

# 에이다(Ada)

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.

Cardano 독스에 오신 것을 환영합니다. 이곳에서는 Cardano 메인넷과 테스트넷 환경 모두에서 제공되는 기능을 설명하고 지원하는 콘텐츠를 확인할 수 있습니다.

여기에는 Cardano에 처음 입문하는 이용자를 위한 기본 설명, 핵심 기능에 대한 해설, Cardano의 설계에 관한 세부 내용, Cardano 네트워크가 작동하는 방식에 대한 통찰, 그리고 플랫폼 아키텍처가 포함됩니다. 또한 핵심 개념을 설명하고 보다 기술적인 튜토리얼을 위한 개발자 문서로 연결되는 개발자 리소스에도 접근할 수 있습니다.

## Cardano 설명

Cardano는 탈중앙화된 3세대 지분증명(Proof-of-Stake) 블록체인 플랫폼이자 ADA 암호화폐의 기반이다. Cardano는 과학적 철학과 연구 우선 접근 방식에서 발전한 최초의 블록체인 플랫폼이다.

Cardano 플랫폼은 기초부터 설계되었으며, 블록체인과 암호학 분야의 최고 엔지니어 및 학계 전문가들이 결합한 업계 선도적 검증 과정을 거쳤다. Cardano는 지속 가능성, 확장성, 투명성에 강력히 집중하고 있으며, 글로벌 차원의 금융 및 사회적 애플리케이션을 위한 포용적이고 공정하며 회복력 있는 인프라를 제공하는 것을 목표로 하는 완전한 오픈 소스 프로젝트다. 주요 목표 중 하나는 현재 금융 서비스에 접근할 수 없는 사람들에게 신뢰할 수 있고 안전한 금융 서비스를 제공하는 것이다.

Cardano는 보안을 설계의 근본 원칙 중 하나로 삼아 구축되었다. Cardano는 함수형 프로그래밍 언어인 Haskell로 작성되었다. Haskell과 같은 함수형 언어에서는 순수 함수(pure function)를 사용하여 시스템을 구축하는 것이 권장되며, 이는 컴포넌트를 개별적으로 편리하게 테스트할 수 있는 설계로 이어진다. 또한 Haskell의 고급 기능은 코드의 정확성을 보장하기 위해 강력한 방법들을 활용할 수 있게 한다. 예를 들어, 형식적이고 실행 가능한 스펙에 기반한 구현, 광범위한 속성 기반 테스트, 시뮬레이션 환경에서의 테스트 수행 등이 있다.

Cardano의 스마트 컨트랙트 플랫폼은 지금까지 개발된 어떤 프로토콜보다도 고급 기능을 제공하는 것을 목표로 하며, 기업 수준의 DApp 개발을 위한 안정적이고 안전한 플랫폼 역할을 할 것이다. CIP-1694 온체인 거버넌스 메커니즘을 기반으로 구현 중인 Cardano의 민주적 거버넌스 시스템은 프로젝트가 시간에 따라 진화할 수 있게 하며, 혁신적인 재무 시스템을 통해 지속 가능한 자금 조달을 가능하게 할 것이다.

# Cardano가 처음이신가요?

기본 개념의 이해는 블록체인, 특히 Cardano에 익숙해지는 데 핵심적인 역할을 한다. 이 섹션에서는 블록체인의 개념, 지분증명(Proof of Stake)의 이해, 암호화폐란 무엇인지와 같은 기본 개념부터 여정을 시작한다. 또한 다양한 유형의 지갑과 추적 도구를 알아보고, 위임(delegation) 옵션에 대해서도 학습하게 될 것이다.

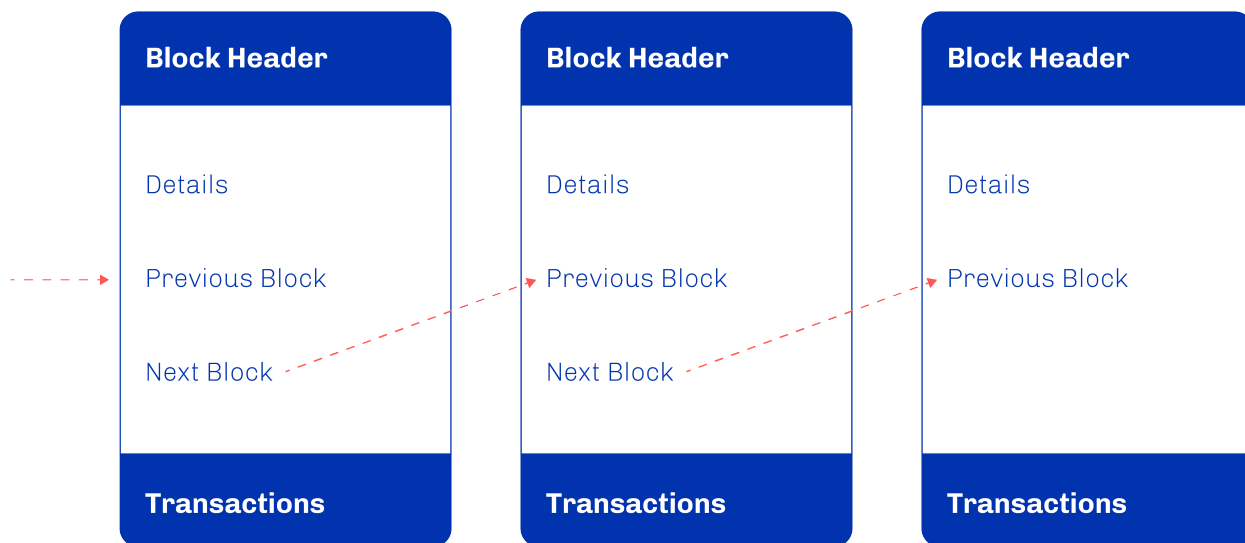
## 블록체인이란 무엇인가?

블록체인은 데이터베이스 또는 원장의 한 형태로, 블록체인 네트워크 내 모든 참여자에게 복제 및 분산된다. 이는 데이터를 저장하거나 가치를 지닌 항목을 저장하는 노드들의 집합으로 구성되며, 이 노드들은 상호 연결되어 블록을 형성한다. 블록은 검증되고 암호학적으로 보호되며, 시간 순서에 따라 체인 형태로 서로 연결된다. 블록체인에 검증된 블록에 저장된 정보는 이후 변경될 수 없으며, 영구적으로 분산 원장에 기록된다.

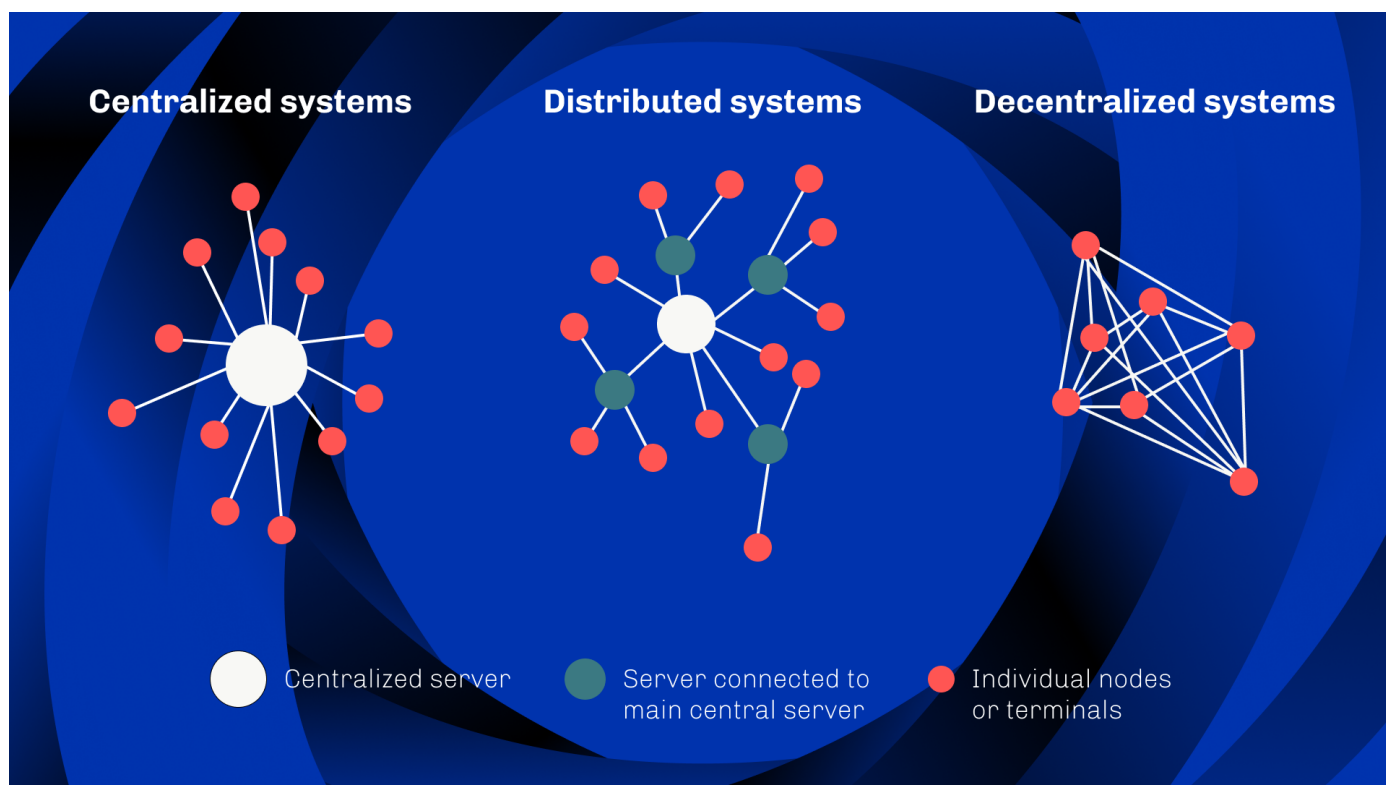
블록체인 기술은 분산 원장 기술(DLT, Distributed Ledger Technology)이라고도 불리며, 다양한 기록을 위한 탈중앙화되고 접근 가능한 데이터 구조를 제공한다. 이러한 기록에는 금융 지불 및 거래 내역뿐만 아니라, 상업 활동에서 사물인터넷(IoT) 기록에 이르기까지 다양한 정보가 포함될 수 있다.

블록체인은 데이터를 탈중앙화 방식으로 저장하기 때문에 중앙화된 통제 기관이나 중개자에 의존하지 않는다. 이는 데이터 저장 및 관리의 투명성을 강화한다. 블록체인의 중요한 특징은 기록을 불변하게 저장한다는 점인데, 이는 기록이 변경되거나, 위조되거나, 삭제될 수 없음을 의미하며, 그렇지 않을 경우 기록 체인이 깨지기 때문이다.

블록체인은 영구 기록 장부에 비유될 수 있으며, 여기서 각 페이지는 정보를 담는 역할을 한다:



이제 이러한 시스템 간 차이를 이해하기 위해 기존 데이터 저장 솔루션을 더 자세히 살펴보자:



- **중앙화 시스템(Centralized systems)** — 모든 데이터 입력과 활동이 일반적으로 하나의 중앙 서버를 통해 관리된다. 이는 단일 실패 지점(SPOF)의 위험을 증가시키며, 은행이나 정부 기관과 같은 통제 기관이 의사 결정권자로 작동함을 의미한다.
- **분산 시스템(Distributed systems)** — 일반적으로 여러 서버 노드에 의존하며, 각 노드는 전체 최종 사용자 집합의 일부를 담당한다.
- **탈중앙화 시스템(Decentralized systems)** — 모든 데이터와 거래 기록이 단일 서버에 저장되는

것이 아니라, 상호 연결된 독립 노드 및 단말기 시스템에 저장된다. 이는 중앙화 기관으로부터의 독립성, 투명성, 보안을 보장한다.

마지막으로, 블록체인은 불변적이고 안전한 데이터베이스를 제공할 뿐만 아니라, 자금 이체, 디지털 화폐 생성, 디지털 계약(스마트 컨트랙트)을 통한 복잡한 거래 처리까지 가능한 기능적 환경으로도 작동한다.

## 암호화폐란 무엇인가?

암호화폐(cryptocurrency)는 원장에 저장된 디지털 자산으로, 재화나 서비스 교환을 위한 매개체로 설계되었다. 줄여서 크립토(crypto)라고도 불린다.

블록체인 원장은 탈중앙화 환경에서 암호화폐 생성을 위한 기반 기술로 사용된다. 블록체인 프로토콜은 엄격한 암호학적 기법을 사용하여 암호화폐의 발행(생성)을 가능하게 하고, 암호 자산의 소유권 및 자금 이동 기록을 보호하고 검증한다. 암호화폐의 가격은 정부나 중앙화된 금융 기관에 의해 통제되지 않는다. 이는 그 자체의 가치, 현실 세계 지표와의 상관관계, 그리고 시장의 수요와 공급에 의해 결정된다.

암호화폐를 전송할 때는 주소가 사용된다. 주소는 고유 식별자로, 사용자의 공개키에서 파생된 숫자와 문자로 이루어진 문자열로 표현된다.

## Ada는 Cardano의 기본 통화이다

각 블록체인 원장에는 고유한 암호화폐 또는 기본 통화가 존재한다. Cardano의 기본 통화는 ada이다. 이는 ada가 Cardano에서의 주요 결제 단위임을 의미하며, 수수료 지불, 예치금 납부에 사용되며, 보상이 분배되는 유일한 통화이기도 하다.

Lovelace는 ada의 최소 단위이다.  $1 \text{ ada} = 1,000,000 \text{ lovelace}$ 이다. Ada는 소수점 여섯 자리까지 분할 가능하므로, 소액 단위로 쉽게 나눌 수 있다.

## 네이티브 토큰

Cardano는 네이티브 토큰(native tokens)의 생성을 지원한다. 네이티브 토큰은 특정 목적을 위해 만들어진 디지털 자산이다. 이는 사용자, 개발자, 기업이 Cardano 블록체인을 활용하여 커뮤니티, 시장 상황, 또는 독립적 주체에 의해 정의된 가치를 나타내는 토큰을 생성할 수 있음을 의미한다. 토큰은 대체 가능(fungible)할 수도 있고, 대체 불가능(non-fungible)할 수도 있으며, 결제 단위, 보상 수단, 거래 자산, 또는 정보 보관 수단으로 기능할 수 있다.

## 지분증명(Proof of Stake)

지분증명(PoS)은 시스템에 보유된 지분(또는 가치)의 양을 이용해 합의를 결정하는 합의 메커니즘 또는 프로토콜의 한 형태이다. 본질적으로 합의 프로토콜은 블록체인의 동작을 규율하는 법칙과 매개변수를 통제한다. 합의란 네트워크의 각 참여자가 준수해야 하는 규칙 집합으로 생각할 수 있다. 블록체인은 단일 중앙 권위에 의해 통제되지 않기 때문에, 합의 프로토콜을 통해 분산 네트워크 참여자들이 블록체인에 기록된 네트워크의 *이력*에 동의할 수 있도록 한다. 즉, 무엇이 발생했는지에 대한 합의를 이루고, 단일한 진실의 원천에서 계

속 나아가는 것이다.

Cardano는 혁신적인 PoS 합의 프로토콜인 Ouroboros 위에 구축되었으며, 동료 검토(peer review)를 거친 연구를 통해 개발된 최초의 블록체인 합의 프로토콜이다. 이 프로토콜의 핵심에는 스테이크 풀(stake pool)이 있다. 이는 스테이크 풀 운영자가 실행하는 안정적인 서버 노드로, ada 보유자는 자신의 지분을 위임할 수 있다. 스테이크 풀은 노드를 직접 운영할 기술적 경험이나 가용성이 없는 사람도 프로토콜에 참여할 수 있도록 보장한다. 이러한 스테이크 풀은 유지 관리에 집중하며, 다양한 이해관계자의 결합된 지분을 단일 엔티티로 보유한다.

## 지분증명과 작업증명 프로토콜의 비교

대조적으로, 작업증명(PoW)은 블록 내 문제를 가장 먼저 해결하려는 채굴자들의 경쟁을 장려하는 동기화 프로토콜이다. 보상 시스템이 이러한 문제 해결을 유인한다. 그러나 이 접근 방식은 전력 사용량 증가와 체인 내 문제 해결에 더 긴 시간이 소요된다는 대가를 치른다. 이러한 요인은 네트워크를 크게 느려지게 하고 유지 비용을 높인다.

## 지분증명의 특징

PoS의 핵심 특징 중 하나는 사용자의 가치가 증가함에 따라 원장을 유지할 기회도 증가한다는 것이다. 이는 블록체인에 추가될 새로운 블록을 생성할 확률이 높아짐을 의미하며, 블록은 그에 맞게 타임스탬프가 찍힌다. 새로운 블록의 생성자는 무작위 선택과 지분 크기에 따른 결정의 조합을 통해 선정된다. 이는 체인 내에서 일종의 리더 선출이 일어나는 것이다. PoS 프로토콜에서는 참여자가 거래 수수료를 축적하여 시간이 지남에 따라 자신의 부를 늘린다는 점을 기억할 필요가 있다. 이러한 접근 방식은 블록체인의 안정적이고 지속적인 성장을 장려하며, 체인 성장을 방해할 수 있는 거래 정체 현상을 줄인다.

## 지분증명의 주요 장점

PoS가 PoW에 비해 가지는 주요 장점은 다음과 같다:

- 엄격한 보안 프로토콜이 PoS에 통합되어 있음
- 중앙화 감소 – 네트워크 내 이기적 행위에 벌칙을 부과하여 중앙화 위험을 완화
- 에너지 효율성 – 블록체인을 생성하고 운영하는 데 필요한 전력 및 하드웨어 자원이 훨씬 적기 때문에 에너지 소비가 매우 효율적임
- 비용 효율성 – PoS 기반 통화는 PoW 프로토콜 기반 통화보다 훨씬 비용 효율적임

## Cardano 노드

Cardano 노드는 네트워크 내 최상위 컴포넌트이다. 네트워크 노드는 네트워킹 계층에서 서로 연결되며, 이는 정보 교환 요구를 전달하는 구동력 역할을 한다. 여기에는 더 나은 데이터 흐름을 확립하기 위한 신규 블록 확산 및 거래 정보가 포함된다. Cardano 노드는 맞춤형 피어 선택 프로세스를 통해 선택된 피어와 연결을 유지한다. Cardano 노드를 실행함으로써, 사용자는 네트워크에 참여하고 기여하게 된다.

## 작동 방식

스테이크 풀은 Cardano 노드를 사용하여 풀이 네트워크와 상호작용하는 방식을 검증하며, 거래 처리와 블록 생성을 담당한다. 이들은 다양한 이해관계자의 결합된 지분을 단일 엔티티로 보유·유지하는 신뢰할 수 있는 서버 노드 역할을 한다.

## 블록 생성

블록체인 기술의 목표는 독립적으로 검증 가능하며 암호학적으로 연결된 기록(블록)의 체인을 생산하는 것이다. 블록 생산자 네트워크는 협력하여 블록체인을 발전시킨다. 합의 프로토콜은 투명성을 제공하고 어떤 후보 블록이 체인을 확장하는 데 사용될지를 결정한다.

제출된 유효 거래는 신규 블록에 포함될 수 있다. 블록은 그 생산자에 의해 암호학적으로 서명되며, 체인 내 이전 블록과 연결된다. 이는 블록에서 거래를 삭제하거나, 블록의 순서를 변경하거나, (이미 뒤따르는 블록이 여러 개 존재하는 경우) 블록을 체인에서 제거하거나, 네트워크 모든 참여자에게 알리지 않고 새로운 블록을 체인에 삽입하는 것을 불가능하게 만든다. 이러한 구조는 블록체인 확장의 무결성과 투명성을 보장한다.

## 슬롯과 에포크

Cardano 블록체인은 체인 상의 합의를 촉진하기 위해 Ouroboros Praos 프로토콜을 사용한다. Ouroboros Praos는 시간을 에포크(epoch)로 나눈다. 각 Cardano 에포크는 여러 슬롯(slot)으로 구성되며, 각 슬롯은 1초 동안 지속된다. 현재 Cardano의 한 에포크에는 432,000개의 슬롯(5일)이 포함된다. 각 슬롯에서는 0개 이상의 블록 생성 노드가 슬롯 리더(slot leader)로 지명될 수 있다. 평균적으로 20초마다 한 개의 노드가 지명되어, 한 에포크당 총 21,600번의 지명이 이루어진다. 무작위로 선출된 슬롯 리더가 블록을 생성하면, 그 중 하나가 체인에 추가되며 나머지 후보 블록은 폐기된다.

## 슬롯 리더 선출

Cardano 네트워크는 소유자와 위임자(delegator)로 알려진 기타 이해관계자의 지분을 합산하여 관리하는 여러 스테이크 풀(stake pool)로 구성된다. 슬롯 리더는 이러한 스테이크 풀 중 무작위로 선출된다. 풀의 지분이 많을수록 슬롯 리더로 선출되어 블록체인에 추가되는 새로운 블록을 생성할 가능성이 커진다. 이것이 지분증명(PoS)의 기본 개념이다. 공정한 경쟁 환경을 유지하고 소수의 대형 풀이 지분 대부분을 통제하는 상황을 방지하기 위해, Cardano는 이미 전체 지분의 상당 부분을 통제하는 풀에 대한 위임을 억제하는 인센티브 시스템을 갖추고 있다.

## 거래 검증

거래를 검증할 때 슬롯 리더는 송신자가 해당 거래를 지불할 충분한 자금을 보유했는지 확인해야 하며, 거래의 매개변수가 충족되었는지도 확인해야 한다. 거래가 이러한 요건을 모두 충족하면, 슬롯 리더는 이를 새로운 블록의 일부로 기록하고, 이 블록은 체인 내 다른 블록들과 연결된다.

## 스테이크 풀

스테이크 풀은 원장 유지에 집중하며 여러 이해관계자의 결합된 자원(즉, '스테이크')을 단일 엔티티로 보유하는 신뢰할 수 있는 서버 노드이다. 스테이크 풀은 원장에 기록될 거래를 처리하고 새로운 블록을 생성하는 역할을 담당한다. 스테이크 풀은 Cardano의 지분증명 프로토콜인 Ouroboros의 핵심이다.

Ouroboros가 안전하게 작동하려면 충분한 수의 이해관계자가 항상 온라인 상태를 유지하고 양호한 네트워크 연결성을 보장해야 한다. 이 때문에 Ouroboros는 ada를 보유한 기여 이해관계자를 대신하여 24/7 프로토콜을 운영하는 데 전념하는 스테이크 풀에 의존한다. 이 개념은 자원 보유자들이 자신들의 자원(지분)을 모아 풀을 형성하는 것으로, 일반적으로 한 명은 풀의 운영자(operator)가 되고, 나머지는 위임자(delegatee)가 된다. 스테이크 풀 운영자(SPO)는 플랫폼과 호환되는 소프트웨어(서버 노드)를 설치 및 실행하는 역할을 맡으며, 위임자는 보다 수동적인 역할을 하며 자신의 지분을 풀에 위임한다.

Ouroboros는 작업증명(PoW) 프로토콜보다 운영 비용이 저렴하지만, 여전히 실행에는 일정한 비용이 발생한다. 따라서 SPO는 거래 수수료와 순환 중인 ada 공급의 인플레이션에서 발생하는 인센티브의 형태로 보상을 받는다.

## 위임(Delegation)

Cardano는 지분증명(PoS) 시스템이므로, ada를 보유하는 것은 단순히 재화나 서비스를 구매할 수 있게 해줄 뿐만 아니라, 프로토콜에 참여하고 블록을 생성할 권리와 의무를 부여한다. 스테이크 위임은 이해관계자 집합이 매우 분산된 환경에서도 프로토콜이 확장될 수 있도록 하는 Ouroboros 프로토콜 고유의 메커니즘이다.

ada를 보유한 누구나 지출 권한을 유지하면서 스테이크 위임에 참여할 수 있다. 위임 방식과 관계없이 언제든지 정상적으로 ada를 사용할 수 있음을 유의해야 한다. 이 메커니즘을 통해 이해관계자는 각 에포크마다 슬롯 리더 선출 과정에 참여할 수 있다.

스테이크 위임은 비트코인 프로토콜의 채굴 풀과 유사한 스테이크 풀을 탄생시킨다. 스테이크 풀 운영자(SPO)는 슬롯 리더로 선정될 경우 블록을 생성하기 위해 온라인 상태를 유지해야 한다.

ada 보유자가 스테이크를 위임할 때 고려할 수 있는 세 가지 옵션은 다음과 같다:

- 자신만의 스테이크 풀 운영
- 제3자와 합의하여 자신을 위한 개인 스테이크 풀 운영
- 다른 스테이크 풀에 위임

## 스테이크 위임 요건

스테이크를 위임하려면 두 가지 인증서를 체인에 게시해야 한다: 스테이킹 주소 등록과 위임 인증서. 인증서를 게시하려면 자금이 필요하므로, 첫 지갑을 설정하는 사용자는 부트스트래핑 메커니즘이 필요하다. 이 메커니즘은 등록 인증서를 게시하기 전에 기본 주소가 스테이킹 키를 사용할 수 있다는 가능성에 의존한다. 스테이크 주소는 단일 키 기반이거나 다중 서명(multi-sig)과 같은 스크립트 기반일 수 있다.

## 위임 방식

위임 개념을 통해, 이해관계자는 Cardano 네트워크를 위해 스테이크 풀이 블록을 생성하도록 허용할 수 있다. 이후 프로토콜은 SPO 수수료를 포함해 모든 참여자에게 보상을 분배한다. 이해관계자는 운영자의 검증 키 해시인 특정 풀 ID에 위임한다.

대리인의 블록 생성 권한을 특정 에포크 및 슬롯 범위로 제한하기 위해, 이해관계자는 대리 서명 키의 유효 메시지 공간을 특정 값 범위의 슬롯 번호로 끝나는 문자열로 제한할 수 있다. 이 단순한 방식은 대리 서명 체계의 검증 가능성과 오용 방지 속성 덕분에 안전하다. 이를 통해 이해관계자는 특정 대리 서명 키가 실제로 특정 이해관계자에 의해 특정 대리인에게 발급되었음을 검증할 수 있으며, 대리인은 해당 키의 유효 메시지 공간 내에서만 메시지에 서명할 수 있다.

사용자 지갑의 하나의 스테이킹 키에 속한 자금을 위임하려면 위임 인증서를 포함하는 단일 거래를 게시해야 한다. 이는 일반적인 거래 수수료만 발생시킨다. 특히, 이해관계자는 스테이크 주소를 등록할 때 보증금을 지불해야 하지만, 스테이크 위임 자체에는 지불하지 않는다. 스테이크 주소가 등록되면, 이해관계자는 단지 위임 대상을 설정하기 위해 수수료를 지불하면 된다.

이해관계자의 스테이크는 보상 계산 시 풀의 스테이크로 반영된다는 점을 유의해야 한다.

## 스테이크 위임 시나리오

사용자가 처음으로 ada를 받으려 한다고 가정해보자. 이는 교환소에서의 거래, 리DEM션, 혹은 다른 출처를 통해 얻은 것일 수 있다. 사용자는 새 지갑을 설정하고 해당 자금을 받을 주소를 생성할 것이다. 이 주소는 지갑에서 생성되었으나 체인에 아직 등록되지 않은 스테이킹 키를 사용하는 기본 주소(base address)가 될 것이다.

초기 자금을 받은 후, 사용자는 스테이킹 키 등록 인증서와 자신의 스테이킹 키에 대한 위임 인증서를 게시함으로써 스테이킹에 참여할 수 있다. 키가 등록되면, 새로 생성된 주소는 스테이킹 키 등록 인증서를 가리키는 포인터 주소(pointer address)가 될 수 있다.

## 서약(Pledging)과 보상

서약은 Cardano 블록체인 내에서 건전한 생태계의 성장을 장려하는 중요한 메커니즘이다. 스테이크 풀을 등록할 때 일부 또는 전체 ada를 풀에 서약(pledge)함으로써, 위임하고자 하는 사람들에게 더 매력적으로 보이게 할 수 있다. 스테이크 풀 설정 시 서약은 필수는 아니지만, 더 많은 ada가 서약될수록 위임자에게 더 매력적으로 보이며, 그 결과 더 높은 보상이 지급된다. a0 프로토콜 파라미터는 서약이 풀 보상에 미치는 영향을 정의한다.

### 보상 분배

각 에포크 동안, 보상은 자신만의 스테이크 풀이나 다른 풀에 위임한 모든 이해관계자에게 분배된다. 이 보상은 프로토콜에 의해 자동 생성되며, 스테이크 풀 운영자(SPO)가 관리하지 않는다. 보상은 두 가지 출처에서 나온다:

- 모든 거래 수수료: 해당 에포크 동안 생성된 블록에 포함된 거래에서 수집됨

- 통화 확장(Monetary expansion): ada의 총 발행량(total supply)과 최대 발행량(maximal supply)을 구분한다. 총 발행량은 현재 유통 중인 ada와 재무부(treasury)에 있는 ada로 구성된다. 최대 발행량은 존재할 수 있는 ada의 최대치이다. 이 두 수치의 차이를 준비금(reserve)이라 한다. 각 에포크마다 남아 있는 준비금의 일정 비율(조정 가능)이 준비금에서 차감되어 보상과 재무부로 사용되며, 준비금에서 차감된 금액의 일정 비율이 재무부로 전송된다.

보상 공유에 대한 더 자세한 내용은 Cardano의 *rewards sharing and pledge* 영상에서 확인할 수 있다.

다음 공식은 보상 메커니즘이 작동하는 방식을 보여준다. 사용 가능한 보상 금액  $R$ (거래 수수료 + 통화 확장)에서 특정 풀이 받을 수 있는 보상의 몫은 다음과 같이 결정된다:

$$f(s, \sigma) := \frac{R}{1 + a_0} \cdot \left( \sigma' + s' \cdot a_0 \cdot \frac{\sigma' - s' \frac{z_0 - \sigma'}{z_0}}{z_0} \right)$$

요소 정의:

- $R$  - 해당 에포크의 총 보상 가능 금액
- $a_0$  - 서약 영향 계수(0과 무한대 사이의 값 가능)
- $z_0$  - 상대적 풀 포화 크기, 예: 원하는 풀 수( $k=200$ )에 기반하여 0.5%
- $\sigma$  - 풀에 위임된 지분(소유자가 서약한 지분 및 타인이 위임한 지분 포함)
- $\sigma' = \min(\sigma, z_0) - \sigma$ 이지만  $z_0$ 에서 상한 처리됨
- $s$  - 소유자가 서약한 지분
- $s' = \min(s, z_0) - s$ 이지만  $z_0$ 에서 상한 처리됨

$z_0$ ,  $\sigma$ ,  $s$ 는 모두 상대적인 값으로, 총 발행량의 분수(0~1 사이 값)임을 유의해야 한다.

두 가지 중요한 고려 사항:

1. 보상은  $\sigma$ 가 증가함에 따라 증가하지만,  $\sigma$ 가  $z_0$ 에 도달하면(즉, 풀이 포화 상태가 되면) 더 이상 증가하지 않는다.
2.  $a_0$ (서약 영향)이 0이면 공식은 단순히  $R \cdot \sigma'$ 로 변하며, 이는 포화 상태에 도달할 때까지 풀의 지분에 비례한다.  $a_0$ 가 클수록 서약  $s$ 의 중요성이 커진다.

서약은 풀 등록 시(비용 및 마진 값과 함께) 선언되며, 풀에 위임하는 소유자는 이를 반드시 이행해야 한다. 만약 실제 위임된 금액이 선언된 서약보다 적다면, 해당 에포크의 풀 보상은 0이 된다. 또한 운영자 마진이 100% 미만으로 설정된 경우 풀은 퍼블릭으로 간주된다.

이 공식에서 산출된 보상은 풀의 성과에 따라 조정된다. 즉,  $\beta/\sigma a$ 를 곱하는데,  $\beta$ 는 해당 에포크 동안 풀이 생성한 블록 비율이며,  $\sigma a$ 는 풀에 위임된 지분이 전체 활성 지분(비은퇴 풀에 올바르게 위임된 총 지분)에서 차지하는 비율이다.

최적의 성과를 내는 풀(즉, 생성할 수 있는 모든 블록을 생성하는 풀)의 경우, 이 계수는 평균적으로 10이 된다. 실제 값은 Ouroboros Praos 합의 알고리즘의 확률적 특성, 즉 무작위성 때문에 변동할 수 있다.

풀 보상이 계산되고 성과에 따라 조정된 후, 이는 풀 운영자와 풀에 지분을 위임한 모든 구성원에게 분배된다. 분배 과정은 여러 단계로 이루어진다:

- 먼저, 선언된 비용이 차감되어 풀 운영자에게 지급된다.
- 다음으로, 선언된 마진이 차감되어 풀 운영자에게 지급된다.
- 마지막으로, 남은 금액은 위임된 지분에 비례해 풀에 위임한 모든 이해관계자에게 공정하게 분배된다 (풀 소유자 포함).

실제로 받은 ada 보상의 금액은 변동할 수 있으며, 이는 여러 요인에 따라 달라진다. 여기에는 스테이크 풀의 실제 성과(특정 에포크에서 풀이 생성한 블록 수가 기대치와 얼마나 일치하는지), 네트워크 파라미터 변경 등이 포함된다.

## 합의(Consensus) 설명

합의는 블록체인을 운영하는 모든 참여자가 다수 의견에 도달하는 과정이다. 어떤 블록을 생성할지, 어떤 체인을 채택할지, 그리고 네트워크의 단일 상태를 결정하기 위해 합의가 필요하다. 합의 프로토콜은 개별 노드가 원장의 현재 상태를 어떻게 평가하고 합의에 도달하는지를 정의한다.

블록체인은 참여자가 다른 사람들이 제출한 거래들을 블록에 묶어 체인(블록들의 연속)에 추가하도록 허용함으로써 합의를 형성한다. 누가 언제 블록을 생성할 수 있는지, 그리고 두 참여자가 동일한 지점에 서로 다른 블록을 추가하는 것과 같은 충돌 상황이 발생했을 때 어떻게 처리할지를 결정하는 것이 합의 프로토콜의 목적이다.

프로토콜의 주요 책임은 세 가지다:

- 리더 검사를 수행하고 블록 생성 여부를 결정
- 체인 선택 처리
- 생성된 블록 검증

## Ouroboros 소개

Cardano는 Ouroboros 합의 프로토콜 위에서 운영되며, 이는 사이버 보안 및 암호학 분야의 최고 학회와 저널에 발표된 다수의 동료 검토 논문을 통해 제시되었다. 작업증명(PoW) 프로토콜에서처럼 복잡한 연산 문제를 해결하여 블록을 생성하고 가장 먼저 성공한 사람에게 보상을 주는 방식 대신, 지분증명(PoS)에서는 네트워크에서 보유한 지분의 크기에 따라 스테이크 풀을 선정하여 새로운 블록을 생성한다.

## Ouroboros 작동 방식

Ouroboros는 Cardano의 시간을 에포크(epoch)로 나누며, 각 에포크는 슬롯(slot)으로 다시 나누어진다. 슬롯은 블록을 생성할 수 있는 짧은 시간 단위이다. 슬롯을 에포크로 묶는 것은 동적으로 변하는 지분 분포에 맞춰 리더 선출 과정을 조정하는 데 핵심적이다.

Ouroboros 설계의 핵심은 공격이 발생하더라도 보안을 유지해야 한다는 점이다. 따라서 이 프로토콜은 공격자가 블록체인의 대체 버전을 전파하는 것을 방지하는 내재적 내성을 가지고 있으며, 공격자가 언제든지 임의의 메시지를 어떤 참여자에게든 보낼 수 있다고 가정한다. 메시지 전달 시간이 강력히 보장되는 동기적 환경(synchronous setting)에서, 전체 지분의 51% 이상이 정직한 참여자(즉, 프로토콜을 따르는 참여자)에 의해 통제되는 한, 프로토콜의 보안은 보장된다.

각 슬롯에는 슬롯 리더가 선출되며, 이들은 체인에 블록을 추가하고 다음 슬롯 리더에게 전달할 책임을 가진다. 프로토콜을 무너뜨리려는 공격 시도를 방어하기 위해, 각 신규 슬롯 리더는 수신한 체인의 최근 몇 개 블록을 임시(transient)로 간주해야 한다. 미리 정해진 개수의 임시 블록 이전의 체인만이 확정(settled)된 것으로 간주된다. 이를 정산 지연(settlement delay)이라고 한다. 이는 이해관계자가 일정 기간(정산 지연보다 길지 않은 기간) 동안 오프라인 상태였다 하더라도 블록체인과 동기화 상태를 유지할 수 있음을 의미한다.

Ouroboros 프로토콜에서 각 네트워크 노드는 거래 메모리풀(mempool)과 블록체인을 저장한다. 메모리풀에는 기존 거래와 일관된 경우 거래가 추가된다. 노드는 더 길고 유효한 대체 체인을 인식하면 로컬에 저장된 블록체인을 해당 체인으로 교체한다.

## Ouroboros 개요

신화에서 Ouroboros(우로보로스, uroboros라고도 함)는 보통 자기 꼬리를 물고 있는 뱀(혹은 때로는 용)으로 묘사된다. “Ouroboros”라는 단어 자체는 고대 그리스어에서 유래했으며, 문자 그대로의 의미는 “꼬리를 먹는” 혹은 “꼬리를 삼키는 자”이다.

상징적으로 Ouroboros는 끊임없이 순환하는 끝없는 주기 속에서 자기 자신으로 되돌아오는 시간의 무한성을 나타낸다. Ouroboros는 기원전 13세기 이집트에서 처음 등장했으며, 이후 연금술사들이 신비적 상징으로 채택하였다.

세월이 흐르면서 Ouroboros는 수많은 문화에서 다양한 방식으로 해석되고 사용되었다. 가장 일반적인 해석 중 하나는 이 상징이 우주의 상호 연결성과 무한성을 의미한다는 것이다.

2017년 Charles Hoskinson은 Cardano의 지분증명 합의 프로토콜에 “Ouroboros”라는 이름을 붙였다. 이 맥락에서 Ouroboros는 블록체인의 무한하고 윤리적인 성장과 확장 가능성을 의미한다. Ouroboros의 핵심 메시지는 에너지 소비를 크게 줄이면서도 세계에 더 많은 기회를 제공하고 이를 지속시키는 것이다.

## Ouroboros란 무엇인가

Ouroboros는 Cardano의 합의 프로토콜로, 최초로 수학적으로 보안성이 입증된 지분증명 프로토콜이자 동료 검토된 연구를 기반으로 한 최초의 블록체인 프로토콜이다.

행동심리학과 경제 철학 원칙을 포함한 고유 기술과 수학적으로 검증된 메커니즘을 결합한 Ouroboros는 이를 구현하는 블록체인의 보안성과 지속 가능성을 보장한다. 그 결과, 보안성이 입증된 프로토콜이 탄생했으며, 최소한의 에너지 요구만으로도 글로벌하고 퍼미션리스 네트워크의 확산을 가능하게 한다. Cardano는 이러한 네트워크의 첫 사례이다.

Ouroboros는 네트워크에서 보유한 지분 크기에 따라 참가자(즉, 스테이크 풀)를 선택해 새로운 블록을 생성하며, 새로운 시장을 지속적으로 지원할 수 있는 분산형 퍼미션리스 네트워크 생성을 촉진한다.

## Ouroboros 구현

Ouroboros는 여러 버전으로 제공된다:

- Ouroboros Classic
- Ouroboros BFT
- Ouroboros Praos
- Ouroboros Genesis
- Ouroboros Cryptsinous
- Ouroboros Chronos
- Ouroboros Leios

## Ouroboros Classic

Ouroboros의 첫 번째 구현은 세 가지 주요 성과를 달성했다:

- 작업증명과 경쟁할 수 있는 에너지 효율적 프로토콜의 기초 마련
- 지분증명을 분석하기 위한 수학적 프레임워크 도입
- 지분증명 환경에서 참여자를 보상하기 위한 새로운 인센티브 메커니즘 구현

그러나 Ouroboros를 다른 블록체인 프로토콜(특히 지분증명 프로토콜)과 차별화시킨 진정한 특징은 프로토콜의 리더 선출 알고리즘에서 편향 없는 무작위성을 생성할 수 있다는 점과, 이를 통해 제공되는 보안 보장이었다. 무작위성은 패턴 형성을 방지하며, 이는 프로토콜의 보안을 유지하는 데 핵심적이다. Ouroboros는 이와 같은 엄격한 보안 분석으로 개발된 최초의 블록체인 프로토콜이었다.

## Ouroboros BFT

Ouroboros BFT(Byzantine Fault Tolerance)는 두 번째 구현으로, Byron 업데이트(기존 Cardano 코드베이스에서 새로운 코드베이스로의 전환)에서 사용되었다. 이 두 번째 구현은 Shelley 릴리스와 함께 도입된 탈중앙화를 준비시켰다.

Ouroboros BFT는 연합 서버 네트워크(즉, 블록체인) 간 동기식 통신을 가능하게 하여, 보다 단순하고 결정론적인 방식으로 원장 합의를 제공했다.

## Ouroboros Praos

Ouroboros Praos는 Classic 구현에 상당한 보안성과 확장성 개선을 도입했다. Praos는 체인을 슬롯으로 나누고 이를 에포크로 집계하여 거래 블록을 처리한다. 그러나 Ouroboros Classic과 달리, Praos는 준동기적 환경에서 분석되며, 적응적 공격자에 대해서도 안전하다. 이를 위해 비공개 리더 선출과 키 발전형 서명(key-evolving signatures)을 사용하여 강력한 공격자가 다음 슬롯 리더를 예측하고 집중 공격(DDoS 등)을 수행하지 못하도록 한다.

## Ouroboros Genesis

Ouroboros의 네 번째 버전인 Genesis는 Ouroboros Praos를 개선하여, 신뢰할 수 있는 체크포인트나 과거 가용성에 대한 가정 없이 제네시스 블록에서 부트스트랩할 수 있게 하는 새로운 체인 선택 규칙을 추가했다. Genesis 논문은 또한 프로토콜의 범용 합성 가능성(Universal Composability)을 입증했으며, 이는 보안 속성을 잃지 않고도 실제 환경에서 다른 프로토콜과 임의로 조합될 수 있음을 보여준다.

## Ouroboros Crypsinous

Ouroboros Crypsinous는 Genesis에 프라이버시 보존 속성을 추가한다. 이는 최초로 공식적으로 분석된 프라이버시 보존 지분증명 블록체인 프로토콜로, Snark와 키-프라이빗 전방위 안전 암호화를 활용한 새로운 코인 진화 기법을 도입하여 강력한 적응형 공격에 대한 보안을 유지하면서도 강력한 프라이버시 보장을 제공한다. Crypsinous는 현재 Cardano에 구현될 계획은 없지만, 프라이버시 강화 환경이 필요한 다른 체인에서는 활용될 수 있다.

## Ouroboros Chronos

Chronos는 두 가지 목표를 달성한다. 첫째, 블록체인 프로토콜이 새로운 시간 동기화 메커니즘을 통해 안전하게 시계를 동기화할 수 있음을 보여주며, 이를 통해 외부 시간 서비스에 의존하지 않게 만든다. 둘째, 다른 프로토콜에 암호학적으로 안전한 시간 소스를 제공한다. 요약하면, Chronos는 시간 정보를 노린 공격에 대해 원장을 더 강력하게 만든다.

응용 관점에서 Chronos는 단일 실패 지점이 없는 통합 네트워크 클록에 로컬 시간을 동기화해야 하는 통신, 교통, 기타 IT 인프라의 회복력을 획기적으로 높일 수 있다.

## Ouroboros Leios

현재 연구·개발 중인 Ouroboros Leios는 사용 가능한 자원의 활용을 최적화하고 더 빠른 거래 처리와 확정을 가능하게 함으로써 네트워크 처리량을 증가시키도록 설계된 버전이다.

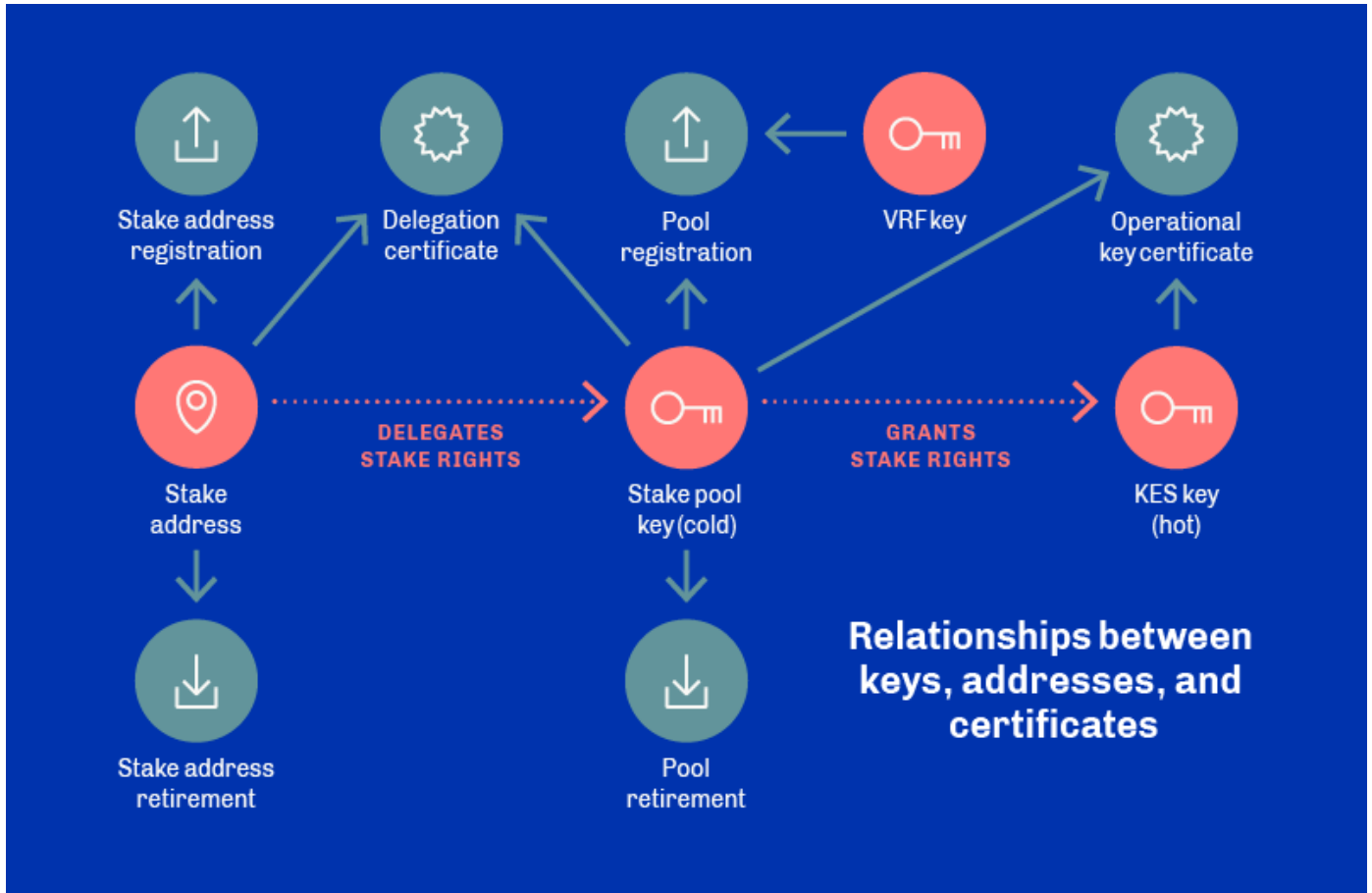
Leios는 기존 시스템의 확장성 병목을 해결하기 위해 기본 프로토콜 위의 고처리량 오버레이로 설계되었다. 이는 유효한 메시지를 갑작스럽게 대량 전송하여 네트워크를 혼잡하게 만드는 프로토콜 버스트(protocol bursts)나 이중 서명 공격(equivocations)과 같은 악의적 행위를 방어하며, 거의 최적에 가까운 거래 처리를 가능하게 한다.

## Cardano 키

Cardano 키는 비대칭 암호화 키 쌍으로, 다음과 같은 용도로 사용된다:

- 결제 및 스테이킹 인증서의 서명과 검증
- Cardano 블록체인 상의 주소 식별 및 정의

아래 도식은 키, 주소, 인증서 간의 관계를 보여준다:



## 키의 유형

Cardano에는 두 가지 주요 키 유형이 있다:

- 노드 키(node keys)
- 주소 키(address keys)

## 노드 키

노드 키는 블록체인의 보안을 나타내며, 다음과 같은 키로 구성된다:

- 운영자/운영 키(operator/operational key)
- 키 진화 서명(KES, Key Evolving Signature) 키 쌍
- 검증 가능한 난수 함수(VRF, Verifiable Random Function) 키

## 운영자/운영 키

운영자 키는 오프라인 키 쌍으로, 새 인증서에 대한 인증서 카운터를 포함한다.

운영자는 풀의 핫 키(온라인)와 콜드 키(오프라인) 모두를 관리할 책임이 있다. 콜드 키는 반드시 안전하게 보관되어야 하며 인터넷 연결이 있는 장치에 저장되어서는 안 된다. 콜드 키는 여러 개의 백업을 유지하는 것이 권장된다.

## KES 키 쌍

블록 생성 노드의 운영 인증서를 생성하려면, 본인을 인증하는 KES 키 쌍이 필요하다.

KES 키는 일정 기간 동안만 진화할 수 있으며, 그 후에는 무용지물이 된다. 이는 공격자가 키를 탈취해 서명 키에 접근하더라도 앞으로 생성되는 블록에만 서명할 수 있고, 과거 블록에는 서명할 수 없기 때문에 블록체인 역사를 조작하는 것이 불가능하다는 점에서 유용하다.

설정된 기간이 지나면 노드 운영자는 새로운 KES 키 쌍을 생성하고, 해당 키 쌍으로 새로운 노드 운영 인증서를 발급한 뒤, 새로운 인증서로 노드를 재시작해야 한다.

## VRF 키

Ouroboros Praos는 VRF 키를 통해 블록 생성에 추가적인 보안 계층을 더한다.

다른 지분증명 블록체인 프로토콜(Ouroboros Classic이나 BFT 등)에서는 슬롯 리더 일정이 공개되어 있어 각 슬롯에서 누가 블록을 생성할 권리가 있는지를 알 수 있다. 이 경우, 자신이 누구인지 증명하기만 하면 되고, 누구나 공개된 슬롯 리더 일정을 확인하여 검증할 수 있다.

그러나 Ouroboros Praos에서는 슬롯 리더 일정이 비공개로 유지된다. 이는 누가 슬롯 리더가 될지 사전에 알 수 없음을 의미하지만, 일단 누군가 슬롯 리더가 되면 VRF 키를 사용해 자신이 정당한 리더임을 다른 모든 이에게 증명할 수 있다.

VRF 키는 운영 인증서에 저장된 서명 검증 키이며, 특정 슬롯에서 노드가 블록을 생성할 권리를 보유했음을 입증한다.

## 주소 키

주소 키는 블록체인에서 자금을 식별하기 위해 파생된 주소 기능을 나타내며, 다음과 같은 키로 구성된다:

- 결제 키(Payment key): 보통 UTXO 주소 생성을 위해 사용되는 단일 주소 키 쌍
- 스테이킹 키(Staking key): 계정/보상 주소 생성을 위해 사용되는 스테이크/보상 주소 키 쌍

## Cardano 주소

주소는 관련 검증/공개 키를 blake2b-224 해시로 처리하고 일부 메타데이터와 연결하여 생성되며, 이는 Cardano 블록체인에 저장될 수 있다.

Shelley 시대에 네 가지 다른 유형의 주소가 도입되었다:

- 기본 주소(base addresses)
- 포인터 주소(pointer addresses)

- 엔터프라이즈 주소(enterprise addresses)
- 보상 계정 주소(reward account addresses)

이 새로운 주소 유형들 외에도, Shelley는 Byron 시대의 부트스트랩 주소와 스크립트 주소를 계속 지원했지만, 실제로 스테이크 권리를 보유하는 것은 새로운 기본 주소와 포인터 주소뿐이었다. 따라서 주소는 블록체인 블록에 저장된 원장 명세에 지정된 직렬화 데이터로 구성되며, 예를 들어 미사용 트랜잭션 출력(UTXO) 주소가 있다.

직렬화 데이터(주소)는 두 부분으로 이루어진다:

- 메타데이터(metadata): 해석을 위해 사용됨
- 페이로드(payload): 원시 또는 인코딩된 데이터

## 기본 주소 (Base addresses)

기본 주소는 해당 주소의 지분을 통제해야 하는 스테이킹 키를 직접 지정한다. 이 주소에 보관된 자금과 관련된 스테이크 권리는 스테이킹 키 소유자가 행사할 수 있다. 기본 주소는 스테이킹 키를 사전에 등록하지 않고도 거래에 사용할 수 있다.

스테이크 권리를 행사하려면 스테이크 키를 등록하고 스테이크 풀에 위임해야 한다. 스테이크 키가 등록되면, 등록 전후에 거래에서 사용된 기본 주소에 대해서도 스테이크 권리를 행사할 수 있다.

## 포인터 주소 (Pointer addresses)

포인터 주소는 해당 주소의 스테이크를 통제해야 하는 스테이킹 키를 간접적으로 지정한다. 포인터 주소는 스테이킹 키 포인터를 참조하는데, 이는 해당 키의 스테이킹 키 등록 인증서가 블록체인에 저장된 위치이다. 포인터 주소는 대상이 활성 스테이킹 키 등록이 아니더라도 거래에 사용할 수 있다. 이는 키가 거래 이후(혹은 이전)에 등록 취소된 경우나 명백히 무효한 대상을 가리키는 경우를 포함한다. 이렇게 무효 대상을 허용하는 이유는 노드가 현재 활성 스테이킹 키만 추적하면 되도록 하기 위함이다.

포인터는 기본 주소에 사용되는 해시보다 훨씬 짧을 수 있다.

포인터 주소에는 미묘한 점이 있다. 포인터 주소가 참조하는 스테이킹 키 등록 인증서가 롤백으로 인해 손실될 수 있다. 이러한 시나리오에서 자금 손실을 방지하기 위해, 시스템은 포인터가 무효한 포인터 주소라도 해당 주소에 저장된 자금을 거래 입력으로 사용하는 데는 유효하다고 간주한다(다만 지분증명 참여 목적에서는 무시한다). 선택적으로, 지갑은 참조된 인증서가 불변 상태가 되기 전까지는 포인터 주소로 거래를 생성하지 않도록 제한할 수 있는데, 이는 롤백 시 자금이 지분증명에서 제외되는 것을 방지하기 위함이다.

## 엔터프라이즈 주소 (Enterprise addresses)

엔터프라이즈 주소는 스테이크 권리를 보유하지 않으므로, 이러한 주소를 사용하는 것은 지분증명 프로토콜 참여를 선택적으로 포기하는 것을 의미한다.

다른 사용자를 대신하여 대량의 ada를 보유하는 거래소나 기관은 스테이크 권리를 행사하지 않겠다는 정책을 따를 수 있다. 엔터프라이즈 주소를 사용함으로써 거래소는 이러한 정책을 따르고 있음을 증명할 수 있다. 엔터프라이즈 주소는 어떠한 스테이킹 키와도 연결되지 않으므로, 슬롯 리더십 일정에 영향을 주는 메커니즘에서 자동으로 제외된다. 스테이크 권리가 없는 주소를 사용하면 전체 스테이크 총량이 감소하여 잠재적 공격자에게 유리해질 수 있다.

또한 엔터프라이즈 주소는 여전히 PolicyID가 부여된 토큰(비-ada 자산)을 수신, 보관, 전송하는 데 사용할 수 있다.

## 보상 계정 주소 (Reward account addresses)

보상 주소는 해당 주소의 공개 스테이킹 키를 암호학적으로 해싱한 것이다. 보상 계정 주소는 지분증명 프로토콜(직접 또는 위임을 통해)에 참여한 대가로 보상을 분배하는 데 사용된다.

보상 주소의 특징은 다음과 같다:

- 계정 기반(account-style) 회계 방식이 사용되며, UTXO 방식이 아님
- 거래를 통해 자금을 수신할 수 없으며, 보상이 분배될 때만 잔고가 증가
- 등록된 스테이킹 키와 보상 계정 주소는 일대일 대응 관계

자금을 인출할 때는 해당 키가 사용된다. 또한 보상 주소에 있는 자금과 관련된 스테이크는 해당 키의 지분에 기여한다. 엔터프라이즈 주소와 마찬가지로, 보상 주소의 스테이킹 객체에는 추가 정보가 포함될 필요가 없다.

## 체인 확정(Chain confirmation)과 거래 확정(Transaction confirmation)

Cardano를 논의할 때 자주 반복되는 질문은 “Cardano의 거래 시간은 얼마인가?”, “Cardano에서 거래가 완료되기 위해 몇 번의 네트워크 확정이 필요한가?”이다. 이러한 질문에 답하기 위해서는 체인 확정과 거래 확정 개념, 그리고 이들이 Ouroboros 프로토콜과 어떻게 연결되는지를 깊이 이해해야 한다.

### 체인 확정 (Chain confirmation)

체인 확정은 무작위성이나 예측 불가능한 사건으로 인해 이후 더 이상 변경되지 않을 것임을 프로토콜이 보장하는 지점을 말한다.

체인 확정은 일정 수의 미래  $k$  블록이 생성된 이후 미래 시점에서 발생한다. 특정 거래의 체인 확정이 발생하기까지의 시간은 안정성 윈도우(stability window)라고 부른다. 이는 블록이 안정적(stable)이라고 간주되기까지 필요한 슬롯 수를 의미하며, 여기서 안정적이란 롤백될 수 없는 블록을 뜻한다. 이 윈도우를 계산하는 공식은  $3k/f$ 이다. (여기서  $k$ 는 제네시스에서 정의된 보안 파라미터이며,  $f$ 는 제네시스에서 정의된 활성 슬롯 계수로, 한 에포크에서 생성되는 블록 수의 확률을 결정한다.)

### 거래 확정 (Transaction confirmation)

거래 확정은 거래가 체인에 받아들여지고 불변 상태가 되는 시점을 의미한다. 여기에는 블록 깊이(block depth)와 정산 윈도우(settlement window) 개념이 적용된다.

거래가 포함된 블록이 충분히 깊다면 해당 거래는 확정된 것으로 간주된다. “충분히 깊다”는 상대적 개념이다. 블록 깊이는 특정 블록이 체인에 추가된 이후 몇 개의 블록이 더 추가되었는지를 나타낸다. 블록이 깊이를 가지므로, 그 안에 포함된 거래 역시 깊이를 가진다.

특정 블록의 깊이가 사전에 정의된 임계값보다 크다면, 해당 거래는 확정된 것으로 간주되며, 그 거래에서 발생한 자산은 “안전하게” 사용할 수 있다(즉, 프로토콜이 해당 거래가 불변임을 보장하므로, 해당 자산은 거래, 교환 등에서 안전하게 사용 가능하다).

거래가 확정된 시점부터 해당 거래 자산을 다른 자산과 교환에 사용할 수 있을 때까지의 기간을 정산 윈도우(settlement window)라고 한다.

## 불변성 가능성 (Likelihood of immutability)

거래가 확정되었는지를 판단하는 또 다른 방법은 그 거래의 불변성 가능성을 고려하는 것이다. 거래가 불변일 확률은 그 거래가 체인에 포함된 이후 몇 개의 블록이 더 추가되었는지에 달려 있다. 더 많은 블록이 추가될수록 거래가 불변이 될 확률은 높아진다.

거래는 그 깊이가 3k/f 슬롯보다 커지는 순간 불변 상태가 된다. 이는 Ouroboros Praos 프로토콜에 의해 보장된다. 그러나 3k/f 슬롯은 대부분의 상황에서 요구 조건을 초과하기 때문에, 보다 실용적인 접근은 거래가 불변이 될 확률을 고려하는 것이다. 이 경우, 거래가 불변일 확률이 충분히 높다면 거래는 확정된 것으로 본다.

## 확장 UTXO(EUTXO) 모델

Cardano는 (비트코인처럼) 미사용 트랜잭션 출력(UTXO, Unspent Transaction Output) 기반 블록체인으로, Ethereum과 같은 계정 기반(account-based) 블록체인과는 다른 원장 회계 모델을 사용한다. Cardano는 Alonzo 업그레이드에서 멀티에셋 및 스마트 컨트랙트를 지원하기 위해 혁신적인 확장 UTXO(EUTXO, Extended UTXO) 모델을 도입하였다.

### UTXO 모델 개요

UTXO 모델에서 트랜잭션은 입력과 출력으로 구성되며, 입력은 이전 트랜잭션의 출력이다. 즉, 트랜잭션은 과거에 사용되지 않은 미사용 출력(UTXO)만을 입력으로 사용할 수 있다.

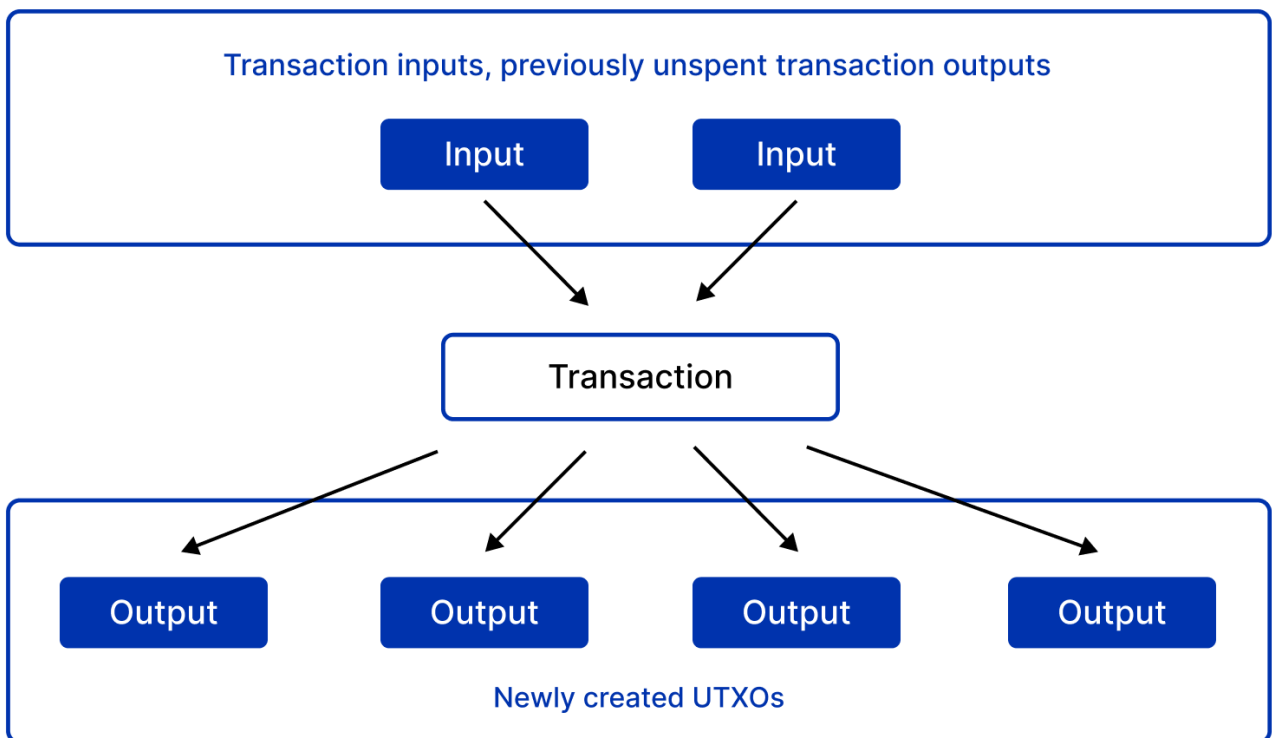
### 트랜잭션 출력

트랜잭션 출력에는 주소(자물쇠로 비유 가능)와 값이 포함된다. 이때 주소에 속하는 서명이 출력 해제의 열쇠에 해당한다. 일단 해제되면 해당 출력은 입력으로 사용할 수 있다. 새로운 트랜잭션은 이전 트랜잭션의 출력을 소비하여 새로운 출력을 생성하며, 이 새로운 출력은 이후 트랜잭션의 입력으로 사용된다. 각 UTXO는 단 한 번만, 그리고 전체 단위로 소비될 수 있다. 즉, 각 출력은 정확히 하나의 입력에 의해 소비된다.

## 트랜잭션 입력

트랜잭션 입력은 이전 트랜잭션의 출력이다. 트랜잭션 입력에는 포인터와 암호학적 서명이 포함되며, 이는 해제 키로 작동한다. 포인터는 이전 트랜잭션 출력을 가리키고, 키는 해당 출력을 해제한다. 출력이 입력에 의해 해제되면 블록체인은 해당 출력을 “사용됨(spent)”으로 표시한다. 이후 새로 생성된 출력은 차후 트랜잭션의 입력으로 지정될 수 있으며, 이로써 체인이 계속 이어진다. 이렇게 아직 해제되지 않은(즉, 소비되지 않은) 출력이 바로 UTXO이다.

정리하면, 트랜잭션은 과거 트랜잭션의 미사용 출력을 소비하고, 미래 트랜잭션에서 입력으로 사용할 새로운 출력을 생성한다.



사용자의 지갑은 이러한 UTXO를 관리하며, 사용자가 보유한 UTXO를 포함하는 트랜잭션을 시작한다. 모든 노드는 현재 미사용 트랜잭션 출력 집합(UTXO set)을 기록하며, 이를 체인 상태(chainstate)라 부른다. 체인 상태는 각 노드의 데이터 디렉터리에 저장된다. 새 블록이 체인에 추가되면 체인 상태는 이에 맞게 업데이트된다. 새 블록에는 최신 트랜잭션 목록이 포함되며, 여기에는 소비된 UTXO 기록과 새롭게 생성된 UTXO가 기록된다. 모든 노드는 체인 상태의 동일한 복사본을 유지한다.

## Cardano의 확장 UTXO 모델

EUTXO 모델은 UTXO 모델을 두 가지 방식으로 확장한다:

1. **주소 개념의 일반화:** EUTXO는 자물쇠-열쇠(lock-and-key) 비유를 확장한다. 자물쇠를 공개키로, 열쇠를 서명으로 제한하지 않고, EUTXO의 주소는 스크립트 형태의 임의의 로직을 포함할 수 있다. 예를 들어 노드가 트랜잭션을 검증할 때, 특정 출력이 입력으로 사용될 수 있는지를 판단하기 위해 출력 주소에 포함된 스크립트를 조회하고 실행한다.
2. **출력에 임의 데이터 포함 가능:** UTXO와 달리, EUTXO 출력은 주소와 값 외에도 (거의) 임의의 데이터

터를 포함할 수 있다. 이를 통해 스크립트가 상태 정보를 유지할 수 있어 훨씬 더 강력해진다.

나아가, EUTXO는 출력 주소에 복잡한 로직을 포함시켜 어떤 트랜잭션이 이를 해제할 수 있는지 결정하고, 모든 출력에 맞춤형 데이터를 추가할 수 있게 한다. 주소 검증 시 스크립트는 출력이 보유한 데이터, 검증 중인 트랜잭션, 그리고 트랜잭션이 각 입력에 대해 제공하는 리디머(redeemer)라는 추가 데이터를 참조한다. 이 모든 정보를 기반으로 스크립트는 매우 복잡한 상황에서도 “예/아니오” 판단을 내릴 수 있다.

EUTXO는 스크립트 형태의 임의 로직을 허용한다. 이 로직은 트랜잭션과 데이터를 검사하여 입력 사용 여부를 결정한다.

UTXO 모델의 그래프 구조는 기존 스마트 컨트랙트 지원 블록체인에서 사용하는 계정 기반 모델과 근본적으로 다르다. 따라서 계정 기반 블록체인에서 DApp에 사용되는 설계 패턴은 Cardano에 그대로 적용되지 않는다. 데이터 표현이 다르기 때문에 새로운 설계 패턴이 필요하다.

EUTXO는 비트코인 UTXO 모델의 분기(per-branches) 설계를 계승하며, 각 분기는 일련의 검증이 필요한 일련의 트랜잭션으로 정의된다. 서로 다른 분기로 로직을 나누고 병렬성을 강화하기 위해, 여러 UTXO를 활용한 DApp 및 솔루션 개발이 필수적이다. 이는 비트코인 서비스 개발에서 하나의 지갑을 여러 서브 지갑으로 분할해야 하는 것처럼 확장성 측면에서 이점을 제공한다.

## EUTXO의 장점

Cardano의 EUTXO 모델은 시스템 오류 없이 다중 연산을 처리할 수 있는 안전하고 다재다능한 환경을 제공한다. 이 모델은 각 UTXO가 한 번만, 그리고 전체 단위로 소비될 수 있어 트랜잭션 검증이 훨씬 단순해지므로 더 나은 확장성과 프라이버시, 단순화된 트랜잭션 로직을 제공한다.

EUTXO 모델은 다른 회계 모델에 비해 고유한 장점을 제공한다. 트랜잭션 검증의 성공 여부는 트랜잭션과 그 입력 자체에만 의존하며, 블록체인의 다른 요소에는 의존하지 않는다. 따라서 트랜잭션이 블록체인에 제출되기 전에 오프체인에서 그 유효성을 확인할 수 있다. 다만, 다른 트랜잭션이 동시에 동일한 입력을 소비할 경우 실패할 수 있다. 그러나 입력이 모두 남아 있는 경우 트랜잭션은 반드시 성공한다.

이는 이더리움처럼 계정 기반 모델과 대조적이다. 계정 기반에서는 트랜잭션이 스크립트 실행 도중 실패할 수 있지만, EUTXO에서는 그런 일이 발생하지 않는다.

트랜잭션 검증이 “로컬”한 성격을 가지므로 높은 수준의 병렬 처리가 가능하다. 동일한 입력을 소비하지 않는 한, 노드는 이론적으로 트랜잭션을 병렬로 검증할 수 있다. 이는 효율성뿐 아니라 분석 및 검증에도 유리하여, 잠재적 결과를 단순화하고 “나쁜 일이 발생하지 않음”을 증명하는 데 도움이 된다.

EUTXO 모델의 강력한 기능 중 하나는 유효한 트랜잭션에 필요한 수수료를 사전에 정확히 예측할 수 있다는 것이다. 이는 계정 기반 모델에서는 볼 수 없는 독특한 기능이다. 계정 기반 블록체인(예: 이더리움)은 비결정론적이므로 트랜잭션의 체인 상 효과를 보장할 수 없다. 이 불확실성은 금전적 손실, 예상치 못한 높은 수수료, 악의적 행위 기회의 위험을 초래한다.

정리하면, EUTXO는 더 큰 보안성, 스마트 컨트랙트 실행 비용 예측 가능성(불쾌한 놀람 없음), 더 강력한 병렬 처리를 제공한다.

# 트랜잭션 비용과 결정론(Determinism)

Cardano의 가격 책정 접근 방식은 실제 공급보다 시장 수요에 더 크게 의존한다. Cardano에서는 여러 유형의 수요가 공통된 공급을 두고 경쟁하므로, 상대 가격과 절대 가격을 모두 고려하는 것이 중요하다. 이를 수행하는 한 가지 방법은 스마트 컨트랙트 비용, 대체 불가능 토큰(NFT) 작업 등이 Cardano의 처리 능력 소비라는 공통 가치와 어떤 관계가 있는지를 살펴보는 것이다.

Cardano 원장은 높은 신뢰성, 보안성, 그리고 입증된 형식 검증(formal verification)에 초점을 맞추어 설계되었다. 이 전략에 맞춰, 트랜잭션 처리가 결정론적(deterministic)이어야 한다는 점도 중요하다. 즉, 사용자는 트랜잭션을 실제 실행하기 전에 그 영향과 결과를 예측할 수 있어야 한다.

스마트 컨트랙트 지원이 2021년에 도입되면서, 트랜잭션 실행 비용과 원장에서의 동작을 사전에 보장할 수 있는 능력은 더욱 중요해졌다. 이는 Ethereum을 포함한 다른 블록체인과 다른 점으로, 그곳에서는 네트워크 활동이 가스 비용에 영향을 줄 수 있다. Cardano와 Plutus 스크립트의 결정론적 특성이 바로 이러한 예측 가능성을 보장한다.

## 결정론(Determinism)

트랜잭션 및 스크립트 처리 맥락에서 결정론은 예측 가능성과 동의어이다. 이는 사용자가 오프체인 환경에서 자신의 트랜잭션이 원장의 온체인 상태에 어떤 영향을 미칠지를 다음과 같은 불확실성 없이 예측할 수 있음을 의미한다:

- 예기치 않은 스크립트 검증 결과나 실패
- 예기치 않은 수수료
- 예기치 않은 원장 또는 스크립트 상태 업데이트

## 검증(Validation)

트랜잭션 처리에서 중요한 부분은 트랜잭션이 수행하는 동작을 검증하는 것이다. 특정 필드에 데이터가 포함되어 있을 때, 트랜잭션은 해당 동작을 수행한다. 예를 들어, 입력 필드에 UTXO U를 참조하면 해당 트랜잭션은 U를 소비하는 것이며, 민트(mint) 필드에 토큰 X가 포함되면 토큰 X를 발행하는 것이다.

Cardano는 스크립트를 사용해 이러한 동작을 검증한다. 스크립트는 True 또는 False를 출력하는 순수 함수로 구성된 코드 조각이다. 스크립트 검증은 스크립트 인터프리터가 주어진 인자를 사용해 특정 스크립트를 실행하는 과정이다.

스크립트 검증은 다음과 같은 동작에 대해 수행될 수 있다:

- 스크립트 주소에 잠긴 UTXO 소비: 실행되는 스크립트는 해당 주소를 구성하는 해시이다.
- 토큰 발행: 실행되는 스크립트는 발행되는 토큰의 정책 ID를 구성하는 해시이다.
- 보상 인출: 실행되는 스크립트는 스테이킹 주소를 구성하는 해시이다.
- 인증서 적용: 실행되는 스크립트는 인증서 발급자의 자격 증명을 구성하는 해시이다.

트랜잭션 동작은 어떤 스크립트를 실행할지 알려줄 뿐만 아니라, 해당 스크립트에 전달할 인자를 어떻게 조합할지도 정의한다. Alonzo 업그레이드는 Plutus 스크립트 구현에 따라 Cardano의 트랜잭션 검증 방식을 새롭게 도입했다.

## 원장의 기능

Alonzo 업그레이드는 원장 데이터를 다음과 같이 변경했다:

1. Plutus 스크립트가 UTXO를 잠글 수 있다.
2. UTXO 출력 부분에 스크립트 상태와 유사한 기능을 가능케 하는 데이터 구성 요소가 추가되었다. 즉, 자산과 주소 외에도 Plutus 스크립트로 잠긴 UTXO는 데이터(datum)를 포함한다. 데이터는 스크립트 상태의 해석으로 간주될 수 있는 정보이다.
3. 트랜잭션에 추가 검증 요구를 부과하는 여러 프로토콜 파라미터가 존재한다. 여기에는 스크립트가 소비할 수 있는 계산 자원의 상한이 포함된다.

Plutus 스크립트를 지원하기 위해, 트랜잭션은 다음과 같은 기능을 가진다:

1. 각 동작에 대해 사용자가 지정한 인자(redeemer)를 포함한다. Redeemer는 스크립트에 따라 다른 역할을 수행할 수 있다(예: 경매에서의 입찰, 추측 게임에서의 사용자의 추측 등).
2. 각 스크립트에 대해 계산 실행 예산을 지정한다.
3. 트랜잭션이 실행 수수료를 지불할 수 있도록 담보(collateral)를 포함한다.
4. 트랜잭션의 무결성을 보장하기 위해 무결성 해시(integrity hash)를 포함한다.

Vasil 업그레이드에서는 Plutus 스크립트가 V2 기능으로 업그레이드되었으며, 개선된 비용 모델과 새로운 내장 기능이 도입되었다. 참조 입력(reference inputs), 인라인 데이터(inline datums), 참조 스크립트(reference scripts)의 사용으로 처리량이 향상되고 성능이 크게 증가했다.

노드는 트랜잭션이 올바르게 구성되었는지 확인하는 검사를 수행한다. 예를 들어, 최대 실행 자원 예산을 초과해서는 안 된다. 또한 Plutus 스크립트 인터프리터를 호출해 스크립트를 실행한다.

비결정론적 가스 모델은 사용자가 예측 불가능하게 높은 수수료를 지불하게 만들 수 있다. Cardano 스크립트는 이 문제를 해결하기 위해, 트랜잭션에 자원 예산과 이를 충족할 수수료를 반드시 포함하도록 요구한다. 스크립트 실행은 반드시 True 또는 False를 반환하며, 무한 루프에 빠지지 않는다. 이는 스크립트가 수행하는 모든 연산이 0이 아닌 자원을 소비하며, 이 자원이 인터프리터에 의해 추적되기 때문이다. 트랜잭션이 지정한 예산을 초과하면 스크립트 실행은 종료되며 False를 반환한다.

스크립트 및 트랜잭션 검증 결과를 예측 가능하게 만드는 핵심 요소는 다음과 같다:

- 동일한 인자에 대해 스크립트 인터프리터는 항상 종료되며 동일한 검증 결과를 반환한다.
- 트랜잭션은 검증 시 스크립트 인터프리터에 전달될 모든 인자를 고정한다.
- 트랜잭션은 스크립트 검증이 필요한 모든 동작을 명시한다.
- 트랜잭션에 필수 서명이 포함되어 있어, 공격자가 스크립트 실패를 유발할 수 있도록 트랜잭션을 변경할 수 없다.
- EUTXO 원장 모델에서 트랜잭션 적용은 결정론적이다.

스크립트 검증의 성공 또는 실패는 트랜잭션 처리 방식에 영향을 미친다. 그러나 True/False 결과와 그에 따른 원장 변경은 특정 트랜잭션에 대해 예측 가능하다.

## 담보(collateral) 메커니즘에 대하여

담보 메커니즘은 스마트 컨트랙트 실행의 성공을 보장하기 위해 설계된 중요한 기능이다.

원장의 결정론적 설계가 제공하는 보장을 기반으로, Cardano는 **2단계 검증 체계**를 구현한다. 2단계 검증의 주요 목적은 노드가 보상받지 못하는 불필요한 검증 작업을 최소화하는 것이다. 각 단계는 이 목표를 달성하기 위해 다음과 같은 역할을 한다:

- **1단계:** 트랜잭션이 올바르게 구성되었는지, 그리고 처리 수수료를 지불할 수 있는지 확인
- **2단계:** 트랜잭션에 포함된 스크립트를 실행

트랜잭션이 1단계를 통과하면 2단계 스크립트가 실행된다. 1단계에서 실패하면 스크립트는 실행되지 않고 트랜잭션은 즉시 폐기된다.

담보는 2단계 검증이 실패했을 때도 노드가 수행한 작업에 대해 보상받도록 보장하는 장치다. 따라서 담보는 사용자가 계약이 신중히 설계되고 철저히 테스트되었음을 보증하기 위해 제공하는 금전적 보증이다. 담보 금액은 트랜잭션을 구성할 때 지정되며, 직접 지정되는 것이 아니라 담보 입력(collateral inputs)을 추가함으로써 지정된다. 이 특별히 표시된 입력에 해당하는 UTXO 잔액의 총합이 트랜잭션의 담보 금액이다. 만약 조건이 충족되어 계약이 정상 실행되면 담보는 안전하게 유지된다.

### 시나리오

담보가 없다면, 스마트 컨트랙트가 실패해도 사용자는 비용을 지불하지 않는다. 그러나 트랜잭션이 실패하기 전까지 네트워크는 해당 트랜잭션을 시작하고 검증하는 데 비용을 이미 소모한다. 이는 악의적 행위자가 무효한 트랜잭션으로 네트워크를 대량 공격하여, 소규모 비용만 들이고도 서비스 거부(DoS) 공격을 실행할 수 있음을 의미한다.

### 해결책

사용자가 트랜잭션을 시작할 때, 실행 비용을 충당할 충분한 ada를 담보로 제공한다. Cardano에서는 네이티브가 아닌 스마트 컨트랙트(2단계 계약)를 호출하고 사용할 때, 잠재적인 트랜잭션 실패 비용을 충당할 수 있는 충분한 담보도 필요하다. 이 금액은 크지 않지만, DoS 공격을 경제적으로 불가능하게 만들기에는 충분하다.

담보 수수료는 트랜잭션 검증이 실패했을 때만 징수된다. 계약이 검증을 통과하면 거래 수수료는 징수되지만 담보는 유지된다.

### 근거

정직한 사용자는 담보를 잃을 위험이 전혀 없다.

Cardano 블록체인은 트랜잭션 비용과 관련해 결정론적이다. 비용은 오직 로컬 값과 로컬 상태에만 의존하기 때문이다. 즉, 사용자는 트랜잭션을 제출하기 전에 실행 비용(ada 단위)을 계산할 수 있다. 이는 Ethereum을 포함한 다른 블록체인과 달리, 네트워크 활동이 가스 비용에 영향을 줄 수 없는 차별화된 기능이다. 필요한 담보 금액은 오직 실행 비용에만 의존한다.

Cardano 테스트넷은 무료 테스트 ada를 제공하는 안전한 환경을 제공하므로, DApp 개발자는 메인넷 배포 전에 스마트 컨트랙트를 철저히 시험할 수 있다. 테스트넷에서 트랜잭션이 성공하면, 개발자는 스크립트가 실제로도 반드시 성공할 것임을 확신할 수 있다.

온체인 조건이 트랜잭션이 구성된 이후 변경된 경우, 해당 트랜잭션은 전체적으로 거부되며 수수료도 징수되지 않는다. 예를 들어, 서명이 누락된 경우 담보는 징수되지 않는다.

## 기술적 세부사항

담보란 담보 입력이 참조하는 UTXO에 포함된 ada 총액을 의미한다. 트랜잭션은 2단계 스크립트가 실패할 경우, 이 담보 입력을 사용해 수수료를 충당한다.

Shelley 형식 사양은 ‘다중 서명(multi-signature)’ 스크립트 개념을 도입했다. 1단계 스크립트는 원장 규칙에 의해 완전히 처리되므로, 실행 비용을 처리 전에 쉽게 평가할 수 있으며, 예를 들어 스크립트를 포함하는 트랜잭션의 크기에 따라 원장 규칙 구현 내에서 직접 수수료를 계산할 수 있다.

반대로, 2단계 스크립트는 임의의 계산(이론적으로 튜링 완전)을 수행할 수 있다. Cardano는 2단계 스크립트를 사용하는 트랜잭션에 대해 추상적 실행 단위(ExUnits)로 표현되는 예산을 요구한다. 이 예산은 메모리 사용량, 실행 단계 수 등 특정 지표에 기반해 자원 사용량에 정량적 한계를 부여한다. 예산은 이후 트랜잭션 수수료 계산의 일부로 사용된다.

Vasil 업그레이드 이후, DApp 개발자는 스크립트 담보를 위한 변경 주소(change address)를 지정할 수도 있다. 이는 스크립트가 2단계 검증에서 실패할 경우, 필요한 금액만 차감되고 나머지 자금은 지정된 변경 주소로 반환됨을 의미한다. “how to use collateral outputs” 튜토리얼에서 더 자세한 내용을 확인할 수 있다.

# 거버넌스 개요

Cardano의 거버넌스는 **Cardano 개선 제안(CIP) #1694**의 도입 이후 크게 발전하였다. 이 제안은 더 탈중앙화되고 커뮤니티 주도적인 의사결정 과정을 위한 토대를 마련하였다. 철학자 볼테르의 출생연도(1694)를 따서 명명된 이 제안은, 거버넌스가 자립적(self-sustaining)이며 Cardano 커뮤니티에 의해 통제되는 **Voltaire 개발 단계**로의 전환을 의미한다.

CIP-1694는 \*\*대표자(DRep), 헌법 위원회(constitutional committee), 스테이크 풀 운영자(SPO)\*\*로 구성된 삼자 구조(tripartite governance structure)를 도입하였다. 이들은 협력하여 누구나 제출할 수 있는 거버넌스 안건을 검토하고 승인하며, 이를 통해 투명하고 민주적인 절차를 보장한다.

Cardano의 자립적 거버넌스에는 다음과 같은 역할이 필요하다:

- **Ada 보유자**: 게임에 직접 참여하는 주체('skin in the game')
- **DRep**: Ada 보유자로부터 투표권을 위임받은 자
- **SPO**: 네트워크를 유지하고 특정 거버넌스 안건에 투표하는 블록 생산자
- **헌법 위원회**: Cardano 헌법 준수를 보장하는 선출 대표자

스테이크 풀과 마찬가지로, 모든 Ada 보유자는 DRep으로 등록하여 자신 또는 다른 사람을 대표할 수 있다. 또한 Ada 보유자는 투표권을 원하는 DRep에게 위임할 수도 있다. 투표권은 위임된 Ada 총량에 따라 결정되며, lovelace 단위(1 ada = 1,000,000 lovelaces)로 계산된다.

## Cardano 헌법에 의해 주도됨

**\*\*Cardano 블록체인 생태계 헌법(Cardano constitution)\*\***은 커뮤니티의 가치와 비전을 모아 규칙과 원칙으로 명문화한 근본 문서이다. 이는 Cardano 네트워크의 지속 가능성을 유지하기 위한 기준이 된다.

## 왜 중요한가?

Cardano의 창립 주체들 — **EMURGO, Input Output, Cardano 재단** — 은 블록체인의 제네시스 키를 반납하고, 더 성숙한 거버넌스 체계를 커뮤니티에 이양했다. 이제 커뮤니티가 이 과제를 이어받아 Cardano를 다음 단계로 이끌어야 하며, 이는 모든 Ada 보유자가 참여해야 함을 의미한다.

이 과정에서 **Intersect**가 중요한 역할을 한다. Intersect 회원이 되면 오프체인에서 Cardano 거버넌스를 형성하고 성숙시킬 수 있는 다양한 기회가 주어진다.

Intersect 회원 외에도, Cardano 포럼 및 소셜 네트워크 참여 등을 통해 거버넌스에 기여할 수 있다.

Cardano 커뮤니티와 함께 Cardano의 미래를 이끌고 대중적 채택을 촉진하여, 가장 탈중앙화된 블록체인의 성공을 보장하라. 아래 섹션에서 더 자세한 내용을 확인할 수 있다.

## 참여 방법

탈중앙화된 의사결정에 참여하려면, 먼저 거버넌스 호환 지갑을 선택하고 설치해야 한다. Intersect MBO가 최신 목록을 관리한다. 그 후 거버넌스 도구 문서를 확인하여 할 수 있는 활동과 절차를 이해한다.

거버넌스 도구를 활용해 다음을 수행할 수 있다:

- 투표권을 DRep에게 위임
- 직접 DRep이 되기
- 거버넌스 안건 검토 및 투표
- 자체 거버넌스 안건 제출 등

## 거버넌스 상세

모든 Ada 보유자는 Cardano 블록체인에 거버넌스 안건을 제출할 수 있다. 각 거버넌스 안건은 온체인 투표를 통해 세 가지 거버넌스 기구 중 최소 두 곳에서 비준되어야 한다. 어떤 기구가 이를 비준해야 하는지는 안건의 유형과 거버넌스 체계의 상태에 따라 달라진다.

헌법 위원회는 **1인 1표** 방식으로 투표하며, SPO와 DRep은 **1 lovelace 1표** 방식으로 투표한다.

| Governance action | Name                                                | CC vote | DRep vote | SPO vote |
|-------------------|-----------------------------------------------------|---------|-----------|----------|
| 1                 | Motion of no-confidence                             | -       | ✓         | ✓        |
| 2a                | Update committee/threshold (normal state)           | -       | ✓         | ✓        |
| 2b                | Update committee/threshold (state of no-confidence) | -       | ✓         | ✓        |
| 3                 | New constitution or guardrails script               | ✓       | ✓         | -        |
| 4                 | Hard fork initiation                                | ✓       | ✓         | ✓        |
| 5a                | Protocol parameter changes, network group           | ✓       | ✓         | -        |
| 5b                | Protocol parameter changes, economic group          | ✓       | ✓         | -        |
| 5c                | Protocol parameter changes, technical group         | ✓       | ✓         | -        |
| 5d                | Protocol parameter changes, governance group        | ✓       | ✓         | -        |
| 6                 | Treasury withdrawal                                 | ✓       | ✓         | -        |
| 7                 | Info                                                | ✓       | ✓         | ✓        |

## Intersect 회원 기반 조직

**Intersect MBO**는 미국 와이오밍에 설립된 비영리 조직으로, 새로운 거버넌스 시스템을 지원하기 위해 만들어졌다. Intersect는 Cardano의 연속성과 미래 개발을 보장하고, 거버넌스 프로세스를 촉진한다. 이를 위해 이사회와 여러 자문 위원회를 두어 Cardano 블록체인 및 생태계의 유지·개발을 조율한다. 위원회는 연 2회 실시되는 선거를 통해 Intersect 회원이 선출한다. 모든 커뮤니티 구성원이나 조직은 Intersect 회원이 될 수 있다. 회원은 Ada 보유량과 관계없이 **1인 1표** 방식으로 위원회 선거에 투표한다.

Intersect 회원 등급은 세 가지로 나뉜다:

- **준회원(Associate level):** 무료 가입, 커뮤니티 행사 초대, 커뮤니티 뉴스 공유
- **개인 회원(Individual level):** 소액 가입비(현재 미화 10달러), Intersect 선거 투표권, 위원회 참여 자격, 보조금 신청 가능
- **기업 회원(Enterprise level):** 더 높은 가입비(현재 미화 1,000달러), 개인 회원 혜택 포함, Intersect 웹사이트 및 연례 보고서에 기업 프로필 게재