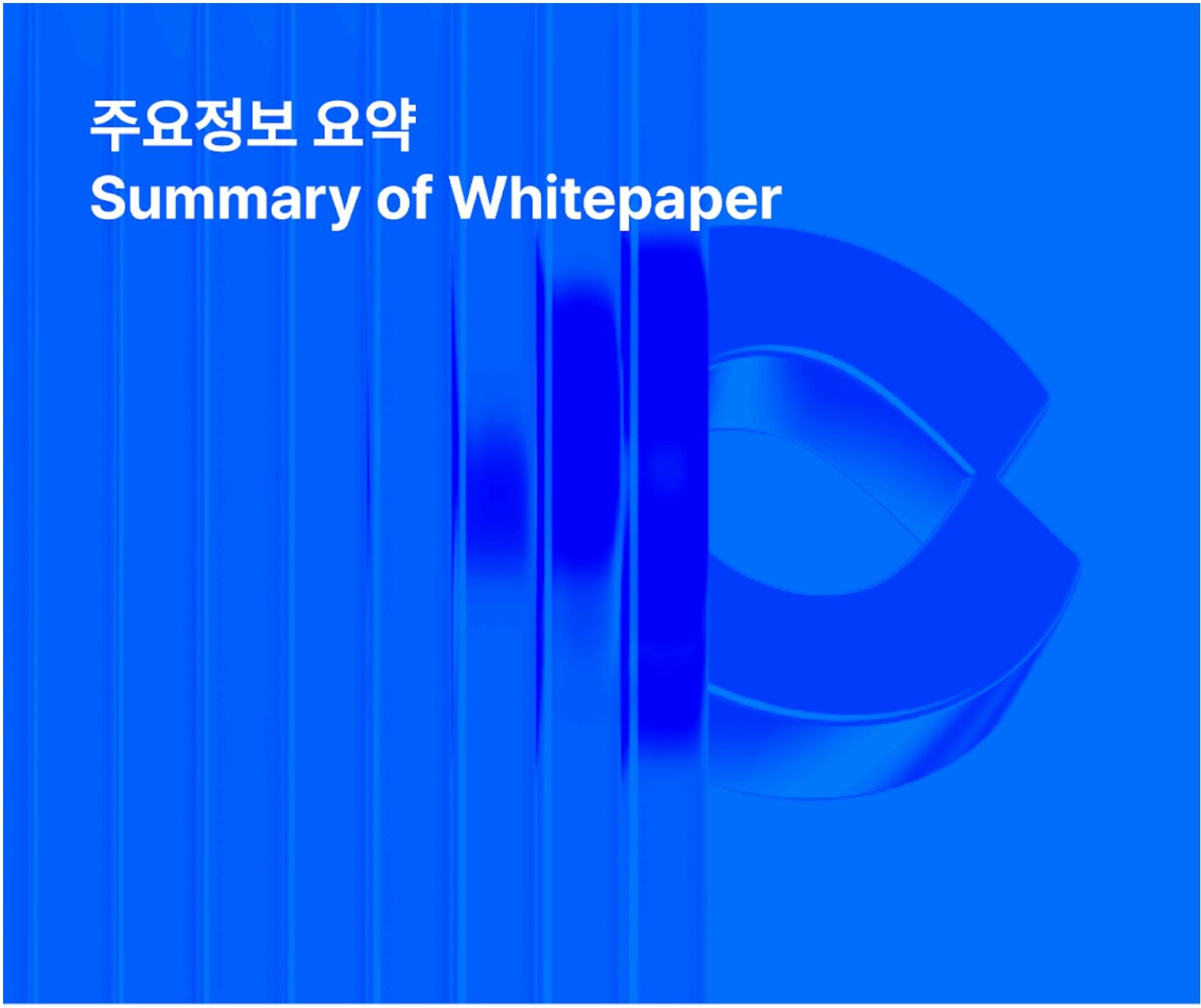
주요정보 요약
Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.
코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

coinone

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	BNB Smart Chain
홈페이지	https://www.bnbchain.org/en
참고문헌 (백서, Docs 등)	https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md

1. 프로젝트 정보

프로젝트 개요

2019년 4월 커뮤니티 기반 메인넷 출시에 이어, '비콘체인' 은 고속 및 대용량 처리 설계를 보여주었습니다. 비콘체인의 주요 초점은 네이티브이면서 저지연, 고성능의 탈중앙화 거래소(DEX)를 지원하는 데에 있었습니다. 가장 많이 요청된 기능 중 하나는 프로그래머블 확장성으로, 특히 스마트 계약 및 가상 머신 기능의 구현이었습니다. 이 수요를 해결하기 위해 우리는 비콘체인과 병렬로 실행되는 'BNB 스마트 체인' 을 제안하며, 사용자 친화적인 스마트 계약 환경을 제공하고자 합니다.

BNB 스마트 체인(BSC)은 BNB 체인 생태계에 프로그래머블성과 상호운용성을 제공하기 위해 설계된 EVM(Ethereum Virtual Machine) 호환 블록체인입니다. BNB 체인의 일환으로서 BSC는 탈중앙화 애플리케이션(dApp)과 디지털 자산을 위한 고처리량, 저지연, 저비용 환경을 제공하는 것을 목표로 합니다. 이 백서는 BSC의 아키텍처, 메커니즘, 진화 과정을 설명합니다. 몇 년이 지난 문서이지만, 여전히 유용한 참고 자료이며 BNB 스마트 체인을 정확히 반영하기 때문에 유지됩니다.

BNB 체인의 진화

- **초기 출시 및 비콘체인**
  2019년 4월에 출시된 비콘체인은 BNB DEX를 지원하기 위해 설계되었으며, 고속 및 대용량 처리 기능을 갖추고 있었습니다. 그러나 스마트 계약 기능이 없고 프로그래밍이 불가능하다는 점에서 개발자와 사용자에게는 한계가 있었습니다.

- **BNB 스마트 체인의 도입**
  이러한 한계를 해결하기 위해 2020년에 BNB 스마트 체인이 도입되었습니다. 스마트 계약을 지원하는 병렬 블록체인 아키텍처를 활용하면서도 DEX의 고성능 특성을 유지하였습니다.

- **BNB 체인 통합**
  2023년 11월, BNB 체인 통합 제안서(BEP-333)는 중요한 전환점을 맞이했습니다. 이 제안은 비콘체인의 기능을 종료하고 BSC와 통합하여 단일의 고성능 블록체인 네트워크를 구성하는 내용을 담고 있습니다. 이 통합은 운영을 간소화하고, 보안을 강화하며, BSC에서의 사용자 경험을 단순화하는 것을 목표로 했습니다.

- **opBNB**
  2023년에 출시된 opBNB는 Optimism OP 스택 기반의 Ethereum Virtual Machine(EVM) 호환 Layer 2 체인입니다. 낮은 가스비를 제공하며 블록체인 기술에 대한 접근성을 민주화함으로써 블록체인 산업의 혁신을 목표로 합니다.

- **BNB Greenfield**
  Greenfield는 BNB 스마트 체인(BSC)과 네이티브 브릿지로 연결된 새로운 형태의 탈중앙화 데이터 저장 네트워크입니다. 이 네트워크는 사용자 권한 관리, 버킷 생성,

파일 삭제 등을 처리하여 사용자가 데이터와 상호작용하는 방식을 혁신합니다.

BNB 체인은 지속적으로 진화하는 생태계이며, BSC가 그 핵심에 있습니다. 금융 시스템의 핵심으로서 BSC는 가장 많은 암호화폐 자산 가치를 보유하고 있으며, opBNB 및 기타 Layer 2 솔루션을 위한 정산 및 데이터 가용성 레이어로 기능하여 Layer 2의 보안을 보장합니다. 또한 BSC는 Greenfield의 스마트 계약 프로그래밍 플랫폼으로서 데이터 교환 및 순환을 촉진합니다.

BSC는 초기 이중 체인 아키텍처에서 상당한 발전을 이루었습니다. 초기에는 스테이킹, 검증, 거버넌스가 비콘체인에 위임되었으나, BC 통합 이후 BSC는 완전한 독립 체인으로 전환되었고 상당한 아키텍처 변화를 겪었습니다.

설계 원칙

다음은 BSC의 설계 원칙입니다:

- 독립형 블록체인: 기술적으로, BSC는 Layer 2 솔루션이 아닌 독립형 블록체인입니다. 대부분의 BSC 기술 및 비즈니스 기능은 자체적으로 독립되어야 하며, 비콘체인이 일시적으로 멈추더라도 BSC는 잘 작동할 수 있어야 합니다.

- 이더리움 호환성: 최초로 실용적이고 널리 사용된 스마트 계약 플랫폼은 이더리움입니다. 비교적 성숙한 애플리케이션 및 커뮤니티의 이점을 활용하기 위해, BSC는 기존 이더리움 메인넷과 호환되도록 선택하였습니다. 이는 대부분의 dApp, 생태계 구성 요소 및 툴이 BSC에서도 작동하며, 거의 또는 전혀 변경이 필요 없다는 것을 의미합니다. BSC 노드는 비슷하거나 약간 높은 수준의 하드웨어 사양 및 운영 기술이 필요합니다. 구현은 이더리움의 향후 업그레이드를 따라갈 수 있는 여지를 남겨두어야 합니다.

- 스테이킹 기반 합의 및 거버넌스: 스테이킹 기반 합의는 환경친화적이며 커뮤니티 거버넌스를 위한 유연한 선택지를 제공합니다. 이러한 합의는 작업 증명(Proof-of-Work) 블록체인 시스템보다 더 나은 네트워크 성능(즉, 더 빠른 블록 생성 시간과 더 높은 트랜잭션 처리량)을 가능하게 해야 합니다.

- 빠른 블록 생성 및 빠른 최종성: BSC는 빠른 최종성 메커니즘을 구현하여 정상적인 상황에서는 두 개의 블록 확인만으로 블록이 확정되도록 합니다. 이 기능은 BSC의 3초 블록 시간과 결합되어 거의 즉각적인 트랜잭션 확정성과 우수한 사용자 경험을 제공합니다.

토큰 이코노미

BSC, opBNB, 그리고 Greenfield는 BNB를 중심으로 하는 동일한 토큰 생태계를 공유합니다. 이는 다음과 같은 원칙을 따릅니다:

- BNB는 모든 네트워크에서 유통 가능하며, 크로스체인 통신 메커니즘을 통해 이동할 수 있습니다.
- BNB의 총 유통량은 세 네트워크 전체에서 통합적으로 관리되어야 하며, 각 네트워크의 유효 유통량 합계가 전체 공급량이 됩니다.

네이티브 토큰

BNB는 BSC에서 이더리움의 ETH처럼 작동하며, BSC의 **"네이티브 토큰"**으로 유지됩니다. 즉, BNB는 다음 용도로 사용됩니다:

- BSC에서 스마트 계약을 배포하기 위한 수수료 지불
- 선택된 BSC 검증자에 대한 스테이킹 및 그에 따른 보상 수령
- BSC, opBNB, Greenfield 간 토큰 자산의 크로스체인 이동

시드 펀드
제네시스 단계에서 일정량의 BNB가 비콘체인에서 소각되고 BSC에서 발행됩니다. 이 양은 **"시드 펀드(Seed Fund)"**라 불리며, 제네시스 이후 BSC에서 순환됩니다. 이는 제네시스 단계에서 도입된 초기 검증자 세트에 분배됩니다.

실시간 소각
BNB의 소각 속도를 높이고 BSC의 탈중앙화를 촉진하기 위해, 일부 가스비가 각 블록마다 소각됩니다. 검증자가 수집하는 가스비 중 고정된 비율이 소각되며, 이 비율은 BSC 검증자들에 의해 거버넌스 방식으로 조정될 수 있습니다.

합의 및 검증자 구조

앞서 제시한 설계 원칙을 바탕으로, BSC의 합의 프로토콜은 다음 목표를 충족해야 합니다:

- 블록 생성 시간은 이더리움 네트워크보다 짧아야 하며, 예: 3초
- 트랜잭션 확정성은 짧은 시간 안에 보장되어야 하며, 예: 10초 이하
- 네이티브 토큰인 BNB에 대한 인플레이션은 없어야 하며, 블록 보상은 트랜잭션 수수료에서 충당되어야 합니다
- 이더리움 시스템과 최대한 호환되어야 합니다
- 현대적인 지분 증명 기반 블록체인 거버넌스를 허용해야 합니다

지분 기반 권한 증명

작업 증명(PoW)은 분산 네트워크를 구현하는 실용적인 메커니즘으로 인정받고 있으나, 환경에 좋지 않으며 보안을 유지하려면 많은 수의 참가자가 필요합니다.

이더리움과 MATIC Bor, TOMOChain, GoChain, xDAI 등의 블록체인은 다양한 시나리오(테스트넷 또는 메인넷)에서 권한 증명(PoA) 또는 그 변형을 사용합니다. PoA는 51% 공격에 대한 일부 방어를 제공하며, 효율성과 일부 비잔틴 노드(악의적이거나 해킹된 노드)에 대한 내성을 개선합니다.

그러나 PoA 프로토콜은 완전한 탈중앙화가 부족하다는 비판을 받습니다. 블록을 생성하는 검증자 노드들이 모든 권한을 갖고 있으며, 부패나 보안 공격에 취약하기 때문입니다. EOS, Lisk 등의 블록체인은 토큰 보유자가 투표로 검증자를 선출할 수 있는 다양한 형태의 위임 지분 증명(DPoS)을 도입하여 이러한 단점을 보완합니다. 이는 탈중앙화를 높이고 커뮤니티 기반 거버넌스를 촉진합니다.

BSC는 DPoS와 PoA를 결합한 합의를 제안합니다:

- 블록은 제한된 수의 검증자에 의해 생성됩니다
- 검증자들은 PoA 방식(Ethereum의 Clique 합의와 유사)으로 순서대로 블록을 생성합니다
- 검증자 세트는 스테이킹 기반의 거버넌스를 통해 선출됩니다
- 네트워크 처리량을 높이기 위해, 검증자는 정해진 조건 내에서 연속적으로 블록을 생성할 수 있습니다

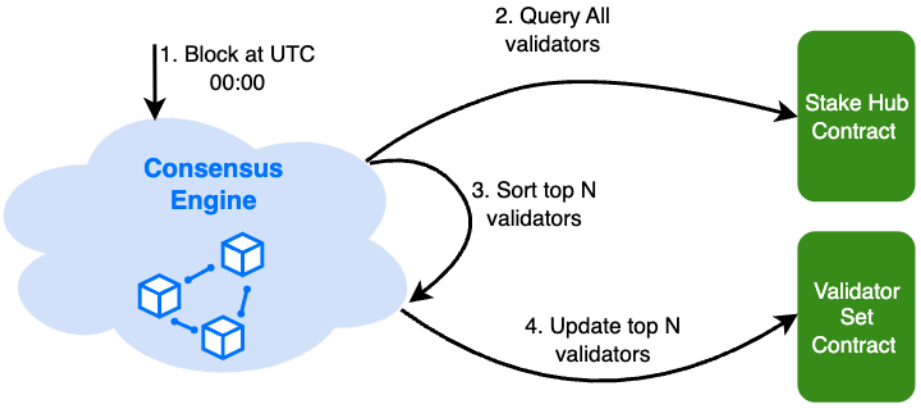
검증자 세트
검증자 세트는 BSC에서 트랜잭션을 검증하고 블록을 생성하는 책임을 지는 노드 그룹입니다. 검증자 세트는 각 검증자의 스테이킹 수량에 따라 결정되며, 이는 검증자와 해당 검증자에게 위임한 사용자들의 BNB 총합을 반영합니다. 가장 많은 스테이킹을 보유한 상위 검증자들이 **활성 검증자 세트(active validator set)**로 선정되며, 이들은 블록을 제안하고 투표하는 역할을 수행합니다. 나머지 검증자들은 **대기 검증자 세트(standby validator set)**에 속하며, 스테이킹이 증가하거나 기존 활성 검증자가 탈락할 경우 활성 세트에 합류할 수 있습니다.

어떤 조직이나 개인도 온체인 상에서 자신의 검증자를 생성하고 충분한 위임을 확보함으로써 검증자 세트에 합류할 수 있습니다. 마찬가지로 모든 BNB 위임을 철회함으로써 탈퇴할 수도 있습니다. 검증자가 오작동하거나 오프라인 상태일 경우, 슬래싱을 통해 강제로 제거될 수도 있습니다.

제네시스 단계에서는 몇 개의 신뢰할 수 있는 노드가 초기 검증자 세트로 활동하게 됩니다. 블록 생성을 시작한 후에는 누구나 검증자 후보로 참여할 수 있으며, 선거를 통해 정식 검증자가 될 수 있습니다.

검증자 선출
검증자는 다음과 같이 세 가지 역할로 구분됩니다:

- Cabinet: 블록 생성 확률이 가장 높은 상위 K개(기본적으로 21개)의 검증자
- Candidate: (K+1)번째부터 K+NumOfCandidates까지의 검증자들로, 소량의 블록 생성 기회를 가짐
- Inactive: 나머지 검증자들로, 블록 생성 기회 없음



출처: BNB Whitepaper

검증자 세트의 역할은 매일 UTC 기준 00:00에 최신 스테이킹 정보를 기반으로 재정의됩니다. 합의 엔진은 검증자를 정렬하고 이 정보를 바탕으로 BSC의 검증자 세트를 갱신합니다.

시스템 계약
BSC는 스테이킹과 검증자 선출을 지원하기 위해 여러 내장 스마트 계약(시스템 계약)을 운영합니다:

- Validator Set Contract: 정기적으로 검증자 세트를 선출합니다. 또한 이 계약은 검증자 보상을 일시적으로 저장하는 금고 역할도 합니다.
- System Reward Contract: 이 계약은 거래 수수료 일부를 수집하는 금고 역할을 하며, 빠른 최종성 보상 분배와 같은 공공 목적에 사용됩니다.
- Slash Contract: 이 계약은 검증자의 블록 생성 실패 횟수를 추적하며, 일정 임계값을 초과하면 벌칙을 부여합니다. 이 계약은 이중 서명 또는 악의적인 최종성 투표 같은 다른 슬래시 이벤트도 처리합니다.

Stake Hub Contract: 이 계약은 검증자 및 위임 관리를 위한 진입점이며, 특정 검증자에 대한 슬래싱 로직도 구현합니다. 위임/위임 해제/재위임 등의 작업은 각각의 검증자 구현

계약을 호출하여 사용자의 스테이크를 관리합니다.

보상 분배
스테이킹 보상은 거래 수수료에서 비롯됩니다. 블록이 생성될 때, 대부분의 블록 수수료는 해당 블록을 제안한 검증자에게 보상으로 제공됩니다.

매일 수집된 보상의 일부는 검증자의 운영자 계정으로 커미션 형태로 직접 전송되며, 나머지는 해당 검증자의 크레딧 계약으로 전송됩니다. 사용자가 위임을 해제하고 자신의 스테이크를 청구할 때, 누적된 보상과 원래의 스테이크가 사용자에게 반환됩니다.

보안 및 최종성
전체 검증자 수의 과반수 이상인 (N/2 + 1) 명의 검증자가 정직하다는 전제하에, PoA 기반 네트워크는 일반적으로 안정적이고 안전하게 작동합니다. 그러나 일부 비잔틴 검증자들이 네트워크를 공격하는 시나리오도 존재합니다. 예를 들어 “클론 공격(Clone Attack)”이 있습니다. BSC의 보안을 비콘체인과 유사한 수준으로 유지하려면, 사용자들은 2/3*N + 1명 이상의 서로 다른 검증자가 서명한 블록을 수신한 뒤 트랜잭션을 신뢰하는 것이 권장됩니다. 이를 통해 전체 검증자의 1/3 미만이 악의적인 경우라도 BSC는 안전하게 작동할 수 있습니다.

BSC는 확률적 최종성 외에도 빠른 최종성(fast finality) 메커니즘을 제안합니다. 한 번 블록이 최종화되면 되돌릴 수 없습니다. 이 메커니즘은 Ethereum 2.0의 Casper FFG와 유사하며 다음 단계를 따릅니다:

- 검증자가 블록을 제안하고 다른 검증자에게 전파합니다.
- 검증자들은 자신의 BLS 개인 키를 사용해 해당 블록에 서명한 투표 메시지를 생성합니다.
- 이러한 투표는 풀(pool)에 수집됩니다.
- 새로운 블록이 제안될 때, 직전 블록에 충분한 투표가 있었다면 BLS 서명 집계가 이뤄집니다.
- 이 집계된 서명은 새 블록의 헤더에 extra field로 포함됩니다.
- 새로운 블록을 수신한 검증자 및 전체 노드는 이 서명을 근거로 **직전 블록을 정당화(justify)**합니다.
- 연속된 두 블록이 정당화되면, 앞선 블록은 **최종화(finalized)**됩니다.

거버넌스
BSC는 OpenZeppelin의 Governor 모듈에서 영감을 받아 자체 네이티브 거버넌스 모듈을 도입합니다. 주요 기능은 다음과 같습니다:

제안 및 투표권: 스테이킹 크레딧 보유자는 거버넌스 사안에 대해 제안하고 투표할 수 있습니다.

- 지속적 보상: 투표 기간 중에도 투표자는 스테이킹 보상을 계속해서 수령할 수 있습니다.
- 유연한 위임: 사용자는 자신의 투표권을 다른 사용자에게 위임할 수 있습니다.
- 보안 실행: 제안이 통과되면 일정 기간의 타임락(time-lock) 후 실행됩니다.

BNB 체인의 거버넌스는 2단계 절차로 구성됩니다:

- 온도 체크(Temperature Check): Snapshot 플랫폼 등을 통해 누구나 커뮤니티의 의견을 수렴할 수 있습니다.
- 최종 투표(Final Voting): 제안이 충분한 지지를 얻으면, 스테이킹된 BNB 보유자 또는

검증자가 온체인 투표를 통해 최종 결정을 내립니다.

슬래싱 및 페널티
슬래싱(Slashing)은 온체인 거버넌스의 일부로서, 악의적이거나 부정적인 행동에 대해 벌칙을 부과합니다. 누구나 슬래시 트랜잭션을 제출할 수 있으며, 증거와 수수료를 함께 제공해야 합니다. 제출이 성공하면 상당한 보상이 주어집니다. 현재 슬래시가 가능한 행위는 세 가지입니다.

이중 서명
동일한 높이 및 동일한 부모 블록에 대해 둘 이상의 블록에 서명하는 경우는 심각한 오류이며, 고의일 가능성이 큽니다. 참조 프로토콜 구현에는 이를 방지하는 로직이 포함되어 있어야 하며, 악의적인 코드만이 이를 유발할 수 있습니다.
이중 서명이 발생하면 해당 검증자는 즉시 검증자 세트에서 제거되어야 합니다.

누구나 두 개의 블록 헤더(높이와 부모 블록이 동일하고, 문제의 검증자가 서명한)를 슬래시 계약(Slash Contract)**에 제출하여 슬래싱을 트리거할 수 있습니다. 계약은 유효성을 검증하고, 해당 검증자를 제거하며 자체 스테이킹한 BNB의 일부를 소각합니다.

악의적인 빠른 최종성 투표
동일한 타겟 높이 또는 서로를 포함하는 범위로 상충하는 두 개의 최종성 투표를 서명한 경우, 이는 또 다른 심각한 오류입니다.
이런 악의적 투표가 발생하면 검증자는 즉시 세트에서 제거되어야 하며, 신고자는 증거(두 개의 충돌 투표 및 서명 키)를 제출하여 보상을 받을 수 있습니다.

가용성 부족
BSC는 PoSA 방식이기 때문에, 모든 검증자가 자신의 턴에 맞춰 제시간에 블록을 생성해야 네트워크의 생존성이 유지됩니다. 검증자는 하드웨어, 소프트웨어, 구성, 네트워크 문제 등으로 블록 생성을 놓칠 수 있으며, 이는 네트워크 성능 저하 및 불확실성 증가로 이어집니다.

- 스마트 계약은 각 검증자의 누락 블록 수를 기록합니다.

- 기준치를 초과하면, 블록 생성 보상은 해당 검증자에게 지급되지 않고 다른 성능 좋은 검증자들과 공유됩니다.

- 더 높은 임계값을 넘기면 검증자는 회전에서 제외되고, 자체 스테이킹 BNB 일부가 소각됩니다. 이로 인해 검증자뿐 아니라 위임자도 보상을 받을 수 없습니다.

전망

BNB 체인은 지금까지 끊임없이 진화해왔으며, 앞으로도 다음과 같은 주제들이 주요한 발전 방향이 될 것입니다:

- 병렬 EVM (Parallel EVM): 여러 명령어를 병렬로 실행할 수 있게 하여 네트워크 성능을 향상시킴
- 상태 만료(State Expiry): BSC의 월드 스테이트(world state) 스토리지 증가 문제를 해결하기 위해 만료된 상태 데이터를 제거함
- 지속적인 탈중앙화 추진
- 대중 채택을 위한 인프라(Mass Adoption Infra): 대규모 애플리케이션을 위한 견고한 기반 인프라 구축을 BNB 체인 커뮤니티가 책임지고 추진

위험고지 안내
Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.

coinone