

아이오타(IOTA)

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.

IOTA 기술 및 토크노믹스 백서

목차

1. [소개](#)
2. [토크노믹스](#)
 - 2.1. [스테이킹 및 보상](#)
 - 2.1.1. [검증자 스테이킹 풀 요건](#)
 - 2.2. [수수료 구조](#)
3. [기술 기반](#)
 - 3.1. [객체 중심 설계](#)
 - 3.2. [합의 메커니즘](#)
 - 3.3. [스마트 컨트랙트](#)
 - 3.4. [트랜잭션 생애주기](#)

부록: [총 공급량 및 유통량](#)

소개

IOTA는 실제 응용 사례를 온체인으로 구현하기 위해 설계된 오픈소스 분산 원장 기술이다. 확장 가능하고, 효율적이며, 안전한 IOTA는 기업 솔루션과 Web3 혁신에 최적화된 공공재 인프라를 구동한다. 스마트 컨트랙트와 모듈형 아키텍처를 갖춘 IOTA 메인넷은 다양한 애플리케이션을 위한 글로벌 퍼미션리스 기반과 시장 채택으로 이어지는 효율적인 경로를 제공한다.

산업 및 공공 부문 협업에서 입증된 실적을 바탕으로, IOTA는 공급망 관리, 디지털 신원, 에너지 시스템 등 다양한 분야에 적용되어 왔다. 또한 개발자들이 탈중앙화 애플리케이션, 디파이(DeFi) 프로젝트, 맞춤형 블록체인 기반 솔루션을 구축할 수 있도록 지원한다.

소개

IOTA는 실제 응용 사례를 온체인으로 구현하기 위해 설계된 오픈소스 분산 원장 기술이다. 확장 가능하고 효율적이며 안전한 IOTA는 기업 솔루션과 Web3 혁신에 최적화된 공공재 인프라를 구동한다. 스마트 컨트랙트와 모듈형 아키텍처를 통해 IOTA 메인넷은 다양한 애플리케이션을 위한 글로벌 퍼미션리스 기반과 시장 채택을 위한 간결한 경로를 제공한다.

산업 및 공공 부문과의 협업에서 입증된 실적을 바탕으로, IOTA는 공급망 관리, 디지털 신원, 에너지 시스템 등 다양한 분야에 적용되어 왔다. 또한 개발자들이 탈중앙화 애플리케이션, 디파이(DeFi) 프로젝트, 맞춤형 블록체인 기반 솔루션을 구축할 수 있도록 지원한다.

토크노믹스

IOTA 토큰(\$IOTA)은 IOTA 네트워크 내 경제 활동의 기반이 되는 네이티브 자산이다. 이 토큰의 설계는 사용자가 시스템과 상호작용하는 방식, 자원이 할당되는 방식, 합의가 유지되는 방식을 규정한다. IOTA의 토크노믹스는 인센티브, 네트워크 보안, 지속 가능한 성장을 균형 있게 조율하며 IOTA의 비전과 정렬되도록 정교하게 설계되어 있다.

IOTA 네트워크의 리베이스(rebase)와 함께, 총 46억 개의 IOTA 토큰이 이전 Stardust 네트워크에서 마이그레이션되었다. 모든 기존 토큰은 이제 IOTA 메인넷에서 0x2::iota::IOTA 타입의 객체로 표현된다. 이러한 토큰은 Stardust 기반 네트워크에서 사용된 동일한 16진수 주소에서 계속 접근 가능하며, 별도의 수동 마이그레이션은 필요하지 않다. 각 IOTA 토큰은 NANO라는 더 작은 단위로 분할될 수 있으며, 1 IOTA는 10억 NANO와 동일하다. 유통량과 인플레이션에 대한 요약은 부록: 총 공급량 및 유통량에서 확인할 수 있다.

\$IOTA는 또한 스테이킹을 통해 네트워크 보안에 필수적이다. 본 프로토콜은 위임 지분 증명(Delegated Proof-of-Stake, DPoS) 메커니즘을 사용하며, 이는 검증자의 영향력이 위임된 지분에 의해 결정됨을 의미한다. 사용자는 자신의 IOTA 토큰을 검증자에게 위임하여 네트워크 보안을 지원하고 발행되는 보조금(subsidy)의 일부를 보상으로 획득한다. 24시간 에포크(epoch)가 종료될 때마다 767,000개의 새로운 IOTA 토큰이 발행되며, 이는 전체 공급량 대비 연간 6%의 초기 발행률에 해당한다. 새롭게 발행되는 IOTA 토큰의 수는 에포크마다 고정되어 있으므로, 비율 기준으로는 시간이 지남에 따라 발행률이 변한다. 이 토큰은 검증자 성능, 수수료율, 위임 지분의 양에 따라 참여자에게 분배된다.

IOTA 토큰은 교환 수단 외에도 여러 핵심 기능을 갖는다. 우선, 네트워크에서 발생하는 트랜잭션 수수료와 스토리지 예치금을 지불하는 데 사용된다. 모든 트랜잭션은 자동으로 소각되는 소량의 수수료를 발생시키며, 이는 전체 토큰 공급량을 줄이는 효과를 갖는다. 또한, 검증자에게 스토리지 부담을 증가시키는 트랜잭션의 경우 소량의 예치금이 잠금된다. 이 예치금은 해당 스토리지 수요가 해제되면 사용자에게 반환된다.

따라서 IOTA 토큰의 총 공급량은 시간이 지남에 따라 변동하며, 이는 새로운 토큰 발행과 수수료 소각이라는 상반된 두 힘에 의해 영향을 받는다. 보조금 발행은 프로토콜 수준에서 처리되며, 수수료 소각은 네트워크 사용에 따라 자동으로 발생한다. 결과적으로, IOTA 토큰 공급량에는 상한선이 없지만, 그 증가율은 시간이 지나도 최대한 선형(linear)을 유지하도록 설계되어 있다.

다음 섹션에서는 수수료, 스테이킹 메커니즘, 검증자 구조 등 IOTA 경제의 각 구성 요소를 보다 자세히 살펴본다.

스테이킹 및 보상

독립적인 검증자 집합이 IOTA 네트워크에 참여하며, 각 검증자는 전용 장비나 가상 서버에서 자체적인 IOTA 소프트웨어 인스턴스를 운영한다. 각 검증자는 클라이언트가 전송한 읽기 및 쓰기 요청을 처리하며, 트랜잭션을 검증하고 온체인 정보를 갱신한다. 이러한 활동은 당연히 보상된다. 본 섹션에서는 해당 보상 방식에 대해 자세히 설명한다.

IOTA는 Delegated Proof-of-Stake(DPoS)를 사용하여 네트워크를 운영하는 검증자와 그들의 투표권을 결정한다. 합의에 참여하는 검증자 위원회는 처음에는 최소 요건을 충족하는 후보 중 상위 50명의 스테이커로 구성된다(참고: [2.1.1. 검증자 스테이킹 풀 요건](#)). 탈중앙화를 강화하면서 성능을 저해하지 않도록, 최대 위원회 규모는 150명으로 점차 확대할 계획이다. 이러한 검증자들은 스테이킹 보상을 통해 선의의 참여를 유도하며, 부정행위 발생 시 보상이 삭감된다(slash). 검증자와 해당 위임자 집합을 “스테이킹 풀”이라 지칭한다.

IOTA는 자체 보관(self-custodial) 스테이킹 방식을 채택하고 있으며, 스테이커는 스테이킹한 IOTA 토큰을 자신의 계정에 보관한다. IOTA 토큰 보유자는 언제든지 IOTA를 인출하거나 선택한 검증자를 변경할 수 있다. 중앙 집중화와 관련된 보안 위험을 완화하기 위해, 단일 검증자의 투표권은 전체 위임 지분의 10%로 상한이 설정된다. 특정 검증자가 전체 위임 지분의 10%를 초과하여 받는 경우, 초과분은 이 한도 이상 반영되지 않으며, 그 초과 지분은 다른 검증자에게 분산된다. 이후 문서에서 “투표권” 또는 “풀 지분”이라는 용어는 이 상한이 적용된 값을 의미한다.

IOTA 네트워크의 운영은 시간적으로 겹치지 않는 고정된 지속시간(약 24시간)의 에포크(epoch)로 구분된다. 특정 에포크 동안에는 네트워크에 참여하는 검증자 집합과 그들의 투표권이 고정된다. 에포크 경계에서는 재구성이 발생할 수 있으며, 이로 인해 참여 검증자 집합과 그들의 투표권이 변경될 수 있다. 사용자가 특정 검증자에게 스테이킹을 하면, 그 지분은 다음 에포크부터 해당 검증자의 투표권에 반영된다. 마찬가지로 사용자가 스테이킹을 철회하면, 그 지분은 다음 에포크부터 투표권에 반영되지 않는다. 스테이킹 보상의 분배 또한 에포크 경계에서 처리된다. 이 과정은 다음과 같이 진행된다:

1. 각 에포크 E의 시작 시점에, 주어진 검증자 i에 대한 위임된 토큰 $poolStake(i, E)$ 이 합산되어 새로운 검증자 위원회가 구성된다. 이 작업 이후, 프로토콜은 모든 검증자에게 위임된 IOTA의 합을 통해 총 스테이킹 양 $totalStake(E)$ 을 계산한다.
2. 에포크 동안 사용자는 IOTA 네트워크에 트랜잭션을 제출하고, 검증자는 이를 처리한다. 각 트랜잭션마다 사용자는 계산 수수료, 스토리지 예치금, 그리고 선택적으로 우선 처리를 위한 팁을 지불한다(참고: [2.2. 수수료 구조](#)). 사용자가 기존 객체나 객체 내 데이터를 삭제하는 경우, 스토리지 예치금의 일부를 환급받는다. 검증자는 서로의 행위를 모니터링하고 성능을 평가한다.

3. 각 에포크 E 종료 시점에, 프로토콜은 참여자에게 스테이킹 보상을 분배한다. 이 분배 과정은 다음과 같은 주요 단계로 이루어진다:

a) 각 스테이킹 풀에 최대 보상 금액이 할당되며, 이는 각 풀의 지분과 전체 보상 총액에 비례하여 계산된다. 스테이킹 보상은 검증자 보조금 subsidy(현재 에포크당 767,000 IOTA 토큰)와, 해당 에포크 동안 사용자가 지불한 팁의 총액 tips(E)으로 구성된다. 에포크 \$E\$에서 검증자 풀 \$i\$의 최대 보상 금액 maxPoolReward(i,E)는 다음과 같이 계산된다:

$$\text{maxPoolReward}(i,E) = \frac{\text{poolStake}(i,E)}{\text{totalStake}(E)} \times (\text{subsidy} + \text{tips}(E))$$

b) 위 값은 최소 성능 요건을 충족하지 못한 검증자를 반영하도록 조정된다. 검증자 i의 에포크 E에 대한 성능 계수는 performance(i,E)로 나타내며, 완전한 성능을 보인 경우 performance(i,E) = 1, 성능이 부족한 경우 performance(i,E) < 1이다. 이 변수는 검증자가 금전적 위험을 감수하며 IOTA 네트워크를 효율적으로 운영하도록 유도하기 위해 존재한다. 각 풀에 실제로 분배되는 보상 poolReward(i,E)는 다음과 같이 계산된다:

$$\text{poolReward}(i,E) = \text{performance}(i,E) \times \text{maxPoolReward}(i,E)$$

c) 이제 각 풀의 보상 금액은 검증자와 위임자 간에 분배된다. 검증자는 총 풀 보상에서 운영 비용을 충당하기 위해 최대 20%까지의 커미션 com(i,E)을 수수료로 차감한다. 나머지 보상은 검증자 외의 모든 사용자에게 그들의 지분 비율에 따라 분배된다. 구체적으로, 위임자 j가 에포크 E에서 풀 i에 위임한 지분을 stake(j,E)라 할 때, 해당 에포크에서 위임자 j의 보상과 검증자 i의 보상은 다음과 같다:

$$\text{delegatorReward}(j,E) = \frac{\text{stake}(j,E)}{\text{poolStake}(i,E)} \times (1 - \text{com}(i,E)) \times \text{poolReward}(i,E)$$

$$\text{validatorReward}(i,E) = \text{com}(i,E) \times \text{poolReward}(i,E)$$

결과적으로, 검증자는 성능이 우수하고 더 많은 위임 지분을 유치할수록 더 많은 보상을 받을 수 있다. 반면, IOTA 토큰 스테이커는 자신이 선택한 검증자가 성능 저하로 인해 페널티를 받을 경우 보상이 줄어든다. 응답하지 않는 검증자는 IOTA 인센티브 구조에 이중으로 노출되며, 직접적으로는 보상이 삭감되고, 간접적으로는 스테이커들이 보다 응답성이 높은 검증자로 토큰을 이동시키면서 향후 에포크에서 위임 지분이 줄어든다.

검증자 스테이킹 풀 요건

검증자가 검증자 위원회에 포함되기 위해 충족해야 하는 최소 스테이킹 요건이 존재한다. 구체적으로는 다음과 같다:

- 검증자 후보는 검증자 세트에 가입을 요청하기 전에 최소 200만 IOTA의 위임 지분을 확보해야 한다.
- 활성 검증자의 위임 지분이 150만 IOTA 이하로 떨어질 경우, 검증자 세트에서 제외되기 전까지 7 에포크의 유예 기간이 주어진다.
- 활성 검증자의 위임 지분이 100만 IOTA 미만으로 떨어질 경우, 해당 에포크 종료 시점에 검증자 세트에서 제외된다.

수수료 구조

IOTA 경제 모델 및 인센티브 구조의 핵심 요소로서, IOTA의 트랜잭션 수수료 메커니즘은 두 가지 목적을 달성한다:

1. 낮고 예측 가능한 트랜잭션 수수료 제공
2. 스팸 공격 방지

이를 통해 사용자는 가스비의 현재 시장 가격을 예측할 필요 없이 IOTA 네트워크 사용에 집중하여 최상의 사용자 경험을 제공할 수 있다. 검증자는 자신의 역할을 제대로 수행함으로써 보조금을 받기 때문에, 사용자 수수료에만 의존하지 않는다.

IOTA 네트워크의 트랜잭션 수수료는 의도적으로 최소화되어 있으며, 접근성을 높이면서 경제적 지속 가능성을 유지하도록 설계되었다. 이 수수료의 일부는 소각되며, 이는 스테이킹 보상에 사용되는 토큰의 인플레이션 발행을 상쇄하는 디플레이션 메커니즘을 도입한다. 또 다른 일부는 원장 상의 데이터 저장 비용을 충당하기 위해 할당되며, 이를 통해 네트워크의 경제적 인센티브가 자원 사용의 책임성과 연계된다. 원장에 저장된 데이터가 이후 해제될 경우, 해당 저장 공간에 할당된 토큰은 전액 환급되어 스토리지 자원의 효율적 사용을 장려하고 시간이 지나도 원장이 최적화된 상태를 유지하도록 한다.

사용자가 실제로 지불하는 순수수수료(net fees)는 다음과 같이 계산된다:

$$\text{net_gas_fees} = \text{computation_fee} + \text{storage_deposit} - \text{storage_rebate}$$

트랜잭션 블록마다 IOTA 네트워크 익스플로러에는 순수 가스비 정보가 표시된다.

계산 수수료와 스토리지 예치금은 서로 다른 결제 항목으로 간주되지만, 개념적으로는 유사하다. 각각은 연산 또는 저장 단위를 해당 단가와 곱하여 IOTA 단위로 환산되기 때문이다. 스토리지 항목은 100% 환급 가능하므로, ‘스토리지 수수료’와 ‘스토리지 예치금’이라는 용어는 혼용되어 사용된다.

스토리지 수수료

스토리지 수수료는 온체인 스토리지에 기록되는 신규 데이터의 양에 따라 달라진다. 저장되는 각 바이트는 100개의 스토리지 단위(storage units)로 환산된다. 예를 들어, 저장 효과가 25바이트인 트랜잭션은 2,500 스토리지 단위에 해당하는 수수료를 발생시킨다. 중요한 점은, 환급 메커니즘이 사용자로 하여금 저장 요구량을 줄이고 사용하지 않는 객체를 정리함으로써 전체 노드에 가해지는 스토리지 부담을 최소화하도록 유도한다는 것이다. 트랜잭션의 스토리지 수수료는 다음과 같이 주어진다:

$$\text{storage_fee} = \text{storage_units} \times \text{storage_price}$$

여기서 storage_price는 프로토콜에 의해 설정되며, storage_units는 사용자가 사전에 인지할 수 있다.

연산 수수료

IOTA의 트랜잭션 유형마다 처리 및 실행에 필요한 연산량이 다르다. IOTA는 각 트랜잭션을 연산 단위(computation units)로 측정하여 이러한 다양한 연산 부하를 트랜잭션 수수료로 환산한다. 일반적으로, 복잡한 트랜잭션일수록 더 많은 연산 단위를 필요로 한다.

IOTA는 연산 단위를 1,000 단위로 반올림하여 가스 소비량을 계산하며, 모든 트랜잭션은 최소 1,000 연산 단위를 소비한다. 최대 소비 가능량은 5,000,000 연산 단위이며, 이 이상이 필요한 트랜잭션은 실행이 중단된다. IOTA 가스 가격 책정은 다음과 같이 연산 수수료를 계산한다:

$$\text{computation_fee} = \text{computation_units} \times \text{gas_price}$$

여기서 사용자가 \$gas_price\$를 지정한다. 이 값은 프로토콜에서 정의한 reference_gas_price 이상이어야 한다. 이 수수료 중 소각되는 부분은 다음과 같다:

$\text{computation_units} \times \text{reference_gas_price}$

소각되지 않은 초과분은 검증자에게 전달되는 팁으로 간주되며, 보상과 함께 분배된다. 팁의 구체적인 값은 다음과 같이 계산된다:

$\text{tip} = (\text{gas_price} - \text{reference_gas_price}) \times \text{computation_units} \geq 0$

이 팁은 소각되지 않으며, 대신 참여자 간에 분배된다(참고: [2.1. 스테이킹 및 보상](#); 에포크 \$E\$에서 분배되는 보상은 $\text{subsidy} + \text{tips}(E)$ 에 비례한다는 점에 유의). 다만, 일반적인 네트워크 운영 중에는 $\text{gas_price} = \text{reference_gas_price}$ 로 설정하여 수수료의 소각분만 지불해도 트랜잭션이 신속히 포함되는 것이 기대된다.

gas_price 외에도 사용자는 gas_budget을 정의해야 한다. 이는 트랜잭션 제출 이전에 정확한 실행 비용을 예측할 수 없기 때문에, 사용자가 지불할 가스 수수료의 상한선을 설정하는 역할을 한다. IOTA 트랜잭션의 가스 예산은 IOTA 단위로 정의되며, 다음 조건을 만족해야 트랜잭션이 성공적으로 실행된다:

$\text{gas_budget} \geq \{\text{computation_fees}, \text{net_gas_fees}\}$

궁극적으로, 성공적인 트랜잭션은 사용자가 해당 트랜잭션의 net_gas_fees를 지불해야 한다. 다만, 스토리지 수수료와 환급은 트랜잭션이 완전히 실행된 후에만 계산될 수 있기 때문에, 실행 도중 노드는 computation_fees의 하한값만 추정 가능하고 net_gas_fees는 알 수 없다. 가스 예산의 검사는 다음 방식으로 이루어진다:

- 실행 도중, computation_units(및 결과적으로 computation_fees)의 하한값이 주기적으로 계산된다. 만약 해당 트랜잭션의 gas_budget이 이러한 연산 수수료를 감당할 수 없을 경우, 트랜잭션은 중단(abort)된다. 이 경우 전체 gas_budget이 청구된다.
- 실행이 중단되지 않은 경우(gas_budget이 computation_fees를 충분히 감당할 수 있었음을 의미), 트랜잭션의 효과를 기준으로 스토리지 수수료와 환급이 계산된다.
 - 스토리지 환급이 스토리지 수수료보다 크거나 같은 경우, $\text{net_gas_fees} \leq \text{computation_fees}$ 이며, 이는 사용자가 설정한 예산이 반드시 충분하다는 것을 의미한다. 이 경우 트랜잭션은 성공적으로 실행되며, 사용자에게는 net_gas_fees가 청구된다.
 - 스토리지 환급이 스토리지 수수료보다 적은 경우($\text{net_gas_fees} > \text{computation_fees}$ 를 의미)이고, 사용자가 설정한 예산이 이러한 net_gas_fees를 감당할 수 있을 경우, 트랜잭션은 성공적으로 실행되며, 사용자에게는 net_gas_fees가 청구된다.
 - 마지막으로, $\text{net_gas_fees} > \text{computation_fees}$ 이지만 사용자가 설정한 예산이 해당 net_gas_fees를 감당하지 못하는 경우, 트랜잭션은 실패하게 된다. 이 경우, 트랜잭션 입력 객체의 변경과 관련된 스토리지 수수료와 함께 computation_fees가 청구된다.

일부 경우—특히 스토리지 환급이 많아 순 스토리지 수수료가 음수가 되는 경우—사용자가 실제로 지불하는 전체 가스 수수료(즉, net_gas_fees)가 연산 수수료보다 낮을 수 있다는 점에 유의해야 한다. 따라서 일반적으로, 트랜잭션이 성공적으로 처리되기 위해서는 사용자가 설정한 가스 예산이 최종적으로 지불하게 되는 순 가스 수수료보다 상당히 높아야 할 때가 많다.

중요하게도, 최소 가스 예산은 1,000,000 나노(NANOS) 또는 0.001 IOTA이다(모든 트랜잭션은 최소 1,000 연산 단위를 사용하며, reference_gas_price가 1,000 NANOS일 때를 기준으로 한다).

기술 기반

IOTA는 이전 블록체인 시스템의 확장성, 프로그래머빌리티, 탈중앙화 측면의 한계를 해결하기 위해 설계된 차세대 분산 원장 기술이다. 거의 10년에 걸친 연구 개발을 기반으로, IOTA는 Move 가상 머신 (MoveVM)과 같은 첨단 혁신을 아키텍처에 통합하여 전 세계 금융 및 산업 응용에 적합한 안전하고 확장 가능하며 효율적인 플랫폼을 구축한다.

IOTA는 Byzantine Fault Tolerant(비잔틴 장애 허용) 합의 프로토콜인 Mysticeti를 사용하여 강력한 네트워크 보안과 높은 처리량을 달성한다. 이를 통해 트랜잭션은 수 초 미만(sub-second) 내에 확정되며, 초당 수만 건의 트랜잭션을 지원할 수 있다. Mysticeti의 기반 구조인 DAG는 기존 블록체인의 병목 현상을 제거하여 시스템이 높은 수요 하에서도 효율적으로 유지되도록 한다. 프로토콜에 기본으로 내장된 디지털 자산 기능은 사용자가 스마트 컨트랙트에 의존하지 않고 직접 토큰을 생성하고 관리할 수 있게 하여 복잡성과 비용을 줄인다.

IOTA 생태계는 L1과 L2 모두에서 프로그래머빌리티를 제공하며, 각각 Move와 EVM/Solidity 스마트 컨트랙트를 사용한다:

레이어 1

Move는 디지털 자산 관리 및 스마트 컨트랙트를 위해 특별히 설계된 강력하고 안전한 프로그래밍 언어이다. 그 고유한 기능은 블록체인 환경에서 개발자에게 이상적인 선택지를 제공한다. IOTA에서 Move가 갖는 핵심 특징은 다음과 같다:

- **객체 중심 설계:** Move는 본질적으로 객체 중심 언어로, 개발자가 복잡한 데이터 구조와 상호작용을 직관적으로 모델링할 수 있게 한다. Move에서는 자산, 사용자, 계약 등을 나타내는 객체를 정의할 수 있으며, 상태와 동작을 자연스럽게 명확하게 관리할 수 있도록 지원한다.
- **성능:** IOTA에서의 Move는 전역 공유 상태가 아닌 객체 모델을 기반으로 한다. 이 구조 덕분에 트랜잭션이 병렬로 실행될 수 있으며, 이는 높은 네트워크 처리량, 낮은 혼잡도, 결과적으로 더 낮은 가스비로 이어진다.
- **보안성:** Move는 안전성과 효율성을 최우선으로 하며, Rust의 소유권 모델에서 영감을 받은 메모리 관리 및 자원 제어 방식을 채택한다. 컴파일러는 일반적인 프로그래밍 오류를 방지하기 위한 엄격한 규칙을 강제하며, 자산이 사용자 계정 내에서 안전하게 유지되고 올바른 키 없이는 접근할 수 없도록 보장한다. 컴파일러가 배포 전 많은 잠재적 문제를 탐지하지만, 개발자는 스마트 컨트랙트 구현 시 논리 오류, 산술 오버플로우, 기타 런타임 문제에 주의해야 한다.

레이어 2

EVM은 “Ethereum Virtual Machine(이더리움 가상 머신)”의 약자로, 현재 대부분의 스마트 컨트랙트 네트워크에서 검증된 가상 머신이다. Solidity는 EVM 전용으로 만들어진 주요 프로그래밍 언어이다. EVM/Solidity를 사용하는 가장 큰 장점은 수년간의 개발을 통해 축적된 방대한 개발 리소스이다. IOTA 스마트 컨트랙트 구현은 이러한 리소스와 완벽히 호환되며, IOTA EVM 상에서 개발할 때 기존의 모든 EVM 개발 도구를 그대로 활용할 수 있게 해준다. 기존에 작성된 모든 스마트 컨트랙트는 수정 없이 IOTA 스마트 컨트랙트 상에서 배포할 수 있다. 다만, EVM은 L2 상에서의 스마트 컨트랙트 실행 표준으로 자리잡았지만, Move 스마트 컨트랙트와 같은 L1의 고유 기능과 역량을 염두에 두고 설계된 것은 아니다. Move는

자산 보안, 자원 관리, 형식적 검증에 중점을 둔 언어로서 L1 수준에서 근본적으로 다른 접근 방식을 제공한다.

이러한 고유 기능들을 결합함으로써, IOTA는 탈중앙화 금융부터 공급망 관리에 이르기까지 다양한 산업을 위한 견고하고 미래지향적인 인프라를 제공하며, 분산 원장 기술에서 보안, 효율성, 확장성의 새로운 기준을 제시한다.

객체 중심 설계

IOTA에서 스토리지의 기본 단위는 객체(object)이다. 키-값 저장소를 기반으로 하는 계정 중심의 많은 블록체인들과 달리, IOTA의 저장 모델은 객체 중심이며, 각 객체는 온체인에서 고유한 ID를 통해 주소화된다. IOTA에서 스마트 컨트랙트는 패키지(package)로 알려진 객체이며, 이 스마트 컨트랙트들은 IOTA 네트워크 상의 다른 객체들과 상호작용한다:

- **IOTA Move 패키지:** IOTA Move 바이트코드 모듈의 모음이다. 각 모듈은 해당 패키지 내에서 고유한 이름을 갖는다. 패키지의 온체인 ID와 모듈 이름을 결합하면 모듈이 고유하게 식별된다. IOTA에서 스마트 컨트랙트를 게시할 때, 패키지가 게시 단위가 된다. 일단 게시되면, 해당 패키지 객체는 적절한 권한이 있는 경우에만 업그레이드할 수 있다. 패키지 객체는 IOTA에 이전에 게시된 다른 패키지 객체에 의존할 수 있다.
- **IOTA Move 객체:** 특정 IOTA Move 패키지의 IOTA Move 모듈에 의해 관리되는 타입 지정된 데이터이다. 각 객체 값은 구조체(struct)이며, 필드에는 정수나 주소와 같은 기본형, 다른 객체, 객체가 아닌 구조체 등이 포함될 수 있다.

IOTA에서의 트랜잭션은 객체를 입력으로 받아 이를 수정하고, 새로운 또는 수정된 객체를 출력으로 생성한다. 각 객체는 자신을 출력으로 생성한 마지막 트랜잭션의 해시를 기록한다. 객체와 트랜잭션 사이의 이러한 관계는 방향성 비순환 그래프(DAG)로 표현될 수 있으며, 여기서:

- 노드는 트랜잭션을 나타낸다.
- 방향성 간선은 트랜잭션 A의 출력 객체가 트랜잭션 B의 입력으로 사용될 경우 A에서 B로 연결된다. 이러한 간선은 객체 참조로 라벨링되며, A에 의해 생성되고 B에 의해 사용된 정확한 버전을 명시한다. 이 DAG의 루트는 입력이 없고 시스템의 초기 상태에서 존재하는 객체들을 생성하는 제네시스 트랜잭션이다. 이 DAG는 아직 소비되지 않은 변경 가능한 트랜잭션 출력들을 식별하고, 이들을 입력으로 사용하는(선택적으로 변경 불가능한 출력도 포함할 수 있는) 새로운 트랜잭션을 발행함으로써 확장될 수 있다.

트랜잭션의 입력으로 사용 가능한 객체들의 집합은 라이브 객체(live objects)이며, IOTA가 유지하는 전역 상태는 이러한 모든 객체들로 구성된다. 특정 IOTA 주소 A의 라이브 객체는 A가 소유한 모든 객체와 시스템 내의 모든 공유 및 변경 불가능 객체를 포함한다.

이 DAG가 모든 커밋된 트랜잭션을 포함하면, 시스템의 상태 및 이력에 대한 완전하고 암호학적으로 검증 가능한 뷰(view)를 형성한다. 또한 단일 주소가 소유한 객체 등, 특정 트랜잭션이나 객체 집합에 대한 관련 이력을 기반으로 한 DAG를 별도로 구성할 수도 있다.

IOTA 네트워크의 모든 객체는 해당 객체가 트랜잭션 내에서 어떻게 접근되고 사용할 수 있는지를 정의하는 소유권 모델을 가진다. 객체의 소유권 유형은 누가 해당 객체에 대해 상호작용할 권한을 갖는지, 그리고 어떻게 조작할 수 있는지를 결정한다. IOTA에서 객체는 다음과 같을 수 있다:

- **공유 객체(Shared):** 어떤 트랜잭션이든 읽기 및 쓰기 접근 가능
- **소유 객체(Owned):** 해당 소유자의 서명이 있는 트랜잭션만 읽기 및 쓰기 접근 가능

공유 객체와 소유 객체는 각각 고유한 장점과 단점을 제공하므로, 애플리케이션 설계 시 신중한 고려가 필요하다. 오직 소유 객체만을 포함하는 트랜잭션은 합의 절차를 우회하기 때문에 매우 짧은 확정(latency to finality) 시간을 갖는 이점을 제공한다. 그러나 이러한 객체는 오직 소유자만 접근할 수 있어, 다수의 주체 간 상호작용이 필요한 처리 절차를 복잡하게 만든다. 반면, 공유 객체가 포함된 트랜잭션은 읽기 및 쓰기 접근을 관리하기 위해 합의를 필요로 하며, 이는 다소 높은 가스 비용과 지연 시간 증가로 이어질 수 있다. 다수의 공유 객체나 자주 접근되는 인기 객체에 대한 동시 접근이 발생할 경우, 경쟁으로 인해 지연이 더욱 커질 수 있다.

아래는 IOTA에서의 객체 유형과 그 소유권에 대한 예시이다:

- **변경 불가능 객체(Immutable Objects):** IOTA에서는 객체가 변경 가능하거나 변경 불가능할 수 있다. 변경 불가능 객체는 생성 이후 수정, 이전, 삭제가 불가능하다는 점에서 고유하다. 객체가 한 번 변경 불가능 상태로 지정되면 소유자가 존재하지 않으며, 네트워크상의 누구나 접근할 수 있다.
- **주소 기반 소유 객체(Address-Owned Objects):** 주소 기반 소유 객체는 특정 32바이트 주소에 연결된다. 이 주소는 특정 서명 체계에서 유도된 계정 주소이거나 객체 ID일 수 있다. 이러한 객체는 오직 소유자만이 접근할 수 있으며, 소유권이 이전되지 않는 한 다른 주체는 상호작용할 수 없다.
- **공유 객체(Shared Objects):** 공유 객체는 `0x2::transfer::share_object` 함수를 통해 네트워크상의 모든 사용자에게 공개된다. 주소 기반 객체와 달리, 공유 객체는 단일 소유자에 의해 제한되지 않으며, 네트워크상의 어떤 주체든 해당 객체를 읽거나 수정할 수 있다. 이처럼 확장된 접근성은 특정 응용에 유리할 수 있으나, 민감한 작업이 포함된 경우 보안에 대한 신중한 고려가 요구된다.

합의 메커니즘

IOTA는 Mysticeti 합의 메커니즘을 사용한다. 이는 보안성, 확장성, 에너지 효율성을 보장하기 위해 설계된 최첨단 프로토콜이다. Mysticeti는 Delegated Proof-of-Stake(DPoS) 프레임워크 내에서 작동하며, 검증자는 스테이크를 기준으로 선택되어 합의 과정에 참여한다. 이러한 기술 조합은 IOTA가 강력한 탈중앙화와 네트워크 안정성을 달성하는 동시에 고성능과 지속 가능성을 유지할 수 있게 해준다.

Mysticeti는 방향성 비순환 그래프(DAG) 아키텍처를 활용하여 트랜잭션을 병렬로 처리하며, 수 초 미만(sub-second)의 확정성과 초당 5만 건 이상의 처리량을 지원한다. 기존 블록체인 시스템과 달리, Mysticeti는 명시적인 블록 인증 단계를 제거하고 합의 과정을 DAG 구조에 직접 통합함으로써 계산 오버헤드와 지연 시간을 획기적으로 줄인다. 리더가 없는 설계는 트랜잭션 검증 과정을 단일 주체가 통제하지 않도록 하여 장애 허용성을 강화한다.

Mysticeti 프로토콜은 고급 암호 기술을 기반으로 하여 네트워크의 보안성과 무결성을 보장한다. DPoS 프레임워크와 DAG의 혁신적 특성을 결합함으로써, IOTA는 다양한 산업에서 실제 응용을 안전하게 구동할 수 있는 확장 가능하고 효율적이며 탈중앙화된 인프라를 실현한다.

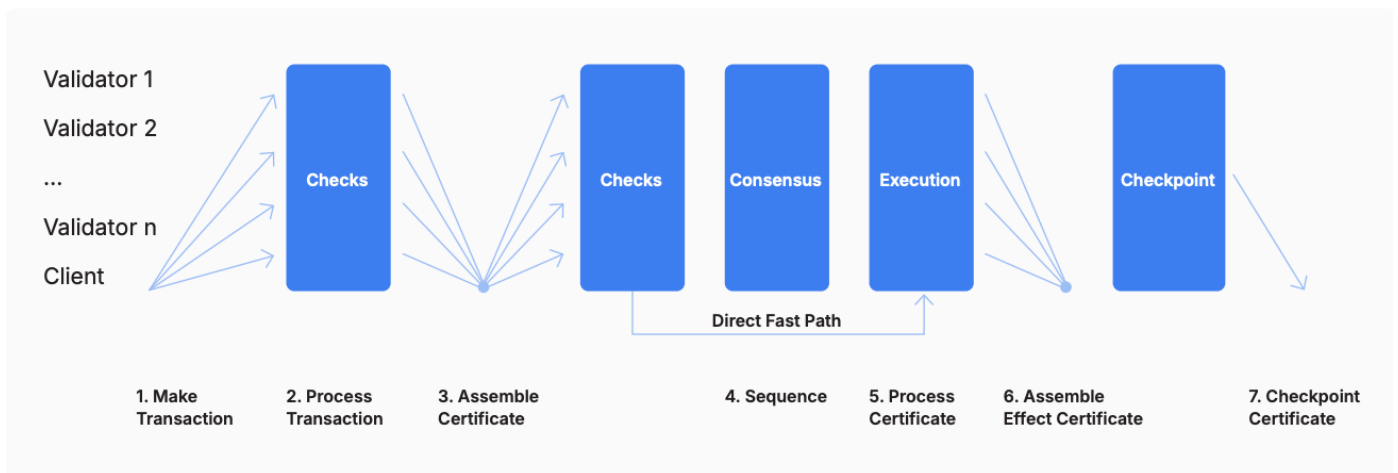
스마트 컨트랙트

IOTA의 베이스레이어 프로토콜은 강력한 분산 원장일 뿐만 아니라, 추가적인 기술 표준 및 계약 기반 프로토콜을 위한 유연한 기반으로 설계되었다. 이 비전의 핵심에는 Move 가상 머신(MoveVM)이 있으며, 이는 안전하고 자원 지향적인 프로그래밍 환경을 제공한다. MoveVM 계층은 개발자가 스마트 컨트랙트를 통해 새로운 기술 표준을 정의하고 강제할 수 있도록 하여, IOTA 베이스레이어 위에 구축된 프로토콜이 새로운 기술 및 산업 수요에 따라 진화할 수 있도록 지원한다.

IOTA 프로토콜은 Move 가상 머신(MoveVM)과 Move 프로그래밍 언어를 활용하여 안전하고 효율적인 스마트 컨트랙트 및 네이티브 자산 관리를 가능하게 한다. Move의 자원 지향적 프로그래밍 모델은 디지털 자산의 생성, 이전, 소각 과정에서 엄격한 보안 조치를 보장하며, 이중 지불(double-spending)이나 재진입 공격(re-entrancy attack)과 같은 취약점을 방지한다. 이 견고한 모델은 고급 탈중앙화 애플리케이션(dApp) 및 토큰화 생태계 개발을 지원한다.

IOTA의 원장은 외부 계층이나 추가 스마트 컨트랙트에 의존하지 않고도 디지털 자산의 생성 및 관리를 네이티브하게 지원한다. 개발자는 조건부 전송, 베스팅 일정, 준수 요건 등 사용자 지정 로직을 기반으로 자산을 프로그래밍 방식으로 발행(mint)하거나 소각(burn)할 수 있다.

Move 스마트 컨트랙트는 네이티브 자산과 원활하게 상호작용하며, 탈중앙화 금융(DeFi), NFT, 기타 토큰화 애플리케이션을 위한 안전하고 프로그래머블한 기능을 제공한다. 자원 지향적 설계는 자산 무결성을 강제하며 복잡한 워크플로우를 단순화하여 효율성과 확장성을 동시에 달성한다.



IOTA는 Move와 네이티브 자산 기능의 결합을 통해 디지털 생태계를 최소한의 복잡성으로 설계하고 관리할 수 있는 안전하고 확장 가능한 플랫폼을 제공하며, 최대한의 유연성을 실현한다.

트랜잭션 생애주기

트랜잭션 생애주기에 대한 고수준 개요는 아래와 같이 도식화 및 설명된다:

- **트랜잭션 생성:** 사용자는 트랜잭션을 풀 노드에 제출하고 개인 키로 서명한다. 트랜잭션은 사용자가 소유한 객체뿐만 아니라 공유 객체에도 영향을 미칠 수 있다.
- **검증자에게 제출:** 풀 노드는 해당 트랜잭션을 검증자 집합에 전달한다. 검증자들은 트랜잭션의 유효성을 확인하고, 이중 지불을 방지하기 위해 관련된 “소유 객체”를 잠근다. 검증이 완료되면, 검증자들은

자신의 서명을 풀 노드로 다시 전송한다.

- **트랜잭션 인증서 생성:** 풀 노드는 슈퍼다수(supermajority)의 검증자로부터 응답을 수집한 후, 트랜잭션 및 검증자 서명을 포함한 트랜잭션 인증서(transaction certificate)를 생성할 수 있다. 이 인증서는 모든 검증자에게 전송된다.
- **합의 및 실행:** 검증자들은 인증서의 트랜잭션 유효성을 검증하고, 트랜잭션 포함을 위한 절차를 시작한다. 트랜잭션이 오직 소유 객체만 포함하는 경우, IOTA는 합의를 기다릴 필요 없이 즉시 처리 및 실행할 수 있다(패스트 패스 합의). 그렇지 않은 경우, 트랜잭션은 IOTA의 합의 및 시퀀싱 모듈에 제출된 후 실행된다.
- **효과 인증서(Effects Certificate):** 트랜잭션이 실행된 후, 각 검증자는 해당 트랜잭션의 실행 효과에 서명하고 이를 풀 노드에 다시 전송한다. 트랜잭션의 효과는 변경되거나 생성되거나, 래핑되거나 언래핑되거나 삭제된 객체, 소비된 가스량, 트랜잭션의 실행 상태 등 발생한 내용을 상세히 기록한 것이다. 풀 노드는 이러한 서명된 효과를 다수의 검증자로부터 수집하여 효과 인증서(effects certificate)를 생성하고, 이를 통해 트랜잭션의 확정성을 보장한다.
- **체크포인트 포함:** 트랜잭션 생애주기의 마지막 단계는 체크포인트에 포함되는 것이다. 합의 계층은 전 세계적으로 합의된 트랜잭션 순서를 생성한다. 검증자들은 이 순서에서 일정 구간을 가져와 체크포인트를 형성하는데, 여기에는 트랜잭션 다이제스트 목록과 해당 효과의 다이제스트가 포함된다. 트랜잭션이 체크포인트에 포함되면, 이는 IOTA 네트워크의 영구 기록의 일부가 된다.

부록: 총 공급량 및 유통량

IOTA는 유통 토큰 공급량을 동적으로 조절하기 위해 발행(minting) 및 소각(burning) 메커니즘을 사용한다. 총 공급량 또는 유통 공급량에 사전 정의된 상한은 없지만, 해당 설계는 시간이 지남에 따라 공급량 증가가 최대한 선형(linear)으로 유지되도록 보장한다.

총 공급량 개요

IOTA 네트워크는 리베이스(Rebase) 시점에 4,600,000,000 IOTA 토큰의 초기 총 공급량으로 시작되었다. 각 에포크(약 하루마다)마다 최대 767,000 IOTA가 새로 발행되어 참여자에게 분배될 수 있다. 동시에 네트워크의 모든 트랜잭션은 소량의 토큰을 소각한다.

매일 최대 발행이 이루어지고 소각이 전혀 없다고 가정할 경우, 총 공급량은 365개의 에포크(약 1년)에 걸쳐 최대 279,955,000 IOTA만큼 증가할 수 있으며, 이는 첫 해에 최대 6.1%의 연간 성장률에 해당한다. 이후 연도에는 공급량 변화에 따라 증가율은 달라지겠지만, 절대적인 연간 공급량 증가는 일정하게 유지된다.

유통 공급량 개요

유통 공급량은 특정 시점에 잠금되지 않은 모든 토큰을 포함한다. 2025년 5월 5일에 새로운 IOTA 메인넷이 출시되었을 때, 초기 총 공급량의 일부는 IOTA의 [Stardust](#) 및 [Tokenomics](#) 업데이트에 따라 잠긴 상태로 유지되었다. 출시 시점에서의 유통 공급량은 3,746,223,720 IOTA였다.

발행 및 소각 메커니즘 외에도, 예정된 토큰 언락 일정에 따라 유통 공급량은 2027년 10월까지 점진적으로 증가하게 된다. 해당 시점 이후에는 모든 토큰이 언락되므로 총 공급량과 유통 공급량은 동일하게 된다.

언락 일정

2025년 5월 14일 – 10월 1일: 2주마다 19,137,719 IOTA가 언락되며, 10월 1일까지 총 210,514,906 IOTA가 언락된다. 토큰 발행량을 포함하면, 이 시점의 최대 유통 공급량은 약 4,074,089,626 IOTA에 달한다.

2025년 10월 – 2027년 9월 29일: 2주마다 언락되는 토큰 수량은 12,370,411 IOTA로 줄어들며, 이 기간 동안 추가로 643,261,373 IOTA가 언락된다. 지속적인 발행을 포함하면, 이 기간 종료 시점의 최대 유통 공급량은 5,274,192,999 IOTA에 도달하게 된다.

아래 그래프는 시간 경과에 따른 예상 최대 총 공급량 및 유통 공급량을 보여준다. 토큰 발행이 일정한 비율로 계속되는 한, 이 추세는 2027년 이후까지 외삽(extrapolate)될 수 있다.

IOTA Maximum Supply (millions of IOTAs)

