 관점에서 특정 스톤 j의 공급 비중은 다음과 같이 표현할 수 있다.

$$P_{\text{stone},j} = N_j \div N_{\text{total}}$$

여기서 N_j 는 특정 스톤의 최대 발행량이고, N_{total} 은 전체 Gem NFT 최대 발행량이다. 이 값은 후술하는 확률 기반 희귀도 지표에서 스톤 종류의 상대적 희소성을 설명하는 기초값으로 활용될 수 있다.

CryptoStone의 총 Gem NFT 공급량은 단일 희귀 NFT 컬렉션의 단순 발행량을 의미하지 않는다. 이는 12개 스톤 풀과 다층 속성 조합으로 구성된 장기 채굴형 디지털 보석 자산군을 의미한다. 희소성은 총수량 하나만으로 결정되지 않으며, 스톤 종류, 채굴 시점, 반감기 구간, Weight, Color, Clarity, Cut,

tokenId, Probability Rarity Index가 복합적으로 작용한다.

따라서 CryptoStone에서 1,980,000개의 총 공급량은 단기 민팅 이벤트를 위한 대량 발행 구조가 아니라, 장기간에 걸쳐 다양한 참여자가 서로 다른 스톤과 속성 조합을 채굴할 수 있도록 설계된 디지털 보석생태계의 총 매장량으로 해석되어야 한다.

13. 채굴 주기의 설계

각 스톤은 서로 다른 기본 채굴 주기를 가진다.

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

기본 채굴 주기가 길수록 동일한 마이닝 파워로 채굴하기 어렵다. 따라서 스톤별 희소성은 다음 두 가지요소로 1차 형성된다.

Max Supply 해당 스톤의 총 발행 가능 수량

Base Mining Interval 기준 마이닝 단위로 1개를 채굴하는 데 걸리는 시간예를 들어 Diamond는 공급량이 가장 적고 기본 채굴 주기도 가장 길다. 이는 Diamond가 CryptoStone 생태계 안에서 가장 높은구조적 희소성을 갖도록 설계된 것이다.

14. STONE 초기 발행량의 산정

CryptoStone은 12개의 스톤별 토큰을 각각 발행하지 않고, 하나의 STONE 토큰을 사용한다.

초기 총 발행량은 다음과 같이 설정한다.

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

STONE을 1,200,000,000개로 설정하는 이유는 단순히 토큰 수량을 확대하기 위한 것이 아니다.

CryptoStone은 향후 100,000명 이상의 사용자가 다양한 규모로 마이닝 풀에 참여할 수 있는 구조를 지향한다. 이를 위해서는 소액 참여자, 중간 규모 참여자, 고마이닝 파워 참여자가 모두 자연스럽게

게 참여할수 있는 단위 구조가 필요하다.

1,200,000,000 STONE 구조에서는 100,000명 이상의 참여자를 전제로 하더라도 수천 STONE 단위의 자연스러운 참여 UX를 설계할 수 있다. 이는 소액 참여자에게는 진입 장벽을 낮추고, 중간 규모 참여자에게는 실질적인 마이닝 참여 단위를 제공하며, 고마이닝 파워 참여자에게는 장기적인 채굴 전략을 가능하게 한다.

따라서 12억 개 발행은 공급을 무분별하게 늘리는 것이 아니라, 더 넓은 사용자 기반과 Proof of Mining 구조를 수용하기 위한 단위 설계로 해석되어야 한다.

```
Expected Active Mining Ratio = 약 30% ~ 40%
1,200,000,000 STONE × 40%
= 480,000,000 Active Mining STONE
```

100,000명의 참여자를 기준으로 하면 평균 active stake는 다음과 같다.

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

즉, 1,200,000,000 STONE 구조는 대규모 참여자 기반을 수용하면서도, 소액 참여자가 마이닝 생태계에 접근할 수 있도록 하기 위한 설계다.

15. STONE의 100% 공개유통 구조

CryptoStone에서 STONE은 디지털 보석 채굴에 참여하기 위한 단일 마이닝 자원이다. 필자는 STONE의 배포 구조가 특정 내부자에게 사전적으로 권리를 부여하는 방식보다, 누구나 동일한 조건에서 접근할수 있는 공개 시장 구조를 따르는 것이 CryptoStone의 철학에 부합한다고 본다.

따라서 STONE은 100% 공개유통 구조를 따른다. 이는 STONE이 특정 주체에게 사전 배정되는 방식이 아니라, 공개 DEX 유동성을 통해 시장에 유통되며, 누구나 동일한 공개 시장 조건에서 취득할 수 있음을 의미한다.

항목 구조

Total Supply 1,200,000,000 STONE Distribution Principle 100% 공개유통 Market Access 공개 DEX 유동성 Additional Mint 없음 Access Rule 누구나 동일한 공개 시장 조건에서 취득 가능 Primary Utility Gem NFT 채굴을 위한 마이닝 풀 참여

```
Mechanism STONE 취득 → 스테이킹 → Mining Power 생성 → PoM 누적 →
```

Gem NFT claim

Supply Trust 발행량, 풀 구조, 확률표, claim 조건은 컨트랙트로 검증 가능사용자는 공개 시장에서 STONE을 취득한 뒤, 원하는 스톤 마이닝 풀에 이를 투입할 수 있다. 이후 사용자는 스테이킹한

STONE을 기반으로 Mining Power를 생성하고, 시간이 지남에 따라 Proof of Mining, PoM 값을 누적한다. 누적된 PoM 값이 해당 풀의 필요 임계값에 도달하면 Gem NFT를 claim할 수 있다.

이 구조에서 DEX는 STONE에 접근하기 위한 공개 진입 경로이며, 마이닝 풀은 STONE의 실제 사용처이다. 즉, STONE의 목적은 단순 보유나 투기적 유통이 아니라, 디지털 보석 채굴에 참여하기 위한 프로토콜 자원으로 기능하는 데있다.

재단 또는 초기 생태계 기여자 역시 별도의 사전 배정이 아니라, 공개 시장에서 동일한 조건으로 STONE 을 취득할 수 있다. 이 방식은 특정 주체의 선점 구조를 최소화하고, 프로토콜 참여의 기준을 공개 시장과 온체인 규칙에 맞추기 위한 것이다.

100% 공개유통 구조가 신뢰를 얻기 위해서는 초기 유동성 공급 방식, LP 처리 방식, 컨트랙트 권한, 추가 발행 불가 여부가 명확히 공개되어야 한다. 초기 유동성은 공개 DEX 풀을 통해 형성되며, 초기 LP 토큰의 처리 방식은 장기 락업 또는 소각 방식으로 공개되는 것이 바람직하다. 이는 유동성 회수에 대한 우려를 줄이고, STONE의 공개 시장 접근 구조에 대한 신뢰를 높이기 위한 것이다.

재단 또는 초기 기여자가 STONE을 취득하는 경우에도 별도 사전 배정이 아니라 공개 시장에서 동일 조건으로 취득해야 하며, 주요 보유 지갑은 온체인에서 확인 가능하도록 공개하는 것이 바람직하다. 이 구조는 재단의 존재를 부정하기 위한 것이 아니라, 재단 역시 프로토콜 외부의 특권적 배정이 아니라 공개 시장과 동일한 규칙 안에서 참여해야 한다는 원칙을 표현한다.

CryptoStone의 신뢰는 특정 주체의 사전 배정 물량이 아니라, 고정된 총 발행량, 100% 공개유통 구조, 변경 불가능한 채굴 규칙, 검증 가능한 PoM 구조, 그리고 온체인 데이터의 투명성에 의해 형성된다.

16. Base Mining Unit과 소액 참여 구조

CryptoStone의 기준 마이닝 단위는 다음과 같이 설정한다.

Base Mining Unit = 100,000 STONE

다만 이는 최소 참여 수량이 아니다. Base Mining Unit은 채굴 속도와 난이도를 계산하기 위한 기준 단위이다.

CryptoStone은 가능한 많은 사용자가 채굴에 참여할 수 있도록 PoM 누적 구조를 채택한다. 사용자는 100,000 STONE 미만의 수량으로도 마이닝 풀에 참여할 수 있으며, 스테이킹 수량과 시간에 비례하여 PoM 값을 누적한다.

사용자는 누적 PoM 값이 해당 풀의 필요 PoM 임계값 R_j 이상이 되었을 때 Gem NFT를 claim할 수 있다.

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

예를 들어 Diamond Pool의 초기 조건에서 Pool Difficulty와 Scarcity Multiplier가 모두 1x라고 가정하면 다음과 같다.

Active Stake Diamond NFT 1개 예상 채굴 시간 100,000 STONE 약 2.55일 10,000 STONE 약 25.5 일 5,000 STONE 약 51일 1,000 STONE 약 255일 100 STONE 약 6.98년이 구조는 고마

이닝 파워 유저에게는 빠른 채굴 기회를 제공하면서도, 소액 참여자도 장기적으로 PoM 값을 누적하여 Gem NFT를 claim할 수 있도록 한다.

필자는 이 구조가 CryptoStone의 생태계 확장에 매우 중요하다고 본다. NFT의 희소성은 총 발행량, 속성 확률, 반감기구조로 유지하고, 사용자 참여성은 낮은 진입장벽과 PoM 누적 구조로 확대해야 하기 때문이다.

17. Target Pool Power와 장기 채굴 기간

CryptoStone의 Target Pool Power는 전체 STONE 공급량이 아니라, 실제로 마이닝에 참여할 것으로 예상되는 유효스테이킹 물량을 기준으로 산정한다.

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

이는 전체 STONE 공급량 1,200,000,000개 중 약 40%가 장기적으로 마이닝 생태계에 참여할 수 있다는 가정을 반영한값이다.

특정 풀 j의 전체 마이닝 파워를 P_j , Target Pool Power를 P_j^* 라고 할 때, 전체 풀 파워는 다음과 같이 정의된다.

```

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

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

```

참여자가 매년 10,000명씩 증가하고, 10년 후 약 100,000명이 참여하며, 평균 active stake가 약 4,800 STONE 수준이라고 가정하면, 전체 Gem NFT 공급량의 약 90%가 채굴되는 데에는 약 8~9년이 소요될 수 있다.

반감기 구조로 인해 90% 이후의 채굴 속도는 더욱 느려진다. 따라서 전체 Gem NFT의 100%가 모두 채굴되기까지는 약 12년 이상이 소요될 수 있다.

이러한 기간 추정은 특정 수익률이나 가격을 예측하기 위한 것이 아니라, CryptoStone이 단기 NFT 민팅이벤트가 아니라 장기간에 걸쳐 디지털 보석이 점진적으로 채굴되는 탈중앙 마이닝 생태계를 지향한다는 점을 설명하기 위한 모델이다.

18. 수치와 파라미터에 대한 해석

본 백서에서 제시하는 스톤별 공급량, 기본 채굴 주기, 마이닝 파워 공식, PoM 임계값, 반감기 배수, Weight·Color·Clarity·Cut 확률표, Rarity Score 공식은 현실 보석 생태계를 완벽히 복제한 절대적 기준이 아니다.

이 수치들은 다음 목적을 위해 설계된 초기 기준 파라미터다.

디지털 희소성 표현 보석의 희소성을 온체인 환경에서 표현채굴 난이도 구현 스마트컨트랙트로 채굴 난이도와 공급 제한 구현상대적 희소성 구분 스톤별 희소성 차이를 비교 가능하게 설계수집 가치

구분 회귀도와 티어 구조를 통해 수집 시장 이해도 강화장기 공급 제어 반감기와 난이도 상승을 통해 공급 속도 관리참여 확장성 소액 참여자와 대규모 참여자를 동시에 수용따라서 본 백서의 수치들은 현실 보석 시장의 모든 가격 형성 요인, 감정 기준, 유통 구조, 수요와 공급, 문화적 가치, 실물보관 비용, 감정기관의 평가모델을 완벽히 반영한다고 볼 수 없다.

CryptoStone은 현실 보석 시장을 그대로 복제하려는 것이 아니라, 보석의 핵심 속성인 희소성, 등급성, 채굴성, 수집성을 디지털 환경에서 탈중앙 방식으로 구현해보기 위한 프로젝트다.

필자는 본 백서의 수치들이 단순한 임의값이 아니라, 탈중앙 디지털 보석이라는 개념을 설명하고 실험하기 위한 초기 기준값이라고 본다. 향후 연구, 시장 반응, 커뮤니티 검토, 기술 검증, 법률 검토에 따라 더정교한 모델로 발전할 수 있다. 다만 프로토콜이 공식 배포되고 핵심 규칙이 확정된 이후에는, 사전에 확정된 핵심 수치가 운영자에 의해 임의로 변경되어서는 안 된다.

19. 마이닝 파워의 계산

CryptoStone에서 마이닝 파워는 사용자가 보석을 채굴할 수 있는 속도와 기회를 결정한다. STONE을 더 많이 스테이킹한 참여자는 더 많은 마이닝 파워를 획득하고, 더 자주 claim 조건에 도달할 수 있다.

사용자 i 의 스테이킹 수량을 $s_{\{i,j\}}$, 락업 배수를 L_i , 사용자 마이닝 파워를 $P_{\{i,j\}}$ 라고 하면

다음과 같이 계산된다.

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

마이닝 파워는 보석의 등급 확률을 직접 높이지 않는다. 마이닝 파워는 PoM 누적 속도에만 영향을 준다.

이는 비트코인 채굴 구조와 유사하다. 더 많은 채굴 장비를 가진 참여자는 더 많은 채굴 기회를 얻지만, 채굴 규칙 자체를 바꿀 수는 없다. CryptoStone에서도 더 많은 STONE을 스테이킹한 참여자는 더 빠르게 PoM을 누적하지만, 더 좋은 보

석이 나올 확률을 임의로 높일 수는 없다.

20. 장기 참여 보정과 Flexible Cooldown

장기 참여자를 보상하기 위해 스테이킹 기간에 따른 Lock Multiplier를 적용할 수 있다.

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

Flexible Lock은 감가상각 소각이 없으나, 단기 유동성이 지나치게 빠르게 들어오고 나가는 것을 방지하기 위해 unstake 요청 후 7일의 cooldown 기간을 둔다.

장기 락업은 필수 조건이 아니라 선택 조건이다. 사용자는 감가상각이 없는 Flexible 방식을 선택할 수 있으며, 더 높은 Mining Power를 원하는 경우에만 일정 감가상각을 수반하는 장기 락업을 선택한다.

이 구조는 다음 균형을 추구한다.

선택 장점 비용

Flexible 자유로운 참여, 감가상각 없음 7일 반환 대기 90일 Lock 약간 높은 마이닝 파워 2.5% 감가상각 180일 Lock 중간 수준의 마이닝 파워 5% 감가상각 365일 Lock 가장 높은 마이닝 파워 10% 감가상각 락업 배수는 최대 1.25배로 제한된다. 이는 장기 참여자에게 합리적 보상을 제공하면서도 특정 대형참여자가 과도하게 유리한 위치를 갖지 않도록 하기 위한 설계다.

락업 기간 중에도 사용자의 PoM 값이 필요 임계값에 도달하면 Gem NFT를 claim할 수 있다. 즉, 락업은 STONE 반환

가능 시점을 제한하는 구조이지, Gem NFT claim 자체를 금지하는 구조가 아니다.

21. Proof of Mining, PoM의 누적

CryptoStone은 단순한 포인트 또는 크레딧 방식이 아니라, 비트코인의 Proof-of-Work 개념을 디지털보석 채굴 구조에 맞게 추상화한 Proof of Mining, PoM 모델을 사용한다.

PoM은 사용자가 특정 스톤 풀에 STONE을 스테이킹하고, 시간이 지남에 따라 누적한 채굴 작업량을 의미한다. PoM은

별도로 전송되거나 거래되는 토큰이 아니라, 사용자의 채굴 참여와 시간 경과를 컨트랙트가 기록하는 온체인 작업량 지표이다.

사용자 i 의 특정 스톤 풀 j 에 대한 PoM 값은 다음과 같이 시간에 따라 누적된다.

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

예를 들어 100,000 STONE을 Flexible 조건으로 Diamond Pool에 스테이킹한 사용자의 마이닝 파워는 다음과 같다.

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

해당 사용자가 100,000초 동안 대기했다면 누적되는 PoM 값은 다음과 같다.

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

사용자의 누적 PoM 값이 해당 풀의 필요 PoM 임계값 이상이 되면 Gem NFT를 claim할 수 있다.

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

Gem NFT가 claim되면 사용자의 해당 풀 PoM 값에서 필요한 임계값 R_j 가 차감된다.

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

이 구조는 사용자가 임계값을 초과하여 누적한 PoM을 불필요하게 소멸시키지 않는다. 예를 들어 필요한 PoM 임계값이

22,000,000,000이고, 사용자가 23,000,000,000 PoM을 보유한 상태에서 Gem NFT를 claim하면, claim 이후 1,000,000,000 PoM은 다음 채굴을 위한 잔여 PoM으로 유지된다.

PoM은 각 스톤 풀별로 독립적으로 누적된다. Diamond Pool에서 누적된 PoM은 Diamond NFT claim에만 사용될 수 있으며, Ruby Pool 또는 Sapphire Pool의 PoM으로 전환될 수 없다. 이 구조는 각 스톤 풀의 독립성, 희소성, 채굴

난이도를 보호한다.

사용자가 특정 풀에서 STONE을 unstake하더라도, 이미 누적된 PoM은 해당 풀에 기록된 상태로 유지될 수 있다. 다만 unstake 이후에는 해당 풀에서 사용자의 Mining Power가 0이 되므로 추가 PoM은 누적되지 않는다.

사용자가 다시 같

은 풀에 STONE을 스테이킹하면 기존 PoM에 이어서 새 PoM이 누적된다.

사용자가 같은 풀에 STONE을 추가로 스테이킹하는 경우, 기존 PoM은 유지되며 추가 스테이킹 이후의 Mining Power만 증가한다. 반대로 스테이킹 수량을 줄이는 경우, 기존 PoM은 유지되지만 이후 누적 속도는 감소한다.

PoM은 외부로 양도되거나 거래될 수 없으며, 다른 스톤 풀로 이전될 수 없다. 이는 PoM이 자산 자체가 아니라, 특정 풀에서 특정 사용자가 실제로 채굴 참여를 통해 축적한 작업량 지표이기 때문이다.

22. 필요 PoM 임계값

보석 1개를 채굴하기 위해 필요한 PoM 임계값은 Base Mining Unit, 스톤별 기본 채굴 주기, 풀 난이도, 희소성 배수에

의해 결정된다.

스톤 j의 기본 채굴 주기를 T_j , Base Mining Unit을 B, 풀 난이도를 D_j , 희소성 배수를 S_j 라고 할 때, 필요 PoM 임계

값 R_j 는 다음과 같이 정의된다.

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

CryptoStone의 기준값은 다음과 같다.

$$B = 100,000 \text{ STONE}$$
$$\text{Target Pool Power} = 40,000,000 \text{ Power}$$

예를 들어 Diamond Pool의 기본 채굴 주기가 220,000초이고, Pool Difficulty와 Scarcity Multiplier 가 모두 1x라면 다음과 같다.

$$R_{\text{Diamond}} = 100,000 \times 220,000 \times 1 \times 1$$

$$R_{\text{Diamond}} = 22,000,000,000 \text{ PoM}$$

사용자 i 의 마이닝 파워가 $P_{\{i,j\}}$ 일 때, 해당 사용자가 스톤 j 의 NFT 1개를 claim하기까지 필요한

예상 시간은 다음과 같

이 표현할 수 있다.

$$E[T_{\{i,j\}}] = R_j \div P_{\{i,j\}}$$

예를 들어 사용자가 Diamond Pool에 100,000 STONE을 Flexible 조건으로 스테이킹한 경우:

$$\begin{aligned} E[T_{\{i,\text{Diamond}\}}] &= 22,000,000,000 \div 100,000 \\ &= 220,000\text{초} \end{aligned}$$

$\approx 2.55\text{일}$

즉, 초기 조건에서 100,000 STONE을 스테이킹한 사용자는 약 2.55일마다 Diamond NFT 1개를 claim할 수 있다.

23. 풀 난이도의 조정

참여자 많아져 전체 마이닝 파워가 증가하면 보석이 지나치게 빠르게 채굴될 수 있다. 이를 방지하기 위해 각 풀은 전체마이닝 파워에 따라 난이도를 조정한다.

스톤 풀 j 의 전체 마이닝 파워를 P_j , Target Pool Power를 P_j^{*} , 풀 난이도를 D_j 라고 할 때 다음과 같이 계산한다.

$$D_j = \max(1, P_j \div P_j^{*})$$

CryptoStone의 기준값은 다음과 같다.

$$P_j^{*} = 40,000,000 \text{ Power}$$

예시는 다음과 같다.

Target Pool Power Total Pool Mining Power 계산 Pool Difficulty

$$\begin{aligned} 40,000,000 \quad 20,000,000 \quad 20,000,000 \div 40,000,000 &= \\ 0.5 \rightarrow \max(1, 0.5) \end{aligned}$$

1.0x

$$40,000,000 \quad 40,000,000 \quad 40,000,000 \div 40,000,000 =$$

1.0

1.0x

$$40,000,000 \times 80,000,000 \div 40,000,000 = 80,000,000$$

2.0

2.0x

$$40,000,000 \times 200,000,000 \div 40,000,000 = 200,000,000$$

5.0

5.0x

이 공식에서 $\max(1, \cdot)$ 구조를 적용하는 이유는, 전체 마이닝 파워가 Target Pool Power보다 낮을

때에도 난이도가

1.0x 미만으로 내려가지 않도록 하기 위함이다. 즉, 참여자가 적은 초기 구간에서도 채굴 속도가 기준보다 과도하게 빨라지는 것을 방지한다.

반대로 전체 마이닝 파워가 Target Pool Power를 초과하면 Pool Difficulty는 비례적으로 상승한다. 예를 들어 특정 풀의 전체 마이닝 파워가 80,000,000 Power로 증가하면 Pool Difficulty는 2.0x가 된다.

이 경우 동일한 사용자가 NFT 1 개를 채굴하는 데 필요한 시간도 약 2배로 증가한다.

스마트컨트랙트 구현에서는 소수점 연산을 피하기 위해 BPS 방식으로 표현할 수 있다.

$$D_{\{j, BPS\}} = \max(10,000, P_j \times 10,000 \div P_j^*)$$

여기서 10,000 BPS = 1.0x를 의미한다.

이 구조는 참여자가 증가할수록 전체 채굴 속도가 자연스럽게 조정되도록 하며, 각 스톤의 공급이 단기간에 과도하게 고갈되는 것을 방지한다.

24. 반감기와 희소성 배수

CryptoStone의 반감기는 전체 컬렉션 기준이 아니라 각 스톤별로 독립 적용된다.

스톤 j의 최대 발행량을 N_j , 현재까지 채굴된 수량을 n_j , 채굴 진행률을 q_j 라고 하면 다음과 같이 계산된다.

$$q_j = n_j \div N_j$$

예를 들어 Diamond의 최대 발행량이 110,000개이고 현재 55,000개가 채굴되었다면:

$$q_{\text{Diamond}} = 55,000 \div 110,000 = 0.5$$

즉, Diamond Pool은 50% 채굴 구간에 도달한 것이다.

스톤별 희소성 배수 S_j 는 채굴 진행률 q_j 에 따라 증가한다.

Mined Supply Ratio Remaining Supply Scarcity Multiplier 0% ~ 50% 100% ~ 50% 1x
 50% ~ 75% 50% ~ 25% 2x Mined Supply Ratio Remaining Supply Scarcity Multiplier
 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% 이상 3.125% 이하 32x 이를 수식으로 일반화하면
 다음과 같이 표현할 수 있다.

$$S_j(q_j) = 2^{\min(5, \text{floor}(\log_2(1 \div (1 - q_j))))}$$

단, q_j 가 초기 구간에 해당하는 경우 $S_j(q_j)$ 는 최소 1x로 유지된다. 실제 스마트컨트랙트에서는 위 수식을 직접 계산하기보다, 사전에 공개된 구간표를 기준으로 구현할 수 있다.

이 공식은 스톤별 잔여 공급량이 줄어들수록 채굴 난이도가 기하급수적으로 상승하는 구조를 표현한다.

이는 현실의 광산에서 매장량이 줄어들수록 채굴 비용과 난이도가 상승하는 구조를 디지털 환경으로 옮긴 것이다.

25. 채굴 속도와 공급 고갈의 비선형 구조

CryptoStone의 채굴 구조는 단순한 선형 민팅 모델이 아니다. 각 스톤은 독립적인 공급량, 채굴 주기, 풀난이도, 희소성배수를 가지며, 채굴 진행률이 높아질수록 희소성 배수에 의해 채굴 속도가 둔화된다.

스톤 풀 j의 유효 마이닝 파워를 $P_{\text{eff},j}$ 라고 하면 다음과 같이 표현할 수 있다.

$$P_{\text{eff},j} = \min(P_j, P_j^*)$$

이는 전체 마이닝 파워가 Target Pool Power보다 낮을 때는 실제 참여 파워가 채굴 속도에 영향을 주고, Target Pool Power를 초과하면 난이도 상승을 통해 유효 채굴 속도가 제한됨을 의미한다.

스톤 풀 j의 단위 시간당 예상 채굴량 λ_j 는 개념적으로 다음과 같이 표현할 수 있다.

$$\lambda_j = P_{\text{eff},j} \div (B \times T_j \times S_j)$$

여기서 B는 Base Mining Unit, T_j 는 스톤별 Base Mining Interval, S_j 는 Scarcity Multiplier이다.

특정 스톤이 채굴 진행률 q에 도달하는 데 필요한 시간은 다음과 같은 비선형 모델로 표현할 수 있다.

$$\text{Time}_j(q) = (N_j \times B \times T_j \div P_{\text{eff},j}) \times \int^q S_j(x) dx$$

이 수식은 CryptoStone의 채굴 구조가 선형적으로 고갈되는 모델이 아니라, 스톤의 잔여 공급량이 줄어들수록 점진적으로 느려지는 비선형 채굴 모델임을 보여준다.

따라서 초기 구간에서는 비교적 활발하게 Gem NFT가 채굴되지만, 90% 이후 구간에서는 Scarcity Multiplier가 상승하여 남은 공급량의 채굴 속도가 크게 둔화된다.

26. Weight 속성의 디지털화

무게는 모든 스톤이 공통적으로 CT, 즉 캐럿 단위를 사용한다. 그러나 각 보석의 무게 값은 랜덤으로 생성된다.

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

스마트컨트랙트에서는 소수점을 직접 저장하지 않고, 0.01 CT 단위의 정수로 저장한다.

표시 무게 컨트랙트 저장값

0.10 CT 10

1.25 CT 125

10.50 CT 1050

200.00 CT 20000

무게는 균등 확률로 생성되지 않는다. 현실 보석에서 큰 캐럿일수록 희귀한 것처럼, CryptoStone에서도 큰 무게일수록 낮은 확률로 생성된다.

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 속성의 디지털화

Color는 보석의 색상 등급을 표현한다. 등급이 높을수록 낮은 확률로 생성된다.

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 속성의 디지털화

Clarity는 보석의 투명도 등급을 표현한다.

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
S11	25.0%	4
S12	45.5%	1

29. Cut 속성의 디지털화

Cut은 보석의 커팅 등급을 표현한다.

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. 속성 생성과 랜덤 검증

보석의 속성은 운영자가 수동으로 입력하지 않는다. 채굴 시점에 마이닝 컨트랙트가 랜덤값을 기반으로 Weight, Color, Clarity, Cut을 결정한다.

중요한 점은 랜덤 생성 방식이 검증 가능해야 한다는 것이다. 만약 운영자가 임의로 높은 등급의 NFT를 생성할 수 있다면 CryptoStone의 탈중앙성과 희소성은 훼손된다.

따라서 CryptoStone의 랜덤 생성 방식은 다음 원칙을 따른다.

원칙 설명

사전 예측 불가 운영자와 사용자 모두 결과를 사전에 알 수 없어야 한다.

결과 선택 불가 운영자가 유리한 결과만 선택하거나 불리한 결과를 거부할 수 없어야 한다.

재시도 방지 랜덤 요청 이후 결과 확정 전 사용자가 claim을 취소하거나 재시도할 수 없어야 한다.

Admin Reroll 금지 운영자는 특정 결과를 재추첨하거나 대체할 수 없어야 한다.

공개 검증 결과 생성 과정은 온체인 또는 공개 검증 가능한 방식이어야 한다.

확률표 고정 속성 확률표는 배포 전 공개되고 finalize 이후 변경될 수 없어야 한다.

민팅 후 불변 민팅 이후 속성은 변경될 수 없어야 한다.

초기 구현에서는 검증 가능한 외부 VRF 구조를 우선 검토할 수 있다. 또는 Commit-then-Reveal 구조와 같은 방식으로 랜덤 요청 시점과 결과 확정 시점을 분리할 수 있다. 어떤 방식이 사용되더라도 사용자는 결과 확정 전 claim을 취소하거나 재시도할 수 없어야 하며, 운영자 역시 특정 결과를 선택하거나 재추첨할 수 없어야 한다.

랜덤 결과가 요청된 이후 사용자는 결과가 불리하다는 이유로 claim을 취소하거나 재시도할 수 없어야 한다. 운영자 또한 특정 사용자에게 유리한 결과를 배정하거나, 특정 속성 조합이 나오도록

seed를 선택할 수 없어야 한다. 이는 희귀 보석의 생성이 운영자의 재량이 아니라 검증 가능한 랜덤 구조에 의해 결정되도록 하기 위한 핵심 조건이다.

민팅 이후 Gem NFT의 핵심 속성은 freeze되어야 하며, Weight, Color, Clarity, Cut, stoneType, minedAt, minedFromPool과 같은 핵심 metadata는 운영자에 의해 변경될 수 없어야 한다.

초기에는 실무적으로 검증 가능한 랜덤 인프라를 사용하되, 장기적으로는 CryptoStone 네트워크 자체가 랜덤 생성과검증을 담당하는 구조로 진화할 수 있다.

31. Rarity Score와 Probability Rarity Index

CryptoStone은 각 보석의 희귀도를 수치화하기 위해 두 가지 지표를 사용한다.

지표 목적

Rarity Score 사용자가 직관적으로 이해할 수 있는 0~100 점수 Probability Rarity Index 실제 발생 확

률에 기반한 수학적 희귀도 지표 31.1 Rarity Score Rarity Score

= Stone Scarcity Score

+ Weight Score

+ Color Score

+ Clarity Score

+ Cut Score

점수 배분은 다음과 같다.

Stone Scarcity 20

Weight 25

Color 15

Clarity 20

Cut 20

Total 100

Stone Scarcity Score는 스톤별 총 발행량을 기준으로 계산된다.

Stone Scarcity Score

$$= 20 \times (\text{MaxCollectionSupply} - \text{StoneMaxSupply}) \\ \div (\text{MaxCollectionSupply} - \text{MinCollectionSupply})$$

기준값은 다음과 같다.

$$\text{MaxCollectionSupply} = 220,000 \\ \text{MinCollectionSupply} = 110,000$$

예를 들어 Diamond의 Max Supply는 110,000개이므로 가장 높은 Stone Scarcity Score를 가진다.

Zircon의 Max Supply는 220,000개이므로 가장 낮은 Stone Scarcity Score를 가진다.

31.2 Probability Rarity Index Rarity Score가 사용자 친화적 비교 지표라면, Probability Rarity Index

는 각 속성의 발생 확률을 기반으로 한 수학적희귀도 지표다.

Gem NFT g의 속성 조합이 발생할 확률 P(g)는 다음과 같이 정의된다.

$$P(g) = P_{\text{stone}} \times P_{\text{weight}} \times P_{\text{color}} \times P_{\text{clarity}} \times P_{\text{cut}}$$

이를 바탕으로 확률 기반 희귀도 지표를 산정한다.

$$\text{Probability Rarity Index} = -\log_{10}(P(g))$$

이 지표는 특정 Gem NFT가 확률적으로 얼마나 희귀한 조합인지 보여준다.

예를 들어 다음 조합은 극히 희귀하다.

Diamond

+ 100.00 CT 이상

+ D Color

+ FL Clarity

+ 6 Star Cut

이러한 조합은 Rarity Score상 높은 점수를 받을 뿐 아니라, Probability Rarity Index에서도 매우 높은

희귀도를 갖게된다.

CryptoStone은 이 두 지표를 함께 사용함으로써 수집자가 직관적으로 이해할 수 있는 점수 체계와 데이터 기반으로 검증 가능한 희귀도 체계를 동시에 제공한다.

32. 희귀도 티어 구조

완벽한 최상위 조합은 극도로 낮은 확률로만 생성될 수 있다. 이는 희소성 측면에서는 장점이지만, 수집시장에서는 다양한 상위 티어가 형성되어야 거래와 수집 활동이 더 활발해질 수 있다.

따라서 CryptoStone은 Rarity Score와 Probability Rarity Index를 기반으로 다음과 같은 희귀도 티어

를 적용할 수 있다.

Common 일반 속성 중심 가장 흔한 보석군

Rare 상위 속성 1개 이상 일반 희귀 보석

Epic 상위 속성 2개 이상 수집 가치가 높은 보석 Legendary 상위 속성 3개 이상 매우 희귀한 보석 Genesis 극단적 조합 또는 초기 채굴 고유성 최상위 수집 자산 Genesis Tier는 단순히 점수만으로 결정되지 않을 수 있다. 초기 채굴 시점, 낮은 tokenId, 극단적 확률 조합, 특정 스톤의 희소성 등이 복합적으로 고려될 수 있다.

이 구조는 포켓몬 카드, 스포츠 카드, 한정판 수집품 시장에서 희귀 등급이 수집 가치를 형성하는 방식과 유사하다. 다만 CryptoStone에서는 희귀도가 운영자의 주관적 판단이 아니라, 공개된 확률표와 온체인속성값에 의해 계산된다는 차이가 있다.

33. 수집 가치의 형성

수집 시장에서 희귀성은 중요한 가치 형성 요소다. 포켓몬 카드, 스포츠 카드, 한정판 피규어, 예술품, 고급 시계 등은 단순한 사용 가치만으로 가격이 형성되지 않는다. 특정 시리즈, 한정 수량, 희귀 등급, 보존상태, 시장의 수요, 커뮤니티의 인식이 결합되면서 가격이 형성된다.

CryptoStone은 이러한 수집 경제의 원리를 디지털 보석에 적용한다.

스톤별 총 발행량 Diamond, Ruby, Sapphire 등 스톤별 공급 차이 풀별 채굴 난이도 각 풀의 Target Power와 Difficulty 스톤별 반감기 채굴량 증가에 따른 Scarcity Multiplier 상승 Weight 확률 큰 캐럿일수록 낮은 확률요소 설명 Color 확률 높은 색상 등급일수록 낮은 확률 Clarity 확률 높은 투명도 등급일수록 낮은 확률 Cut 확률 높은 커팅 등급일수록 낮은 확률 낮은 tokenId 초기 채굴 보석의 수집성 채굴 시점 특정 시기, 특정 반감기 전후의 의미 온체인 거래 이력 소유권과 provenance 기록 이러한 구조는 사용자가 단순히 NFT 이미지를 구매하는 것이 아니라, 공개된 확률 구조 안에서 채굴된 고유한 디지털 보석을 수집하게 만든다.

CryptoStone에서 희귀성은 마케팅 문구가 아니다. 희귀성은 컨트랙트에 고정된 수량, 확률표, 채굴 난이도, 반감기 구조에 의해 형성된다.

34. 탈중앙 채굴 구조

CryptoStone에서 채굴은 서버가 대신 실행하는 방식이 아니다. 사용자는 자신이 원하는 스톤 풀에 STONE을 스테이킹하고, 시간이 지나 PoM 값이 해당 풀의 필요 임계값에 도달하면 직접 claimGem()과 같은 컨트랙트함수를 호출하여

Gem NFT를 수령한다.

단계 설명

- 1 유저가 STONE을 보유한다.
- 2 원하는 스톤 풀을 선택한다.
- 3 STONE을 스테이킹한다.
- 4 마이닝 파워가 발생한다.
- 5 시간이 지남에 따라 PoM 값이 누적된다.
- 6 PoM 값이 필요 임계값에 도달하면 claimGem()을 호출한다.
- 7 컨트랙트가 채굴 가능 여부를 검증한다.
- 8 검증 가능한 랜덤값으로 속성을 생성한다.
- 9 ERC-721 Gem NFT를 민팅한다.
- 10 NFT가 유저 지갑으로 전송된다.

이 과정에서 중앙 서버가 보석을 발행하거나 속성을 지정하지 않는다. 채굴 조건과 결과는 코드에 의해 결정된다.

스마트컨트랙트는 스스로 자동 실행되지 않는다. 그러나 누구나 컨트랙트를 호출할 수 있고, 컨트랙트는 사전에 정해진 조건에 따라 결과를 검증하고 실행한다. 따라서 CryptoStone의 채굴 구조는 중앙 서버 없이도 작동할 수 있다.

필자는 이 구조에서 중요한 점이 “서버가 없다”는 사실이 아니라, “서버가 없어도 사용자가 직접 컨트랙트를 호출하여 정해진 규칙에 따라 채굴 결과를 받을 수 있다”는 점이라고 본다.

35. 채굴 비용과 STONE 소각 구조

CryptoStone에서 STONE은 단순한 결제 수단이 아니라 디지털 보석 채굴에 참여하기 위한 마이닝 자원이다. 현실의 광산에서 채굴 장비와 에너지가 사용되고 시간이 지남에 따라 장비가 마모되는 것처럼, CryptoStone에서도 마이닝 풀에 투입된 STONE은 채굴 과정에서 일정한 디지털 감가상각 구조를 갖는다.

필자는 STONE의 소각 구조가 토큰 가격 상승을 보장하기 위한 장치가 아니라, 디지털 보석 채굴에 필요한 자원 소비와 희소성 구조를 표현하기 위한 장치라고 본다.

CryptoStone의 STONE 소각은 크게 두 가지 경우에 발생할 수 있다.

소각 유형 발생 시점 목적

Claim Burn Gem NFT를 claim하는 시점 채굴 비용과 희소성 표현 Maturity Burn 락업 종료 후 unstake 시점 마이닝 자원의 감가상각 표현 Gem NFT를 claim할 때 발생하는 소각량 $B_{\{claim,j\}}$ 은 다음 공식으로 계산된다.

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

여기서 β 는 Base Claim Burn이고, S_j 는 해당 스톤의 Scarcity Multiplier이다.

초기 기준값은 다음과 같이 설정한다.

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

Scarcity Multiplier Claim Burn 1x 20 STONE 2x 40 STONE 4x 80 STONE 8x 160 STONE 16x 320 STONE 32x 640 STONE Base Claim Burn은 채굴 비용을 표현하는 최소 소비 구조이며, 전체 공급량을 급격히 축소시키기 위한 장치가 아니다.

소각된 STONE은 운영자나 재단에 지급되지 않고 영구적으로 유통량에서 제거된다. 이를 통해 STONE은 단순히 예치되는 자산이 아니라, CryptoStone 생태계 안에서 실제로 사용되고 소비되는 디지털 마이닝 자원으로 기능한다.

36. 락업 감가상각 및 반환 구조

사용자가 락업 기간을 선택하여 마이닝 풀에 STONE을 투입한 경우, 락업 종료 후 unstake 시점에 락업기간에 따라 일부 STONE이 감가상각 소각되고 나머지 STONE이 반환된다.

Lock Type Lock Period Mining Multiplier Maturity Burn Returned STONE Cooldown
Flexible 없음 1.00x 0% 100% 7 days Short Lock 90일 1.05x 2.5% 97.5% 없음 Medium Lock 180일 1.12x 5% 95% 없음 Long Lock 365일 1.25x 10% 90% 없음
사용자 i 가 스테이킹한 STONE 수량을 s_i , 락업 기간에 따른 감가상각률을 δ_i 라고 할 때, 만기 시 소각되는 STONE 수량 M_i 는 다음과 같이 정의된다.

$$M_i = s_i \times \delta_i$$

반환되는 STONE 수량 R_i 는 다음과 같다.

$$R_i = s_i - M_i$$

이 구조는 장기 참여자에게 더 높은 마이닝 파워를 제공하면서도, 마이닝 자원의 사용에 따른 비용을 함께 반영한다. 즉, 사용자는 더 긴 락업을 선택하여 더 높은 채굴 속도를 얻을 수 있지만, 락업 종료 시 더 높은 감가상각 소각을 감수해야 한다.

장기 락업은 강제 조건이 아니다. 사용자는 STONE 소각 부담을 원하지 않을 경우 Flexible 방식을 선택할 수 있다. 장기락업은 더 높은 Mining Power를 원하는 참여자를 위한 선택형 구조이며, 감가상각은 그 선택에 수반되는 디지털 채굴자원의 사용 비용으로 해석된다.

필자는 이 구조가 단순한 패널티가 아니라 “디지털 채굴 장비의 사용에 따른 감가상각”으로 해석되어야 한다고 본다. 현실의 채굴 장비가 사용 기간에 따라 마모되듯이, CryptoStone에서 STONE은 마이닝 풀에 투입되는 동안 마이닝 파워를 제공하고, 그 사용 기간에 따라 일부가 소각된다.

37. 개발 구조의 선택

CryptoStone은 다음 구조를 채택한다.

STONE ERC-20

+ ERC-721 CryptoStone Gem NFT + 12개의 Mining Pool Contract + Pool Factory 이 구조는 단순히 기술 표준을 나열하기 위한 것이 아니라, CryptoStone이 구현하려는 속성과 기능을 충족하기 위한 설계다.

STONE ERC-20 하나의 마이닝 자원과 유동성 구조를 제공한다.

ERC-721 Gem NFT 각 보석의 고유성과 속성을 표현한다.

12 Mining Pools 스톤별 독립 광산 구조를 구현한다.

Pool Factory 동일한 검증된 템플릿으로 풀을 배포한다.

Unified NFT Contract 하나의 컬렉션 정체성과 거래 데이터를 집중시킨다.

Verifiable Randomness 운영자 조작 없는 속성 생성을 가능하게 한다.

Finalize Mechanism 핵심 규칙 변경을 방지한다.

첫째, STONE과 Gem NFT의 역할을 분리한다. STONE은 마이닝 파워를 위한 토큰이고, Gem NFT는 채굴 결과물이다.

둘째, 보석의 고유성을 보호한다. 각 Gem NFT는 tokenId와 속성 조합을 가지며, 민팅 이후 속성이 변경되지 않는다.

셋째, 스톤별 독립성을 유지한다. 각 마이닝 풀은 독립적인 공급량, 채굴 주기, 반감기를 가지므로 현실의 개별 광산 개념을 디지털로 표현하기에 적합하다.

넷째, NFT 컬렉션은 하나로 유지된다. 이는 CryptoStone의 브랜드와 시장 데이터를 하나로 집중시키며, 거래와 희귀도랭킹을 통합적으로 관리할 수 있게 한다.

다섯째, 향후 확장성이 높다. 초기에는 EVM 기반 스마트컨트랙트로 시작하되, 장기적으로 독립적인 Appchain 또는 Mainnet으로 확장할 수 있다.

여섯째, 중앙화 의존성을 줄인다. 채굴과 민팅은 서버가 아니라 컨트랙트에 의해 실행되며, 누구나 조건을 검증할 수 있다.

38. 프로토콜 고정 원칙

CryptoStone이 비트코인과 같은 탈중앙 자산성을 지향하기 위해서는 배포 이후 핵심 규칙이 임의로 변경되지 않아야 한다.

STONE 총 발행량 1,200,000,000 STONE STONE 유통 구조 100% 공개유통스톤별 Max Supply 각스톤별 최대 NFT 발행량스톤별 Base Mining Interval 기본 채굴 주기 Target Pool Power 초기 기준값 40,000,000 Power Base Mining Unit 100,000 STONE Weight 확률표 무게 생성 확률 Color 확률표 색상 등급 생성 확률 Clarity 확률표 투명도 등급 생성 확률 Cut 확률표 커팅 등급 생성 확률 Scarcity Multiplier 반감기 기반 난이도 배수 Claim Burn 공식 claim 시 조각 공식 Mining Power 공식 스테이킹 기반 마이닝 파워 공식 PoM 공식 Proof of Mining 누적 및 claim 조건

Lock Multiplier 락업 기간별 마이닝 배수 Maturity Burn 공식 락업 종료 시 감가상각 조각 공식 초기 설정이 완료되면 프로토콜은 finalize되어야 한다. 이후 운영자는 임의로 발행량을 늘리거나, 희귀도 확률을 바꾸거나, 특정 사용자에게 NFT를 수동으로 민팅할 수 없어야 한다.

CryptoStone의 핵심 컨트랙트는 배포 이후 소스코드가 공개 검증되어야 하며, 토큰 발행량, NFT 공급량, 확률표, 마이닝 공식, PoM 임계값 산정 구조는 finalize 이후 변경될 수 없어야 한다.

finalize 이전에 필요한 제한적 관리 기능이 존재한다면, 해당 기능의 목록, 목적, 제거 시점, 통제 방식은 명확히 공개되어야 한다. finalize 이후에는 핵심 발행량, 확률표, 민팅 권한, PoM 산정 방식과 관련된 관리자 권한이 제거되거나 비활성화되어야 한다.

탈중앙성은 단순히 블록체인 위에 배포되었다는 사실만으로 완성되지 않는다. 탈중앙성은 운영자가 바꿀수 없는 규칙, 누구나 검증 가능한 코드, 누구나 참여 가능한 구조에서 형성된다.

39. 보안 대응과 탈중앙성의 균형

CryptoStone은 No Admin Mint, No Central Server를 핵심 원칙으로 한다. 그러나 초기 개발 및 배포단계에서는 보안 감사, 테스트, 취약점 대응을 위한 제한적 관리 구조가 필요할 수 있다.

단계 관리 구조

테스트넷 및 감사 단계 제한적 관리 권한 가능

공식 배포 전 파라미터 검증 및 보안 점검

공식 론칭 후 핵심 민팅·공급·확률 변경 권한 제거

finalize 이후 No Admin Mint, No Supply Change, No Probability Change 비상 정지 기능이 존재할 경우, 이는 민팅 결과 조작이나 공급량 변경을 위한 기능이 아니라 보안 사고 방지를 위한 제한적 기능으로만 사용되어야 한다. 또한 비상 기능은 타임락 또는 다중 서명 구조 등 공개적으로 검증 가능한 방식으로 제한되어야 하며, 운영자가 임의로 희귀도나 발행량을 변경하는 수단이 되어서는 안 된다.

CryptoStone의 주요 컨트랙트는 토큰 컨트랙트, Gem NFT 컨트랙트, Mining Pool Template, Pool Factory, 랜덤생성 구조로 구성된다. 이들 컨트랙트는 배포 전후로 보안 감사를 거치는 것이 바람직하며, 감사 결과와 주요 취약점 대응 내역은 공개되어야 한다.

공개되어야 할 핵심 검증 요소는 다음과 같다.

Contract Source Verification 배포된 컨트랙트 소스코드 공개 및 검증 Audit Report 주요 컨트랙트와 랜덤 구조에 대한 감사 보고서 Admin Function List 관리자 함수의 존재 여부와 제거 계획 Finalize Event 핵심 파라미터 고정 시점과 이벤트 기록 검증 항목 설명 LP Lock / Burn Proof 초기 유동성 관련 LP 처리 내역 Probability Table Hash 확률표가 배포 전 공개된 값과 일치하는지 확인 Metadata Freeze 민팅 후 핵심 속성 변경 불가 여부가 구조는 실무적 보안 대응과 탈중앙 자산성 사이의 균형을 맞추기 위한 것이다.

40. 이미지와 메타데이터의 위치

CryptoStone은 시각적 표현을 부정하지 않는다. 보석 NFT는 사용자의 경험과 수집 편의성을 위해 이미지, 3D 모델, 시각적 카드 형태로 표현될 수 있다.

그러나 이미지는 CryptoStone의 본질이 아니다.

CryptoStone의 본질은 다음 데이터에 있다.

stoneType 보석 종류

weight 무게

colorGrade 색상 등급

clarityGrade 투명도 등급

cutGrade 컷팅 등급

rarityScore 사용자 친화적 희귀도 점수

probabilityRarityIndex 확률 기반 희귀도 지표 minedAt 채굴 시점 minedFromPool 채굴된 마이닝 풀 tokenId NFT 고유 식별자따라서 이미지 서버가 일시적으로 중단되더라도 CryptoStone NFT의 핵심 속성은 온체인에 남아 있어야 한다. 이는 기존 NFT가 외부 이미지나 중앙 서버에 과도하게 의존하는 문제를 보완하기 위한 설계다.

41. 생태계 확장 모듈과 Gem Refinement

CryptoStone의 핵심 프로토콜은 STONE, 12개의 스톤별 마이닝 풀, Proof of Mining, 그리고 ERC-721 기반 Gem NFT로 구성된다. 다만 CryptoStone 생태계는 핵심 채굴 구조에만 한정되지 않으며, 향후 별도의 스마트컨트랙트를 추가하거나 기존 컨트랙트와 연동되는 확장 모듈을 통해 다양한 활용 기능으로 확장될 수 있다. 이러한 확장 기능에는 Marketplace, Arena Game, Ranking System, Collection Quest, Gem Refinement 등이 포함될 수 있다.

Gem Refinement, 즉 보석 제련은 이러한 생태계 확장 모듈의 하나로서, 채굴된 Gem NFT를 다시 활용할 수 있도록 설계된 선택형 사후 유틸리티 구조이다. Gem Refinement는 추가적인 무제한 NFT 발행 구조가 아니라, 동일한 stoneType을 가진 Gem NFT 2개를 결합하여 동일한 stoneType의 Refined Gem NFT 1개를 생성하는 공급 압축 메커니즘이다.

Gem NFT 2개
+ 소량의 STONE 사용 또는 소각
→ Parent Gem NFTs Burned
→ Refined Gem NFT 1개 Minted

제련이 1회 실행될 때마다 부모 Gem NFT 2개는 소각되거나 회수 불가능한 방식으로 처리되고, 새로운 Refined Gem NFT 1개만 생성된다. 따라서 전체 유통 NFT 수량은 1개 감소한다.

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

초기 Gem Refinement는 동일 스톤 기반 제련만 허용하는 것이 바람직하다. 예를 들어 Diamond Gem NFT 2개는 Refined Diamond Gem NFT 1개로, Ruby Gem NFT 2개는 Refined Ruby Gem NFT 1개로 제련될 수 있다. 서로 다른 스톤 간 제련은 스톤별 공급량, 희소성, 반감기, 채굴 난이도 구조를 복잡하게 만들 수 있으므로 초기 모델에서는 제외하는 것이 적절하다.

항목	원칙
필요 재료	동일한 stoneType의 Gem NFT 2개
추가 비용	소량의 STONE 사용 또는 소각
부모 NFT 처리	부모 Gem NFT 2개 소각 또는 회수 불가능 처리
결과물	동일한 stoneType의 Refined Gem NFT 1개
세대 정보	Gen1 또는 Refined Generation으로 기록
공급 효과	전체 유통 NFT 수량 감소
민팅 권한	Refining Contract에 한정
Admin Mint	없음
랜덤성	검증 가능한 랜덤 구조 사용

Refined Gem NFT의 기준 등급은 두 부모 Gem NFT 중 더 높은 등급을 기준으로 산정할 수 있다.

$$T_{base} = \max(T_1, T_2)$$

여기서 T_1, T_2 는 두 부모 Gem NFT의 등급이며, T_{base} 는 제련 결과 산정의 기준 등급이다.

Tier Level	Tier
1	Common
2	Rare
3	Epic
4	Legendary

제련 결과는 기준 등급과 동일한 등급이 나올 확률을 가장 높게 설정한다. 한 단계 낮은 등급이 나올 확률은 매우 낮게 두며, 상향 결과가 발생하더라도 최대 1~2단계 상승으로 제한한다. 또한 낮은 등급일수록 상향 가능성을 상대적으로 높게 두고, 높은 등급일수록 상향 가능성을 낮게 설정함으로써 고등급 Gem NFT의 희소성을 보호한다.

$$U \in [0, 9,999]$$

$$10,000 \text{ BPS} = 100\%$$

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

위 구조에서 Common과 Rare는 제련을 통한 상향 가능성이 상대적으로 높지만, Epic부터는 상향 확률이 크게 낮아진다. Legendary는 제련 모델의 최상위 등급으로 취급되며, 추가 상향은 허용하지 않는다. 이 구조는 제련의 기대감을 유지하면서도, 고등급 NFT가 과도하게 생성되는 것을 방지하기 위한 것이다.

두 부모 Gem NFT 간 등급 차이가 클 경우, 상향 확률은 추가로 조정될 수 있다. 등급 차이 G는 다음과 같이 정의한다.

$$G = |T_1 - T_2|$$

Tier Gap G	Upgrade Modifier	처리 원칙
0	100%	동일 등급 제련. 기본 확률 적용
1	70%	인접 등급 제련. 상향 확률 일부 감소
2	35%	큰 등급 차이. 상향 확률 크게 감소
3 이상	제한	초기 모델에서는 제련 제한 가능

상향 확률은 다음과 같이 조정할 수 있다.

$$\begin{aligned} &\text{Adjusted Upgrade Probability} \\ &= \text{Base Upgrade Probability} \times \text{Upgrade Modifier} \end{aligned}$$

조정으로 감소한 상향 확률은 동일 등급 유지 확률에 더해진다. 이를 통해 높은 등급 Gem NFT 1개에 낮은 등급 Gem NFT를 반복적으로 결합하여 상위 등급 생성을 시도하는 행위를 제한할 수 있다.

Refining Contract는 소유권 검증, 동일 스톤 검증, 등급 차이 검증, STONE 사용 또는 소각, 부모 NFT 소각, 랜덤값 요청, Refined Gem NFT 발행 요청을 수행한다. Refined Gem NFT는 운영자의 임의 발행으로 생성되어서는 안 되며, 오직 Refining Contract가 사전에 정의된 조건을 검증한 경우에만 생성되어야 한다.

Gem Refinement는 CryptoStone의 기본 채굴 구조를 대체하는 기능이 아니다. 이는 채굴 이후 Gem NFT의 활용성, 수집성, 거래 수요, 게임 활용성을 확장하기 위한 선택형 모듈이다. 향후 CryptoStone은 Gem Refinement 외에도 Marketplace, Arena Game, Ranking System, Collection Quest 등 다양한 확장 모듈을 통해 디지털 보석 생태계를 점진적으로 확장해 나갈 수 있다.

42. 홈페이지, 시뮬레이터 및 익스플로러의 필요성

CryptoStone의 프로토콜 자체는 스마트컨트랙트와 온체인 데이터에 의해 작동하지만, 사용자가 이를 직관적으로 이해하고 참여하기 위해서는 별도의 사용자 인터페이스가 필요하다.

따라서 CryptoStone 생태계에는 다음과 같은 웹 기반 도구가 필요할 수 있다.

도구	역할
Mining Simulator	사용자가 보유한 STONE 수량, 선택한 풀, 락업 기간에 따라 예상 채굴 시간을 계산한다.
PoM Dashboard	사용자의 풀별 PoM 값, 필요 PoM 임계값, claim 가능 여부를 표시한다.
Pool Dashboard	각 스톤 풀의 채굴량, 잔여 수량, Pool Difficulty, Scarcity Multiplier를 표시한다.
Gem Explorer	채굴된 Gem NFT의 속성, 희귀도, tokenId, 채굴 시점, 거래 이력을 조회한다.
Rarity Explorer	Weight, Color, Clarity, Cut 조합별 희귀도와 Probability Rarity Index를 확인한다.
Protocol Status Page	100% 공개유통, No Admin Mint, 총 발행량, 확률표, 풀 상태 등 핵심 프로토콜 정보를 검증 가능하게 보여준다.

이러한 도구들은 프로토콜의 필수 신뢰 기반을 대체하는 것이 아니라, 사용자가 온체인 데이터를 쉽게 이해할 수 있도록 도와주는 인터페이스 역할을 한다. 즉, CryptoStone의 본질은 컨트랙트와 온체인 규칙에 있으며, 홈페이지와 익스플로러는 이를 해석하고 시각화하는 수단이다.

43. 향후 추진 방향

CryptoStone은 초기에는 EVM 호환 네트워크 위에서 ERC-20, ERC-721, Mining Pool Contract 구조로 시작하는 것이 바람직하다. 이 단계에서는 프로토콜의 핵심인 스테이킹, 마이닝 파워 계산, PoM 누적, 스톤별 반감기, 보석 속성 생성, Gem NFT 민팅 구조를 검증하는 데 집중해야 한다.

이후에는 사용자가 쉽게 참여할 수 있도록 마이닝 대시보드, Mining Simulator, PoM Dashboard, Gem Explorer,

Rarity Explorer, 스톤별 거래 데이터, NFT 마켓플레이스 기능을 확장할 필요가 있다.

CryptoStone의 가치는 수집 시장의 이해와 데이터 투명성에서 발생하므로, 각 보석의 희귀도, 거래 이력, 스톤별 바닥가, 고등급 보석 랭킹을 누구나 확인할 수 있는 데이터 레이어가 중요하다.

생태계가 성장하면 CryptoStone은 단순한 스마트컨트랙트 프로젝트를 넘어 전용 Appchain 또는 Rollup으로 확장될 수 있다. 이 경우 STONE은 단순한 마이닝 토큰을 넘어 네트워크의 가스 토큰 또는 네이티브 자산으로 기능할 수 있으며, Gem NFT는 CryptoStone 네트워크의 기본 디지털 자산으로 자리잡을 수 있다.

장기적으로는 독립적인 CryptoStone Mainnet으로 발전하는 것도 고려할 수 있다. 이 경우 자체 검증자, 오픈소스 노드, 네이티브 마이닝 모듈, 온체인 랜덤 모듈, 자체 마켓플레이스, 공개적인 프로토콜 개선절차가 필요하다. 다만 메인넷은 단순히 기술적으로 체인을 만드는 것이 아니라, 충분한 사용자, 유동성, 검증자, 개발자 생태계가 형성된 이후에 추진되어야 한다.

CryptoStone의 장기 방향성은 하나의 NFT 컬렉션을 운영하는 것이 아니라, 디지털 보석이라는 새로운 온체인 자산 카테고리를 형성하는 데 있다.

44. 법률 및 투자성 유의사항

CryptoStone은 실제 보석의 소유권, 교환권, 담보권을 제공하지 않는다. CryptoStone Gem NFT는 현실 보석에 대한 청구권이 아니라, 온체인에서 채굴된 디지털 보석 자산이다.

CryptoStone의 스테이킹 및 락업 구조는 고정 수익, 이자, 배당, 투자 수익을 제공하기 위한 구조가 아니다. STONE을마이닝 풀에 투입하는 행위는 Gem NFT 채굴 기회를 획득하기 위한 프로토콜 참여 행위이며, 특정 수익률이나 시장 가격 상승을 보장하지 않는다.

STONE 보유 또는 스테이킹은 특정 수익, 배당, 이자, 가격 상승, NFT 판매 수익을 보장하지 않는다.

Gem NFT는 수집형 디지털 자산이며, 그 시장 가치는 외부 시장 참여자들의 주관적 평가와 수요에 따라 달라질 수 있다.

PoM은 별도의 투자 자산, 채권, 수익권, 포인트, 거래 가능한 토큰이 아니다. PoM은 특정 스톤 풀에서 사용자가 채굴 작업량을 누적했는지를 나타내는 프로토콜 내부 지표이며, 풀 간 전환되거나 외부로 양도될 수 없다.

또한 CryptoStone은 특정 수익률, 가격 상승, 원금 보장, 시장 유동성을 약속하지 않는다.

CryptoStone의 가치는 시장참여자들의 수집 수요, 희귀성에 대한 인식, 거래 활성화, 생태계 확장성에 따라 형성될 수

있다.

본 백서에서 제시된 수치와 공식은 탈중앙 디지털 보석이라는 개념을 구현하기 위한 초기 설계값이다. 이는 현실 보석 시장의 모든 경제적·문화적·감정학적 요소를 완벽히 표현한 것이 아니며, 생태계의 완전한 경제 모델이라고 단정할 수 없다.

스마트컨트랙트 취약점 코드 오류 또는 해킹 가능성

랜덤 생성 리스크 랜덤 인프라 의존성 또는 구현상 오류 NFT 시장 수요 부족 수집 수요가 충분하지 않을 가능성 STONE 유동성 부족 거래소 및 DEX 유동성 부족 가능성 규제 환경 변화 국가별 디지털 자산 규제 변화 메인넷 확장 실패 장기 로드맵이 실현되지 않을 가능성 희귀성 평가 불확실성 시장이 희귀성을 다르게 평가할 가능성 초기 파라미터 리스크 수치가 실제 시장 수요와 다르게 작동할 가능성 소각 부담 Claim Burn과 Maturity Burn이 참여자 부담으로 작용할 가능성 공개 유통 초기 변동성 100% 공개 유통 구조에서 초기 시장 가격 변동성이 클 가능성 LP 구조 리스크 초기 유동성 공급 및 LP 처리 방식에 대한 신뢰문제가 발생할 가능성 따라서 CryptoStone은 기술적, 경제적, 법률적 검토를 거쳐 신중하게 구현되어야 한다.

45. 프로젝트의 의의

CryptoStone의 의의는 세 가지로 정리할 수 있다.

첫째, CryptoStone은 NFT의 개념을 외부 콘텐츠의 소유권에서 벗어나, NFT 자체가 속성 기반 자산이 될 수 있음을 제안한다. 기존 NFT가 이미지나 플랫폼에 종속되는 경우가 많았다면,

CryptoStone은 보석의 속성을 온체인 데이터로 직접 보유함으로써 NFT 자체의 자산성을 강화하고자 한다.

둘째, CryptoStone은 보석의 희소성과 등급 구조를 디지털 환경으로 옮긴다. 현실의 보석은 무게, 색상, 투명도, 컷팅에 따라 가치가 달라진다. CryptoStone은 이를 확률표, 채굴 난이도, 반감기, 공급량 제한으로 구현한다.

셋째, CryptoStone은 탈중앙 채굴의 개념을 비트코인 이후의 새로운 자산 영역으로 확장한다. 비트코인이 금의 희소성을 디지털화했다면, CryptoStone은 보석의 희소성과 수집성을 디지털화한다.

CryptoStone은 현실 보석을 대체한다고 주장하지 않는다. CryptoStone은 보석이라는 자산 개념을 디지털 환경에서 새롭게 해석하는 프로젝트다.

필자는 이와 같은 시도가 향후 블록체인 기술이 단순한 금융 거래를 넘어, 현실 세계의 추상적 가치와 속성 기반 자산을 디지털 환경에서 표현하는 데 기여할 수 있다고 본다.

46. 결론

CryptoStone은 디지털 보석이라는 새로운 자산 개념을 제안한다.

비트코인이 현실의 금을 직접 보관하지 않고도 디지털 금이라는 개념을 만들어냈듯이, CryptoStone은 현실 보석의 소유권을 담보하지 않으면서도 보석의 핵심 속성인 희소성, 채굴성, 등급성, 수집성을 디지털

환경에서 구현하고자 한다.

CryptoStone의 구조는 다음과 같이 요약된다.

단일 토큰 STONE ERC-20

초기 발행량 1,200,000,000 STONE

유통 구조 100% 공개유통

접근 방식 공개 DEX 유동성을 통한 시장 접근

NFT 구조 하나의 ERC-721 Gem NFT 컨트랙트마이닝 풀 12개의 독립 보석 마이닝 풀풀 구현 동일한 Pool Template + Factory 구조 Base Mining Unit 100,000 STONE Target Pool Power 40,000,000 Power 12개 풀 전체 Target Power 480,000,000 Power PoM 구조 Proof of Mining 기반 누적 작업량 모델

Claim 조건 풀별 $PoM \geq \text{Required PoM Threshold}$
Claim Burn 20 STONE \times Scarcity Multiplier

Lock Model Flexible, 90일, 180일, 365일감가상각 락업 기간에 따른 Maturity Burn 희귀도 Rarity

Score + Probability Rarity Index 반감기 스톤별 Scarcity Multiplier 랜덤성 초기 VRF 또는

Commit-then-Reveal, 장기 네이티브 랜덤 모듈해시파워 대응 개념 STONE 기반 Mining Power 탈중앙성 No Admin Mint, No Central Server, finalize 구조핵심 구조 내용공개 검증 소스코드 공개, 감사보고서, LP 처리 내역, 확률표 검증사용자 도구 Mining Simulator, PoM Dashboard, Gem Explorer, Rarity

Explorer

장기 방향 Appchain 또는 Mainnet 확장 가능성필자는 CryptoStone의 목표가 단기적인 NFT 판매에있지 않다고 본다. CryptoStone의 목표는 디지털 환경에서 보석이라는 자산 개념이 어떻게 탈중앙적으로 구현될 수 있는지를 증명하는 것이다.

CryptoStone의 신뢰는 창립자의 권위, 내부 배정, 중앙 운영 권한이 아니라, 고정된 발행량, 100% 공개유통 구조, 검증가능한 PoM 모델, 변경 불가능한 확률표, 공개 검증 가능한 컨트랙트, 그리고 누구나확인 가능한 온체인 데이터에서 형성된다.

비트코인이 디지털 금이라면,

CryptoStone은 탈중앙 디지털 보석이다.