

콘플럭스(Conflux)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다

Conflux Network 일반 지식

Core Space와 eSpace에 공통으로 적용되는 개념 및 지식

Conflux란 무엇인가

Conflux Network는 기존의 많은 블록체인 네트워크가 직면한 확장성(scalability), 보안성(security), 탈중앙화(decentralization) 문제를 해결하기 위해 설계된 최첨단 퍼블릭 블록체인 시스템이다. Conflux의 핵심에는 Tree-Graph라 불리는 고유한 합의 메커니즘(consensus mechanism)이 있다. 이 메커니즘은 블록과 거래를 병렬로 처리할 수 있도록 하여 합의에 필요한 시간과 자원을 줄이고 네트워크 전체 처리 용량을 향상시킨다.

리소스

Conflux 통합(Conflux Integration)을 지원하기 위해 다양한 가이드, 참고자료 및 예제를 제공한다. Conflux Network의 여러 측면을 심층적으로 살펴보고 자신만의 맞춤형 통합을 구축할 수 있다.

Conflux란 무엇인가?

Conflux는 뛰어난 성능, 고유한 합의 메커니즘, 혁신적인 이중 공간(dual-space) 설계를 갖춘 퍼블릭 블록체인이다. 이러한 특징을 통해 Conflux는 탈중앙화 금융(DeFi)과 게임을 포함한 다양한 애플리케이션에 적합한 빠르고 안전하며 탈중앙화된 플랫폼을 제공한다.

Conflux는 작업증명(PoW)과 지분증명(PoS)을 결합한 하이브리드 합의 메커니즘을 채택하여 높은 보안성, 처리량 및 탈중앙화를 보장한다. Conflux의 PoW 합의는 Tree-Graph 원장 구조와 GHAIST 알고리즘을 활용하여 비트코인과 이더리움과 동일한 수준의 탈중앙화를 유지하면서 최대 3,000 TPS의 높은 거래 처리량과 1분 이내의 확정 지연 시간을 제공한다. Conflux의 PoS 합의는 네트워크에 최종성(finality)을 제공하여 51% 공격 위험을 완화한다. 이에 따라 Conflux는 대규모 거래를 효율적으로 처리할 수 있으며, 다양한 애플리케이션을 위한 견고하고 신뢰할 수 있는 플랫폼으로 기능한다.

Conflux 네트워크는 Conflux Core Space와 Conflux eSpace라는 두 개의 독립적인 공간으로 구성된다. Core Space는 하이브리드 합의 메커니즘을 사용하는 기본 블록체인 네트워크이며, 컨트랙트 스폰서십(contract sponsorship) 메커니즘을 제공한다. 이 스폰서십 메커니즘은 프로젝트 사용자가 잔액 없이도 컨트랙트와 상호작용할 수 있도록 하여 블록체인 사용 장벽을 낮추고 사용자 기반을 확장한다. eSpace는 이더리움 가상머신(EVM)과 완전히 호환되

므로 개발자는 기존 이더리움 스마트 컨트랙트를 쉽게 Conflux eSpace로 이전하여 높은 성능과 확장성의 이점을 활용할 수 있다. Conflux Core Space와 eSpace는 CrossSpaceCall 컨트랙트를 통해 상호 통신할 수 있으며, 이를 통해 두 공간 간 자금의 원자적 전송과 스마트 컨트랙트 호출의 원자적 실행이 가능하다.

Conflux에 대해 더 자세히 알고 싶다면, Tree-Graph 알고리즘, GHOST, Spaces, 그리고 하이브리드 PoW + PoS 합의 메커니즘을 다루는 영상을 참고하기 바란다.

합의(Consensus)

블록체인에서 합의(consensus)란 네트워크의 모든 노드가 현재 원장 상태에 대해 동일한 의견에 도달하는 과정을 의미한다. 합의를 달성하기 위해 네트워크의 각 노드는 블록체인에 추가되는 새로운 거래가 유효하며 프로토콜 규칙을 준수하는지 검증하고 확인해야 한다. 이러한 과정은 일반적으로 작업증명(PoW) 또는 지분증명(PoS)과 같은 합의 알고리즘을 통해 수행되며, 이를 통해 노드들은 블록체인의 일관성과 가용성을 유지하도록 유인된다.

합의는 블록체인의 보안성과 신뢰성을 보장하는 핵심 요소로서, 네트워크 참여자 모두가 원장 상태에 대해 일관된 관점을 유지하고 새로운 거래가 블록체인에 추가될 수 있도록 한다.

Conflux의 합의는 PoW와 PoS를 결합한 하이브리드 메커니즘이다. PoW 채굴자는 블록을 생성하고 Tree-Graph 알고리즘을 사용해 이를 정렬함으로써 높은 처리량과 확장성을 달성한다. PoS 노드는 피벗 블록(pivot block)에 서명하여 이를 최종 확정하며, 이를 통해 포크 발생 확률을 줄인다. PoS 노드는 보유한 CFX 토큰의 지분량에 따라 선정되며, 이는 정직하게 행동하도록 유인한다. 이러한 PoW/PoS 합의는 탈중앙화를 훼손하지 않으면서도 높은 성능을 달성할 수 있도록 한다.

작업증명(Proof of Work)

PoW의 개념

작업증명(PoW) 개념은 1993년 Cynthia Dwork와 Moni Naor에 의해 스팸 이메일을 방지하기 위한 수단으로 처음 제안되었다. 개념은 간단했다. 이메일 발신자가 메시지를 보내기 전에 계산 문제를 풀도록 요구하는 것이다. 이 계산 문제는 해결에 일정 수준의 연산 자원이 필요하도록 설계되어 있어 상당한 시간이 소요된다. 이메일 수신자는 발신자가 해당 계산 문제를 해결했는지 검증한 후 이메일을 수락한다. 이러한 검증 과정은 합법적인 이메일만 수락되도록 보장하며, 스팸 발송자가 원치 않는 이메일로 수신자의 받은 편지함을 채우지 못하도록 한다.

이 아이디어의 목적은 스팸 발송자가 대량 이메일을 보내는 것을 훨씬 어렵고 비용이 많이 들게 만드는 동시에, 정상적인 이메일 발신자는 약간의 불편만 감수하고 계속 이메일을 보낼 수 있도록 하는 것이었다. 이메일 스팸 방지를 위한 PoW 개념은 타당했지만 정상적인 사용자에게도 불편을 초래했기 때문에 널리 채택되지는 못했다. 그러나 이후 사토시 나카모토(Satoshi Nakamoto)가 이 개념을 응용하여 P2P 전자화폐 시스템, 즉 블록체인 "비트코인(Bitcoin)"을 개발하였다.

Bitcoin의 PoW 합의

Bitcoin은 블록체인에서 새로운 블록을 채굴할 수 있는 주체를 결정하기 위해 PoW 메커니즘을 사용한다. 블록 채굴 과정은 네트워크가 설정한 현재 난이도 목표를 충족하는 해시값을 찾기 위해 nonce 값을 변경하며 블록 헤더를 반복적으로 해싱하는 방식으로 이루어진다. 채굴자들은 이 문제를 해결하기 위해 경쟁하며, 가장 먼저 문제를 해결한 채굴자는 새로 발행된 비트코인과 해당 블록에 포함된 거래 수수료를 보상으로 받는다.

또한 네트워크가 블록체인의 단일 버전에 합의할 수 있도록 최장 체인 규칙(Longest Chain Rule)이 도입되었다. 두 명의 채굴자가 동시에 블록을 생성하면 블록체인에 포크가 발생하며, 서로 경쟁하는 두 개의 블록체인 버전이 생성된다. 이때 어느 포크가 유효한지를 결정하기 위해 최장 체인 규칙이 적용된다. 이 규칙은 가장 긴 블록 체인, 즉 가장 많은 작업증명이 투입된 체인이 유효한 포크라고 규정한다.

PoW는 새로운 블록 생성 과정을 어렵고 자원 집약적으로 만듦으로써 네트워크를 보호하며, 전체 연산 능력의 51% 이상을 통제하지 않는 한 단일 주체가 시스템을 지배할 수 없도록 한다. 또한 보상 시스템은 채굴자들이 네트워크에 참여하고 이를 유지하도록 유인한다. PoW의 도입은 탈중앙화 시스템에 대한 인식을 혁신적으로 변화시켰으며, 이후 다양한 암호화폐 및 블록체인 애플리케이션 개발의 기반이 되었다.

Conflux의 PoW 합의

Conflux 역시 네트워크 보안을 위해 PoW 합의 메커니즘을 사용한다. Tree-Graph 원장 구조와 GHOST 체인 선택 규칙(chain selection rule)을 결합함으로써 비트코인 및 이더리움과 동일한 수준의 탈중앙화와 보안성을 유지하면서도 거래 처리량(TPS)과 확정 지연 시간 측면에서 100배 이상의 향상을 제공한다.

Tree-Graph

Conflux의 핵심에는 Tree-Graph 원장 구조와 GHOST 체인 선택 규칙이 존재한다.

분산 원장은 동시에 생성되는 블록, 즉 포크(fork)를 처리해야 한다. 비트코인과 이더리움 같은 블록체인은 최장 체인 규칙을 사용하여 하나의 포크만 선택하고 나머지는 모두 폐기한다. 폐기된 블록은 시스템의 보안성에도, 처리량에도 기여하지 않는다. 그 결과 이러한 블록체인에서는 확장성과 보안성 사이에 본질적인 충돌이 존재한다. 반면 Conflux는 모든 동시 블록을 원장에 포함함으로써 매우 높은 수준의 보안성과 성능을 달성한다.

첫째, Conflux는 최장 체인 규칙을 GHOST 체인 선택 규칙으로 대체한다. 이 규칙에서는 단순히 체인 자체가 아니라 해당 서브트리에 투입된 채굴 파워를 기준으로 포크를 선택하므로 훨씬 더 견고한 선택이 가능하다. 이를 통해 Conflux는 초당 최대 2개의 블록 생성 속도를 사용할 수 있다. 또한 GHOST는 라이브니스 공격(liveness attack)에 대해서도 저항성을 가진다.

둘째, Conflux는 Tree-Graph를 원장 구조로 사용한다. 각 블록은 하나의 부모(parent) 옛지뿐만 아니라 이전 블록들을 가리키는 참조(reference) 옛지 목록도 포함한다. 이를 통해 블록 간 선후 관계에 대한 새로운 정보가 추가된다. 이 구조는 본질적으로 DAG(모든 옛지) 내부에 포함된 방향성 트리(부모 옛지만) 구조이기 때문에 Tree-Graph라는 이름이 붙었다.

거래를 처리할 때 Conflux는 먼저 GHOST를 사용하여 Tree-Graph 내에서 피벗 체인을 선택한다. 이후 피벗 체인과 참조 옛지를 활용해 원장을 선형적인 블록 시퀀스로 정렬한다. 마지막으로 이 선형 순서를 따라 거래를 실행한다.

Tree-Graph

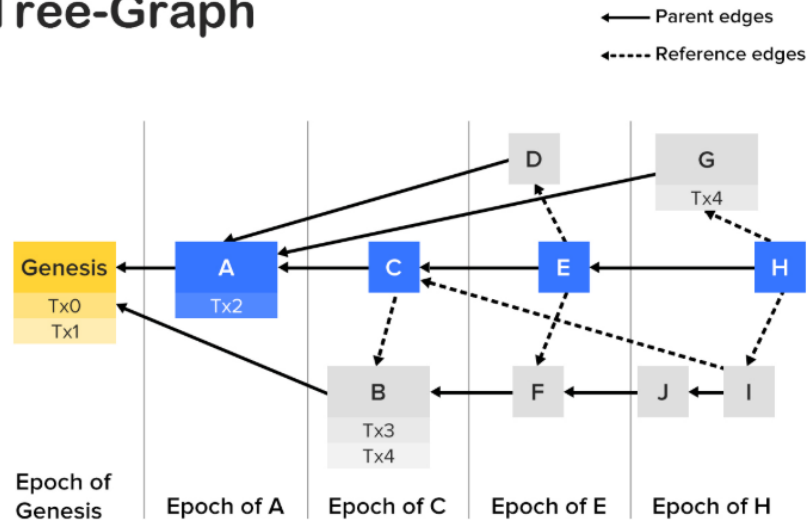


그림 1: Tree-Graph

GHAst

GHAst (Greedy-Heaviest-Adaptive-SubTree)

Conflux 연구 그룹(Conflux Research Group)은 "라이브니스 공격(liveness attack)" 문제를 해결하기 위해 GHAst 메커니즘을 개발하였다. 이 메커니즘은 가장 무거운 체인 규칙(heaviest chain rule)을 적용하되 수정된 블록 가중치 시스템을 사용하는 방식이다. 블록 유형은 채굴자의 임의 선택이 아니라 블록의 과거 Tree-Graph 구조를 기반으로 결정된다. GHAst 메커니즘에서는 현재 마지막 메인 체인 블록의 자식 트리 중 가장 높은 가중치를 가진 자식 블록을 선택하는 방식으로 가장 무거운 체인 규칙이 구현된다. 또한 서브트리의 블록 가중치는 단순한 블록 수가 아니라 가중치 총합을 기준으로 계산된다. GHAst 메커니즘은 채굴자가 특수 블록을 생성할 수 있도록 함으로써 블록 난이도를 높이고 블록 생성 속도를 늦추며, 이를 통해 라이브니스 공격 문제를 완화한다.

GHAst 메커니즘의 핵심 요소는 다음과 같이 요약할 수 있다.

가장 무거운 체인 규칙을 적용하되, 블록은 0, 1, X의 세 가지 서로 다른 가중치를 가진다. 여기서 X는 비교적 큰 수이며, 예를 들어 $X = 1000$ 이다(채굴 난이도 조정이 포함되는 경우는 제외).

네트워크에는 일반 블록(normal block)과 특수 블록(special block)의 두 종류가 존재한다. 일반 블록의 가중치는 항상 1이다. 특수 블록의 가중치는 블록의 난이도(Difficulty)에 따라 결정되며, $1/X$ 의 확률로 가중치 X를 갖고 나머지는 0의 가중치를 갖는다. 일반 블록 채굴 난이도는 특수 블록 채굴 난이도와 동일하다.

블록 유형은 해당 블록의 과거 Tree-Graph 구조에 의해 결정된다. 따라서 블록 생성자는 블록 유형을 임의로 지정할 수 없다.

공격이 없는 상황에서는 새롭게 생성되는 모든 정직한 블록이 일반 블록이 되어야 한다. 반면 공격자가 어떠한 형태의 "라이브니스 공격"을 수행하고 충분히 오랜 기간 이를 지속하면, 이후 생성되는 모든 정직한 블록은 특수 블록이 된다.

Conflux PoS 기술 개요

본 문서는 Conflux의 지분증명(PoS) 메커니즘에 대한 기술적 개요를 제공한다. 실질적인 스테이킹 가이드는 Staking Guide를 참고하기 바란다.

목적 및 설계

Conflux는 작업증명(PoW)과 지분증명(PoS)을 결합한 하이브리드 합의 메커니즘을 구현한다. 이러한 독특한 접근 방식은 다음의 세 가지 핵심 목적을 가진다.

1. 51% 공격 방어: 네트워크 초기 단계와 같이 해시 파워가 제한적인 상황에서 PoS는 잠재적인 공격에 대응하는 추가적인 보안 계층을 제공한다.
2. 체인 최종성(Chain Finality): PoS 메커니즘은 위원회 투표를 통해 PoW 체인에 명확한 최종성을 제공한다.
3. 강화된 보안성: 이중 계층 합의 구조는 단독 메커니즘보다 더욱 견고한 보안 모델을 제공한다.

이 하이브리드 접근 방식에 대한 상세한 분석은 Why PoS를 참고하기 바란다.

기술 아키텍처

PoS 체인 설계

Conflux의 PoS 체인은 필수적인 보안 기능에만 집중하는 최소주의적 구조로 설계되었다.

- 피벗 블록 투표와 위원회 선출 전용 독립 체인으로 운영된다.
- 원활한 동작을 위해 conflux-rust 노드에 직접 통합되어 있다.
- 약 1분의 블록 생성 시간을 유지한다.
- 보안 역할 최적화를 위해 일반적인 블록체인 기능은 포함하지 않는다.

PoS 계정 구조

PoS 계정 시스템은 보안 강화를 위해 이중 키 아키텍처를 사용한다.

주소 형식

각 PoS 계정에는 다음이 필요하다.

- 합의 서명을 위한 BLS 키 쌍
- 무작위 위원회 선출을 위한 VRF 키 쌍

이 키들은 결합되어 고유한 256비트 주소를 생성한다.

`0xd731d7633dd38c47769c2a62926b9a54d288a5e664f4d2108ac5bb66...`

PoS 계정은 PoW 계정과 연결(bind)될 수 있다. 연결된 PoW 계정은 PoS 체인에서 발생하는 이자를 수령한다.

노드 지갑 구현

지갑 기능은 안전하고 자동화된 운영을 위해 Conflux 노드 내부에 직접 내장되어 있다.

- 자동 설정: 노드를 처음 실행하면 키가 생성되고 암호화 비밀번호 설정을 요청한다.

- 안전한 저장: 키는 보호를 위해 비밀번호로 암호화되어 로컬에 저장된다.
- 자율 운영: 사용자 개입 없이 합의 참여를 자동으로 처리한다.
- 기본 인터페이스: 지갑 관리 및 모니터링을 위한 필수 CLI 명령어를 제공한다.

합의 참여

PoS 합의 메커니즘은 네트워크 보안과 효율적인 의사결정을 보장하기 위해 구조화된 투표 시스템과 정교하게 설계된 위원회 조직에 의존한다.

투표권

합의 참여를 위해서는 CFX 토큰 스테이킹이 필요하다.

1. 토큰 잠금(Token Locking): 사용자는 투표권을 얻기 위해 CFX 토큰을 잠가야 한다.
2. 투표 권한(Voting Power): 1,000 CFX를 잠글 때마다 1표가 부여된다.
3. 상태 동기화(State Synchronization): 변경 사항은 약 10분의 동기화 기간 이후 적용된다.
4. 시작 방법(Getting Started): 자세한 내용은 Staking Guide를 참고하기 바란다.

위원회 구조

위원회는 탈중앙화와 효율적인 합의 간 균형을 이루도록 설계되었다.

- 규모(Size): 최대 300석으로 구성되어 광범위한 참여를 보장하면서도 효율성을 유지한다.
- 구성(Organization): 50명씩 6개 그룹으로 나누어 체계적으로 순환한다.
- 순환(Rotation): 가장 오래된 그룹을 매시간 교체하여 지속적인 참여를 유지한다.
- 선출 과정(Selection Process):
 - 1.5시간 전부터 진행되는 선행 선출 과정
 - 공정한 선출을 위한 VRF 기반 무작위성
 - 스테이킹 규모에 따라 하나의 계정이 여러 좌석을 확보할 수 있는 유연한 배분 구조

인센티브 메커니즘

PoS 인센티브 시스템은 균형 잡힌 포인트 분배를 통해 적극적인 참여를 유도하고 네트워크 보안을 유지하도록 설계되었다.

포인트 시스템

위원회 주기마다 총 6,000,000 포인트가 다음 네 가지 활동에 배분된다.

1. 선거 참여(Election Participation, 120만 포인트) 최초 10,000개의 가장 낮은 해시값을 가진 투표 각각에 120포인트를 지급하여 초기 참여를 장려한다.
2. 위원회 구성원 자격(Committee Membership, 450만 포인트) 선출된 각 투표는 15,000포인트를 획득하며, 이를 통해 네트워크 보안에 대한 장기적인 기여를 유도한다.
3. 블록 리더십(Block Leadership, 18만 포인트) 블록 제안자는 PoS 블록당 3,000포인트를 획득하여 효율적인 블록 생산에 대한 보상을 받는다.
4. 추가 서명(Additional Signatures, 최대 12만 포인트) 최소 임계치를 초과하는 서명에 대한 추가 보상을 제공하

여 높은 참여율을 장려한다.

보상 분배

포인트 시스템은 금전적 보상과 직접적으로 연계된다.

- 포인트는 60개 블록(위원회 1주기)마다 계산 및 정산된다.
- 네트워크 이자는 누적 포인트 비율에 따라 분배되며, 연결된 PoW 계정이 이자를 수령한다.
- 배분되지 않은 이자(할당되지 않은 포인트에서 발생한 이자)는 소각된다.
- 현재 보상률은 Staking Guide에서 확인할 수 있다.

누적 이자 공식

네트워크 이자율은 전체 스테이킹 참여 규모에 따라 동적으로 조정된다.

$$\text{Interest per block} = \sqrt{\frac{\text{total\_staking}}{\text{total\_circulation}}} \quad (1)$$

보안상의 이유로 위원회가 7,200개 블록 동안 변경되지 않으면 이자 적립은 중단된다.

락업 기간 및 예시

락업 메커니즘은 예측 가능한 토큰 사용 가능성을 제공하면서도 네트워크 안정성을 보장하도록 설계되었다.

기본 일정

신중하게 설계된 일정은 네트워크 보안과 토큰 보유자의 유연성을 모두 보장한다.

1. 초기 기간: 13일의 의무 스테이킹 기간
2. 상태 전환: 스테이킹(staking) 상태에서 스테이크 완료(staked) 상태로 자동 전환
3. 언스테이킹 기간: 1일의 처리 기간
4. 총 기간: 최소 14일의 참여 기간 필요

예시 시나리오

실제 환경에서 락업 메커니즘이 어떻게 작동하는지 설명한다.

사례 1: 일반적인 언스테이킹

이는 토큰 잠금 해제에 가장 이상적인 경로를 나타낸다.

1. 1일차에 스테이킹
2. 13일차에 언스테이킹 요청(최소 스테이킹 기간 충족 후)
3. 14일차 종료 시점에 토큰 사용 가능

사례 2: 조기 언스테이킹

조기 인출 요청의 영향을 보여준다.

1. 1일차에 스테이킹
2. 2일차에 조기 언스테이킹 요청
3. 토큰은 여전히 14일차 종료 시점까지 잠겨 있음(의무 락업 기간 적용)

현재 스테이킹 수익률 및 상세한 절차는 Staking Guide를 참고하기 바란다.

보안 조치

PoS 시스템의 보안은 다양한 패널티와 보호 장치를 통해 유지된다. 다음 사항에 대한 자세한 내용은:

- 슬래싱 조건 및 규모
- 보안 위험 요소
- 예방 조치

Penalties and Slashing 가이드를 참고하기 바란다.

PoS를 도입한 이유는 무엇인가?

참고

본 문서는 이더리움 머지(Ethereum Merge) 이전에 작성되었으며, Conflux가 PoS 도입을 결정한 이유를 설명하기 위한 글이다.

먼저 Conflux가 상당 기간 동안 51% 공격 위험을 고려해야 하는 현실부터 설명하고자 한다. 이더리움의 막대한 채굴 수익과 그래픽카드 수요 증가로 인해 채굴자들은 이미 대량의 그래픽카드를 구매하였으며, 이는 거대한 해시 파워 풀을 형성하고 있다.

Conflux 역시 그래픽카드를 사용해 채굴하며, Conflux의 보안을 유지하는 그래픽카드 해시 파워는 여전히 이더리움에 비해 크게 부족하다. 따라서 대량의 그래픽카드가 단기간에 Conflux로 전환되어 51% 공격을 수행할 위험이 존재한다.

이와 유사한 51% 공격 위험은 그래픽카드 채굴을 사용하는 다른 PoW 퍼블릭 체인뿐만 아니라, BTC와 동일한 ASIC 채굴 방식을 사용하지만 연산 능력이 훨씬 낮은 BCH와 같은 블록체인에도 존재한다. BCH는 이러한 51% 공격 위험에 대응하기 위해 롤백 가능 길이를 제한하는 비교적 "우아하지 않은" 방법까지 채택한 바 있다.

이론적으로 PoW 기반 퍼블릭 체인은 51% 공격 위험을 완전히 제거할 수 없다. 실제로 공격자가 51% 공격을 수행할지 여부는 공격의 비용과 이익에 크게 좌우된다. 공격자의 이익 측면에서 성공적인 51% 공격은 채굴 수익 자체에는 영향을 주지 않는다. 공격자의 이익이 감소하는 주요 이유는 두 가지이다. 하나는 공격 성공 이후 토큰 가치 붕괴로 인한 손실이며, 다른 하나는 커뮤니티가 하드포크를 통해 상태를 롤백하여 공격자의 이익을 제거하는 데 합의할 수 있다는 점이다. 그러나 오늘날 블록체인은 다양한 온체인 자산과 크로스체인 서비스를 지원하고 있으므로, 단순한 하드포크만으로 이중지불(double-spending) 공격의 영향을 제거하기는 어렵다. 이는 ETC가 ETH로부터 분리되던 시기의 상황과 상당히 다르다.

51% 공격자의 비용을 증가시키는 방법으로는 현재 세 가지 대응 방안이 존재한다.

1. 모든 대규모 해시 파워 풀을 회피하는 것이다. 구체적으로는 그래픽카드 채굴을 포기하고 전용 ASIC 채굴 방식으로 전환하는 것이다.

2. Conflux의 네트워크 해시 파워를 이더리움 수준까지 끌어올리거나 이를 초과하는 것이다. 이를 위해서는 Conflux의 총 채굴 수익을 이더리움 수준까지 증가시켜야 한다. 현재 이더리움의 채굴 발행량은 13초마다 약 2.6 ETH, 즉 초당 평균 0.2 ETH 수준이다. ETH 가격을 3,400달러로 가정하면 초당 약 680달러, 하루 약 58,752,000달러의 채굴 수익이 발생한다. Conflux의 채굴 수익을 이 수준으로 높이려면 약 170배 증가가 필요하다. 이는 CFX 가격을 1달러로 유지할 경우 블록당 보상을 340 CFX 이상으로 늘리거나, 발행량을 유지한 채 CFX 가격을 170배 상승시키는 것을 의미한다. 단기간 내에 이를 달성하려면 아마도 Elon Musk가 매주 또는 매일 CFX에 대해 트윗을 해야 할 것이다.
3. 51% 공격에 대응하기 위해 PoS 메커니즘을 도입하는 것이다. PoS 의사결정 구조에서는 공격자가 단순히 연산 능력 우위만으로는 이중지불 공격을 성공시킬 수 없으며, PoS 의사결정에 영향을 미칠 수 있을 만큼 충분한 CFX를 추가로 확보해야 한다.

이 세 가지 선택지 중 실제로 실행 가능한 것은 마지막 방법뿐이라고 판단한다.

기술 로드맵 측면에서 Conflux의 목표는 "특정 PoW 합의 프로토콜을 가진 퍼블릭 체인"이 아니라 "모든 사람이 접근 가능하고 부담 없이 사용할 수 있는 탈중앙화 퍼블릭 체인 플랫폼"을 구현하는 것이다. 기술적 접근은 목표를 달성하기 위한 수단일 뿐 목표 자체가 아니다. 따라서 기존 PoW 합의 메커니즘에 PoS 기반 최종성 결정을 추가하여 확정 속도를 향상시키고 잠재적인 51% 공격에 대응하는 것은 Conflux의 목표와 부합한다. 또한 PoS 최종성 메커니즘 추가에 따른 복잡성과 잠재적 위험을 줄이기 위해 거래 선택 및 패키징은 전적으로 PoW 채굴자에게 맡기고, 블록 순서는 기존 Tree-Graph 정렬 규칙을 따르며, PoS는 PoW 채굴자가 생성한 블록의 최종성에 대해서만 투표하도록 설계하였다.

PoW와 PoS에 대한 우리의 이해는 변함이 없다. PoW는 더 안전하지만 확정이 느리고, PoS는 더 빠르게 확정되지만 보안성은 상대적으로 낮다. PoW와 PoS의 결합은 보다 이상적인 합의 프로토콜이 될 가능성을 가진다.

PoW + PoS 하이브리드 합의

- PoW 합의의 장점: 보안성과 신뢰성
- PoS 합의의 장점: 효율성(빠른 확정, 낮은 에너지 소비)
- 두 방식 모두 네트워크 용량 한계에 근접한 처리량 달성이 가능함
 - 추가적인 확장은 인프라 업그레이드 또는 Layer 2 솔루션이 필요함
- 두 방식의 장점을 어떻게 결합할 것인가?
 - 높은 보안성
 - 빠른 확정
 - 합리적인 에너지 소비

패널티 및 슬래싱

정직한 PoS 참여를 장려하고 시스템 보안을 유지하기 위해, 합의 참여가 비활성 상태일 경우 보상이 감소하며, 합의 메커니즘에 대한 공격 행위는 슬래싱으로 이어진다.

강제 은퇴(Force Retire)

기준

PoS 노드가 위원회에 선출된 후 3개 연속 에폭(epoch) 동안(약 3시간) 어떠한 합의 메시지도 전송하지 않으면 강제 은퇴 처리된다.

패널티 세부사항

강제 은퇴는 언스테이킹 메커니즘이 자동으로 실행되는 것과 동일하다. 이 과정은 노드 운영자가 직접 실행하지 않는다는 점을 제외하면 자발적 언스테이킹과 동일하다. 강제 은퇴 기간 동안 새롭게 스테이킹된 토큰 역시 자동으로 언스테이킹 절차가 시작된다. 강제 은퇴 기간은 1일 동안 지속된다.

PoS 언락 대기 기간(최소 14일 스테이킹 및 최소 1일 언스테이킹 진행 필요)이 종료된 후, 스테이커는 CFX를 인출하거나 다시 스테이킹할 수 있다.

가능한 원인

1. 네트워크, 저장장치 또는 소프트웨어 문제로 인한 노드 장애.
2. 공식 confluent-rust 코드에 대한 비인가 수정으로 인한 이상 동작.

슬래시(Slash)

기준

합의 메커니즘을 공격하는 행위가 탐지되면 슬래시가 발생한다. 보안상의 이유로 탐지 규칙 전체는 공개되지 않는다.

패널티 세부사항

검증자(validator)의 모든 스테이킹 토큰은 영구적으로 잠기며 언스테이킹할 수 없다.

가능한 원인

1. 동일한 PoS Key를 공유한 상태에서 여러 PoS 노드를 실행하여 동일 키로부터 상충되는 행동이 발생한 경우.
2. pos_db/secure_storage.json 파일의 변조 또는 손실. (파일이 손실된 경우 언스테이킹 후 언락 기간을 기다린 뒤 새로운 PoS Key를 연결하는 것이 권장된다.)
3. 공식 confluent-rust 코드에 대한 비인가 수정으로 인한 이상 동작.

슬래시 방지를 위한 안전한 노드 재시작 절차

패널티 없이 PoS 노드를 안전하게 재시작하려면 Safe Node Restart Procedure 문서를 참고하기 바란다.

토크노믹스(Economics)

Conflux의 경제 모델은 네트워크 참여와 성장을 장려하는 동시에 기술적 안정성을 지원한다. 잘 설계된 경제 모델은 탈중앙화 시스템이 효율적으로 운영되기 위한 핵심 요소이다. 블록체인 기술은 신뢰를 구축하고 참여자 간 효율적인 관계를 형성함으로써 가치 이전을 가속화한다.

Conflux 경제 모델 개요

핵심 요소

1. 가치 시스템(Value System): 퍼블릭 블록체인 시스템은 경제적 가치를 지닌 측정 단위로서 토큰을 필요로 한다. 토큰은 자산 소유권을 명확히 하며 가치 교환의 매개체 역할을 수행한다. 또한 저장 자원과 연결되어 장기적인 인센티브로 배분될 수 있다.

2. 거버넌스 규칙(Governance Rules): 거버넌스 규칙은 토큰의 분배 및 활용 방식과 다양한 조건에서 발생하는 경제적 영향을 포함한다. 토큰은 사용자에게 이자로 지급되거나 채굴자에게 블록 보상으로 지급될 수 있다. 또한 법정화폐 또는 다른 디지털 자산과 교환될 수 있다.
3. 커뮤니티 협력(Community Collaboration): 블록체인 시스템은 "누구에게나 개방되고 모든 참여자에게 이익이 되는 구조"여야 한다. 모든 사용자는 제약 없이 시스템에 참여할 권리를 가지며, 이해관계자가 되어 시스템 구축에 기여하고 그 결과로 보상을 받을 수 있다.

주요 참여자

Conflux Network 생태계의 참여자는 다음 세 그룹으로 구성된다.

1. 직접 구축자(Direct Builders): 기반 기술 개발과 네트워크 운영을 담당하는 Conflux Foundation 및 창립 팀.
2. 시스템 유지자(System Maintainers): 네트워크의 정상적인 운영과 보안을 보장하는 채굴자와 스테이커.
3. 생태계 기여자(Ecosystem Contributors): Conflux Network 생태계에 가치를 창출하는 커뮤니티 사용자.

발전 단계

Conflux Network는 초기 단계에서 운영 단계로 안정적으로 전환하기 위해 발전 단계별로 서로 다른 인센티브 구조를 채택한다.

- 초기 단계(Initial Phase): 직접 구축자와 생태계 기여자에게 인센티브를 제공하여 시스템의 콜드 스타트(cold start) 문제를 해결한다.
- 운영 단계(Operational Phase): 시스템 유지자에게 인센티브를 제공하여 지속적인 시스템 업그레이드를 촉진하며, 시스템 자원의 시장화를 통해 자원의 자기 적응형 구성(self-adaptive configuration)을 유도한다.

인센티브 메커니즘

Conflux의 인센티브 메커니즘은 사용자 참여를 장려하여 최소한의 진입 장벽으로도 안전하고 신뢰할 수 있으며 안정적인 네트워크를 유지하도록 설계되었다. 경제적 인센티브는 다음과 같다.

1. PoW 블록 보상: 채굴자는 PoW 블록을 채굴함으로써 각 블록에 대한 보상을 획득한다.
2. 거래 수수료 보상: 거래 우선순위 수수료(priority fee)와 거래 기본 수수료(base fee)의 일부가 채굴자 보상으로 지급된다.
3. PoS 이자: 사용자는 CFX를 스테이킹하여 PoS 검증자 validator가 됨으로써 이자를 획득할 수 있다.

CFX 토큰 분배

Conflux 가치 시스템의 핵심은 네이티브 토큰인 CFX이다. 각 CFX 토큰은 drip이라 불리는 더 작은 단위로 구성되며($1 \text{ CFX} = 10^{18} \text{ drips}$), 이를 사용한다.

초기 단계 CFX 분배

초기 단계에서는 직접 구축자와 생태계 기여자에게 생태계 구축을 위한 보상이 제공된다. 제네시스 블록에는 사전 발행된(pre-mined) 50억 개의 CFX 토큰이 포함되어 있으며, 다음과 같이 배분되었다.

- 사모 투자자(Private Equity Funders): 전체의 12%가 사모 투자자에게 배정되며, 2년에 걸쳐 해제된다.
- 재단 보유 물량(Foundation Holdings): 전체의 4%와 이전 항목에서 판매되지 않은 토큰이 장기 재정 지원을

위해 배정되며, 2년에 걸쳐 매월 해제된다.

- 제네시스 팀(Genesis Team): 전체의 36%가 IIIS 팀, Conflux Foundation 직원 및 자문단을 포함한 창립 팀에 배정되며, 4년에 걸쳐 해제된다.
- 커뮤니티 펀드(Community Fund): 전체의 8%가 커뮤니티 사용자에게 배정되며, 4년 이내에 해제된다.
- 생태계 펀드(Ecosystem Fund): 전체의 40%가 DApp 개발자를 지원하기 위해 배정되며, 4년 이내에 해제된다.

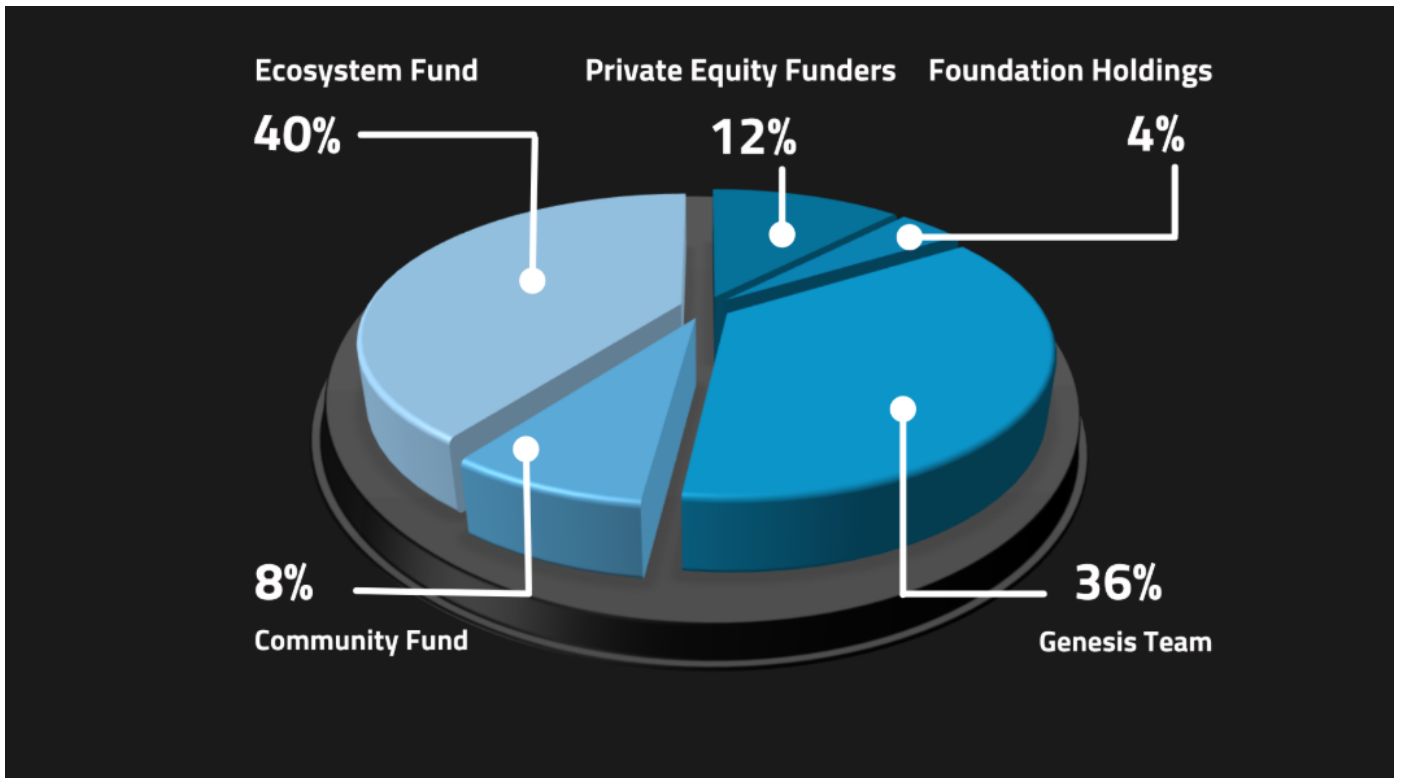


그림 2: 초기 단계 CFX 분배

운영 단계 CFX 분배

운영 단계의 CFX 분배는 토큰 발행과 토큰 소각을 모두 포함하며, 핵심 파라미터에 대한 DAO 투표를 통해 결정된다.

토큰 발행

1. 작업증명(PoW) 채굴:
 - 새롭게 발행된 CFX 토큰은 새 블록을 채굴한 채굴자에게 보상으로 지급된다.
 - 보상 규모는 DAO 투표를 통해 결정되는 `powBaseReward` 파라미터에 의해 정해진다. 2024년 7월 기준으로 블록당 약 1 CFX가 지급된다.
2. 지분증명(PoS) 이자:
 - PoS 검증자는 스테이킹한 CFX 규모에 비례하여 이자를 획득한다.
 - PoS 발행률은 연간 수익률(APY) 공식을 사용하여 계산된다.

$$APY = x \times interestRate \quad (2)$$

여기서 x 는 총 유통량을 총 스테이킹 수량으로 나눈 값의 제곱근을 의미한다. 이자율은 DAO 투표를 통해 결정된다.

토큰 소각 메커니즘

인플레이션을 완화하기 위해 Conflux는 여러 가지 토큰 소각 메커니즘을 운영하며, 이 역시 DAO 투표에 의해 관리된다.

1. 스토리지 포인트 전환(Storage Point Conversion):
 - 저장 공간 담보(collateral for storage)가 스폰서링될 경우, 스폰서링된 CFX의 일부가 소각되어 스토리지 포인트로 전환되며 영구적으로 유통량에서 제거된다.
 - 소각 비율은 DAO 투표로 결정되는 `storagePointProp` 파라미터에 의해 정해진다.
2. 기본 수수료(Base Fee):
 - Conflux Network의 모든 거래에는 기본 수수료가 부과된다.
 - 기본 수수료의 일부는 채굴자에게 분배되며, 나머지는 소각된다. 소각 비율은 DAO 투표로 결정되는 `baseFeeShareProp` 파라미터에 의해 정해진다.

DAO 거버넌스

Conflux는 토큰 발행 및 소각에 영향을 미치는 핵심 파라미터를 제어하기 위해 탈중앙화 자율조직(DAO)을 사용한다. DAO 투표는 Conflux 내부 컨트랙트인 `ParamsControl`에 의해 관리된다. 온체인 DAO 투표를 위한 프론트엔드 패널도 제공된다.

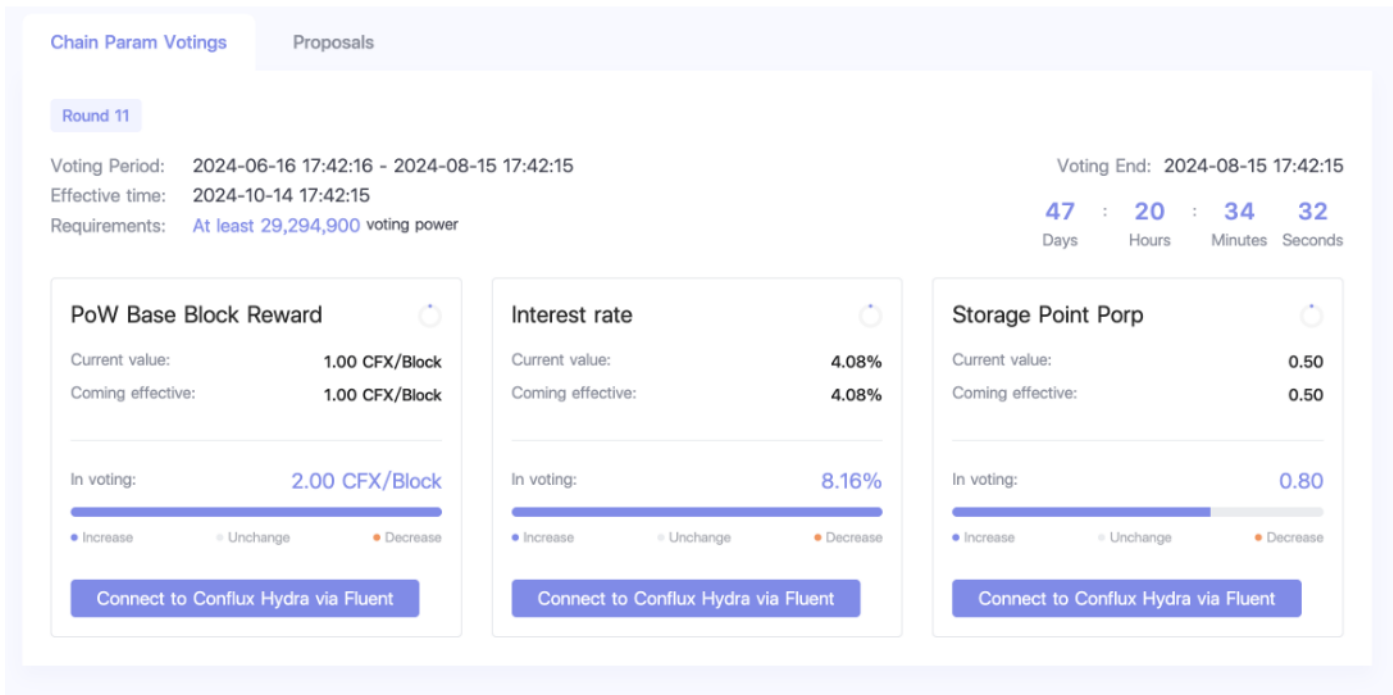


그림 3: DAO 거버넌스 투표 인터페이스

거버넌스 대상 파라미터는 다음과 같다.

- PoW 블록 기본 보상(`powBaseReward`)
- PoS 기본 이자율(`interestRate`)
- 스폰서링된 저장 공간이 스토리지 포인트로 전환되는 비율(`storagePointProp`)
- 거래 기본 수수료 중 소각되는 비율과 채굴자에게 분배되는 비율(`baseFeeShareProp`)

Conflux는 PoW와 PoS를 통한 토큰 발행, 전략적 토큰 소각, 그리고 DAO 거버넌스를 균형 있게 운영함으로써 안정적이고 지속 가능한 경제 모델을 유지하고자 한다.

CFX 연간 인플레이션 (2023년 8월 4일 기준 스냅샷)

참고

본 계산은 2023년 8월 4일 기준의 스냅샷이며 다음 조건을 전제로 한다.

- 작업증명(PoW) 기본 블록 보상: 블록당 1 CFX
- 지분증명(PoS) 기본 이자율: 0.0408 (4.08%)
- PoS 연간 수익률(APY): 12.9%, PoS 스테이킹 규모 3억 4,220만 CFX

해당 조건은 변경될 수 있으므로 정확한 계산을 위해서는 최신 파라미터를 확인해야 한다. 또한 본 스냅샷에는 토큰 소각 메커니즘이 반영되지 않았으며, 실제 인플레이션은 이보다 낮아질 수 있다.

Conflux Network는 일정 수준의 내재적 인플레이션을 포함하고 있으며, 시간이 지남에 따라 전체 유통량에 새로운 CFX가 추가된다. 현재 약 30억 CFX가 유통 중이며, 이는 사전 발행 물량과 채굴 및 스테이킹 보상으로 새롭게 발행된 물량으로 구성된다.

현재 Conflux의 작업증명(PoW) 발행량은 블록당 1 CFX이며, 블록은 0.5초마다 생성된다. 이에 따라 연간 약 6,300만 CFX가 발행된다.

지분증명(PoS) 발행량은 연간 수익률(APY)인 $0.04x$ 를 기준으로 계산된다. 여기서 x 는 총 유통량을 총 스테이킹 수량으로 나눈 값의 제곱근을 의미한다. 현재 총 CFX 유통량은 31억 개(소각 후 제로 주소에 보관된 4억 9,700만 개 포함)이며, 총 PoS 스테이킹 규모는 3억 4,220만 개이다. 이에 따라 현재 APY는 12.9%이며, 연간 약 4,400만 CFX가 PoS를 통해 발행된다.

CFX의 연간 인플레이션 규모는 약 1억 700만 개(PoW 6,300만 개 + PoS 4,400만 개)이다. 이를 제네시스 토큰 50억 개와 이미 발행된 토큰 5억 4,000만 개에 더하면 총 유통량은 55억 4,000만 개가 된다. 따라서 현재 CFX의 인플레이션율은 제네시스 토큰과 발행 토큰을 기준으로 약 1.9% 수준이다.

Conflux Network 생태계

Conflux Network는 확장성과 효율성을 향상시키는 고유한 Tree-Graph 합의 메커니즘을 기반으로 성장하고 있는 블록체인의 생태계이다. 이 생태계는 다양한 프로젝트들로 구성되어 있으며, 각 프로젝트는 네트워크의 활용성과 다양성에 기여하고 있다.

Swappi (AMM/DEX)

Swappi는 Conflux Network의 대표적인 탈중앙화 거래소(DEX)로, 자동화 마켓메이커(AMM) 모델을 사용한다. 이 플랫폼은 원활한 토큰 스왑 기능을 제공하여 사용자에게 탈중앙화되고 효율적인 거래 경험을 제공한다.

Nucleon (유동성 스테이킹 파생상품)

Nucleon은 유동성 스테이킹 파생상품(Liquid Staking Derivative) 형태의 혁신적인 스테이킹 방식을 제공한다. 이를 통해 사용자는 네트워크 보안에 참여하면서도 자산의 유동성을 유지할 수 있으며, 이는 스테이킹의 유연성과 활용성을 크게 향상시키는 중요한 발전이다.

Meson (스테이블코인 크로스체인 브리지)

Meson은 Conflux 생태계의 핵심 프로젝트 중 하나로, 스테이블코인을 위한 크로스체인 브리지를 제공한다. 이 플랫폼은 서로 다른 블록체인 간 안전하고 원활한 자산 이동을 가능하게 하여 탈중앙화 금융(DeFi) 생태계의 유동성과 연결성을 향상시킨다.

Meson 사용 방법을 배우고 싶다면 관련 튜토리얼을 참고하기 바란다.

Zero Gravity (크로스체인 브리지)

1초 미만의 최종성과 대부분의 체인을 지원하는 Zero Gravity는 사용자가 자산을 원활하고 안전하게 이동할 수 있도록 하여 마찰 없는 Web3 경험을 제공한다.

Zero Gravity 사용 방법을 배우고 싶다면 관련 튜토리얼을 참고하기 바란다.

ConfluxHub (크로스 스페이스 브리지, CFX 스테이킹 및 거버넌스)

ConfluxHub는 Conflux 생태계의 핵심 구성 요소로, 크로스 스페이스 브리지, CFX 스테이킹 및 거버넌스 기능을 제공하는 다목적 플랫폼이다.

ConfluxHub 사용 방법을 배우고 싶다면 관련 튜토리얼을 참고하기 바란다.

PoS 검증자

Conflux Network는 지분증명(PoS) 메커니즘을 사용하며, 모든 Conflux PoS 검증자 목록은 전용 웹사이트에서 확인할 수 있다.

Conflux 생태계와 그 다양한 구성 요소에 대해 보다 깊이 이해하고자 한다면, 이 주제를 다루는 아래의 YouTube 영상을 시청하기 바란다.

Spaces

Spaces 소개

Conflux v2.0(Hydra) 업그레이드에서는 CIP-90을 통해 Spaces라는 새로운 기능이 도입되었다. Spaces는 Conflux 형식의 거래와 Ethereum 형식의 거래를 구분하기 위해 사용되는 추상적 개념이다. Spaces는 원래 Conflux 네트워크 위에 eSpace라 불리는 가상 서브체인을 생성하는 방식으로 구현된다.

Core Space는 기존의 Conflux 네트워크를 의미하며, eSpace는 Core Space 네트워크 위에서 실행되는 가상화된 Ethereum 체인이다. 두 공간은 논리적으로 서로 독립적이며 상호 간에 영향을 미치지 않는다.

즉, Spaces는 운영체제 개념의 가상화 기술로 이해할 수 있으며, eSpace는 기존 Conflux 네트워크 위에서 실행되는 가상화된 Ethereum 체인이라고 볼 수 있다.

eSpace를 도입한 이유

Conflux는 혁신적인 Tree-Graph 합의 알고리즘을 기반으로 하는 고성능 완전 탈중앙화 퍼블릭 체인이다. Conflux의 거래 수수료는 매우 낮으며, Ethereum과 같은 다른 네트워크와 비교하면 사실상 무료로 가깝다. 그러나 Ethereum은 이미 다양한 도구, SDK, 지갑 및 Solidity 라이브러리를 포함한 성숙한 생태계를 구축하였다. 프로젝트와 사용자의 이전 비용을 줄이고, 사용자가 Conflux의 낮은 수수료와 높은 TPS의 장점을 경험할 수 있도록 하기 위해 eSpace가 도입되었다.

완전한 호환 인터페이스를 통해 Ethereum의 스마트 컨트랙트와 dApp은 수정 없이 eSpace에 직접 배포할 수 있다. Ethereum의 개발 도구, SDK, 지갑 및 서비스 역시 eSpace에서 그대로 사용할 수 있다. 사용자는 새로운 지식을 학습할 필요 없이 기존 도구를 활용하여 바로 시작할 수 있다.

eSpace는 Ethereum 개발자와 사용자에게 BSC, Polygon, Aurora와 마찬가지로 매우 사용하기 쉬운 환경을 제공한다.

두 공간 간의 관계

Core Space와 eSpace는 동일한 원장을 공유하여 기초 데이터를 저장한다. 하나의 블록에는 두 공간의 거래가 모두 포함될 수 있으며, 거래 인코딩 방식에 따라 구분된다. 그러나 두 공간은 각각 독립적인 거래, 계정 상태 및 컨트랙트를 가지는 논리적으로 독립된 공간으로 동작한다.

dApp 개발자 관점에서 Core Space와 eSpace는 특정 원자적 호출(atomic call)을 지원하는 내부 브리지를 가진 두 개의 별도 체인으로 이해할 수 있다. 각 공간의 거래는 크로스 스페이스 호출이 발생하지 않는 한 해당 공간 내 계정 상태에만 영향을 미친다.

eSpace 거래 패키징

Conflux에서는 블록 높이가 5의 배수인 경우에만 eSpace 거래가 블록에 포함된다. v2.4 하드포크 이후에는 eSpace 거래 포함 여부가 Core Space 거래 패키징에 영향을 주지 않는다. 따라서 블록 높이가 5의 배수인 경우에는 그렇지 않은 경우보다 최대 블록 크기가 더 커질 수 있다.

구조도

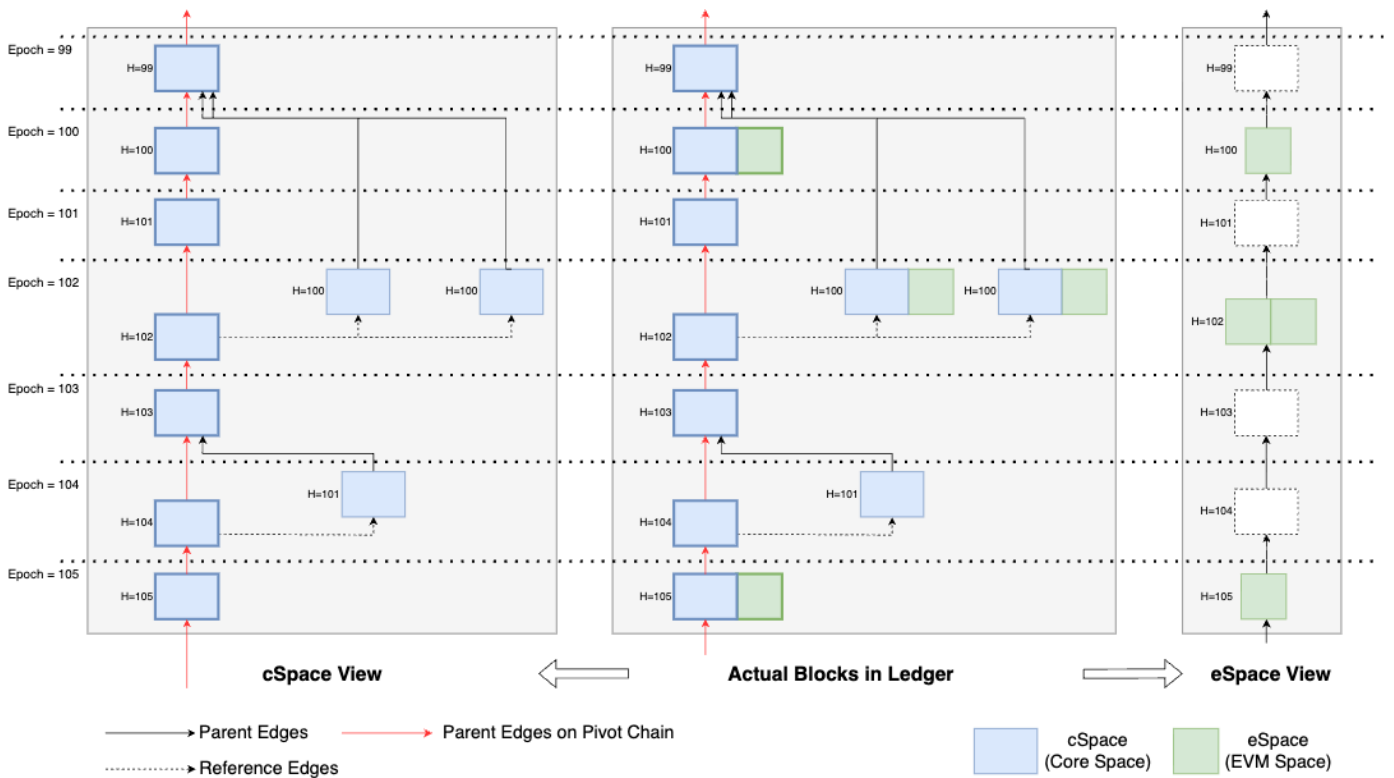


그림 4: 실제 블록, Core Space 뷰 및 eSpace 뷰 간의 관계

위 그림은 원장 내 실제 블록과 Core Space 및 eSpace 관점에서의 뷰 간 관계를 보여준다. H=... 표기는 블록 높이를 의미한다.

실제 블록

Conflux 원장에서는 블록이 방향성 비순환 그래프(DAG) 형태로 구성되며 에폭(epoch) 단위로 구분된다. 블록 높이가 5의 배수인 경우 eSpace 거래를 포함할 수 있으며, 이를 위해 분리된 블록 공간을 활용한다.

block.gasLimit 파라미터는 전체 Conflux 블록의 예상 크기를 나타내며 60,000,000으로 설정되어 있다. 이 값은 cfx_getBlockByHash와 같은 RPC 메서드를 통해 확인할 수 있다. coreSpace.gasLimit은 block.gasLimit의 90%(54,000,000)로 설정되며, eSpace.gasLimit은 block.gasLimit의 50% (30,000,000)로 설정된다.

따라서 블록 높이가 5의 배수인 경우 최대 블록 크기는 $1.4 * \text{block.gasLimit}$ 까지 증가할 수 있으며, 그렇지 않은 경우 최대 크기는 $0.9 * \text{block.gasLimit}$ 이다.

참고

채굴자는 블록마다 블록 가스 한도를 1% 범위 내에서 상향 또는 하향 조정할 수 있으나, 일반적으로는 일정한 값으로 유지된다.

Core Space 뷰

Core 관점에서는 eSpace 거래를 제외하면 실제 블록 구조와 거의 동일하게 보인다. 블록은 DAG 구조로 구성되고 에폭으로 구분되며, 각 블록은 동일한 가스 한도를 가진다.

eSpace 뷰

eSpace 뷰는 Ethereum 원장 구조를 시뮬레이션하기 때문에 실제 블록 구조와 상당히 다르다. 각 Conflux 에폭은 하나의 eSpace 블록으로 매핑된다. eSpace 관점에서는 해당 에폭의 거래들이 대응되는 블록에 포함된다. 따라서 eSpace 관점에서의 블록 크기는 고정되지 않으며, 원래 에폭에 포함된 블록에 따라 0이 될 수도 있고 eSpace.gasLimit의 두 배를 초과할 수도 있다.

그래프의 eSpace 뷰에서는 높이 99, 101, 103, 104에 빈 블록이 존재한다. 높이 100과 105에서는 블록 크기가 eSpace.gasLimit과 동일하다. 높이 102에서는 블록 크기가 $2 * eSpace.gasLimit$ 이다.

개발

Core Space와 상호작용하려면 Conflux 호환 지갑(Fluent), SDK(*-conflux-SDK), 개발 도구(chainIDE, hardhat)를 사용해야 한다. eSpace와 직접 상호작용하려면 Metamask, Hardhat, Ethers.js 등 Ethereum 생태계의 기존 도구와 서비스를 그대로 사용할 수 있다. 단지 해당 도구의 RPC 네트워크를 Conflux eSpace RPC로 설정하면 된다.

Spaces 간 통신 방법

Conflux Core Space와 eSpace 간 통신을 위해 CrossSpaceCall 컨트랙트를 사용할 수 있다. 이를 통해 CFX 전송, Core Space에서 eSpace로의 컨트랙트 배포, 그리고 Core Space에서 eSpace 컨트랙트 메서드 호출이 가능하다. Core Space의 각 계정은 eSpace 내에 대응되는 미리 주소를 가지며, 이는 원래 Base32 주소를 디코딩한 뒤 Keccak 해시를 적용하여 계산된다. 내부 컨트랙트는 동기식(synchronous) 크로스 스페이스 CFX 전송을 제공하므로 단순하고 안전하며 빠르게 자산을 이동할 수 있다. 또한 내장 이벤트 시스템과 온체인 메시지 패싱(On-chain Message Passing)을 통해서도 공간 간 통신이 가능하다.

어떤 공간을 선택해야 하는가

Conflux Core Space는 컨트랙트 스폰서십(contract sponsorship)을 지원하는 네이티브 공간이며, 더 높은 네트워크 처리 용량(TPS)을 제공한다. 그러나 주소 형식과 RPC 인터페이스가 Ethereum과 다르므로 개발자는 Conflux 전용 도구 체인을 사용해야 한다. 따라서 완전히 새로운 프로젝트를 개발하려는 경우 Core Space를 선택할 수 있다. 컨트랙트 스폰서십 메커니즘은 사용자가 잔액 없이도 컨트랙트와 상호작용할 수 있게 하여 블록체인 사용 장벽을 낮추고 사용자 기반 확대에 도움을 준다. 또한 이 기능은 디지털 자산 규제가 엄격한 국가나 지역에서도 규제를 준수하는 퍼블릭 체인 애플리케이션 개발을 가능하게 한다.

Ethereum 프로젝트를 Conflux의 높은 성능과 낮은 비용 환경으로 이전하여 사용자 비용을 줄이고자 한다면 eSpace를 선택할 수 있다. 프로젝트는 수정 없이 바로 배포할 수 있다. 또한 Ethereum 개발 경험이 풍부한 엔지니어라면 익숙한 도구와 SDK를 활용하여 빠르게 개발을 시작할 수 있으므로 eSpace를 선택하는 것이 적합하다.

참고자료

- CIP-90
- Espace RPC Compatibility
- Espace EVM Compatibility

지갑(Wallets)

이 가이드는 지갑의 기본 개념, 목적, 그리고 Conflux Network에서 수행하는 역할을 이해하는 데 도움을 준다.

지갑이란 무엇인가?

블록체인과 암호화폐 환경에서 지갑(wallet)은 사용자가 블록체인 네트워크와 상호작용할 수 있도록 해주는 디지털 도구이다. 은행 계좌와 유사하게 디지털 자산을 송금, 수신 및 관리할 수 있는 기능을 제공한다. 그러나 전통적인 은행 계좌와 달리 이러한 지갑은 전적으로 사용자가 직접 통제할 수 있다.

지갑은 소프트웨어(데스크톱 또는 모바일 애플리케이션), 물리적 장치(하드웨어 지갑), 또는 종이 형태(페이퍼 월렛)로 존재할 수 있다. 각 유형은 보안성, 접근성 및 편의성 측면에서 서로 다른 장단점을 가진다.

Conflux Network의 지갑

Conflux Network에서 지갑은 매우 중요한 역할을 수행한다. 사용자는 지갑을 통해 Conflux 블록체인과 상호작용하며, CFX 및 Conflux Network 기반 토큰을 송수신할 수 있다.

Conflux 지갑의 주요 특징은 다음과 같다.

1. 개인키와 공개키(Private and Public Keys): 각 지갑은 암호학적 키 쌍을 가진다. 공개키는 은행 계좌번호와 유사하며 자금을 수신하는 데 사용된다. 개인키는 PIN 번호와 유사하며 거래 서명과 자산 접근에 사용된다. 개인키는 민감한 정보이므로 절대로 공유해서는 안 된다.
2. 주소(Address): 주소는 공개키로부터 생성되며, 자금을 수신하기 위해 다른 사람과 공유하는 값이다. 공개키를 더 짧고 관리하기 쉬운 형태로 표현한 것이다.
3. 보안(Security): Conflux Network의 지갑은 안전하게 설계되어 있다. 그러나 실제 보안 수준은 개인키 관리 방식에 크게 좌우된다. 많은 양의 CFX를 보관할 경우 더 높은 보안성을 제공하는 하드웨어 지갑 사용이 권장된다.
4. DApp과의 상호작용(Interacting with DApps): Conflux 지갑은 Conflux Network 기반 탈중앙화 애플리케이션(DApp)과 상호작용하는 데도 사용된다. 이를 통해 사용자는 탈중앙화 금융(DeFi), 게임 및 기타 다양한 애플리케이션에 참여할 수 있다.

지갑 선택

지갑 선택은 사용자의 요구사항에 따라 달라진다. 개발자라면 개발 환경과 쉽게 연동되는 지갑을 선호할 수 있으며, 일반 사용자라면 사용 편의성과 보안성을 우선적으로 고려할 수 있다.

Conflux Network는 다음을 포함한 여러 지갑을 지원한다.

- Fluent: Chrome(대부분의 Chromium 기반 브라우저)과 Firefox용 브라우저 확장 지갑으로, MetaMask와 유사하지만 Conflux Network 전용으로 설계되었다. Core Space와 eSpace를 모두 지원한다.
- Ledger: 높은 보안성으로 잘 알려진 하드웨어 지갑이다. Core Space와 eSpace를 모두 지원한다.
- MetaMask: Conflux Network eSpace와 연동하도록 설정할 수 있는 대표적인 지갑이다.

지원되는 지갑에 대한 자세한 정보는 관련 문서를 참고하기 바란다.

자산의 안전성은 개인키와 지갑을 얼마나 안전하게 관리하는지에 크게 좌우된다. 항상 개인키를 안전하게 보관하고, 보안이 확보된 인터넷 연결을 사용하며, 지갑 소프트웨어를 최신 버전으로 유지해야 한다.

스마트 컨트랙트 소개

스마트 컨트랙트란 무엇인가?

스마트 컨트랙트 개념은 1995년 Nick Szabo에 의해 처음 제안되었다. 스마트 컨트랙트는 계약을 정보화된 방식으로 배포, 검증 및 실행하기 위해 설계된 컴퓨터 프로토콜이다. 스마트 컨트랙트는 신뢰할 수 있는 제3자 없이도 거래를 실행할 수 있도록 하며, 거래 내역은 추적 가능하고 되돌릴 수 없다.

스마트 컨트랙트의 목적은 기존 계약보다 우수한 보안성을 제공하고 계약과 관련된 다양한 거래 비용을 절감하는 것이다.

Conflux Network에서 *스마트 컨트랙트(smart contract)*는 Conflux Network 상에서 실행되는 간단한 프로그램이다. 스마트 컨트랙트의 각 인스턴스는 Conflux Network 내 특정 주소에 존재하는 코드와 데이터의 집합이다. 블록체인 상태는 완전히 결정론적(deterministic)이므로 스마트 컨트랙트 연산은 모든 블록체인 노드에서 동일한 결과를 생성한다. 또한 스마트 컨트랙트는 블록체인 위에서 실행되므로, 블록체인의 탈중앙성과 위변조 불가능성은 컨트랙트 실행의 확실성과 보안성을 보장한다. 이에 따라 게임, 디지털 수집품(NFT), 온라인 투표 시스템, 금융 상품(DeFi) 등 다양한 탈중앙화 애플리케이션(dApp)이 스마트 컨트랙트를 기반으로 구축된다.

Conflux Network에는 사용자 계정과 스마트 컨트랙트 계정이라는 두 종류의 계정이 존재한다. 스마트 컨트랙트가 배포되면 이에 대응되는 스마트 컨트랙트 계정이 생성된다. 스마트 컨트랙트 계정은 CFX 잔액을 보유할 수 있으며 다른 계정과 상호작용할 수도 있다. 그러나 사용자가 직접 제어하는 것이 아니라 네트워크에 배포된 프로그램에 의해 제어된다. 사용자 계정은 스마트 컨트랙트에 정의된 함수를 실행하는 거래를 제출함으로써 스마트 컨트랙트와 상호작용할 수 있다. 스마트 컨트랙트는 전통적인 계약처럼 규칙을 정의할 수 있으며, 코드 실행을 통해 이를 자동으로 집행한다.

Nick Szabo는 자판기(vending machine)를 예로 들어 현실 세계의 계약상 의무가 어떻게 소프트웨어와 하드웨어 시스템에 프로그래밍될 수 있는지 설명하였다. 사용자는 정확한 금액의 동전을 넣으면 그 대가로 상품을 받을 수 있다고 기대한다. 마찬가지로 Conflux에서 스마트 컨트랙트는 특정 조건이 충족되었을 때 특정 작업을 수행하고 정해진 결과를 반환할 수 있다.

정의 및 개요

Conflux의 스마트 컨트랙트는 사전에 정의된 조건이 충족되면 실행되는 블록체인 상의 프로그램이다. 스마트 컨트랙트는 불변성(immutability)과 분산성을 가지므로, 한 번 배포되면 수정할 수 없으며 네트워크에 의해 실행된다.

스마트 컨트랙트의 동작 방식

스마트 컨트랙트는 Ethereum과 마찬가지로 Solidity와 같은 고급 프로그래밍 언어로 작성된다. 이들은 블록체인과 상호작용하여 데이터를 저장하거나 수정하고 거래를 전송하며, 중개자 없이 복잡한 프로세스를 자동화한다.

Conflux Network에서의 장점

Conflux의 스마트 컨트랙트는 강화된 보안성, 낮은 거래 비용, 향상된 효율성과 같은 장점을 제공한다. Conflux의 고유한 Tree-Graph 구조는 더 높은 처리량과 낮은 수수료를 가능하게 하므로 스마트 컨트랙트 배포에 적합한 플랫폼을 제공한다.

활용 사례

스마트 컨트랙트의 활용 분야는 매우 다양하며, 탈중앙화 금융(DeFi), 토큰 발행, 공급망 관리, 게임 등을 포함한다. 스마트 컨트랙트는 Conflux 기반 DApp(탈중앙화 애플리케이션)의 핵심 기반으로 기능하며 혁신적인 비즈니스 모델과 서비스를 가능하게 한다.

보안 고려사항

스마트 컨트랙트에서 보안은 가장 중요한 요소 중 하나이다. 스마트 컨트랙트는 불변성을 가지지만 코드 내 취약점은 공격자에 의해 악용될 수 있다. Conflux Network는 철저한 테스트와 감사(audit)를 포함한 스마트 컨트랙트 개발 모범 사례를 강조한다.

거래(Transactions)

거래(transaction)는 Conflux 계정을 보유한 외부 주체가 생성한 단일 명령이며, 발신자 계정의 개인키를 사용하여 암호학적으로 서명된다. 거래는 CFX(Conflux의 네이티브 통화)의 단순 전송, 토큰 전송(ERC20 또는 ERC721 등), 새로운 스마트 컨트랙트 배포, 또는 기존 스마트 컨트랙트 함수 실행을 포함할 수 있다. 거래는 블록체인에 데이터를 저장하거나 갱신할 수 있는 유일한 방법이다.

사전 요구사항

이 문서를 더 잘 이해하기 위해 먼저 Accounts 문서를 읽는 것을 권장한다.

거래란 무엇인가?

거래(transaction)는 외부 소유 계정(EOA, Externally-Owned Account), 즉 컨트랙트가 아닌 사람이 관리하는 계정에 의해 시작되는 행위를 의미한다. 예를 들어 Bob이 Alice에게 1 CFX를 전송한다면 Bob의 계정에서는 잔액이 차감되고 Alice의 계정에는 잔액이 추가되어야 한다. 이러한 상태 변경(state-changing) 행위는 거래 내에서 발생한다.

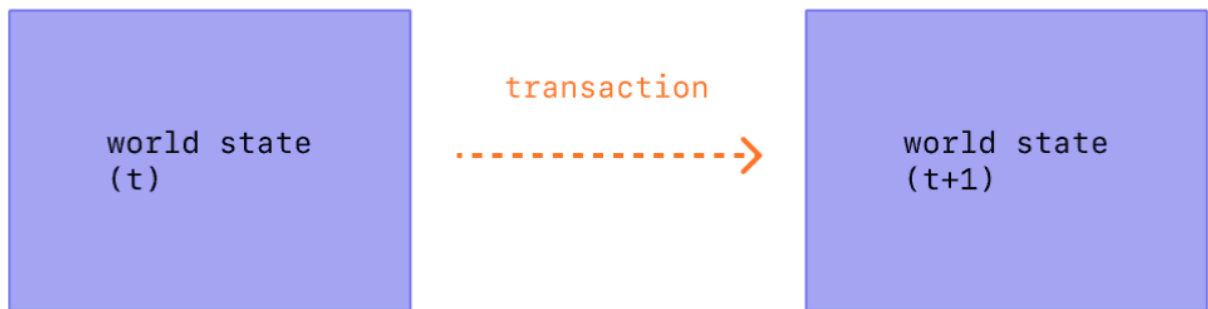


그림 5: 거래를 통한 전역 상태(World State) 전이

EVM 상태를 변경하는 거래는 네트워크 전체에 전파되어야 한다. 어떤 노드든 거래 실행 요청을 네트워크에 브로드캐스트할 수 있으며, 이후 검증자가 거래를 실행하고 그 결과 발생한 상태 변경을 네트워크 전체에 전파한다.

제출된 거래에는 다음 정보가 포함된다.

- **from** – 거래에 서명하는 발신자 주소. 컨트랙트 계정은 거래를 보낼 수 없으므로 반드시 외부 소유 계정이어야 한다.
- **recipient** – 수신 주소. 외부 소유 계정인 경우 가치가 전송되며, 컨트랙트 계정인 경우 컨트랙트 코드가 실행된

다.

- **signature** – 발신자를 식별하는 서명. 발신자의 개인키로 거래에 서명하여 생성되며, 발신자가 해당 거래를 승인했음을 증명한다.
- **nonce** – 계정의 거래 순서를 나타내는 순차 증가 카운터.
- **value** – 발신자에서 수신자로 전송되는 CFX 수량(단위는 Drip이며, $1 \text{ CFX} = 1e + 18 \text{ Drip}$).
- **input data** – 임의 데이터를 포함할 수 있는 선택적 필드.
- **gasLimit** – 거래가 소비할 수 있는 최대 가스 단위 수. EVM은 각 연산 단계에 필요한 가스 단위를 정의한다.
- **gasPrice** – 소비된 가스에 대해 검증자에게 팁으로 지급되는 가스 가격.
- **chainId** – 리플레이 공격(replay attack)을 방지하기 위해 사용되는 블록체인 식별자.

Core Space 거래에는 추가적으로 다음 정보가 포함된다.

- **storageLimit** – 거래가 사용할 수 있는 최대 저장 공간 크기.
- **epochHeight** – 거래 만료 시간을 설정하기 위해 사용되는 블록체인 에폭 번호.

가스 수수료(Gas Fee)

거래는 수수료를 필요로 하며 검증된 블록에 포함되어야 한다. 수수료는 CFX로 지불되며, **gasCharged**와 **gasPrice**를 곱하여 계산된다.

가스 수수료는 채굴자에게 보상을 제공하여 블록 패키징, 검증 및 블록체인 보안 유지에 대한 동기를 부여한다.

구체적인 계산 방식은 Transaction Fee 문서를 참고하기 바란다.

거래 생명주기(Transaction Lifecycle)

거래가 제출되면 다음 과정이 진행된다.

1. 거래 해시가 암호학적으로 생성된다.
`0x97d99bc7729211111a21b12c933c949d4f31684f1d6954ff477d0477538ff017`
2. 생성된 거래는 네트워크에 브로드캐스트되며, 다른 대기 중 거래들과 함께 거래 풀(transaction pool)에 추가된다.
3. 검증자는 해당 거래를 선택하여 블록에 포함시켜야 하며, 이를 통해 거래가 검증되고 "성공(successful)" 상태로 간주된다.
4. 시간이 지나면서 거래가 포함된 블록은 "정당화됨(justified)" 상태를 거쳐 "최종 확정(finalized)" 상태로 승격된다. 이러한 단계는 거래가 성공적으로 처리되었으며 향후 변경되지 않을 것이라는 확신을 크게 높여준다. 블록이 "최종 확정" 상태에 도달하면 수십억 달러 규모의 비용이 필요한 네트워크 수준 공격이 아닌 이상 변경될 수 없다.

거래 생명주기에 대한 보다 자세한 내용은 Transaction Lifecycle 문서를 참고하기 바란다.

거래 상태(Transaction Status)

블록에 포함된 거래는 최종적으로 실행되며 거래 영수증(Transaction Receipt)을 생성한다. 그러나 모든 거래가 성공적으로 실행되는 것은 아니며, 일반적으로 거래는 성공(Success) 또는 실패(Failure) 상태를 가진다.

eSpace 거래의 경우 Receipt 내 status 필드를 통해 실행 결과를 확인할 수 있으며, 1은 성공, 0은 실패를 의미한다.

Core Space 거래의 경우 Receipt 내 outcomeStatus 필드를 통해 실행 결과를 확인할 수 있으며, 0은 성공, 1은 실패, 2는 건너뛴(skipping, Conflux의 DAG 구조로 인해 발생) 을 의미한다.

Receipt에는 이 외에도 블록 정보, 이벤트 정보 등 거래 실행에 대한 다양한 정보가 포함된다.

특수 사례: Nonce 증가 없이 실패하는 경우

일반적으로 거래가 실패하더라도 발신자의 nonce는 증가하며 사용자는 가스 수수료를 지불해야 한다. 그러나 v2.4 하드 포크에서는 특수한 사례가 도입되었다. 비피벗(non-pivot) 블록에서 거래 수수료 설정이 소각 수수료를 충당하기에 충분하지 않은 경우 거래는 실패하지만 발신자의 nonce는 증가하지 않는다. 자세한 내용은 Base Fee 문서를 참고하기 바란다.

상세 정보

거래에 대한 보다 자세한 설명은 Core Space의 거래 설명 문서를 참고하기 바란다.

계정 및 주소(Accounts and Addresses)

개요

Conflux의 계정은 CFX를 보관한다는 점에서 "은행 계좌"와 유사하다. 사용자는 계정을 생성 및 관리하고, CFX를 입금하며, 거래를 전송할 수 있다. 계정 주소는 계정을 식별하는 고유 문자열이며, Conflux VM의 대규모 상태 테이블에서 계정 정보와 잔액을 조회하는 데 사용된다.

참고

계정 구조, 계정 내용 및 주소 생성 규칙은 Core Space와 eSpace에서 약간 다르다.

주소(Address)

계정 주소는 은행 계좌번호와 마찬가지로 계정을 식별하며 ConfluxScan에서 확인할 수 있다. 다만 주소 형식은 Core Space와 eSpace 간에 다르다. Core Space는 CIP-37 인코딩 방식을 사용하며, eSpace는 Ethereum과 동일한 주소 형식을 사용한다.

다음은 두 공간의 주소 형식 예시이다.

```
// eSpace 주소
0x1e97870f263700f46aa00d967821199b9bc5a120

// Core Space 메인넷 주소
cfx:aatktb2te25ub7dmyag3p8bbdgr31vrbeackztm2rj

// Core Space 테스트넷 주소
cfxtest:aatktb2te25ub7dmyag3p8bbdgr31vrbeajcg9pwkc
```

계정 유형

계정에는 외부 소유 계정(EOA)과 컨트랙트 계정(contract account)의 두 가지 유형이 존재한다. EOA는 해당 계정의 개인키를 보유한 사람이 제어하며, 컨트랙트 계정은 네트워크에 배포된 스마트 컨트랙트 코드에 의해 제어된다.

외부 계정과 공개키-개인키 쌍

EOA는 공개키와 개인키로 구성된 암호학적 키 쌍을 가진다. 개인키는 64자리 16진수 문자열로 구성되며 거래 서명과 계정 자산에 대한 통제권을 제공한다. 공개키 암호화 기술은 거래 위조를 방지하고 발신자가 거래 요청의 진위를 증명할 수 있도록 한다. 이를 통해 악의적인 사용자가 허위 거래를 브로드캐스트하는 것을 방지할 수 있다.

다음은 개인키 예시이다.

```
c5eca1e5de819725cf7c6764f4bba7eea95549a40275b21eaff91554c5...
```

공개키는 타원곡선 암호 알고리즘(Elliptic Curve Cryptography Algorithm)을 통해 개인키로부터 계산된다.

```
0xa82d8039606ea598798ae1c995e2dbad90561d67ffa9555f96e0bc3...
```

EOA 주소는 공개키로부터 계산된다.

```
// eSpace 주소 (EIP-55 체크섬 형식)  
0x7058Ce27AF14B05943B879E530Df642867dFcf57
```

```
// Core Space 메인넷 주소 (CIP-37 형식)  
cfx:aajfvxvhz6mna0md1b68mpg9puygt18tm6nynadnf6
```

스마트 컨트랙트 계정

스마트 컨트랙트도 주소를 가지며, 사용자는 거래를 전송하여 이들과 상호작용할 수 있다. 컨트랙트 주소는 배포 시점에 결정되며, 계산 규칙은 Core Space와 eSpace에서 서로 다르다.

계정 유형 비교

공통점

- 두 유형 모두 CFX를 수신, 보유 및 전송할 수 있다.
- 두 유형 모두 네트워크 내 스마트 컨트랙트와 상호작용할 수 있다.

차이점

외부 계정

- 외부 계정 생성에는 CFX 또는 기타 자원이 필요하지 않다.
- 다른 계정으로 거래를 전송할 수 있다.
- 외부 계정 간 거래는 CFX 또는 토큰 전송으로만 제한된다.

스마트 컨트랙트

- 스마트 컨트랙트 생성에는 네트워크 저장 공간 및 연산 자원을 사용하므로 비용이 발생한다.
- 거래는 수신된 거래에 대한 응답으로 다른 컨트랙트에만 전송할 수 있다.

- 외부 계정에서 컨트랙트 계정으로 전송된 거래는 스마트 컨트랙트 코드를 실행하여 토큰 전송, 신규 컨트랙트 생성 등 다양한 작업을 수행할 수 있다.

가스 및 수수료(Gas and Fees)

가스란 무엇인가?

블록체인 기술에서 "가스(gas)" 개념은 자동차의 연료와 유사하다. 자동차가 주행하기 위해 연료를 소비하며 더 멀리 갈수록 더 많은 연료가 필요한 것처럼, Conflux에서 가스는 연산 수행에 필요한 계산 노력(computational effort)을 측정하는 단위이다. 거래의 연산 요구량이 클수록 더 많은 가스를 소비한다.

보다 구체적으로 설명하면, Conflux의 모든 거래는 가상머신(VM)에서 처리된다. 여기에는 단순한 CFX 전송뿐만 아니라 스마트 컨트랙트 호출도 포함된다. 각 거래는 다양한 opcode로 구성된 일련의 연산을 순차적으로 실행하며, opcode마다 요구되는 연산량이 다르다. 관련 EVM opcode 목록은 별도 문서를 참고할 수 있다.

참고

Conflux Core Space에서는 거래 실행 중 필요한 데이터를 저장하기 위해 가스 외에도 저장 담보(storage collateral)라는 자원이 사용된다.

Gas Limit, Gas Used 및 Gas Charged

자동차의 연료 탱크 크기에 한계가 있는 것처럼 블록체인 거래 역시 사용할 수 있는 가스 양에 제한이 있다. 각 거래에는 gas 필드(또는 gas limit)가 포함되며, 이는 거래가 소비할 수 있는 최대 가스량을 의미한다. 이러한 제한은 거래가 무한 루프에 빠지는 것을 방지한다. 거래가 지정된 가스를 모두 소비한 상태에서 완료되지 못하면 실패한다. 튜링 완전(Turing-complete) 언어를 사용하기 때문에 정지 문제(Halting Problem)로 인해 실행 전에는 거래 성공 여부를 이론적으로 예측할 수 없으므로 gas limit은 필수적이다.

일반적으로 거래는 gas limit의 일부만 사용하며 이를 gas used라 한다. Conflux에서는 gas limit이 적절하게 설정된 경우, 사용되지 않은 가스는 전액 환불되어 추가 비용이 발생하지 않는다. 그러나 gas limit을 지나치게 높게 설정하면 사용하지 않은 가스에 대해 전액 환불받지 못할 수 있다.

gas charged는 사용자가 실제로 비용을 지불하는 가스량이며 다음 공식으로 계산된다.

$$\text{gasCharged} = \max(\text{gasUsed}, \text{RoundUp}(3/4 \times \text{gasLimit})) \quad (3)$$

따라서 불필요한 비용을 피하기 위해 적절한 gas limit 설정이 중요하다. 너무 낮으면 거래가 실패하고, 너무 높으면 과도한 비용을 지불할 수 있다.

다음은 gas limit, gas used, gas charged의 관계를 설명하는 예시이다.

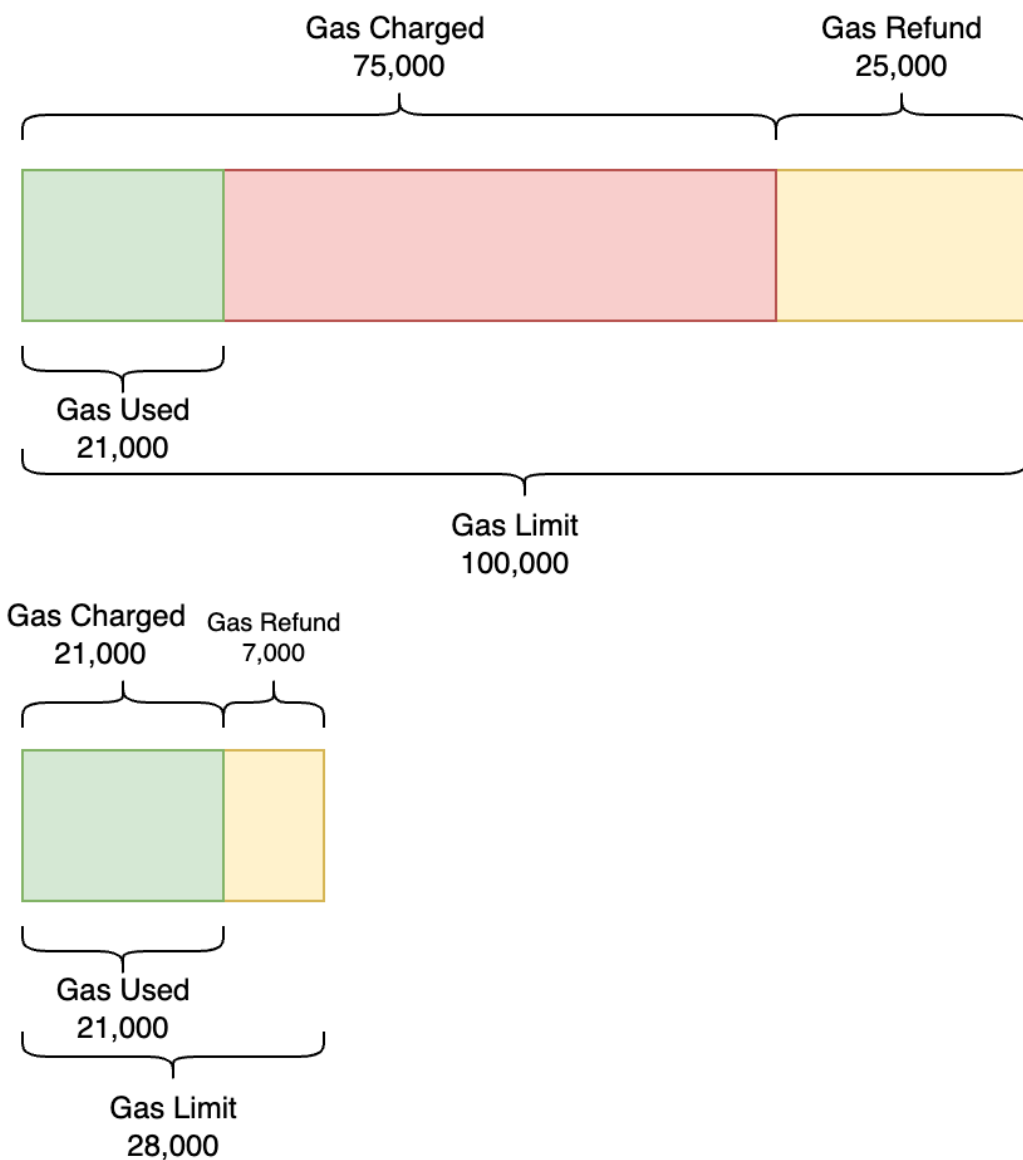


그림 6: Gas Limit, Gas Used, Gas Charged 및 환불 관계 예시

가스 비용이 21,000인 일반적인 CFX 전송을 예로 들어보자.

1. gas limit을 100,000으로 설정하면 gas charged는 75,000($\max(21000, 100000 \times 3/4)$)이 되며, 환불은 25,000 가스만 이루어진다. 결과적으로 실제 사용량 대비 54,000 가스의 추가 비용이 발생한다.
2. gas limit을 28,000으로 설정하면 gas charged는 실제 사용량인 21,000과 동일해지며 추가 비용이 발생하지 않는다.

거래 Gas Limit 설정

대부분의 사용자는 이러한 세부 사항을 직접 신경 쓸 필요가 없다. 일반적으로 지갑(Fluent Wallet, MetaMask 등)이 비용을 최소화할 수 있도록 적절한 가스 설정을 자동으로 수행하기 때문이다.

개발자의 경우 SDK가 gas limit을 지정하지 않으면 적절한 값을 자동으로 선택한다. 또한 `cfx_estimateGasAndCollateral`을 사용하여 거래에 적합한 gas limit을 계산할 수 있다.

EIP-150의 영향으로 인해 gas limit을 정확히 gas used와 동일하게 설정할 경우 거래가 실패할 수 있다는 점에 유의해야 한다.

가스 수수료(Gas Fee)

블록체인의 모든 거래는 실행을 위해 연산 자원을 필요로 한다. 이러한 자원 사용에 대한 보상과 스팸 방지를 위해 사용자는 가스 수수료를 지불해야 한다. 수수료는 다음과 같이 계산된다.

$$\text{gasCharged} \times \text{feePerGas} \quad (4)$$

feePerGas를 지정하는 방법은 baseFeePerGas 개념을 설명한 이후 다룬다.

기본 가스 수수료와 우선순위 수수료

거래 가스 수수료는 기본 수수료(base fee)와 우선순위 수수료(priority fee, tip)로 구성된다.

1. 기본 수수료(Base Fee): 각 Conflux 에폭에서 피벗 블록은 baseFeePerGas 필드를 포함하며, 이는 거래가 블록에 포함되기 위해 필요한 최소 수수료를 의미한다. 사용자가 설정한 거래 수수료가 이 값보다 낮으면 해당 거래는 블록에 포함되지 않는다. baseFeePerGas는 온체인 혼잡도에 따라 조정된다. Conflux v2.4 하드포크 이후 최대 블록 크기와 거래 gas limit 총합이 두 배로 증가하였다. 이를 통해 네트워크는 일시적으로 더 높은 부하를 처리할 수 있게 되었다. 거래량이 기존 블록 가스 한도(현재는 gas target)를 초과하면 해당 블록의 가스 기본 수수료가 상승한다. 이를 통해 수요가 높은 시기에 사용자가 더 높은 비용을 지불하도록 한다.
2. 우선순위 수수료(Priority Fee): 사용자가 자신의 거래를 우선 처리하도록 채굴자에게 추가적으로 지급하는 수수료이다. 더 높은 우선순위 수수료를 설정할수록 채굴자는 해당 거래를 더 빠르게 포함시킬 유인을 갖게 된다.

이러한 수수료 구조를 이해하는 것은 블록체인과 효율적으로 상호작용하고 거래를 적시에 처리하기 위해 중요하다.

고정 수수료와 동적 수수료

참고

설명을 단순화하기 위해 CIP-1559의 CIP-137 Base Fee Sharing과 관련된 특정 예외 상황은 생략한다.

사용자는 거래 수수료를 설정하는 두 가지 방법을 사용할 수 있다.

고정 수수료(Fixed Fee)

사용자는 거래에 gasPrice를 직접 설정할 수 있다. 전체 가스 수수료는 다음과 같이 계산된다.

$$\text{gasPrice} \times \text{gasCharged} \quad (5)$$

채굴자에게 지급되는 우선순위 수수료는 gasPrice와 baseFeePerGas의 차이에 gasCharged를 곱한 값이다.

$$(\text{gasPrice} - \text{baseFeePerGas}) \times \text{gasCharged} \quad (6)$$

동적 수수료(Dynamic Fee)

동적 수수료 방식은 가스 비용을 보다 정교하게 제어할 수 있도록 한다.

- `maxFeePerGas`: 사용자가 지불할 의사가 있는 가스 단위당 최대 총수수료이다. 여기에는 `baseFeePerGas`와 `priorityFeePerGas`가 모두 포함된다.
- `maxPriorityFeePerGas`: 사용자가 채굴자에게 직접 지급할 의사가 있는 가스 단위당 최대 우선순위 수수료이다. 실제 `priorityFeePerGas`는 다음 두 값 중 더 작은 값으로 결정된다.

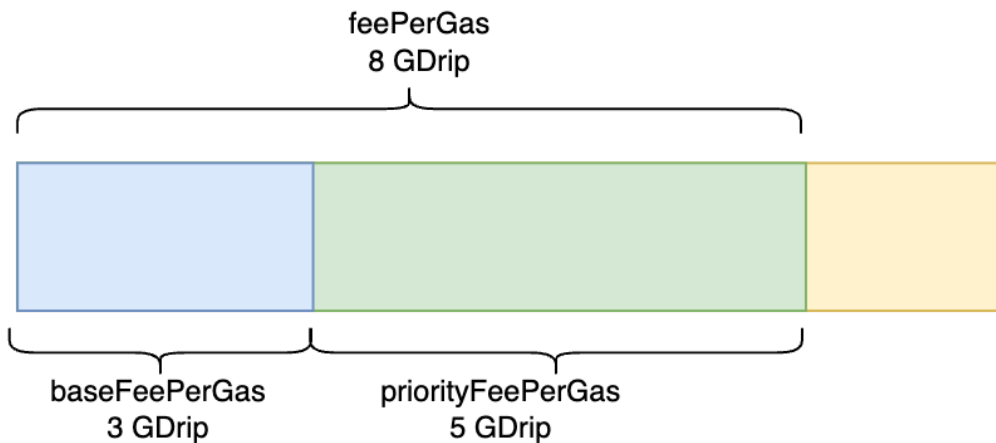
$$\text{maxFeePerGas} - \text{baseFeePerGas} \tag{7}$$

및

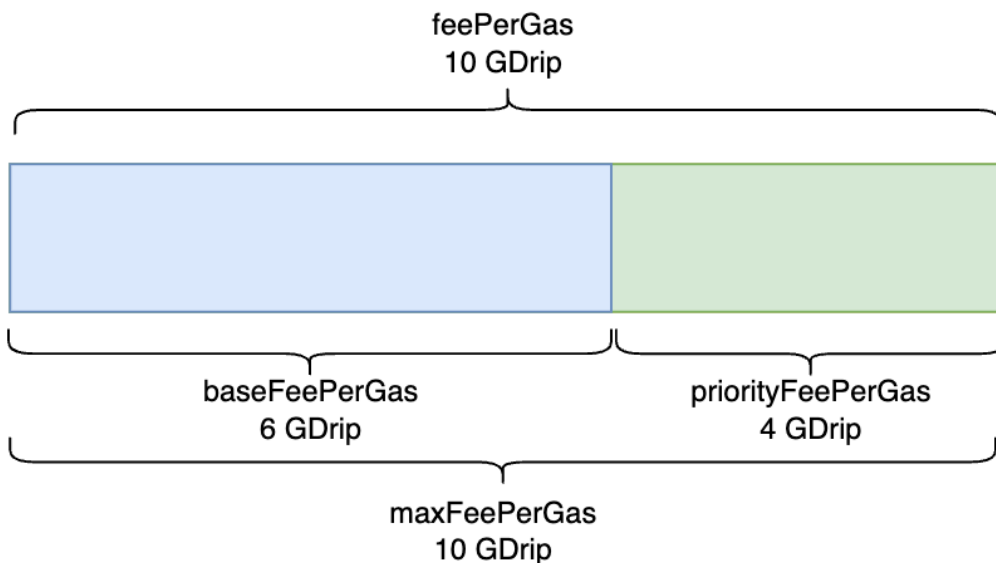
$$\text{maxPriorityFeePerGas} \tag{8}$$

이를 통해 기본 수수료가 `maxFeePerGas` 대부분을 차지하는 경우 남은 금액만 우선순위 수수료로 사용된다.

예를 들어 `maxFeePerGas`를 10 GDrip, `maxPriorityFeePerGas`를 5 GDrip으로 설정한 경우를 살펴보자.



(1) `maxFeePerGas` = 10GDrip, `maxPriorityFee` = 5 GDrip, `baseFeePerGas` = 3 GDrip



(2) `maxFeePerGas` = 10GDrip, `maxPriorityFee` = 5 GDrip, `baseFeePerGas` = 6 GDrip

그림 7: 동적 수수료 계산 예시

- 첫 번째 시나리오에서는 `baseFeePerGas`가 충분히 낮아 기본 수수료와 최대 우선순위 수수료가 모두 `maxFeePerGas` 범위 내에 포함되므로 `priorityFeePerGas`는 5 GDrop이 된다.
- 두 번째 시나리오에서는 `baseFeePerGas`가 6 GDrop까지 상승한다. 이 경우 `maxFeePerGas`는 기본 수수료와 전체 `maxPriorityFeePerGas`를 모두 충당하기에 충분하지 않다. 그럼에도 거래는 정상 처리되며, 최대 수수료에서 기본 수수료를 차감한 나머지 잔액이 우선순위 수수료로 사용된다.

가스 수수료를 줄이는 방법

가스 수수료를 최소화하려면 다음 전략을 고려할 수 있다.

1. 낮은 Fee Per Gas 선택: `baseFeePerGas`는 네트워크 혼잡도에 따라 변동한다. 낮은 `maxFeePerGas`를 설정하면 `baseFeePerGas`가 해당 수준 이하로 내려갔을 때 거래가 처리된다. 네트워크 활동이 적은 시점에 거래를 실행하면 상당한 비용 절감이 가능하다.
2. 가스 소비량 감소: 스마트 컨트랙트 개발자라면 가스 최적화가 중요하다. 데이터 저장 방식을 최적화하고, 함수 실행을 개선하며, 효율적인 반복문 구조를 사용하는 데 집중해야 한다. 가스 사용량 절감에 대한 자세한 내용은 Gas Optimization 튜토리얼을 참고하기 바란다.

Base Fee

Conflux에서 RPC를 통해 조회한 블록 데이터에는 `baseFeePerGas` 필드가 포함되어 있으며, 이는 네트워크 혼잡도를 나타내고 거래에 필요한 최소 가스 단가를 결정한다. 이 메커니즘은 CIP-1559의 일부로 Conflux v2.4 하드포크에서 도입되었으며, Ethereum의 Base Fee 모델을 기반으로 하되 Conflux의 Tree-Graph 블록 구조에 맞게 조정되었다. 이러한 조정 사항은 CIP-1559와 CIP-137에 문서화되어 있다.

본 문서는 Conflux의 Base Fee와 그 동작 방식에 대한 개요를 제공한다. Ethereum 구현과의 비교는 Differences from Ethereum Base Fee 섹션을 참고하기 바란다.

거래 패키징을 위한 최소 가스 가격

`baseFeePerGas`는 거래가 블록에 포함되기 위해 요구되는 최소 가스 단가이다. 거래의 `gasPrice`(Legacy 또는 Type 1 거래) 또는 `maxFeePerGas`(Type 2 거래)가 블록의 `baseFeePerGas`보다 낮으면 해당 거래는 블록에 포함되지 않는다.

네트워크 혼잡도가 높은 시기에는 `baseFeePerGas`가 상승하므로 사용자는 거래 처리를 위해 더 높은 수수료를 지불해야 한다. 반대로 혼잡도가 감소하면 `baseFeePerGas`도 하락하며, 더 낮은 수수료를 설정한 거래도 블록에 포함될 수 있다.

Type 2 거래는 `maxFeePerGas`와 `maxPriorityFeePerGas` 필드를 활용할 수 있으며, 이를 통해 사용자는 높은 `maxFeePerGas`를 설정하더라도 실제로는 현재 네트워크 상황에 따라 결정된 수수료만 지불한다. 동적 수수료에 대한 자세한 내용은 Gas and Fees 문서를 참고하기 바란다.

baseFeePerGas 계산 방식

각 블록의 `baseFeePerGas`는 이전 블록의 `baseFeePerGas`와 현재 블록의 가스 사용량을 기반으로 계산된다.

$$\frac{\sum(\text{transaction gas limit})}{\text{gas target}} \quad (9)$$

gas target은 공간(space)의 가스 한도(gas limit)의 50%이다. 예를 들어 Core Space의 gas limit은 일반적으로 54,000,000이며, 따라서 gas target은 27,000,000이다. eSpace에서는 gas limit이 일반적으로 30,000,000이고 gas target은 15,000,000이다.

거래 gas limit 총합이 gas target을 초과하면 baseFeePerGas는 상승하며, 그렇지 않으면 하락한다. 블록당 baseFeePerGas 변화율의 최대치는 12.5%이다. 빈 블록(empty block)은 12.5% 감소를 유발하며, 가득 찬 블록(full block)은 12.5% 증가를 유발한다.

현재 블록의 baseFeePerGas는 이전 블록의 baseFeePerGas와 deltaRate를 사용하여 계산된다.

$$\text{newBaseFeePerGas} = \text{previousBaseFeePerGas} \times (1 + \text{deltaRate}) \quad (10)$$

Core Space에서는 previousBaseFeePerGas가 직접 부모 블록(parent block)에서 가져오며, eSpace에서는 eSpace 거래가 특정 높이에서만 포함되므로 다섯 블록 전의 부모 블록 값을 사용한다.

수수료 소각(Fee Burn)과 Base Fee 공유

Ethereum의 EIP-1559에서는 Base Fee 전부가 소각되지만, Conflux의 CIP-137은 Base Fee의 일부를 채굴자에게 배분한다. 이 비율은 초기값이 50%이며 온체인 DAO 투표를 통해 결정된다.

Conflux의 거래 수수료는 다음 세 부분으로 구성된다.

1. 소각되는 Base Fee 부분
2. 채굴자에게 분배되는 Base Fee 부분
3. 우선순위 수수료(Priority Fee, 채굴자에게 지급)

이 Base Fee 소각 비율은 비피벗(non-pivot) 블록 거래 처리에도 영향을 미치며, 이에 대한 메커니즘은 다음 섹션에서 설명한다.

에폭 단위의 통일된 Base Gas Price

블록의 Base Gas Price는 채굴자가 거래를 포함시키기 위한 최소 가스 가격을 결정하지만, 실제 실행 시에는 전체 에폭(epoch)의 Base Gas Price가 피벗 블록의 baseFeePerGas에 의해 결정된다. 예를 들어 피벗 체인이 Genesis ← A ← C ← E ← H인 경우, C 에폭에 속한 블록 B의 Base Gas Price는 C의 baseFeePerGas에 의해 결정된다.

Ethereum Base Fee와의 차이점

현재 블록의 Gas Limit을 기반으로 한 조정

Ethereum의 EIP-1559에서는 부모 블록의 실제 가스 사용량(gas used)을 기준으로 Base Fee를 조정한다. 반면 Conflux의 CIP-1559는 현재 블록의 gas limit을 기준으로 Base Fee를 조정한다.

CIP-1559에서는 이러한 차이에 대해 다음과 같이 설명한다. 지연 실행(deferred execution) 메커니즘이 존재하기 때문에 실제 가스 사용량을 기준으로 Base Gas Price를 조정할 수 없으며, 따라서 gas limit을 사용한다. 또한 이전 블록의 gas limit을 사용할 경우 eSpace 블록에서는 다섯 블록 전의 거래 블록을 참조해야 하므로 합의 과정의 오버헤드가 증가하게 된다.

수수료 소각

Ethereum에서는 Base Fee 전액이 소각되지만, Conflux에서는 Base Fee의 일부만 소각되고 나머지는 채굴자에게 지급된다. 이 비율은 Conflux 온체인 DAO 투표를 통해 결정되며 초기값은 50%이다. 소각된 가스 수수료는 거래 Receipt의 burntGasFee 필드에서 확인할 수 있다.

실행 시 검증 방식

Conflux는 거래가 블록에 포함된 이후 5개 에폭 뒤에 실행되는 지연 실행 메커니즘을 사용하기 때문에 실행 단계에서 추가적인 Base Fee 검사를 수행한다. 실행 시 최소 가스 가격은 `block.baseFeePerGas`가 아니라 다음 값이다.

`pivotBlock.baseFeePerGas * burntRatio`

이를 통해 거래 수수료 중 반드시 소각되어야 하는 부분이 충분히 확보되도록 하며, 나머지 수수료는 채굴자에게 지급된다.

거래의 가스 가격이 해당 임계값을 충족하지 못하면 거래는 실패하지만 발신자의 nonce는 증가하지 않는다. 이후 Conflux 노드 구현체는 원래 거래를 노드의 mempool로 다시 전송하여, 네트워크 상황이 개선되었을 때 향후 블록에 다시 포함될 수 있도록 한다.

거버넌스 개요(Governance Overview)

거버넌스 모델 — CFX 투표

프로토콜 변경 사항과 생태계 개발에 사용되는 자금은 궁극적으로 DAO에 의해 관리된다. Conflux 생태계 참여자는 누구나 일정 기간 동안 토큰을 잠금(locking)하여 투표권을 획득할 수 있다. 투표권은 다음 공식에 따라 부여된다.

$$\text{분기 수(number of quarters)} \times \text{토큰 수(number of tokens)} \times 0.25$$

예시는 다음과 같다.

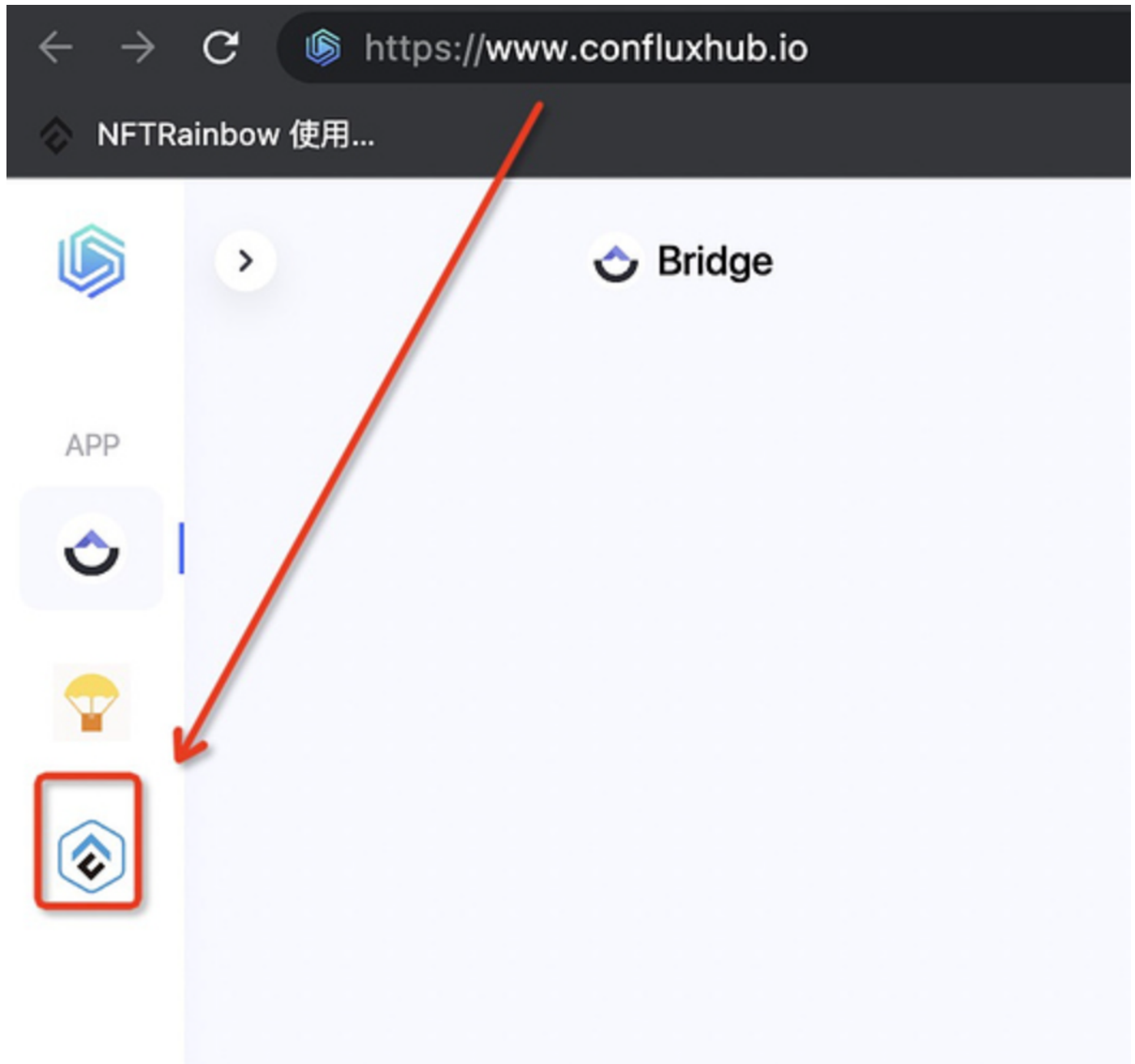
- 잠금 기간이 1분기 미만: 투표권 없음
- 잠금 기간이 1분기 초과: 1 CFX당 0.25표
- 잠금 기간이 6개월 초과: 1 CFX당 0.5표
- 잠금 기간이 1년 초과: 1 CFX당 1표

사용자는 투표권 획득을 위해 토큰을 잠그더라도 스테이킹 이자를 받을 권리는 유지된다. 그러나 토큰을 잠근 이후에는 인출할 수 없으며 잠금 기간을 단축할 수도 없다.

CFX 투표 웹사이트: <https://www.confluxhub.io/>

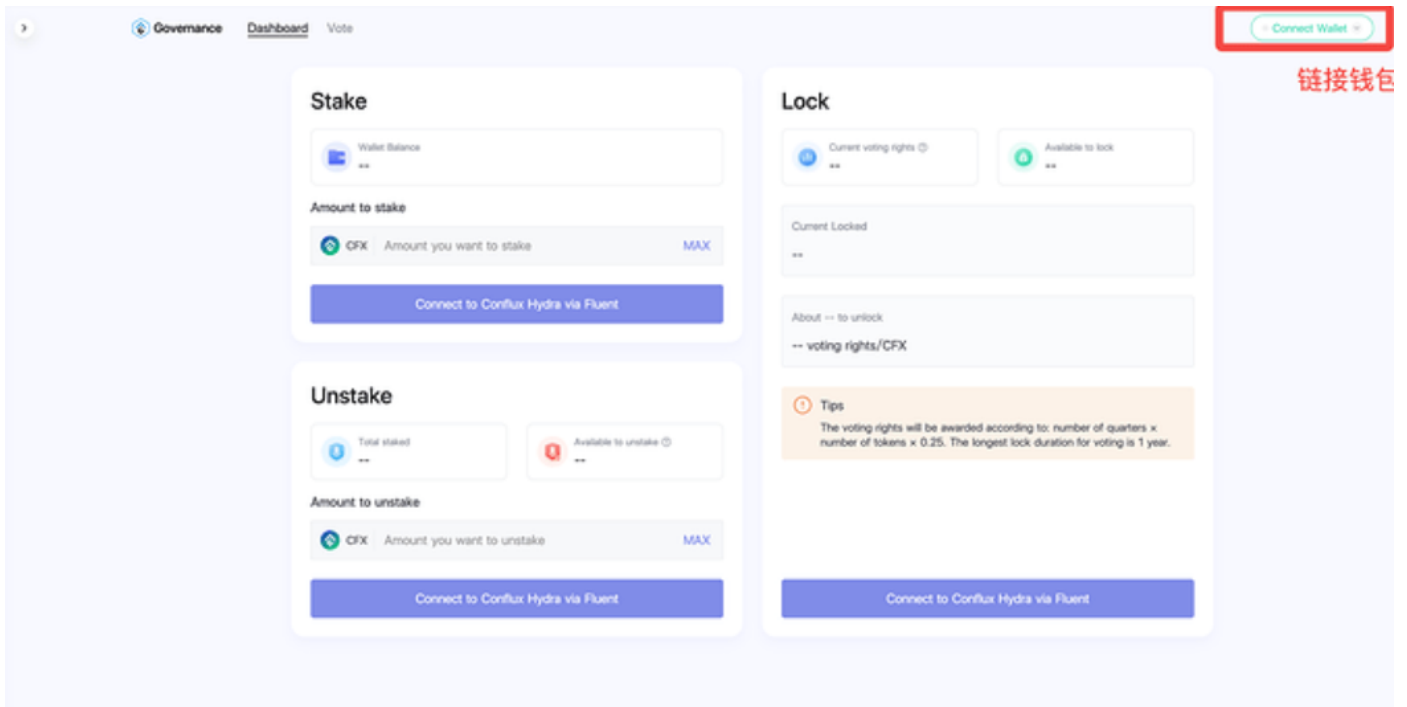
ConfluxHub 거버넌스 플랫폼에서 CFX 스테이킹

1. <https://www.confluxhub.io/> 에 접속한다.
2. 왼쪽 프로젝트 바에서 Governance 아이콘을 클릭하여 Governance Dashboard로 이동한다.



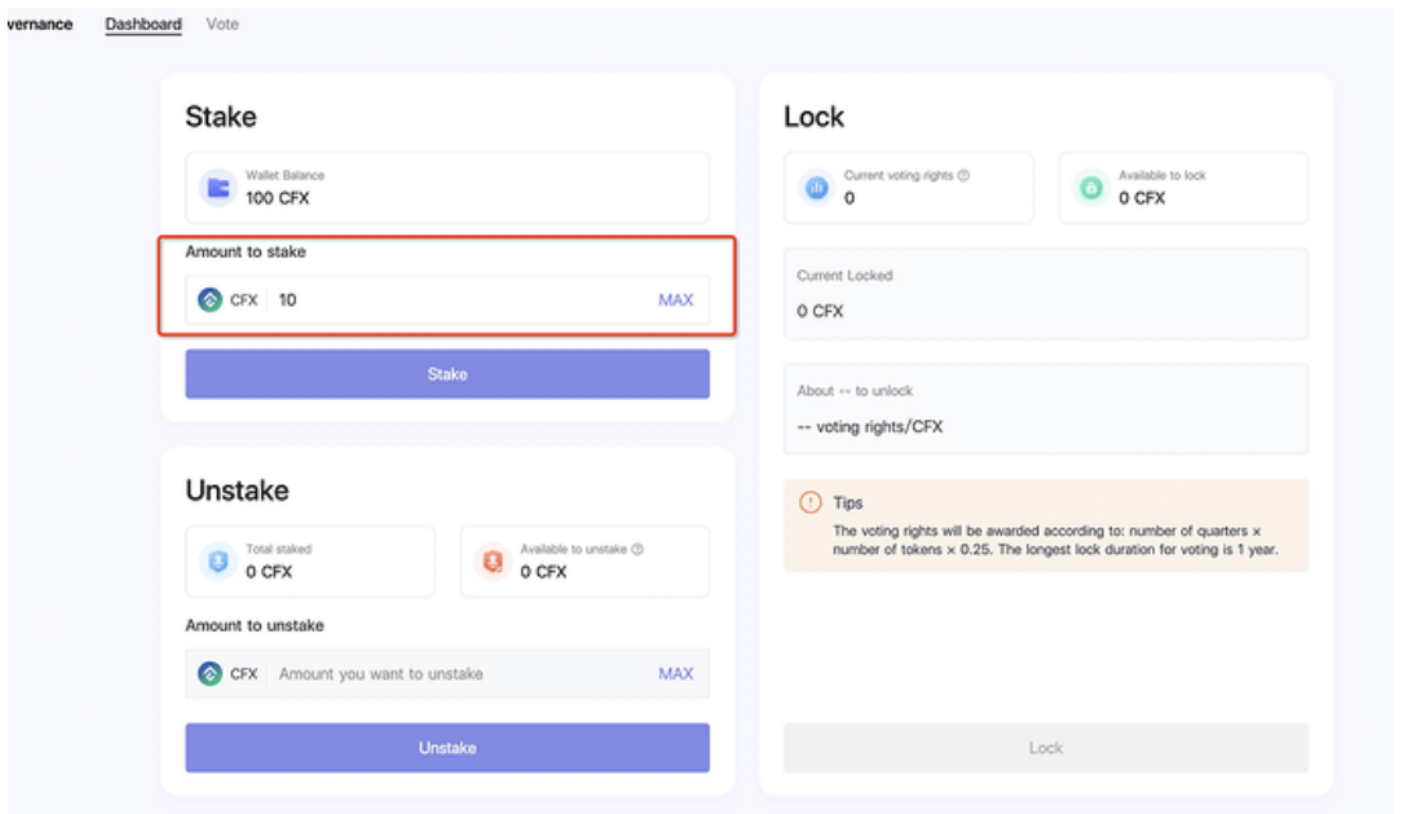
Governance Dashboard 이동

3. 우측 상단의 Connect Wallet을 클릭하여 지갑을 연결한다.



지갑 연결

4. 스테이킹할 CFX 수량을 입력한 후 Stake를 클릭하여 스테이킹을 완료한다.



CFX 스테이킹

5. Lock을 클릭하여 잠금 작업을 수행하고, 투표권으로 교환할 CFX 수량을 입력한다. 투표권은 다음 공식에 따라 부여된다.

$$\text{분기 수(number of quarters)} \times \text{토큰 수(number of tokens)} \times 0.25$$

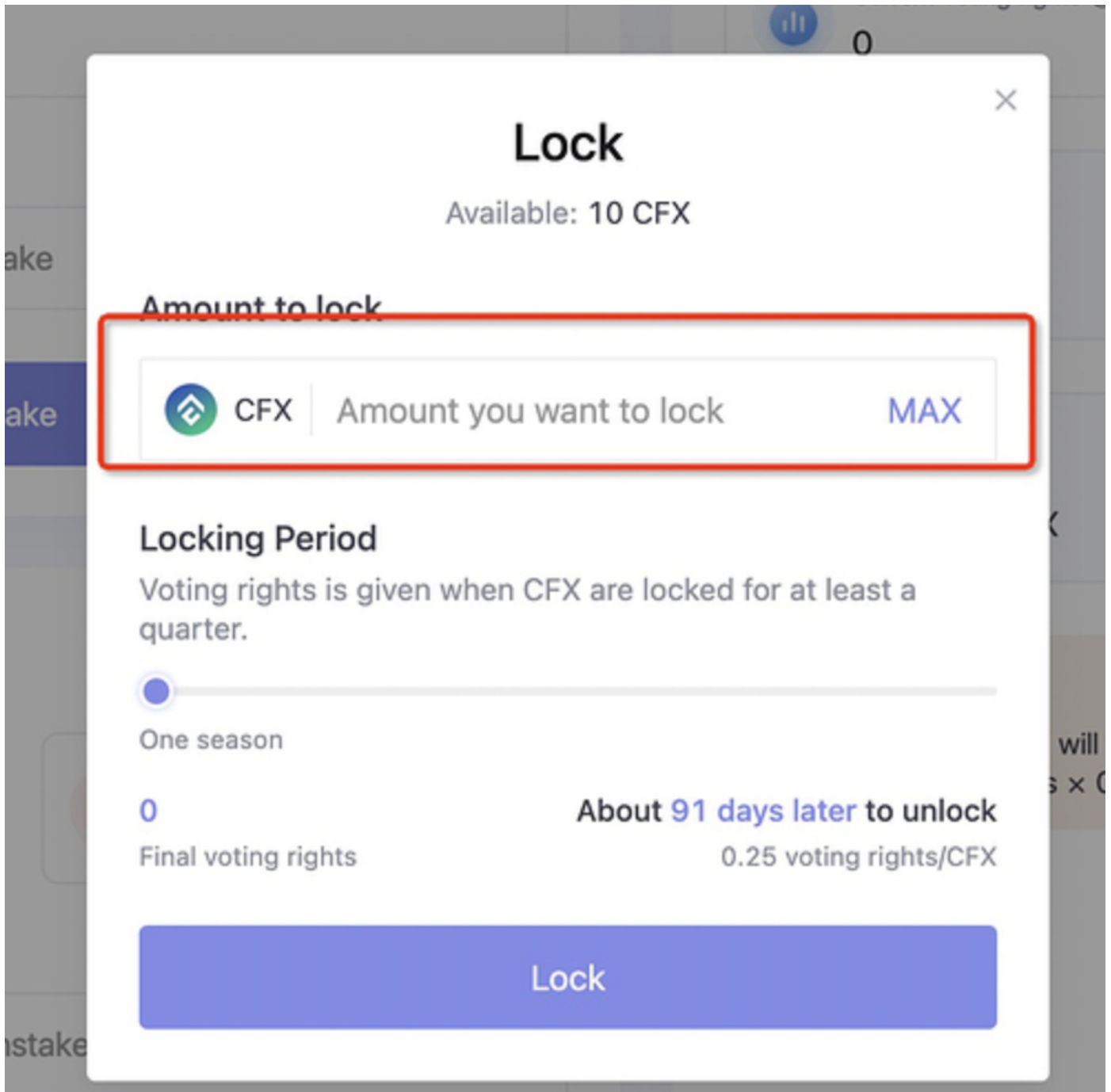
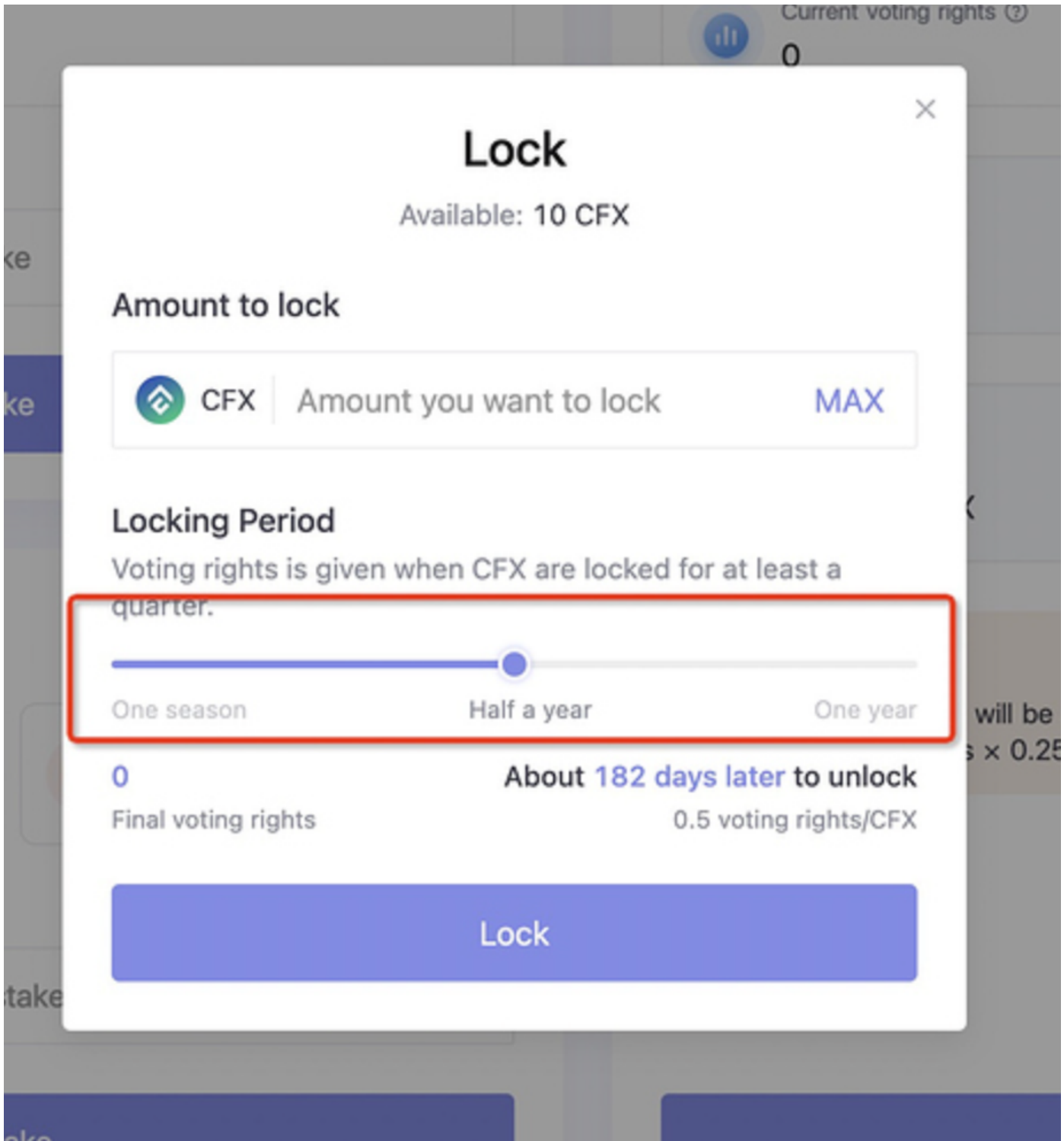


그림 4: 투표권 획득을 위한 토큰 잠금

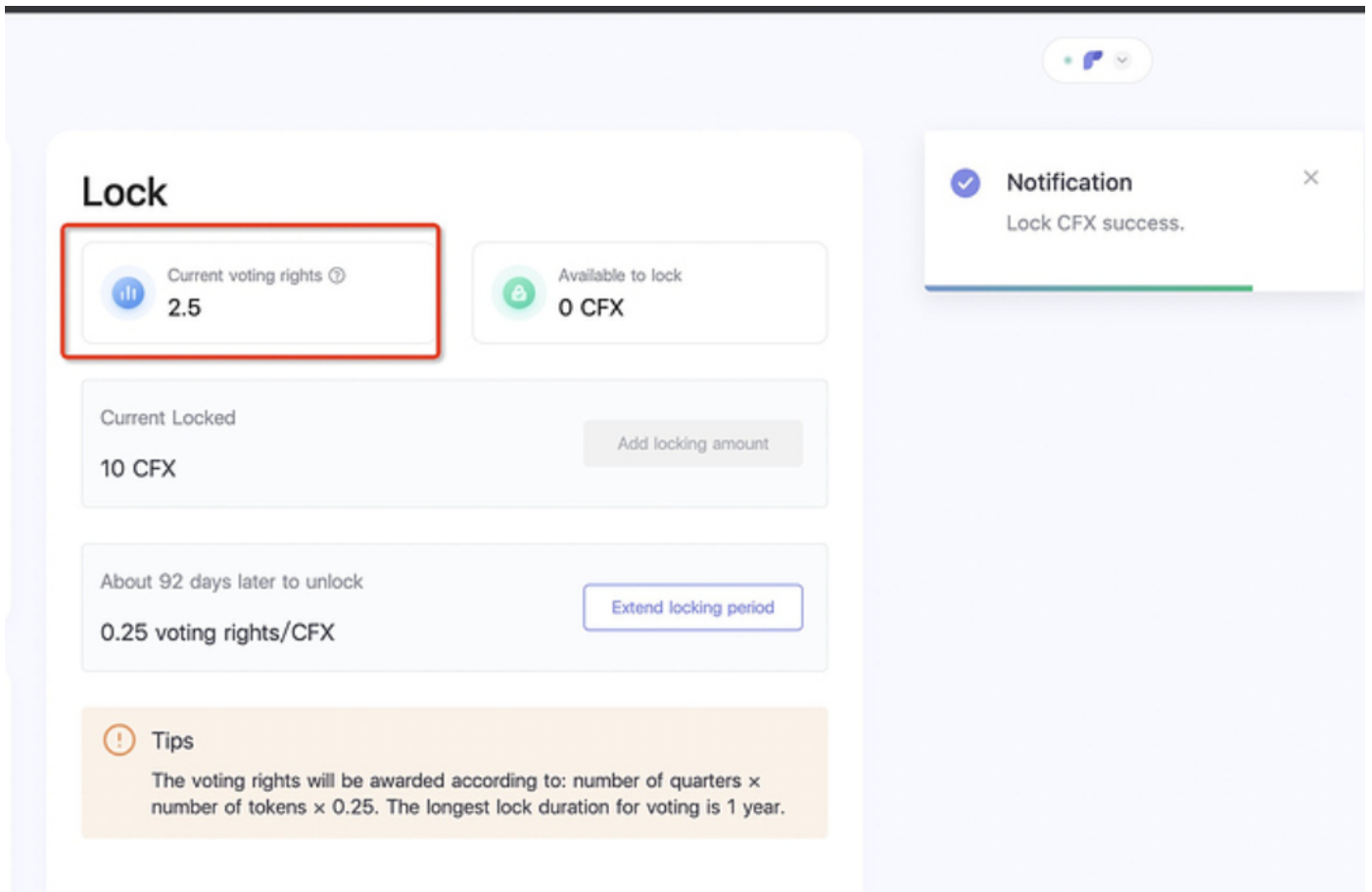
6. 잠금 기간을 선택한다. CFX 잠금 기간은 1분기, 6개월, 1년 중 선택할 수 있다. 최소 기간은 1분기(91일)이며 최대 기간은 1년이다.

$$\text{분기 수}(\text{number of quarters}) \times \text{토큰 수}(\text{number of tokens}) \times 0.25 = \text{투표권}$$



잠금 기간 선택

7. Lock을 클릭하여 잠금을 완료하면 투표권이 부여된다.



잠금 성공 및 투표권 부여

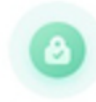
8. extend locking period를 클릭하면 잠금 기간을 연장하여 투표권을 늘릴 수 있으며, add locking amount를 클릭하면 잠금 수량을 늘려 투표권을 증가시킬 수 있다.

Lock



Current voting rights ?

2.5



Available to lock

10 CFX

Current Locked

10 CFX

Add locking amount

About 92 days later to unlock

0.25 voting rights/CFX

Extend locking period



Tips

The voting rights will be awarded according to: number of quarters $\times$ number of tokens $\times$ 0.25. The longest lock duration for voting is 1 year.

투표권 증가 방법

주의사항

- 잠금이 적용된 이후에는 [토큰 수량 증가] 또는 [잠금 기간 연장] 방식으로만 추가 잠금을 수행할 수 있다.
- 마지막으로 설정한 잠금 기간이나 CFX 수량을 줄일 수 없으므로, 더 긴 기간으로 잠그는 방식으로만 투표권을 늘릴 수 있다. (예: 1년 잠금을 설정한 경우 기간을 단축할 수 없다.)
- 잠금 이후 수행할 수 있는 독립적인 작업은 다음 두 가지뿐이다.
 1. 기간 연장 없이 토큰 수량만 증가
 2. 토큰 수량 증가 없이 잠금 기간만 연장

따라서 하나의 프로젝트에 대해 여러 차례 투표에 참여하거나 여러 프로젝트에 동시에 참여하려는 경우에는 별도의 지갑 주소를 사용하는 것이 권장된다.

CIPs

개요

탈중앙화 네트워크인 Conflux에서는 프로토콜의 주요 변경 사항이 적용되기 전에 반드시 합의에 도달해야 한다. 이러한 변경 사항은 Conflux Improvement Proposal(CIP)의 형태로 제안된다. CIP에 대한 논의가 이루어지고, 명세가 확정되며, 충분한 지지를 확보하면 여러 CIP가 구현되어 네트워크 업그레이드 형태로 배포된다. 이러한 네트워크 업그레이드는 일반적으로 하드포크(hard fork)라고 불린다.

CIP 제출 절차는 CIP-1에 설명되어 있다. CIP는 다음과 같은 단계를 거친다.

[IDEA] --> [DRAFT] --> [LAST CALL] --> [ACCEPTED] --> ...

자세한 내용은 CIP-1을 참고하기 바란다.

주요 CIP

아래는 Conflux 메인넷 출시 이후 가장 큰 영향을 미친 주요 CIP들이다.

- CIP-23: 구조화된 데이터의 타입 기반 해싱 및 서명(Typed Structured Data Hashing and Signing). 이 CIP는 Ethereum의 EIP-712를 기반으로 Conflux의 서명 표준을 정의하였다.
- CIP-37: Base32 체크섬 주소(Base32 Checksum Address) 도입. Fluent 및 기타 지갑에서 사용되는 Core Space 주소 형식은 CIP-37에서 정의되었다.
- CIP-40: 블록 기본 보상을 2 CFX로 축소. 메인넷 출시 이후 첫 번째 하드포크 업그레이드에서 블록 기본 보상은 7 CFX에서 2 CFX로 감소하였다. 또한 이는 거버넌스 투표를 통해 확정된 최초의 CIP이기도 하다.
- CIP-43: 스테이킹 참여자의 투표를 통한 최종성(Finality) 도입. 이 CIP는 하이브리드 PoW-PoS 합의 구조의 개념을 도입하였으며, Hydra 하드포크를 통해 구현되었다.
- CIP-90: 완전한 EVM 호환 Space 도입. Hydra 하드포크의 또 다른 주요 업데이트는 Conflux eSpace의 도입이었으며, 이는 CIP-90에서 정의되었다.
- CIP-94: 체인 파라미터를 위한 온체인 DAO 투표. 커뮤니티 거버넌스를 위한 온체인 메커니즘을 정의하며, 이후 네트워크 업그레이드를 통해 도입될 예정이다.

CIP는 어떻게 제출할 수 있는가?

Conflux Improvement Proposal을 제출하려면 먼저 CIP Markdown 템플릿을 복사한 후, 해당 CIP의 제목, 작성자 목록, 제안하려는 변경 사항의 유형과 같은 기본 정보를 프리앰블(preamble)에 입력해야 한다. 이후 다음 섹션들을 작성해야 한다.

Simple Summary, Abstract, Motivation, Specification, Rationale, Backwards Compatibility, Test Cases, Implementation, Security Considerations

초기 공개를 위한 CIP 초안이 준비되면 CIPs GitHub 저장소에 새로운 Pull Request(PR)를 생성하여 제출한다.

다음 단계

CIP 초안이 제출되면 CIP 편집자(CIP Editors)가 이를 검토하고 편집상 문제를 확인한다. 이후 작성자는 해당 CIP를 Conflux 커뮤니티와 공유하고, 논의를 시작하며, 발견된 문제를 해결하고, 제안된 변경 사항 또는 개선안에 대한 충분한 지지를 확보하기 위해 노력해야 한다.