코티(COTI)

주요내용설명서(국문백서)

Korean White Paper

2026년 8월 6일

Disclaimer

본 번역본은 2026년 8월 6일 기준의 코티(COTI) 홈페이지 및 블로그의 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총발행량, 유통량 계획, 사업 계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

프로젝트 소개

코티(COTI)는 개인 정보 보호를 중시하는 이더리움 레이어2입니다. 코티는 이더리움에서 가장 빠르고 가벼운 기밀성 레이어입니다.

획기적인 암호 프로토콜 가블드 서킷(Garbled Circuit)으로 구동되고 이더리움으로 보호되는 코티V2(이하 코티)는 퍼블릭 블록체인에서 데이터 보호를 위한 최첨단 솔루션을 제공합니다. 다가올 웹3.0 혁신 및 채택 웨이브를 위한 초석을 다지는 코티는 기밀 트랜잭션[1], 머신 러닝, 디파이[2], 탈중앙화 신원 증명[3] 등을 포함하는 새로운 사용 사례를 열어줍니다.

코티는 가블드 서킷 및 다자간 연산[4]을 중심으로 하는 정교한 암호 프레임워크를 도입하여 EVM5[5] 호환 레이어2로서 온체인 개인 정보 보호를 위한 새로운 표준을 제시하며, 온체인에서 수행되는 다자간 연산은 뛰어난 모듈성, 보안, 개인 정보 보호, 성능을 제공합니다. 또한 코티는 기밀 트랜잭션 및 데이터 관리를 지원하여 이더리움 생태계의 확장성과 보안을 개선합니다.

비즈니스 모델

블록체인 기술에서 프라이버시는 매우 중요한 문제입니다. 분산된 네트워크의 투명성이라는 특징이 사용자들이 기대하는 기밀성과 충돌하기 때문입니다. 접근 제어 및 암호화와 같은 전통적인 시스템과는 달리, 특히 EVM 기반의 블록체인 플랫폼에는 내장된 개인 정보 보호 기능이 부족하여 모든 데이터가 네트워크 전반에 노출됩니다. 이러한 개방성은 기밀 유지가 필수적인 사용자나 산업의 참여를 방해하고, 데이터 노출 및 규제 문제를 야기할 수 있습니다.

---

[1] Transaction

[2] DeFi (decentralized finance)

[3] Decentralized identity (DID)

[4] Multi-party computation (MPC)

[5] Ethereum virtual machine

이러한 문제를 해결하기 위해 코티는 가블드 서킷을 도입하고 있습니다. 이는 블록체인의 투명성과 더 넓은 채택, 규제 준수, 그리고 사용자 프라이버시 존중에 필수적인 기밀성 사이의 균형을 맞추면서 프라이빗 트랜잭션을 가능하게 합니다.

개념적 개요: 가블드 서킷과 개인 정보 보호 원리

가블드 서킷은 개인 정보를 보호하는 암호화 기술로서, 본질적으로는 앤드류 야오[6]가 제시한 '백만장자 문제'를 해결하기 위해 설계되었습니다. 이 이론적인 시나리오에서, 두 백만장자 앨리스와 밥은 자신의 실제 순자산을 공개하지 않고 누가 더 부자인지 알아내고 싶어 합니다.

이를 위해 그들은 가블드 서킷을 사용할 수 있으며, 그 과정은 다음과 같은 단계로 단순화할 수 있습니다.

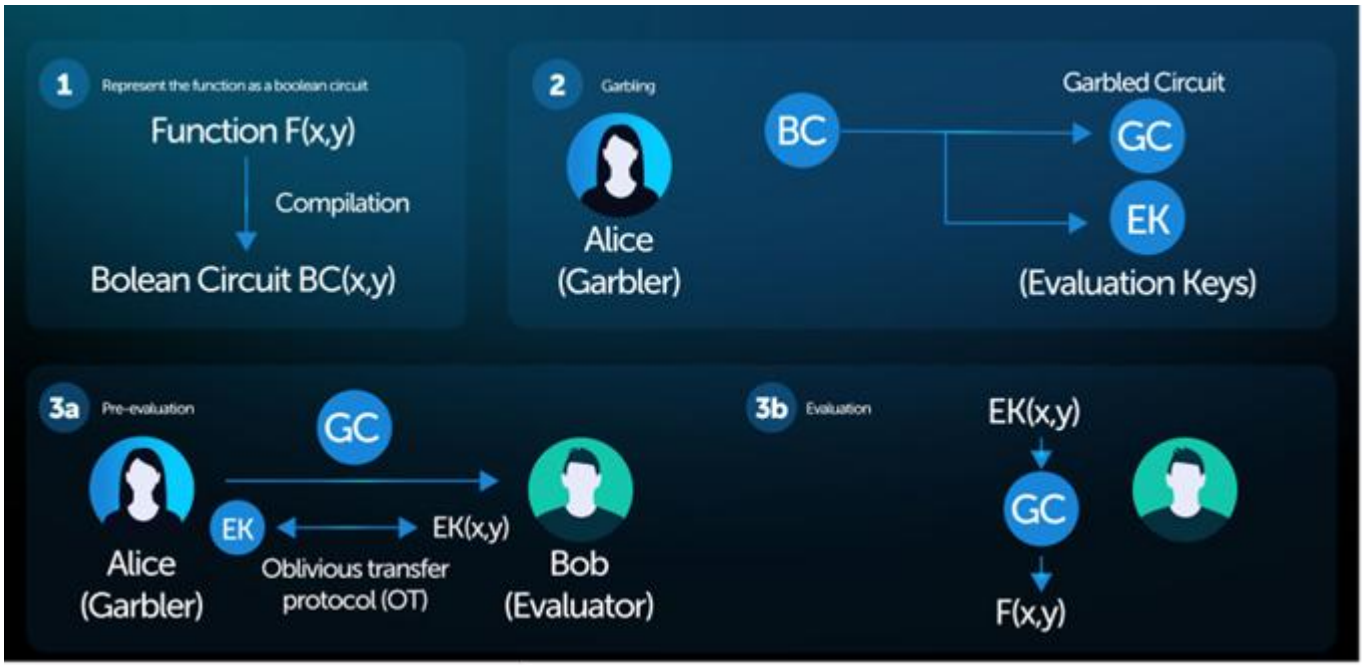
- **1단계** '누가 더 부자인가'라는 문제 또는 '함수'는 논리 게이트를 사용하는 프로그램, 즉 불리언 회로[7] 형태로 작성됩니다. 백만장자 문제에서, 백만장자들의 재단이 8비트 정수에 담긴다고 가정합니다. 이때 불리언 회로는 2X8=16개의 입력 와이어를 가집니다. (이러한 정수는 0에서 $2^8 - 1 = 255$ 사이의 숫자를 수용할 수 있으며 처음 8개의 입력 와이어는 앨리스에게, 다음 8개는 밥에게 속합니다.) 회로 구조는 이 첫 번째와 두 번째 입력 와이어 세트를 받아 각각 숫자 X와 Y로 해석하고, MAX(X,Y)를 계산하도록 되어 있습니다. 그 결과는 단일 비트 B를 인코딩하는 출력 와이어로 나옵니다. 만약 B=0이면 X>Y이고, B는 1이면 X≤ Y입니다.
- **2 단계** 앨리스는 이 불리언 회로를 암호화하거나 '가블링'하며, 그 결과물을 가블드 서킷이라고 부릅니다. 각 입력 와이어(총 16 개)에는 이진 값 0 과 1 을 각각 나타내는 두 개의 길고 무작위적인 레이블 L0 과 L1 이 연결됩니다. 가블링 시점에 앨리스는 모든 와이어에 대한 L0 와 L1 을 가지고 있습니다. 앨리스의 목표는 밥에게 가블드 서킷과 함께, 각 입력 와이어당 단 하나의 레이블만을 제공하여, 밥이 자신이 받은 레이블들을 사용하여 MAX 함수를 오직 한 번만 계산할 수 있도록 하는 것입니다. 가블드 서킷의 입력 와이어들과 연결된 레이블들의 집합을 가블드 입력이라고 합니다. 3a 단계에서 앨리스는 자신에게 속한 첫 번째 8 개 입력 와이어 각각에 대한 레이블 하나를 포함하여 가블드 서킷을 밥에게 보냅니다. 3b 단계에서 밥은 자신에게 속한 두 번째 8 개 입력 와이어 각각에 대한 레이블 하나를 얻습니다.
- **3 단계** 앨리스는 가블드 서킷을 밥에게 보내면서, 자신의 8 개 입력 와이어에 해당하는 올바른 레이블들을 함께 보냅니다.

---

[6] Andrew Yao

[7] Boolean circuit

- **4 단계** 밥은 자신의 숫자도 '가블링'하여, 자신에게 속한 8 개의 입력 와이어 각각에 대한 레이블 하나, 즉 총 8 개의 레이블을 얻습니다. 이제 밥은 실제 계산을 수행할 준비가 되었습니다.
- **5 단계** 밥은 가블드 입력을 가지고 가블드 서킷에 대한 계산을 실행합니다. 이 과정은 비트 B 를 평문으로 출력하며, 이제 밥은 계산의 결과를 알게 됩니다. 특히, 이 결과는 실제 자산 금액을 전혀 드러내지 않고, 단지 누가 더 부자인지에 대한 답만을 알려줍니다.
- **6 단계** 이 시점에서 밥은 앨리스에게 결과 B 를 전달하여, 앨리스 역시 누가 더 부자인지 알 수 있게 됩니다.



[가블드 서킷 작동 방식]

사용 사례 및 응용 분야

첨단 개인 정보 보호 기능의 통합은 다양한 분야에 걸쳐 애플리케이션의 가능성을 확장합니다. 개인 정보 보호는 이러한 블록체인 구현의 최전선에 있으며, 기존의 공개 또는 투명 블록체인에서는 달성할 수 없었던 기능을 제공합니다.

1. 보안 토큰화가 실현되어 거래 세부 정보의 기밀성을 보호하면서 자산 교환이 가능해집니다.
2. 비공개 경매는 최고 수준의 프라이버시로 진행되어, 입찰 금액이 공개적으로 노출되지 않도록 보장합니다.
3. 온체인 게임 경험이 향상되며, 플레이어의 움직임과 선택이 공개를 선택할 때까지 비밀로 유지되도록 개인 정보 보호 메커니즘이 보장됩니다.

4. 기밀 투표 시스템은 유권자 결정의 프라이버시를 보존함으로써 선거의 무결성을 유지합니다.
5. 프라이빗 신원 등록 시스템은 승인된 등록자가 사용자 신원 및 관련 암호화된 식별자를 관리하는 동시에, 권한 및 소유 메커니즘을 통해 접근 통제를 시행할 수 있도록 합니다.

더 많은 활용 사례와 예시는 깃허브의 coti-contracts 저장소에서 확인할 수 있습니다. 이러한 혁신적인 사용 사례들은 프라이빗 블록체인의 혁신적인 잠재력을 강조하며, 탁월한 수준의 기밀성, 보안 및 투명성으로 다양한 산업에 혁명을 일으키고 있습니다.

다음과 같은 주요 애플리케이션이 코티V2 네트워크를 통해 가능해집니다.

1. 기밀 디파이

디파이는 금융 산업의 지형을 재정의하고 새로운 잠재적 기능을 도입했습니다. 그럼에도 불구하고, 온체인 활동의 내재된 투명성은 프라이버시에 대한 타협을 불가피하게 만들어, 규제 문제로 인해 기관의 참여를 막고 있습니다. 코티V2는 기밀 트랜잭션을 도입하여, 기존 서비스에 대한 프라이버시와 보안을 강화하는 동시에 규제 표준을 준수함으로써 디파이 혁신의 잠재력을 확장합니다. 이는 트랜잭션 세부 정보를 암호화함으로써, MEV(최대 추출 가치)[8]를 통한 악용 등 이더리움 디파이의 오랜 취약점을 해결하여 MEV 봇과 프론트 러너[9]의 기회주의적 행위를 방지합니다.
코티 네트워크는 개발자들에게 기존의 탈중앙화 애플리케이션에 첨단 데이터 보안 기능을 추가하거나, 이전에 불가능했던 새로운 디파이 중심 애플리케이션을 혁신할 수 있는 도구를 제공합니다.

2. 결제, 스테이블코인[10], CBDC(중앙은행 디지털화폐)[11] 및 실물 자산[12]을 위한 기밀 트랜잭션

전통적인 금융 생태계는 신뢰를 구축하고 사용자 참여를 장려하기 위해 트랜잭션 기밀성을 강조합니다. 웹3.0의 주류 채택을 위해서는 이러한 속성을 반영하는 것이 중요합니다. 코티V2는 자금 흐름의 투명성을 유지하면서도 트랜잭션 세부 사항을 암호화하는 기밀 결제 메커니즘을 제공하여, 디지털 및 실물 자산에 대한 규제 프레임워크 준수를 유지하면서 트랜잭션 기밀성을 보장합니다.

---

[8] Maximum extractable value

[9] Front runner

[10] Stablecoin

[11] Central bank digital currency

[12] Real-world asset (RWA)

3. 기밀 머신 러닝 및 온체인 민감 데이터 관리

데이터 관리와 프라이버시가 최고로 중요해지는 현 상황에서, 코티V2는 개인의 익명성을 침해하지 않고 AI/머신 러닝 모델을 훈련할 수 있는 프레임워크를 도입합니다. 챗GPT와 같은 거대 언어 모델[13]은 서비스 기능을 향상하기 위해 상당한 양의 데이터에 의존합니다. 이러한 필요성은 사용자 프라이버시와 지적 재산 보호에 대한 우려를 낳습니다. 가블드 서킷과 같은 암호화 방법으로 구현되는 프라이버시 보존 머신 러닝을 활용하여, 코티V2는 이러한 데이터를 이용한 훈련이 데이터 주체의 프라이버시를 침해하지 않도록 보장함으로써 새로운 비즈니스 모델의 길을 열어줍니다.

한 가지 예시는 여러 이해관계자가 협력하여 고유한 데이터세트를 보유하는 연합 학습[14]입니다. 데이터세트의 규모나 다양성으로 인한 제한적인 유용성은 데이터세트를 통합함으로써 극복될 수 있으며, 이는 더 정확한 머신 러닝 모델 개발을 가능하게 하는 공동 데이터 풀을 만듭니다.

또한 독점 데이터에서 파생된 첨단 머신 러닝 모델을 보유하고 이러한 모델을 서비스로 제공하고자 하는 조직은 또 다른 응용 시나리오를 나타냅니다. 예를 들어, 개와 고양이 이미지를 높은 정확도로 구별할 수 있는 모델을 가진 조직은 유사한 모델 개발 리소스가 부족한 다른 조직에 이러한 예측 기능을 제공할 수 있습니다. 이러한 모델을 블록체인 플랫폼에 배포함으로써 해당 조직은 모델의 지적 재산과 분류되는 데이터의 프라이버시를 보호하면서 분류 서비스를 제공할 수 있습니다. 프라이빗 추론이라고 불리는 이 메커니즘은 최종 사용자가 데이터를 공개적으로 노출할 필요 없이 모델의 예측 기능에 접근할 수 있도록 합니다.

이러한 사례들은 프라이버시 보존 기술을 머신러닝과 통합하는 초기 응용 분야를 보여줍니다. 이 분야의 기술 발전이 계속됨에 따라, 이러한 응용 분야의 범위와 영향은 확대될 것으로 예상되며, 이는 AI/머신 러닝 역량 진화에서 프라이버시 보존 방법론의 중요성을 강조합니다.

4. 동적 탈중앙화 신원 증명[15]

코티V2는 실제 데이터를 제3자에게 노출하지 않고 신원 확인 및 개인 데이터 관리가 실행되는 패러다임을 촉진합니다. 사용자는 고객 확인[16] 요구 사항을 충족하면서 자신의 정보에 대한 통제권을 유지합니다. 이 프레임워크는 디지털 신원과 디앱[17] 간의 안전하고 프라이버시를 보존하는 상호 작용을 가능하게 하여, 민감한 데이터를 손상시키지 않고 글로벌 서비스 애플리케이션을 위한 무신뢰 및 규제 환경을 구현합니다.

---

[13] Large language model (LLM)

[14] Federated learning

[15] Dynamic decentralized identity (DyDID)

[16] Know your customer (KYC)

[17] DApp (decentralized application)

코티V2의 등장과 최첨단 가블드 서킷 기술은 웹3.0의 광범위한 채택을 가로막는 주요 프라이버시 문제를 해결합니다. 이는 웹2.0 산업에서 만연한 프라이버시 문제에 대한 우수한 솔루션을 제공하며, 비즈니스 혁신을 위한 상당한 기회를 제시합니다. 전 세계 개발자들은 곧 출시될 코티V2 개발자 네트워크에 참여하여, 보다 프라이빗하고 안전하며 사용자 친화적인 웹3.0 생태계의 발전에 기여하도록 초청됩니다.

토크노믹스

코티 재단이 구상한 대로 여기에는 구조화된 할당 프레임워크가 포함됩니다. 다음 세 가지 핵심 목표를 이행하기 위해 새로 채굴된 토큰의 발행 시마다 미리 정의된 비율이 할당됩니다.

- **보상, 인센티브 및 에어드랍[18] — 58%**

  새로 생성된 토큰의 가장 큰 몫은 보상 보유자, 스테이커[19], 잠재적인 검증인 및 기타 네트워크 참여자에게 할당되어 적극적인 참여를 유도하고 네트워크를 보호합니다. 이 할당량의 초기 수령자는 네트워크 출시 시에 공급량의 100%를 보유할 기존 보유자가 될 것입니다. 따라서 이들의 '희석'은 최소화될 것입니다(첫 1년 이후 5% 미만). 10년이 지나 총 공급량이 50%까지 늘어나더라도 기존 보유자는 여전히 공급량의 85%를 보유할 것입니다.
- **개발 — 18%**

  또 다른 할당량이 개발 노력에 배정되어 코티 생태계의 지속적인 개선, 혁신 및 확장성을 보장합니다.
- **생태계 — 24%**

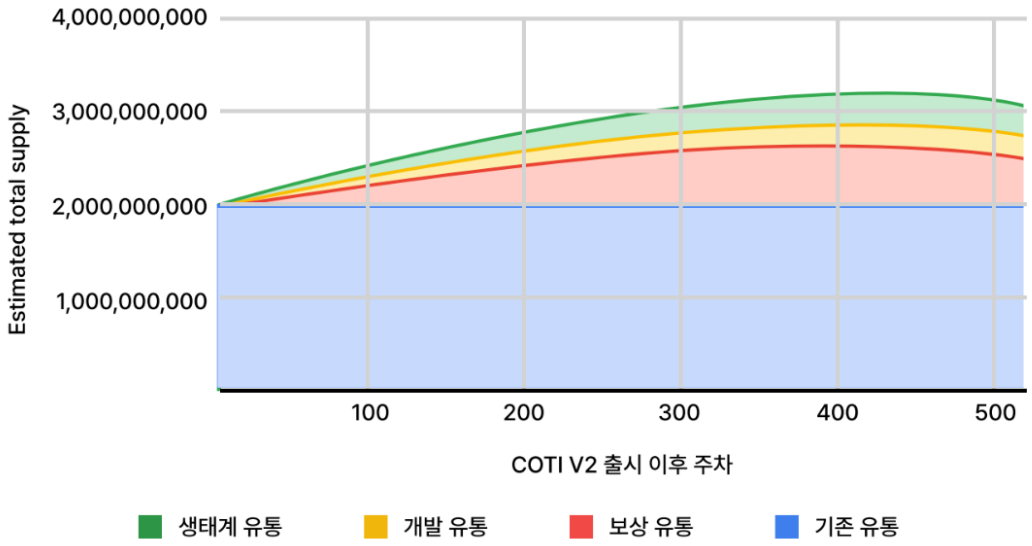
  지정된 할당량이 재단에 지급되어 개발자를 위한 보조금, 디앱, 인센티브 프로그램, 전략적 투자, 유동성 공급을 비롯해 다양한 이니셔티브를 지원하게 됩니다. 이 할당량은 다른 레이어1 및 레이어2 네트워크와 마찬가지로 코티 생태계의 성장 및 활력을 촉진하는데 중요한 역할을 합니다.

다음은 위의 가정을 바탕으로 2025년 이후의 COTI의 총발행량 추이를 추정한 차트입니다.

---

[18] Airdrop

[19] Staker



[2025년 이후의 COTI 총발행량 추정]

코티 토크노믹스 업데이트: 프라이버시 확장 및 가치 강화

하나의 토큰, 여러 개의 체인, 동일한 공급량

코티는 단일 체인 기반의 프라이버시 솔루션에서 세계 최고의 올인원 프라이버시 프로토콜 및 인프라 제공 프로젝트로 발전하고 있습니다. '프라이버시를 위한 맥가이버 칼'이라고 할 수 있는 코티는 기업과 개발자, 사용자 모두에게 각자의 필요에 맞는 이상적인 프라이버시 솔루션을 제공합니다.

- 업데이트 의의: 향후 코티는 테스트넷20에서 새로운 프라이버시 블록체인을 공개할 예정입니다. 새롭게 공개될 블록체인은 주요 기관 파트너의 설계 및 지원을 바탕으로 구축됩니다. 기업 및 개발자는 가블드 서킷을 활용한 개발 방식을 비롯하여 다른 선도적인 프라이버시 기술을 추가적으로 선택할 수 있게 됩니다.
- 멀티체인 프라이버시: 2026년 코티는 프라이버시 온디맨드(Privacy-on-Demand) 모델을 통해 코티의 혁신적인 가블드 서킷 기술을 주요 레이어1 및 레이어2 체인으로 확장합니다. 이로써 타 체인 기반의 많은 애플리케이션 및 디앱에서 코티의 기술을 활용하여 비공개 연산 및 트랜잭션을 실행하게 될 것으로 기대됩니다.
- 단일 통합 토큰: COTI 역시 영역을 넓혀 여러 체인과 다양한 사용 사례에서 활용되면서 코티 전체 프라이버시 네트워크의 작동과 연산 및 트랜잭션을 책임지게 됩니다. COTI는 생태계 전반에서 최대 발행량 상한을

[20] Testnet

동일하게 유지하며, 세계 최대 규모의 프라이버시 네트워크 구축이라는 목표를 실현하기 위해 지속적으로 활용됩니다.

올인원 프라이버시 생태계: 수익 및 수수료

프라이버시 확장성의 미래는 여러 블록체인과 프로토콜, 그리고 빠르게 변화하는 기술 및 AI 분야 전반에서 완전한 결합성[21]과 프로그래밍 가능성을 갖춘 프라이버시를 구현하는 데 달려 있습니다. 코티의 올인원 프라이버시 인프라는 사용량 기반의 새로운 가격 책정 모델을 적용하여 여러 체인과 생태계에 배포될 예정입니다. 비공개 연산 및 트랜잭션 처리 수수료를 통해 유의미한 수익이 지속적으로 창출될 것으로 기대되며, 모든 수수료는 COTI로 지불됩니다.

- **코티 프라이버시 수수료 구조**

  트랜잭션 수수료: 코티의 프라이버시 네트워크에서 실행되는 모든 비공개 트랜잭션에는 가스비[22]가 발생하는데, 비공개 트랜잭션의 가스비는 일반 트랜잭션보다 더 높습니다. 또한 기밀 스마트 컨트랙트 같은 한층 복잡한 작업에는 더 많은 가스비가 필요합니다. 모든 수수료는 COTI로 지불되며, 커뮤니티 관리 지갑에 축적됩니다.
- **프라이버시 브리지[23] 및 크로스체인 프라이버시 온디맨드 수수료**

  프라이버시 브리지를 사용하거나 비공개 크로스체인 전송 절차를 시작하는 경우 각각 별도의 COTI 수수료가 부과되며, 이는 코티의 새로운 수익원이 됩니다.

종합 소각 메커니즘

코티는 네트워크 성장에 맞춰 유통량을 영구적으로 감소시키는 다중 소각 메커니즘을 도입할 계획입니다. 코티와 코티의 프라이버시 기술이 많이 채택되고 사용될수록 총발행량은 더욱 감소하게 됩니다.

- **수수료 기반 소각**
  - 비공개 트랜잭션을 비롯하여 코티V2에서 발생하는 모든 가스비는 모두 커뮤니티 관리 지갑으로 이동됩니다.
  - 프라이버시 브리지 트랜잭션 및 프라이버시 온디맨드 수수료의 50%는 소각됩니다. 나머지 50%는 재단에서 코티의 프라이버시 생태계를 성장시키고 타 체인의 채택을 장려하기 위해 사용합니다.
- **거버넌스 소각**
  - 커뮤니티 트레저리[24]에 누적된 가스비는 투표를 통해 소각할 수 있습니다.
  - 코티 재단은 아래와 같은 연간 소각 제안을 제출할 수 있습니다.

---

[21] Composability

[22] Gas fee

[23] Bridge

[24] Treasury

- **1 억 COTI 소각 약속**

  코티는 앞으로 12 개월 내에 최소 1 억 COTI(총발행량의 약 3%)를 소각할 것을 약속합니다. 소각 대상 토큰에는 커뮤니티 관리 지갑에 축적된 가스비 토큰도 포함됩니다. 모든 소각은 투명하고 검증 가능한 방식으로 이루어지며 공개 소각 주소를 통해 확인할 수 있습니다.

스테이킹[25] 보상 자동 조정

트레저리 V2 출시와 함께 코티는 자체 조절형 스테이킹 모델을 도입할 예정입니다. 이 스테이킹 모델은 스테이킹 참여율에 따라 APY(연간 복리 수익률)[26]를 자동 조정하여 더 많은 참여자를 유인하는 동시에 보상 분배와 과도한 토큰 유통 문제까지 자동으로 관리합니다.

- 작동 방식: 목표 스테이킹 참여율이 유통량의 15%이고, APY는 10%라고 가정해 보겠습니다. 참여율이 낮아지면 APY가 상승하여 더 많은 참여자를 유인하며, 참여율이 높아지면 APY가 자연스럽게 하락하게 됩니다.

이 같은 메커니즘을 통해 수동적인 개입 없이도 안정적인 균형 상태가 형성됩니다. 에포크[27]별 전체 스테이킹 보상은 커뮤니티 할당 물량의 50%로 제한하는 등 보상 분배 예산의 상한선을 명확하게 설정합니다.

토크노믹스 업데이트가 COTII 보유자에게 미치는 영향

이번 토크노믹스 업데이트로 하나의 선순환 구조가 형성됩니다.

- 지원 체인 증가 = 유틸리티 및 수수료 수익 강화, 추가 발행 없음
- 사용량 증가 = 수수료 및 소각량 증가, 유통량 감소
- 참여 증가 = 노드[28] 경제 시스템 강화, 스테이킹 및 토큰 락업[29] 비율 증가
- 소각량 증가 = 발행량 영구적 및 지속적 감소

코티는 토크노믹스 업데이트를 통해 코티의 프라이버시 생태계가 여러 체인과 기업, 애플리케이션으로 확장되는 동시에 토큰 발행량은 감소하는 구조를 구현하고자 합니다. 개선된 토크노믹스는 토큰의 핵심 구조를 유지하면서도 토큰 보유자와 참여자, 개발자 모두에게 이점을 제공합니다.

---

[25] Staking

[26] Annual percentage yield

[27] Epoch

[28] Node

[29] Lockup

토크노믹스 투명성

소각, 수수료 분배, 보상 분배와 관련된 모든 데이터는 온체인에서 검증할 수 있습니다. 검증 가능한 정보에는 연간 소각 보고서, 공개 주소(누구도 사용할 수 없음) 등도 포함됩니다. 코티는 말로만 약속하는 것이 아니라 실제 데이터를 기반으로 신뢰 시스템을 구축하고 있습니다.

로드맵

코티는 별도 로드맵을 공지하고 있지 않으나, 미디엄 및 X(구 트위터)를 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 미디엄 https://cotinetwork.medium.com/
- X(구 트위터) https://x.com/COTInetwork

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.