# **ERC-20 완전 정복: 이더리움 토큰 경제의 핵심 동력에 대한 전문가 보고서**

### **서론: 디지털 자산의 표준, ERC-20 시대를 열다**

ERC-20은 단순한 기술 사양이 아니다. 이는 이더리움 블록체인 위에서 수많은 디지털 자산이 탄생하고, 상호작용하며, 가치를 교환할 수 있는 공통의 언어를 제공한 혁명적인 표준이다.1 2015년 제안되어 공식화된 이 기술 규약은 토큰 발행의 복잡성을 획기적으로 낮춤으로써 2017년 ICO(Initial Coin Offering) 붐을 촉발시킨 핵심 동력이었다.3 프로젝트들은 더 이상 각자의 고유한 블록체인을 구축할 필요 없이, 검증된 이더리움 네트워크 위에서 손쉽게 자신들의 토큰을 발행하고 자금을 조달할 수 있게 되었다. 그 결과, 수만 개가 넘는 토큰 프로젝트가 탄생했으며, 이더리움은 명실상부한 글로벌 디지털 자산 발행 플랫폼으로 자리매김했다.1

오늘날 ERC-20의 영향력은 ICO 시대를 넘어 탈중앙화 금융(DeFi) 생태계의 가장 깊은 근간을 이루고 있다. 대출, 거래, 스테이킹, 파생상품 등 DeFi의 거의 모든 금융 활동은 ERC-20 토큰을 매개로 이루어진다.2 이 표준이 제공하는 상호운용성 덕분에, 다양한 DeFi 프로토콜들은 마치 레고 블록처럼 서로 결합하여 이전에는 상상할 수 없었던 새로운 금융 상품과 서비스를 창출해내고 있다.

이 보고서는 ERC-20의 기술적 본질부터 실용적인 사용법, 그리고 이더리움 생태계 전반에 미치는 심대한 영향까지 모든 것을 아우르는 종합 가이드가 되는 것을 목표로 한다. 독자들은 이 보고서를 통해 ERC-20을 단순한 '암호화폐'나 '코인'이 아닌, 하나의 거대한 디지털 경제 시스템을 움직이는 핵심 인프라이자 프로토콜로 이해하게 될 것이다. 제1장에서는 ERC-20의 기술적 사양을 심층 분석하고, 제2장에서는 토큰의 생성과 관리 방법을 다룬다. 제3장에서는 토큰 전송의 실제 과정과 필수 개념인 가스비, 그리고 거래 내역을 추적하는 이더스캔 활용법을 상세히 설명한다. 제4장에서는 DeFi 생태계에서 ERC-20이 어떻게 활용되는지 구체적인 사례를 통해 살펴보고, 마지막 제5장에서는 보안 위협에 대한 대응책과 미래 기술 표준으로의 진화를 조망한다.

## **제1장: ERC-20 표준의 이해: 기술적 토대와 중요성**

ERC-20 표준의 본질을 이해하는 것은 이더리움 생태계 전체를 이해하는 첫걸음이다. 이 장에서는 ERC-20이 무엇인지 정의하고, 그 기술적 핵심인 함수와 이벤트를 분석하며, 표준화가 가져온 혁신과 내재된 기술적 한계를 고찰한다.

### **1.1. ERC-20의 정의: 단순한 코드를 넘어선 기술 규약**

ERC-20은 'Ethereum Request for Comment 20'의 약자로, 이더리움 개선 제안 20번 문서를 의미한다.2 이는 특정 소프트웨어나 완성된 코드가 아니라, 이더리움 블록체인 위에서 발행되는 토큰들이 상호 호환성을 갖기 위해 반드시 따라야 하는 일련의 규칙과 기능 명세를 정의한 '기술 사양' 또는 '프로토콜'이다.1 즉, 개발자들에게 "이더리움 생태계에서 통용되는 토큰을 만들고 싶다면, 최소한 이러한 기능들을 이런 방식으로 구현해야 한다"고 알려주는 일종의 청사진과 같다.

이러한 토큰들은 이더리움의 핵심 구성 요소인 이더리움 가상 머신(EVM, Ethereum Virtual Machine) 위에서 작동하는 '스마트 계약(Smart Contract)'을 통해 구현된다.7 스마트 계약은 특정 조건이 충족되면 사전에 프로그래밍된 코드를 자동으로 실행하는 프로그램이다. ERC-20 토큰 계약은 이 표준에 명시된 함수들을 포함하고 있어, 모든 외부 계정(사용자 지갑)이나 다른 스마트 계약(예: 탈중앙화 거래소)이 해당 토큰과 예측 가능한 방식으로 상호작용할 수 있게 한다.9 이 덕분에 개발자들은 새로운 토큰이 나올 때마다 호환성 문제를 걱정할 필요 없이, 이미 존재하는 지갑, 거래소, DApp(탈중앙화 애플리케이션) 인프라를 그대로 활용할 수 있다.2

### **1.2. 기술 사양 심층 분석: 6개의 필수 함수와 2개의 필수 이벤트**

ERC-20 표준의 기술적 핵심은 모든 토큰 스마트 계약이 의무적으로 구현해야 하는 6개의 함수(methods)와, 특정 활동이 발생했을 때 네트워크에 알려주는 2개의 이벤트(events)로 구성된다.10 이 8가지 구성 요소는 토큰의 소유권, 전송, 그리고 다른 계약과의 상호작용에 필요한 모든 기본 기능을 정의한다.

#### **필수 함수 (6개)**

1. totalSupply(): 이 함수는 해당 토큰의 총 발행량을 반환한다. 계약이 배포될 때 고정된 총량을 설정하거나, 특정 조건에 따라 총량이 변동(발행 또는 소각)될 수 있다. 이는 토큰 경제 모델의 인플레이션 또는 디플레이션 정책을 결정하는 가장 기본적인 데이터가 된다.6
2. balanceOf(address \_owner): 특정 이더리움 주소(\_owner)가 보유하고 있는 토큰의 잔액을 조회하는 함수다. 사용자의 지갑 애플리케이션이 화면에 토큰 수량을 표시할 때 이 함수를 호출한다.2
3. transfer(address \_to, uint256 \_value): 함수를 호출한 주소(토큰 소유자)가 지정된 수신자 주소(\_to)로 특정 수량(\_value)의 토큰을 전송하는 기능이다. 이는 가장 기본적인 개인 간(P2P) 토큰 전송에 사용되는 함수다.9
4. approve(address \_spender, uint256 \_value): 토큰 소유자가 자신의 토큰 중 특정 수량(\_value)을 다른 주소(일반적으로 스마트 계약 주소, \_spender)가 인출해 갈 수 있도록 '승인'하는 매우 중요한 함수다. 이는 사용자가 자신의 개인 키를 스마트 계약에 직접 노출하지 않고도, 탈중앙화 거래소나 랜딩 프로토콜 같은 서비스가 사용자를 대신해 토큰을 안전하게 처리할 수 있도록 하는 핵심적인 위임 메커니즘이다.9
5. allowance(address \_owner, address \_spender): 특정 주소(\_spender)가 다른 주소(\_owner)로부터 인출하도록 허용된 토큰의 잔여 수량을 확인하는 함수다. approve 함수로 설정된 한도를 조회하는 데 사용된다.9
6. transferFrom(address \_from, address \_to, uint256 \_value): approve 함수를 통해 권한을 위임받은 주소(\_spender)가, 원래 소유자(\_from)의 계정에서 수신자(\_to)의 계정으로 특정 수량(\_value)의 토큰을 전송하는 함수다. 이 함수는 approve 함수와 한 쌍으로 작동하며, 탈중앙화 거래소에서 토큰을 스왑하거나, 스테이킹 프로토콜에 토큰을 예치하는 등 스마트 계약을 통한 모든 자동화된 토큰 거래의 기반이 된다.5

#### **필수 이벤트 (2개)**

1. Transfer(address indexed \_from, address indexed \_to, uint256 \_value): transfer 또는 transferFrom 함수를 통해 토큰 전송이 성공적으로 발생했을 때, 블록체인에 로그를 남기는 이벤트다. 이 이벤트 덕분에 이더스캔과 같은 블록 탐색기나 지갑 애플리케이션은 토큰의 이동 내역을 효율적으로 추적하고 사용자에게 보여줄 수 있다.8
2. Approval(address indexed \_owner, address indexed \_spender, uint256 \_value): approve 함수가 성공적으로 호출되어 특정 주소에 대한 인출 한도가 설정되거나 변경되었을 때 로그를 남기는 이벤트다.8

#### **선택적 함수**

표준에 필수로 명시되어 있지는 않지만, 사용자 편의성을 위해 거의 모든 ERC-20 토큰이 구현하는 3가지 함수가 있다.

* name(): 토큰의 전체 이름 (예: "Tether USD")을 반환한다.3
* symbol(): 토큰의 짧은 기호 (예: "USDT")를 반환한다.3
* decimals(): 토큰이 나뉠 수 있는 소수점 자릿수를 정의한다. 대부분의 토큰은 이더(ETH)와 동일하게 18로 설정되는데, 이는 1 토큰이 $10^{18}$개의 가장 작은 단위로 나뉠 수 있음을 의미한다.3

| 표 1: ERC-20 필수 및 선택 함수/이벤트 요약 |  |  |  |
| --- | --- | --- | --- |
| **구분** | **함수/이벤트명** | **설명** | **주요 역할/사용 사례** |
| **필수 함수** | $totalSupply() | 토큰의 총 발행량을 반환합니다. | 토큰 경제 모델의 총 공급량 확인 |
|  | $balanceOf(address \_owner) | 특정 주소의 토큰 잔액을 반환합니다. | 지갑 앱에서 사용자 잔액 표시 |
|  | $transfer(address \_to, uint256 \_value) | 호출자의 토큰을 수신자에게 전송합니다. | 개인 간(P2P) 토큰 송금 |
|  | $approve(address \_spender, uint256 \_value) | 제3자(\_spender)에게 토큰 인출 권한을 부여합니다. | DEX, 랜딩 프로토콜 등 스마트 계약에 토큰 사용 권한 위임 |
|  | $allowance(address \_owner, address \_spender) | 제3자가 인출할 수 있는 허용량을 확인합니다. | 스마트 계약이 사용 가능한 토큰 수량 확인 |
|  | $transferFrom(address \_from, address \_to, uint256 \_value) | 허용된 범위 내에서 제3자가 토큰을 전송합니다. | DEX에서의 토큰 스왑, 스테이킹 등 자동화된 거래 실행 |
| **필수 이벤트** | $Transfer(address \_from, address \_to, uint256 \_value) | 토큰 전송 발생 시 로그를 남깁니다. | 블록 탐색기, 지갑 등에서 거래 내역 추적 |
|  | $Approval(address \_owner, address \_spender, uint256 \_value) | approve 호출 시 로그를 남깁니다. | 토큰 사용 승인 내역 추적 |
| **선택 함수** | $name() | 토큰의 전체 이름을 반환합니다. | 사용자 인터페이스(UI)에서 토큰 식별 |
|  | $symbol() | 토큰의 심볼(티커)을 반환합니다. | UI 및 거래소에서 간편하게 토큰 표시 |
|  | $decimals() | 토큰의 소수점 자릿수를 반환합니다. | UI에서 정확한 토큰 가치 계산 및 표시 |

approve와 transferFrom 함수의 조합은 단순한 송금 기능을 넘어, 이더리움의 핵심 가치인 '프로그래밍 가능한 돈(Programmable Money)'을 실현하는 결정적인 메커니즘이다. transfer 함수만으로는 사용자가 자신의 자산을 제3자인 스마트 계약에 안전하게 맡길 수 없다. 개인 키를 직접 노출해야 하는 위험이 따르기 때문이다. 그러나 approve 함수를 통해 사용자는 개인 키를 안전하게 보관하면서도, 신뢰할 수 있는 스마트 계약(예: 유니스왑의 라우터 계약)에 한정된 권한만을 부여할 수 있다.12

transferFrom은 이 허가를 받은 스마트 계약이 사용자를 대신하여 약속된 금융 논리를 실행하는 역할을 한다.12 이 두 함수의 유기적인 작동 덕분에, 사용자는 중개자 없이 탈중앙화 거래소에서 토큰을 교환하고, 랜딩 프로토콜에 자산을 예치하여 이자를 받으며, 유동성 풀에 자산을 공급하는 등 복잡하고 자동화된 금융 활동을 비신뢰(trustless) 방식으로 수행할 수 있게 된다. 따라서 이 기능은 ERC-20을 단순한 '디지털 화폐'에서 'DeFi 생태계를 구성하는 핵심 레고 블록'으로 격상시킨 가장 중요한 설계적 특징이라고 할 수 있다.

### **1.3. 표준화의 힘: 상호운용성이 가져온 혁신과 이점**

ERC-20 표준이 가져온 가장 큰 혁신은 '상호운용성(Interoperability)'이다.2 모든 ERC-20 토큰이 동일한 규칙과 함수 인터페이스를 따르기 때문에, 생태계의 모든 참여자들은 어떤 토큰이든 동일한 방식으로 다룰 수 있다.

* **개발 효율성 증대:** 개발자들은 새로운 토큰을 지원하기 위해 매번 코드를 새로 작성할 필요가 없다. 한 번 ERC-20을 지원하는 지갑이나 거래소, DeFi 프로토콜을 만들면, 앞으로 나올 모든 ERC-20 토큰과 자동으로 호환된다. 이는 개발자들이 '바퀴를 다시 발명'하는 데 시간을 낭비하지 않고, 핵심적인 비즈니스 로직과 혁신에 집중할 수 있게 만들었다.1
* **신속한 시장 진입과 유동성 확보:** 새로운 프로젝트는 토큰을 발행하는 즉시 메타마스크, 레저와 같은 기존 지갑에서 지원받을 수 있으며, 유니스왑과 같은 탈중앙화 거래소에 즉시 유동성 풀을 생성하여 거래를 시작할 수 있다. 이는 과거처럼 중앙화 거래소의 상장 심사를 기다릴 필요 없이 신속하게 유동성을 확보하고 커뮤니티를 형성할 수 있게 해준다.2
* **사용자 경험의 일관성:** 사용자들은 여러 종류의 ERC-20 토큰을 보유하더라도 하나의 지갑에서 모두 관리하고 동일한 방식으로 전송할 수 있다. 이는 복잡한 블록체인 기술을 사용하는 데 있어 진입 장벽을 낮추고 일관된 사용자 경험을 제공한다.2
* **투명성과 보안:** 모든 ERC-20 토큰의 거래 내역과 스마트 계약 코드는 이더리움 블록체인에 투명하게 공개된다. 누구나 이더스캔을 통해 특정 토큰의 총 공급량, 유통량, 주요 보유자 등을 확인할 수 있다. 또한, 이 토큰들은 작업증명(PoW) 또는 지분증명(PoS)으로 보호되는 이더리움 메인넷의 강력한 보안성을 그대로 상속받는다.3

### **1.4. 기술적 한계와 고려사항: 기능의 제약과 가스비 문제**

혁신적인 표준임에도 불구하고 ERC-20은 몇 가지 내재적인 한계와 고려사항을 가지고 있다.

* **제한된 기능 (대체 가능성):** ERC-20은 본질적으로 '대체 가능한(Fungible)' 자산을 위한 표준이다. 즉, 내가 가진 1 USDT는 당신이 가진 1 USDT와 가치와 기능 면에서 완전히 동일하다. 하지만 디지털 아트, 게임 내 한정판 아이템, 부동산 소유권 증서처럼 각각의 자산이 고유한 가치와 속성을 가져야 하는 '대체 불가능한(Non-Fungible)' 자산을 표현하기에는 부적합하다. 이러한 필요성으로 인해 각 토큰에 고유 ID를 부여하는 ERC-721(NFT) 표준이 등장하게 되었다.8
* **가스비 변동성:** 모든 ERC-20 토큰 거래는 이더리움 블록체인 위에서 처리되므로, 이더리움 네트워크의 수수료 정책에 종속된다. 네트워크 사용량이 급증하는 시기(예: 새로운 NFT 민팅, 강세장 DeFi 활동 증가)에는 거래 수요가 블록 공간 공급을 초과하여 가스비가 폭등할 수 있다. 이는 소액의 토큰을 전송하거나 교환하려는 사용자에게 큰 부담으로 작용하며, ERC-20 기반 서비스의 대중화를 가로막는 요인이 되기도 한다.5
* **스마트 계약 자체의 취약성:** ERC-20 표준 자체는 안전하지만, 이 표준을 구현하는 개별 토큰의 스마트 계약 코드에 버그나 논리적 결함이 있을 경우 심각한 보안 사고로 이어질 수 있다. 과거 일부 토큰 계약의 취약점으로 인해 자금이 동결되거나 도난당한 사례가 있었다. 따라서 토큰의 안정성은 표준 준수 여부뿐만 아니라, 스마트 계약 코드의 품질과 보안 감사 여부에 크게 좌우된다.8

흥미롭게도, ERC-20 표준의 폭발적인 성공은 역설적으로 이더리움의 확장성 문제를 수면 위로 끌어올린 촉매제가 되었다. ERC-20은 토큰 발행을 민주화하여 수많은 프로젝트와 DApp의 등장을 이끌었고, 이는 이더리움 네트워크의 거래량을 기하급수적으로 증가시켰다.1 특히 DeFi의 부상은 복잡한 상호작용을 포함하는 ERC-20 토큰 거래를 폭발시켰다.4 하지만 이더리움 블록체인의 블록 크기와 블록 생성 시간은 제한되어 있어, 한정된 처리 용량을 두고 경쟁이 치열해졌다. 이로 인한 극심한 네트워크 혼잡과 가스비 급등은 '성공의 저주'와도 같았다.17 이러한 고통스러운 경험은 이더리움 커뮤니티로 하여금 레이어 2 확장 솔루션(롤업 등) 개발에 박차를 가하고, ERC-1155와 같이 여러 토큰을 한 번에 전송하여 가스 효율성을 높이는 새로운 토큰 표준을 모색하게 만드는 직접적인 원동력이 되었다.19 이는 기술 발전이 새로운 문제를 야기하고, 그 문제를 해결하기 위해 또 다른 기술 혁신이 일어나는 전형적인 순환 고리를 보여주는 사례다.

## **제2장: ERC-20 토큰의 생애주기: 발행부터 관리까지**

ERC-20 토큰은 스마트 계약 코드를 통해 탄생하고, 디지털 지갑을 통해 관리되며, 블록체인 위에서 영원히 존재한다. 이 장에서는 토큰을 안전하게 보관하는 지갑의 원리부터, 실제 지갑 설정 및 토큰 추가 방법, 그리고 토큰이 탄생하는 발행 과정까지 토큰의 전체 생애주기를 단계별로 추적한다.

### **2.1. 디지털 자산의 금고: ERC-20 지갑의 원리와 종류**

많은 초보자들이 오해하는 것과 달리, 암호화폐 지갑은 은행 계좌처럼 돈을 물리적으로 '저장'하는 공간이 아니다. ERC-20 토큰을 포함한 모든 암호화폐 자산은 실제로는 이더리움 블록체인이라는 분산 원장 위에 기록되어 있다.20 지갑의 진짜 역할은 이 블록체인 상의 자산에 접근하고, 거래를 승인(서명)하는 데 필요한 극도로 중요한 정보인 '개인 키(Private Key)'를 안전하게 보관하고 관리하는 것이다.20 지갑 주소는 이 개인 키로부터 암호학적으로 파생된 공개 식별자로, 다른 사람에게 토큰을 받기 위해 공유하는 주소다. 지갑은 크게 두 종류로 나뉜다.

* **소프트웨어 지갑 (핫월렛, Hot Wallet):** 메타마스크(MetaMask), 트러스트 월렛(Trust Wallet) 등이 대표적이다. 이들은 웹 브라우저 확장 프로그램이나 스마트폰 앱 형태로 존재하며, 개인 키를 인터넷에 연결된 장치(컴퓨터, 스마트폰)에 암호화하여 저장한다. 사용이 매우 편리하고 DApp과의 연동이 쉬워 일상적인 거래에 널리 사용된다. 하지만 항상 온라인 상태에 노출되어 있어 피싱, 멀웨어 등 해킹 공격에 상대적으로 취약하다는 단점이 있다.21
* **하드웨어 지갑 (콜드월렛, Cold Wallet):** 레저(Ledger), 트레저(Trezor) 등이 대표적이다. 이들은 개인 키를 인터넷과 완전히 분리된 전용 물리적 장치(USB 형태) 내의 보안 칩에 저장한다. 거래에 서명해야 할 때만 컴퓨터에 연결하며, 서명 과정 자체도 장치 내부에서 이루어지기 때문에 개인 키가 절대로 외부로 노출되지 않는다. 이는 온라인 해킹으로부터 자산을 보호하는 가장 강력한 방법으로, 상당한 규모의 자산을 장기 보관할 때 필수적인 보안 도구로 여겨진다.22

최상의 보안 관행은 이 두 가지를 함께 사용하는 것이다. 즉, 하드웨어 지갑에 자산을 보관하면서, 메타마스크와 같은 소프트웨어 지갑을 인터페이스로 연동하여 DApp을 이용하는 방식이다. 이 경우, 모든 거래 승인 요청은 메타마스크를 통해 하드웨어 지갑으로 전달되며, 사용자는 물리적 장치의 버튼을 눌러 최종 서명을 해야만 거래가 실행된다. 이는 하드웨어 지갑의 강력한 보안과 소프트웨어 지갑의 편리함을 동시에 누릴 수 있는 최적의 조합이다.22

| 표 2: 주요 ERC-20 지갑 비교 (소프트웨어 vs. 하드웨어) |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **구분** | **대표 지갑** | **보안 수준** | **편의성** | **비용** | **주요 특징** | **추천 사용자** |
| **소프트웨어 지갑 (핫월렛)** | 메타마스크 | 중상 | 높음 | 무료 | 브라우저 확장, 모바일 앱, DApp 연동 용이 | 소액 자산 관리, 빈번한 DeFi 사용자, 초보자 |
| **하드웨어 지갑 (콜드월렛)** | 레저 나노 시리즈 | 최상 | 중간 | 유료 (기기 구매) | 개인 키 오프라인 저장, 물리적 서명 필요 | 다액 자산 장기 보관, 보안을 최우선으로 하는 모든 사용자 |

### **2.2. 실전 가이드: 메타마스크(MetaMask) 설정 및 토큰 추가**

메타마스크는 가장 널리 사용되는 ERC-20 지갑으로, DApp 생태계로 들어가는 관문 역할을 한다. 다음은 메타마스크를 설정하고 사용하는 단계별 가이드다.

1. **설치 및 계정 생성:**
   * 공식 웹사이트(metamask.io)를 통해 사용하는 브라우저(크롬, 파이어폭스 등)의 확장 프로그램을 설치하거나 모바일 앱을 다운로드한다.
   * '새 지갑 생성'을 선택하고 강력한 비밀번호를 설정한다. 이 비밀번호는 해당 장치에서 지갑을 잠금 해제할 때만 사용된다.
   * 가장 중요한 단계는 \*\*12개의 단어로 구성된 '비밀 복구 구문(Secret Recovery Phrase)'\*\*을 백업하는 것이다. 이 구문은 지갑의 마스터 키와 같아서, 컴퓨터를 바꾸거나 비밀번호를 잊어버렸을 때 자산을 복구할 수 있는 유일한 수단이다. **절대로 이 구문을 컴퓨터나 온라인에 저장하지 말고, 종이에 적어 안전한 곳에 물리적으로 보관해야 한다.**
2. **네트워크 추가:**
   * 메타마스크는 기본적으로 이더리움 메인넷에 연결되어 있다. 폴리곤(Polygon), 바이낸스 스마트 체인(BSC), 아비트럼(Arbitrum)과 같이 이더리움과 호환되는 다른 블록체인(EVM 호환 체인)을 사용하려면 해당 네트워크 정보를 수동으로 추가해야 한다.
   * 메타마스크의 네트워크 설정 메뉴에서 '네트워크 추가'를 선택하고, 네트워크 이름, RPC URL, 체인 ID 등의 정보를 입력한다.
   * 이 과정은 'Chainlist.org'와 같은 신뢰할 수 있는 서비스를 이용하면 더욱 간편하다. 해당 사이트에서 원하는 네트워크를 검색하고 'Add to Metamask' 버튼을 클릭하면 자동으로 네트워크 정보가 추가된다.25
3. **ERC-20 토큰 추가:**
   * 지갑에 ETH가 아닌 다른 ERC-20 토큰을 받으면, 잔액이 자동으로 표시되지 않을 수 있다. 이 경우 토큰을 수동으로 '가져오기' 해야 한다.
   * **방법 1 (검색):** 메타마스크 하단의 '토큰 가져오기(Import tokens)'를 클릭하고, 검색창에 토큰의 심볼(예: USDC)을 입력한다. 목록에 나타나면 선택하여 추가한다.26
   * **방법 2 (맞춤형 토큰 추가):** 검색되지 않는 토큰의 경우, '맞춤형 토큰(Custom token)' 탭을 선택해야 한다. 이 방법이 가장 확실하며, 다음 정보가 필요하다.
     + **토큰 계약 주소 (Token Contract Address):** 이는 토큰의 고유 식별 주소다. 코인마켓캡(CoinMarketCap)이나 코인게코(CoinGecko)와 같은 신뢰할 수 있는 정보 사이트에서 해당 토큰 페이지를 찾아 계약 주소를 복사한다.26
     + 복사한 계약 주소를 메타마스크에 붙여넣으면, 토큰 기호와 소수점 자릿수는 대부분 자동으로 채워진다.26
     + '맞춤형 토큰 추가'를 클릭하면 지갑에 해당 토큰이 표시되고 잔액을 확인할 수 있다.
   * **주의사항:** 동일한 이름의 토큰이라도 각기 다른 블록체인 네트워크에서는 서로 다른 계약 주소를 갖는다. 예를 들어, 이더리움 메인넷의 USDC와 폴리곤 네트워크의 USDC는 계약 주소가 다르다. 따라서 토큰을 추가할 때는 반드시 현재 메타마스크에 연결된 네트워크와 일치하는 계약 주소를 사용해야 한다.26

### **2.3. 토큰 발행의 원리: 스마트 계약의 작성과 배포 과정**

ERC-20 토큰은 비트코인처럼 경쟁적인 채굴 과정을 통해 생성되는 것이 아니다. 대신, 특정 규칙이 담긴 스마트 계약을 이더리움 블록체인에 배포함으로써 '주조(Minting)' 또는 발행된다.23

1. **스마트 계약 작성:** 토큰 발행의 첫 단계는 이더리움의 주요 프로그래밍 언어인 솔리디티(Solidity)를 사용하여 스마트 계약 코드를 작성하는 것이다. 이 코드에는 앞서 설명한 ERC-20 표준 함수들(totalSupply, balanceOf 등)과 함께 토큰의 고유한 속성(이름, 심볼, 총 공급량, 소수점 자릿수)이 정의된다.3
2. **오픈소스 라이브러리 활용:** 보안은 스마트 계약 개발에서 가장 중요한 요소다. 처음부터 모든 코드를 직접 작성하는 것은 버그가 발생할 위험이 크다. 따라서 대부분의 개발자는 OpenZeppelin과 같이 전 세계 수많은 개발자들에 의해 검증되고 널리 사용되는 표준 ERC-20 스마트 계약 라이브러리를 기반으로 자신들의 토큰을 만든다. 이는 개발 시간을 단축하고 보안성을 크게 향상시키는 업계 표준 관행이다.12
3. **컴파일 및 배포 (Deployment):** 작성된 솔리디티 코드는 EVM이 이해할 수 있는 바이트코드로 컴파일(변환)된다. 이후, 리믹스(Remix IDE)와 같은 웹 기반 개발 환경과 메타마스크 지갑을 사용하여 이 컴파일된 계약 코드를 이더리움 네트워크에 배포한다.5 배포는 블록체인에 데이터를 기록하는 트랜잭션이므로, 이 과정에서 이더(ETH)로 가스비를 지불해야 한다.3
4. **발행 완료:** 배포 트랜잭션이 블록체인에 성공적으로 기록되면, 스마트 계약은 이더리움 네트워크 상에 고유한 주소(토큰 계약 주소)를 갖게 되며, 이 주소를 통해 토큰이 공식적으로 존재하게 된다. 이제 이 토큰은 전 세계 누구와도 주고받을 수 있는 디지털 자산이 된다.

이 과정에서 '토큰 계약 주소'의 개념을 명확히 이해하는 것은 매우 중요하다. 이는 ERC-20 생태계의 '주민등록번호'와 같은 역할을 하며, 사용자의 이해도와 보안 수준을 가늠하는 척도가 된다. 사용자는 자신의 자산을 받는 지갑 주소(EOA, Externally Owned Account)와, 자산 자체를 정의하는 토큰의 계약 주소(CA, Contract Address)를 구분할 수 있어야 한다.27 메타마스크에 토큰을 추가할 때, 이더스캔에서 특정 토큰의 총 공급량이나 홀더 분포를 조회할 때, 또는 탈중앙화 거래소에서 스왑할 토큰을 선택할 때 사용자는 항상 이 '토큰 계약 주소'를 확인하고 사용해야 한다.26 피싱 사기꾼들은 종종 유명 토큰과 동일한 이름과 심볼을 가진 가짜 토큰을 만들어, 그 가짜 계약 주소를 유포하여 사용자를 속인다. 따라서 코인마켓캡, 코인게코, 또는 프로젝트 공식 웹사이트와 같은 신뢰할 수 있는 출처에서 '토큰 계약 주소'를 직접 확인하고 사용하는 능력은, 단순한 기술적 절차를 넘어 탈중앙화 세계에서 자신의 자산을 지키는 핵심적인 보안 역량이다. 이는 중앙 기관의 보호 없이 스스로 자신의 자산을 책임져야 하는 '자기 주권(Self-sovereignty)'이 지식과 책임에 기반함을 보여주는 명백한 예시다.

## **제3장: ERC-20 토큰 전송 및 거래의 모든 것**

ERC-20 토큰을 실제로 주고받는 것은 이더리움 생태계에 참여하는 가장 기본적인 활동이다. 이 장에서는 지갑을 이용해 안전하게 토큰을 전송하는 단계별 절차를 알아보고, 모든 거래의 필수 비용인 가스비의 복잡한 구조를 심층적으로 분석한다. 마지막으로, 블록체인의 투명성을 직접 체험할 수 있는 강력한 도구인 이더스캔의 활용법을 마스터한다.

### **3.1. 토큰 전송 단계별 가이드: 지갑을 이용한 안전한 자산 이동**

ERC-20 토큰을 다른 주소로 보내는 과정은 대부분의 암호화폐 지갑에서 유사한 절차를 따른다. 메타마스크를 기준으로 한 일반적인 단계는 다음과 같다.

1. **전송 기능 선택:** 메타마스크 지갑을 열고 전송하려는 토큰을 선택한 후 '보내기(Send)' 버튼을 클릭한다.32
2. **수신자 주소 입력:** 토큰을 받을 사람의 이더리움 지갑 주소를 입력한다. 이더리움 주소는 '0x'로 시작하는 42자의 영숫자 문자열이다.20 주소를 잘못 입력하면 자금을 영원히 잃을 수 있으므로, 직접 타이핑하기보다는 복사하여 붙여넣거나 QR 코드를 스캔하는 것이 안전하다. 자주 거래하는 주소는 주소록에 저장해두는 것이 좋다.32
3. **자산 및 수량 입력:** 전송할 토큰의 종류가 올바르게 선택되었는지 확인하고, 보낼 수량을 입력한다.
4. **가스비 검토 및 설정:** 지갑은 현재 네트워크 혼잡도를 분석하여 거래를 무난하게 처리할 수 있는 추천 가스비를 자동으로 제시한다. 대부분의 경우 이 추천값을 사용하면 되지만, 거래 속도를 조절하고 싶다면 수동으로 가스 가격을 높이거나 낮출 수 있다.
5. **최종 확인 및 전송:** 마지막으로 화면에 표시된 모든 정보, 즉 **받는 사람의 주소, 보내는 토큰의 종류와 수량, 그리고 예상 가스비**를 꼼꼼하게 재차 확인한다. 모든 정보가 정확하다면 '확인(Confirm)' 버튼을 눌러 거래를 최종 승인하고 네트워크에 전송한다.32 하드웨어 지갑을 사용하는 경우, 이 단계에서 물리적 장치의 버튼을 눌러 서명을 완료해야 한다.

**가장 중요한 주의사항** 중 하나는 네트워크 선택이다. 거래소에서 개인 지갑으로 토큰을 출금하거나, 개인 지갑에서 다른 지갑으로 토큰을 보낼 때, 반드시 \*\*ERC-20 네트워크(이더리움 메인넷)\*\*를 선택해야 한다. 만약 실수로 다른 블록체인 네트워크(예: 바이낸스 스마트 체인의 BEP-20)를 선택하여 토큰을 전송하면, 해당 토큰은 의도한 지갑에 나타나지 않으며 최악의 경우 영구적으로 손실될 위험이 있다.24

### **3.2. 이더리움의 연료, 가스비(Gas Fee) 심층 분석**

이더리움 네트워크에서 발생하는 모든 활동에는 비용이 발생하며, 이를 '가스비'라고 한다. 가스비는 이더리움이라는 거대한 분산 컴퓨터를 작동시키는 데 필요한 '연료(Gas)'와 같다.17 가스비의 개념은 다소 복잡하지만, 다음 네 가지 핵심 요소로 구성된다.

* **가스 (Gas):** 트랜잭션을 처리하거나 스마트 계약 코드를 실행하는 데 필요한 총 연산 작업량을 나타내는 추상적인 단위다. 단순한 ETH 전송보다 여러 단계를 거치는 ERC-20 토큰 전송이나 DEX 스왑과 같은 복잡한 작업일수록 더 많은 가스를 소모한다.17
* **Gwei:** '기가웨이(Giga-Wei)'의 줄임말로, 가스 가격을 표시하는 데 사용되는 이더(ETH)의 작은 단위다. 1 ETH는 10억 Gwei와 같으며, 1 Gwei는 0.000000001 ETH에 해당한다. 가스비를 소수점이 많은 ETH로 직접 표기하는 대신 Gwei를 사용함으로써 가독성을 높인다.33
* **가스 한도 (Gas Limit):** 사용자가 하나의 트랜잭션을 위해 지불할 용의가 있는 가스의 최대 상한선이다. 사용자는 트랜잭션이 '가스 부족(Out of Gas)' 오류로 실패하지 않도록 충분한 가스 한도를 설정해야 한다. 예를 들어, 단순 ETH 전송의 표준 가스 한도는 21,000이지만, ERC-20 토큰 전송은 스마트 계약과 상호작용해야 하므로 더 높은 값(예: 50,000~100,000)이 필요하다.35 만약 실제 사용된 가스가 설정한 한도보다 적으면, 남은 가스에 해당하는 비용은 사용자에게 반환된다. 하지만 한도를 너무 낮게 설정하여 거래 도중 가스가 소진되면, 거래는 실패로 기록되고 그때까지 소모된 가스비는 환불되지 않는다.34
* **가스 가격 (Gas Price):** 사용자가 가스 1단위당 지불하고자 하는 가격을 Gwei로 나타낸 것이다. 이는 일종의 '입찰가'와 같아서, 더 높은 가스 가격을 제시한 사용자의 거래가 네트워크의 검증인(Validator)에 의해 더 빨리 선택되어 처리될 가능성이 높다. 가스 가격은 네트워크의 수요와 공급에 따라 실시간으로 변동한다.18

결론적으로, 사용자가 지불하는 \*\*총 가스비(Transaction Fee)\*\*는 다음과 같이 계산된다:

총 가스비 (ETH)=(실제 사용된 가스량)×(가스 가격 (Gwei))/1,000,000,000

34

사용자는 이더스캔의 가스 트래커(Gas Tracker)나 EthGasStation과 같은 전문 사이트를 통해 현재 네트워크의 평균 가스 가격을 확인하고, 거래가 급하지 않다면 네트워크가 덜 혼잡한 시간대(보통 주말이나 특정 시간대)를 이용함으로써 가스비를 절약할 수 있다.35

### **3.3. 블록 탐색기 활용법: 이더스캔(Etherscan) 마스터하기**

이더스캔(Etherscan.io)은 이더리움 블록체인 위의 모든 데이터를 검색하고 조회할 수 있는 가장 대표적인 '블록 탐색기(Block Explorer)'다. 이는 마치 인터넷의 정보를 찾아주는 구글처럼, 블록체인의 정보를 투명하게 보여주는 검색 엔진과 같다.31 이더스캔을 활용하면 자신의 거래 내역을 확인하는 것을 넘어, 이더리움 생태계 전체의 움직임을 파악할 수 있다.

#### **지갑 주소로 거래 내역 추적하기**

자신의 이더리움 지갑 주소를 복사하여 이더스캔 홈페이지의 검색창에 붙여넣고 검색하면, 해당 주소와 관련된 모든 정보를 한눈에 볼 수 있다.31

* **잔액 (Balance):** 해당 주소가 보유한 ETH 잔액.
* **토큰 (Token):** 드롭다운 메뉴를 클릭하면 해당 주소가 보유한 모든 종류의 ERC-20, ERC-721(NFT) 토큰 목록과 각각의 잔액을 확인할 수 있다.
* **거래 내역 (Transactions):** 해당 주소가 참여한 모든 트랜잭션 목록이 시간 순서대로 나열된다. 각 거래의 종류(IN/OUT), 대상 주소, 수량 등을 간략히 볼 수 있다.

#### **트랜잭션 해시(TxID/TxHash)로 상세 정보 확인하기**

모든 이더리움 트랜잭션은 생성될 때마다 고유한 식별 코드인 '트랜잭션 해시'를 부여받는다.40 이 해시를 이더스캔에서 검색하면 해당 거래에 대한 모든 세부 정보를 법의학 수준으로 정밀하게 확인할 수 있다.42

* **Transaction Hash**: 해당 거래의 고유 ID. 거래 관련 문의 시 이 해시를 공유한다.41
* **Status**: 거래의 현재 상태. 'Success'는 성공, 'Failed'는 실패, 'Pending'은 아직 처리 중임을 의미한다. 실패 시 그 원인(예: Out of Gas)도 표시된다.41
* **Block**: 거래가 포함된 블록의 번호. 옆의 'Block Confirmations'는 이 블록 이후에 얼마나 많은 블록이 더 생성되었는지를 나타내며, 이 숫자가 클수록 거래가 되돌릴 수 없게 확정되었음을 의미한다.41
* **Timestamp**: 거래가 블록에 기록된 정확한 시간.41
* **From**: 거래를 보낸 지갑 주소.41
* **To**: 거래를 받은 지갑 주소 또는 상호작용한 스마트 계약 주소.41
* **Value**: 전송된 ETH의 가치. ERC-20 토큰 전송의 경우 이 값은 0 ETH일 수 있다.
* **Tokens Transferred**: **가장 중요한 정보 중 하나.** 어떤 종류의 ERC-20 토큰이, 얼마나, 누구에게서 누구에게로 이동했는지를 명확하게 보여준다.
* **Transaction Fee**: 해당 거래를 처리하기 위해 지불된 총 가스비. (실제 사용된 가스량 × 가스 가격)으로 계산된다.41
* **Gas Price 및 Gas Used by Transaction**: 사용자가 설정한 단위당 가스 가격과, 이 거래를 처리하는 데 실제로 소모된 총 가스량.41

이더스캔은 단순한 '조회 도구'를 넘어, 탈중앙화 시스템의 '신뢰 검증 도구'이자 '분쟁 해결사'로서 결정적인 역할을 수행한다. 중앙화된 금융 시스템에서는 거래에 문제가 생기면 은행이나 카드사의 고객센터에 문의하여 해결을 요청한다. 그러나 중개자가 없는 탈중앙화 세계에서는 이러한 중앙 기관이 존재하지 않는다. 만약 사용자가 암호화폐 거래소에 ERC-20 토큰을 입금했는데 잔액이 반영되지 않는다면 어떻게 해야 할까? 사용자는 자신의 지갑에서 해당 거래의 트랜잭션 해시(TxID)를 찾아 이더스캔에서 직접 조회할 수 있다. 이를 통해 거래의 상태가 'Success'인지, 입금 주소(To 필드)가 정확하게 입력되었는지, 전송된 토큰의 종류와 수량이 맞는지 객관적으로 확인할 수 있다.43 이 블록체인 상의 불변하는 기록을 증거로 거래소에 제시함으로써, 사용자는 중앙 기관의 자의적인 판단에 의존하지 않고 자신의 입금 사실을 증명하고 문제 해결을 요구할 수 있다. 이는 개인 간의 거래에서도 마찬가지다. 판매자는 구매자가 대금 지급의 증거로 제시한 TxID를 이더스캔에서 확인함으로써, 비신뢰(trustless) 방식으로 지급 여부를 검증할 수 있다.46 이처럼 이더스캔은 블록체인의 핵심 가치인 투명성과 불변성을 일반 사용자가 직접 활용할 수 있게 해주는 강력한 창구이며, 탈중앙화 시스템이 실제로 작동하게 만드는 필수적인 사회적 인프라다.

## **제4장: ERC-20 토큰의 활용: 디파이(DeFi)와 그 너머**

ERC-20 표준은 단순히 디지털 자산을 생성하고 전송하는 것을 넘어, 완전히 새로운 금융 시스템인 탈중앙화 금융(DeFi)의 탄생을 가능하게 한 기폭제였다. 이 장에서는 ERC-20 토큰이 DeFi 생태계의 기축 자산으로서 어떻게 기능하는지, 그리고 탈중앙화 거래소, 스테이킹, 유동성 공급 등 구체적인 활용 사례를 통해 그 작동 원리를 탐구한다.

### **4.1. 탈중앙화 금융(DeFi)의 기축 자산이 된 ERC-20**

탈중앙화 금융(DeFi)은 은행, 증권사 같은 전통적인 금융 중개 기관 없이, 오직 블록체인 위의 스마트 계약 코드에 의해 자동화된 금융 서비스를 제공하는 생태계를 의미한다.4 사용자들은 허가나 검열 없이 누구나 자유롭게 대출, 예금, 거래, 투자, 보험 등의 금융 활동에 참여할 수 있다.

이 거대한 DeFi 생태계의 혈액과도 같은 역할을 하는 것이 바로 ERC-20 토큰이다. 현재 대부분의 주요 DeFi 프로토콜은 이더리움 블록체인 위에서 운영되며, 이 안에서 교환되고, 대출의 담보로 제공되고, 예치에 대한 이자로 지급되고, 프로토콜의 운영권을 나타내는 자산은 거의 모두 ERC-20 표준을 따르는 토큰들이다.4 ERC-20이 제공하는 표준화된 인터페이스 덕분에, A 프로토콜의 토큰을 B 프로토콜에 담보로 맡기고, 그 대가로 받은 또 다른 토큰을 C 프로토콜에 예치하는 등, 마치 레고 블록을 조립하듯 다양한 금융 전략을 조합하는 '머니 레고(Money Legos)' 현상이 가능해졌다.

### **4.2. 탈중앙화 거래소(DEX)에서의 토큰 교환 원리**

탈중앙화 거래소(DEX, Decentralized Exchange)는 사용자가 자신의 개인 키와 자산을 직접 통제하는 비위탁형(non-custodial) 방식으로, 중개자 없이 개인 대 개인(P2P)으로 ERC-20 토큰을 교환할 수 있는 플랫폼이다.49 이는 해킹이나 운영 중단 위험이 있는 중앙화 거래소(CEX)에 자산을 예치할 필요가 없다는 점에서 큰 장점을 가진다. DEX는 주로 다음과 같은 방식으로 작동한다.

* **자동화된 마켓 메이커 (AMM, Automated Market Maker) 방식:** 유니스왑(Uniswap)이 대중화시킨 모델로, 전통적인 호가창(order book) 방식 대신 '유동성 풀(Liquidity Pool)'을 사용한다. 유동성 공급자(LP)라고 불리는 사용자들이 두 종류의 ERC-20 토큰 쌍(예: ETH와 USDT)을 스마트 계약으로 이루어진 풀에 예치한다. 그러면 다른 사용자가 이 풀을 상대로 토큰을 교환할 수 있다. 이때 교환 비율은 풀에 예치된 두 토큰의 수량 비율에 따라 $x \times y = k$ 와 같은 단순한 수학적 공식에 의해 자동으로 결정된다. 누군가 풀에서 USDT를 가져가고 ETH를 넣으면, 풀의 USDT 수량은 줄고 ETH 수량은 늘어나므로 다음 거래자는 더 비싼 값에 USDT를 사야 한다. 이처럼 시장 참여자들의 거래 행위 자체가 가격을 결정하는 시장을 만드는 방식이다.50
* **0x 프로토콜 방식:** 이는 AMM과 전통적인 오더북 방식의 장점을 결합한 하이브리드 모델이다. 주문의 생성, 매칭, 취소 등 빈번한 활동은 블록체인 외부, 즉 오프체인(off-chain)에서 '리플레이어(Relayer)'에 의해 관리된다. 그리고 최종적으로 거래가 체결될 때만 그 결과를 온체인(on-chain)에 기록한다. 이 방식은 모든 과정을 블록체인에 기록하는 것보다 가스비를 크게 절감하고 거래 속도를 높일 수 있다는 장점이 있다.49

### **4.3. 패시브 인컴 전략: 스테이킹과 유동성 공급**

DeFi는 ERC-20 토큰 보유자에게 단순히 자산을 보유하는 것을 넘어, 이를 활용하여 추가적인 수익(Yield)을 창출할 수 있는 다양한 기회를 제공한다.

* **유동성 공급 (Liquidity Providing):** 앞서 설명한 AMM 기반 DEX의 유동성 풀에 자신이 보유한 ERC-20 토큰 쌍을 예치하는 행위다. 유동성 공급자는 자신의 기여에 대한 대가로 두 가지 보상을 받는다. 첫째, 해당 풀에서 발생하는 모든 거래 수수료(보통 0.3%)의 일부를 자신의 지분율에 따라 분배받는다. 둘째, 자신이 풀에 예치한 자산의 소유권을 증명하는 'LP 토큰'이라는 새로운 ERC-20 토큰을 받게 된다. 이 LP 토큰 자체도 다른 DeFi 프로토콜에서 거래하거나 담보로 활용할 수 있다.4
* **스테이킹 (Staking) & 이자 농사 (Yield Farming):**
  + **단순 스테이킹:** 특정 프로토콜의 거버넌스 토큰이나 유틸리티 토큰을 해당 프로토콜의 스마트 계약에 일정 기간 예치(잠금)하고, 그 대가로 동일한 토큰이나 다른 보상 토큰을 받는 가장 기본적인 수익 창출 활동이다. 이는 네트워크의 안정성에 기여하거나, 토큰의 유통량을 조절하는 효과를 가진다.52
  + **이자 농사 (Yield Farming):** 유동성 공급으로 받은 LP 토큰을 그냥 보유하는 것이 아니라, 이를 다시 다른 DeFi 프로토콜의 스테이킹 풀에 예치하여 추가적인 보상 토큰(주로 해당 프로토콜의 거버넌스 토큰)을 얻는 등, 여러 프로토콜을 넘나들며 수익률을 극대화하려는 복잡하고 적극적인 전략을 의미한다. 이는 높은 수익을 기대할 수 있지만, 그만큼 스마트 계약 리스크, 가격 변동 리스크 등 더 큰 위험을 수반한다.4
* **유동성 스테이킹 (Liquid Staking):** 이더리움과 같이 지분증명(PoS) 방식의 블록체인에 자산을 스테이킹하면 보통 해당 자산이 락업(lock-up)되어 유동성이 사라진다. 유동성 스테이킹은 이 문제를 해결하기 위해 등장했다. 라이도(Lido)와 같은 플랫폼에 ETH를 스테이킹하면, 그 대가로 스테이킹된 ETH의 가치를 1:1로 표방하는 stETH(Staked ETH)라는 새로운 ERC-20 토큰을 받는다. 사용자는 원본 ETH에 대한 스테이킹 보상을 계속 받으면서도, 이 유동적인 stETH 토큰을 다른 DeFi 프로토콜에서 대출 담보로 사용하거나 유동성 공급에 활용하여 추가 수익을 창출할 수 있다. 이는 자산의 유동성과 수익성을 동시에 추구하는 진일보한 전략이다.52

### **4.4. 실제 사례 분석: 스테이블코인, 거버넌스 토큰, 유틸리티 토큰**

ERC-20 표준을 기반으로 다양한 목적을 가진 토큰들이 발행되어 DeFi 생태계를 풍요롭게 만들고 있다.

* **스테이블코인 (Stablecoins):** 테더(USDT), USD코인(USDC), 다이(DAI) 등이 대표적이다. 이들은 미국 달러와 같은 특정 법정화폐의 가치에 1:1로 가치가 고정(페깅)되도록 설계된 ERC-20 토큰이다. 암호화폐 시장의 극심한 가격 변동성에 대한 '안전한 피난처' 역할을 하며, 국경 간 송금이나 상거래 결제 수단으로도 활용된다. 특히 DeFi 생태계 내에서는 가치 변동의 위험 없이 자산을 예치하거나 대출하고, 거래 쌍의 기준 통화로 사용되는 등 사실상의 기축통화 역할을 한다.4
* **거버넌스 토큰 (Governance Tokens):** 유니스왑(UNI), 에이브(AAVE), 컴파운드(COMP) 등이 대표적이다. 이 토큰의 보유자들은 해당 DeFi 프로토콜의 미래 운영 방향에 대한 의사결정에 참여할 수 있는 투표권을 갖는다. 예를 들어, 프로토콜의 수수료율 변경, 지원하는 자산 목록 추가, 개발 기금 사용처 결정 등 중요한 안건에 대해 투표할 수 있다. 이는 프로토콜의 소유권과 통제권을 중앙화된 개발팀이 아닌, 토큰을 보유한 커뮤니티 구성원들에게 분산시키는 탈중앙화 자율 조직(DAO)의 핵심 요소다.4
* **유틸리티 토큰 (Utility Tokens):** 베이직 어텐션 토큰(BAT), 디센트럴랜드(MANA) 등이 대표적이다. 이들은 특정 플랫폼이나 네트워크 내에서 특정 서비스나 재화를 이용하기 위한 '사용권'의 성격을 갖는다. 예를 들어, BAT는 브레이브(Brave) 브라우저 생태계에서 광고주가 광고를 집행하고 사용자가 광고를 시청한 대가로 받는 토큰이며, MANA는 가상현실 플랫폼인 디센트럴랜드 내에서 가상 토지를 구매하거나 아바타 아이템을 거래하는 데 사용되는 화폐다.21

DeFi에서 얻는 '수익(Yield)'의 본질을 이해하는 것은 매우 중요하다. 이는 전통 금융에서 제공하는 '이자'와는 근본적으로 다르다. 전통 은행의 예금 이자는 주로 중앙은행의 기준금리와 은행의 예대마진이라는 비교적 안정적인 요소에 의해 결정된다. 반면, DeFi의 수익은 여러 복합적인 요소가 결합된 결과물이다. 첫째, \*\*'거래 수수료'\*\*는 유동성 공급에 대한 직접적인 대가로, 해당 풀의 실제 시장 수요(거래량)를 반영한다. 둘째, \*\*'프로토콜 인센티브'\*\*는 이자 농사 과정에서 지급되는 거버넌스 토큰처럼, 프로토콜의 초기 성장을 위해 유동성을 공급하는 위험을 감수한 참여자들에게 지급하는 일종의 '보조금'이다. 이는 프로토콜의 미래 가치와 거버넌스 권한을 초기 기여자들에게 분배하는 메커니즘이다.4 셋째, \*\*'위험 프리미엄'\*\*이 존재한다. DeFi의 높은 수익률은 스마트 계약 코드의 버그로 인한 자금 손실 위험, 유동성 풀 내 자산 가격 변동으로 인한 비영구적 손실(Impermanent Loss) 위험, 그리고 보상으로 받는 토큰 자체의 가격 하락 위험 등 다양한 위험을 감수하는 것에 대한 대가이기도 하다. 따라서 DeFi의 수익률을 단순히 '안전한 예금 이자'로 간주하는 것은 매우 위험한 접근이다. 그것은 시장 수요, 프로토콜의 성장 전략, 그리고 내재된 기술적·경제적 위험이라는 세 가지 요소가 복합적으로 작용한 역동적인 결과물임을 이해하는 것이 성공적인 DeFi 투자의 첫걸음이다.

## **제5장: 안전한 자산 관리를 위한 보안 지침 및 미래 전망**

ERC-20 토큰은 막대한 기회를 제공하지만, 동시에 새로운 형태의 위험에 노출되어 있다. 탈중앙화된 환경에서는 누구도 사용자의 자산을 대신 지켜주지 않으므로, 스스로 보안을 책임지는 자세가 무엇보다 중요하다. 이 장에서는 주요 보안 위협과 그에 대한 전문가 수준의 예방책을 제시하고, ERC-20을 넘어 진화하는 새로운 토큰 표준들을 비교 분석하며 미래를 조망한다.

### **5.1. 주요 보안 위협과 전문가의 예방책**

ERC-20 토큰 사용자가 직면하는 가장 흔하고 치명적인 위협은 기술적 해킹보다는 사용자의 실수를 노리는 사회 공학적 공격이다.

* **피싱 (Phishing) 및 소셜 엔지니어링:** 해커들은 유명 DApp이나 거래소와 똑같이 생긴 가짜 웹사이트를 만들거나, 긴급한 조치를 요구하는 가짜 이메일을 보내 사용자를 속인다. 사용자가 이러한 가짜 사이트에 지갑을 연결하고 거래에 서명하거나, 최악의 경우 비밀 복구 구문을 입력하면 모든 자산을 즉시 탈취당하게 된다. 이를 예방하기 위해서는 항상 북마크된 공식 웹사이트 주소로만 접속하고, 이메일이나 SNS를 통해 받은 알 수 없는 링크는 절대로 클릭하지 않는 습관이 필수적이다.22
* **악성 스마트 계약 및 무한 승인(Infinite Approval) 위험:** DeFi 프로토콜을 이용하기 위해 approve 함수를 통해 토큰 사용을 승인할 때, 많은 DApp들은 편의를 위해 '무제한(unlimited)' 수량을 승인하도록 요청한다. 만약 이 DApp의 스마트 계약 코드에 악의적인 백도어가 숨겨져 있거나, 향후 해킹을 당하게 되면, 해커는 이 '무한 승인' 권한을 악용하여 사용자의 지갑에 있는 해당 토큰 전액을 언제든지 빼갈 수 있다. 이는 매우 심각한 위협이므로, 신뢰할 수 없는 DApp에는 절대로 지갑을 연결하거나 승인 요청에 서명해서는 안 된다. 또한, 이더스캔의 'Token Approval Checker'나 Revoke.cash와 같은 전문 도구를 사용하여 주기적으로 자신의 지갑이 어떤 계약에 얼마만큼의 승인을 해줬는지 확인하고, 더 이상 사용하지 않는 DApp에 대한 승인은 즉시 '취소(Revoke)'해야 한다.56

이러한 위협으로부터 자산을 보호하기 위한 핵심 보안 수칙은 다음과 같다.

1. **하드웨어 지갑 사용:** 아무리 강조해도 지나치지 않은 가장 강력하고 근본적인 보안 대책이다. 개인 키를 오프라인에 보관함으로써 온라인에서 발생하는 거의 모든 해킹 위협을 원천적으로 차단할 수 있다.22
2. **비밀 복구 구문(시드 구문)의 철저한 오프라인 관리:** 복구 구문은 디지털 자산의 전부와 같다. 절대 스크린샷을 찍거나, 이메일, 클라우드, 비밀번호 관리 프로그램 등 디지털 형태로 저장해서는 안 된다. 종이에 적어 화재나 수해로부터 안전한 곳에 물리적으로 분산 보관하는 것이 원칙이다.
3. **브라우저 및 기기 보안:** 브라우저에 지갑 비밀번호를 저장하지 않고, 의심스러운 소프트웨어를 설치하지 않으며, 운영체제와 백신 프로그램을 항상 최신 상태로 유지하는 기본적인 디지털 위생을 지켜야 한다.22
4. **거래 서명 전 꼼꼼한 확인:** 메타마스크와 같은 지갑에서 거래 서명을 요청하는 팝업창이 뜨면, 무심코 '확인'을 누르지 말고 어떤 내용에 서명하는 것인지(어떤 함수를 호출하는지, 어떤 주소와 상호작용하는지 등) 반드시 확인하는 습관을 들여야 한다.

### **5.2. 토큰 표준의 진화: ERC-20, ERC-721, ERC-1155 비교 분석**

ERC-20은 이더리움 토큰 생태계의 문을 열었지만, 시장의 요구는 더 다양하고 효율적인 표준의 등장을 이끌었다.

* **ERC-20 (대체 가능 토큰, Fungible Token):** 이 표준의 핵심은 '대체 가능성'이다. 모든 토큰 단위가 동일한 가치와 속성을 가지므로 서로 교환이 가능하다. 이는 화폐, 지분, 투표권 등을 표현하는 데 이상적이다. 우리가 아는 대부분의 암호화폐, 스테이블코인, 거버넌스 토큰이 이 표준을 따른다.8
* **ERC-721 (대체 불가능 토큰, Non-Fungible Token, NFT):** 이 표준의 핵심은 '대체 불가능성' 또는 '고유성'이다. 각 토큰은 고유한 ID(Token ID)를 가지며, 서로 다른 가치와 속성을 가질 수 있다. 따라서 디지털 아트워크, 한정판 수집품, 게임 내 고유 아이템, 부동산 등기부 등본 등 세상에 단 하나뿐인 자산의 소유권을 블록체인 상에 기록하는 데 사용된다.16
* **ERC-1155 (다중 토큰 표준, Multi-Token Standard):** 이 표준은 ERC-20과 ERC-721의 개념을 하나로 통합하고 효율성을 극대화한 진보된 표준이다. 하나의 스마트 계약 주소 안에서 여러 종류의 대체 가능한 토큰(예: 게임 내 골드)과 대체 불가능한 토큰(예: 전설의 검)을 동시에 발행하고 관리할 수 있다. 가장 큰 기술적 혁신은 **'일괄 전송(Batch Transfer)'** 기능이다. 이 기능을 사용하면 여러 종류의 토큰을 여러 명의 수신자에게 단 한 번의 트랜잭션으로 보낼 수 있다. 이는 ERC-20이나 ERC-721에서 각기 다른 토큰을 보내기 위해 여러 번의 트랜잭션을 일으켜야 했던 것에 비해 가스비를 획기적으로 절감시킨다. 이러한 특징 때문에 복잡한 아이템 경제를 가진 블록체인 게임 분야에서 특히 각광받고 있다.16

| 표 3: 이더리움 토큰 표준 비교 (ERC-20 vs. ERC-721 vs. ERC-1155) |  |  |  |
| --- | --- | --- | --- |
| **특징** | **ERC-20** | **ERC-721** | **ERC-1155** |
| **대체 가능성** | 대체 가능 (Fungible) | 대체 불가능 (Non-Fungible) | 둘 다 지원 (Semi-Fungible) |
| **주요 용도** | 화폐, 스테이블코인, 거버넌스 토큰 | 디지털 아트, 수집품, 고유 아이템 | 게임 아이템, 다종 자산 관리 |
| **계약 구조** | 1 계약 = 1 종류 토큰 | 1 계약 = 1 종류 NFT 컬렉션 | 1 계약 = 다종 토큰/NFT 관리 |
| **핵심 식별자** | 주소별 잔액 (balanceOf) | 개별 토큰 ID (ownerOf) | (토큰 ID + 주소)별 수량 |
| **일괄 전송** | 불가능 | 불가능 | **가능 (핵심 장점)** |
| **가스 효율성** | 보통 | 비효율적 (개별 전송) | **매우 효율적 (일괄 전송)** |
| **거래 취소** | 불가능 | 불가능 | 안전 전송 기능 지원 |

ERC-1155의 등장은 '효율성'이라는 경제적 요구가 블록체인 기술의 진화 방향을 결정하는 핵심 동인임을 명확히 보여준다. ERC-20과 ERC-721은 각각의 목적을 위해 훌륭했지만, 두 종류의 토큰을 모두 사용하는 애플리케이션(특히 게임)에서는 각 토큰 종류마다 별도의 스마트 계약을 배포하고 관리해야 했다. 이는 블록체인에 중복된 코드를 영원히 저장하게 만들고, 여러 아이템을 전송할 때마다 개별 트랜잭션을 발생시켜 막대한 가스비를 낭비하는 경제적 비효율을 낳았다.58 온라인 게임 개발사 엔진(Enjin)이 처음 제안한 ERC-1155는 바로 이 '비용' 문제를 직접적으로 해결하기 위해 탄생했다. 하나의 계약에서 수천 종류의 아이템을 관리하고, 일괄 전송 기능으로 가스비를 최대 90%까지 절감하는 능력은 단순히 기술적 우위를 넘어, DApp 개발과 운영에 있어 명백한 비용 절감 효과를 가져온다.19 이는 블록체인 기술이 더 이상 순수한 기술적 이상만을 추구하는 것이 아니라, 실제 비즈니스 환경의 '비용-효익 분석'이라는 현실적인 압박에 의해 진화하고 있음을 보여주는 강력한 증거다.

### **5.3. ERC-20의 미래와 이더리움 생태계의 발전 방향**

새로운 표준들이 등장했음에도 불구하고, ERC-20의 미래는 여전히 밝다.

* **지속적인 지배력:** ERC-20은 이미 이더리움 생태계에 깊숙이 뿌리내리고 있다. 수많은 DeFi 프로토콜, 지갑, 거래소, 분석 도구들이 ERC-20을 중심으로 구축되어 있으며, 이 강력한 네트워크 효과는 새로운 표준이 쉽게 대체하기 어렵다. 따라서 앞으로도 ERC-20은 DeFi와 토큰 경제의 핵심 표준으로서 그 지위를 유지할 가능성이 높다.8
* **레이어 2(Layer 2)와의 결합:** 이더리움의 높은 가스비와 느린 속도 문제는 아비트럼(Arbitrum), 옵티미즘(Optimism)과 같은 레이어 2 확장 솔루션을 통해 해결되고 있다. 사용자들은 ERC-20 토큰을 레이어 2로 옮겨 거의 즉각적인 거래를 매우 저렴한 비용으로 처리할 수 있다. 앞으로 대부분의 일상적인 ERC-20 토큰 거래는 레이어 2에서 이루어지고, 최종적인 결제만 이더리움 메인넷에 기록되는 형태가 보편화될 것이다.
* **계정 추상화(Account Abstraction)를 통한 사용자 경험 개선:** 현재 사용자는 토큰을 전송할 때 항상 가스비를 ETH로 지불해야 하는 등 불편함을 겪는다. 미래에 도입될 계정 추상화(EIP-4337 등) 기술은 이러한 경험을 크게 개선할 수 있다. 예를 들어, 사용자가 보유한 USDC와 같은 ERC-20 토큰으로 직접 가스비를 지불하거나, DApp 개발사가 사용자를 대신해 가스비를 지불해주는 '가스 스폰서링'이 가능해진다. 이는 사용자가 ERC-20, ERC-721, ERC-1155와 같은 기술적 차이를 의식할 필요 없이, 마치 현대의 간편 결제 앱을 사용하듯 쉽고 직관적으로 블록체인 서비스를 이용하게 만들 것이다.

## **결론: ERC-20 사용자를 위한 최종 권고**

ERC-20은 이더리움 블록체인 위에서 '가치'를 표준화하고 프로그래밍 가능하게 만든 위대한 발명이다. 이 표준이 제공한 상호운용성은 개발자들의 창의력을 해방시켰고, ICO를 통한 자본 조달의 민주화를 이끌었으며, 마침내 국경과 중개자를 넘어선 새로운 금융 패러다임인 DeFi의 초석을 다졌다. 이 보고서는 ERC-20의 기술적 사양부터 실용적 활용법, 보안 위협, 그리고 미래 전망까지 다각도로 조명함으로써 이 혁신적인 기술에 대한 깊이 있는 이해를 제공하고자 했다.

이 방대하고 역동적인 생태계에 참여하는 사용자를 위해 다음과 같은 최종 전문가 제언을 제시한다.

1. **'아는 것이 힘이다':** 이 보고서에서 다룬 가스비의 원리, 이더스캔을 통한 거래 검증 방법, 그리고 approve 함수의 위험성 등 핵심 개념을 명확히 이해하는 것은 선택이 아닌 필수다. 탈중앙화 세계에서 지식은 곧 자신의 자산을 지키는 가장 강력한 방패다.
2. **'의심하고 또 의심하라':** "너무 좋아 보여서 사실이 아닐 것 같은" 높은 수익률을 약속하는 프로젝트는 실제로 사실이 아닐 가능성이 높다. 어떤 DApp과 상호작용하든, 어떤 거래에 서명하든, 그 주체가 신뢰할 수 있는지, 어떤 권한을 요구하는지 항상 비판적으로 확인하는 습관을 들여야 한다.
3. **'보안에 타협은 없다':** 자산 규모와 상관없이 하드웨어 지갑을 사용하는 것을 기본 원칙으로 삼아야 한다. 비밀 복구 구문은 자신의 생명처럼 여기고, 누구와도, 어떤 상황에서도 공유해서는 안 된다. 탈중앙화된 금융 시스템에서 당신은 스스로가 자신의 은행장이자 보안 책임자다.
4. **'생태계와 함께 학습하라':** ERC-20은 결코 정체된 기술이 아니다. 레이어 2 솔루션, ERC-1155와 같은 새로운 표준, 계정 추상화 등 이더리움 생태계는 지금 이 순간에도 끊임없이 진화하고 있다. 이러한 변화의 흐름을 주시하고 지속적으로 학습하는 자세만이 이 혁신적인 기술이 제공하는 기회를 온전히 누리고 잠재적인 위험을 피해갈 수 있는 유일한 길이다.

ERC-20이 연 세상은 복잡하고 때로는 위험하지만, 동시에 전례 없는 금융 주권과 투명성, 그리고 가능성을 개인에게 부여한다. 이 보고서가 그 여정을 시작하는 모든 이들에게 신뢰할 수 있는 나침반이 되기를 바란다.

#### 참고 자료

1. ERC-20 토큰을 만드는 방법과 ERC-20 토큰 생성 비용은 얼마인가요?, 8월 14, 2025에 액세스, <https://bitkan.com/ko/learn/erc-20-%ED%86%A0%ED%81%B0%EC%9D%84-%EB%A7%8C%EB%93%9C%EB%8A%94-%EB%B0%A9%EB%B2%95%EA%B3%BC-erc-20-%ED%86%A0%ED%81%B0-%EC%83%9D%EC%84%B1-%EB%B9%84%EC%9A%A9%EC%9D%80-%EC%96%BC%EB%A7%88%EC%9D%B8%EA%B0%80%EC%9A%94-57226>
2. ERC-20 토큰 크립토의 의미, 8월 14, 2025에 액세스, <https://tangem.com/ko/glossary/erc-20-tokens/>
3. ERC-20 토큰 발행 방법 및 이점 – WEB3.0 - prodao.club, 8월 14, 2025에 액세스, <https://www.prodao.club/erc-20-%ED%86%A0%ED%81%B0-%EB%B0%9C%ED%96%89-%EB%B0%A9%EB%B2%95-%EB%B0%8F-%EC%9D%B4%EC%A0%90/>
4. DeFi 란 무엇입니까? - RUE, 8월 14, 2025에 액세스, <https://rue.ee/kr/blog/what-is-defi/>
5. 15분 안에 ERC20 토큰 생성하기: 단계별 가이드 - ICODA, 8월 14, 2025에 액세스, <https://icoda.io/ko/15-minutes-guide-to-creating-an-erc20-token-based-on-ethereum/>
6. ERC20 - Blockchain Council, 8월 14, 2025에 액세스, <https://www.blockchain-council.org/ethereum/erc20/>
7. ERC-20 토큰 표준이란 무엇입니까 - Cryptomus, 8월 14, 2025에 액세스, <https://cryptomus.com/ko/blog/an-introduction-to-erc-20-tokens>
8. ERC20이란 무엇입니까? 이더리움 토큰 표준 가이드 - Plisio, 8월 14, 2025에 액세스, <https://plisio.net/ko/blog/what-is-erc20>
9. ERC20 Token Essentials: Understanding the Standard for Ethereum Tokens - Coinpaper, 8월 14, 2025에 액세스, <https://coinpaper.com/3516/erc-20-token-essentials-understanding-the-standard-for-ethereum-tokens>
10. What Are ERC-20 Tokens on the Ethereum Network? - Investopedia, 8월 14, 2025에 액세스, <https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/>
11. ERC-20의 정의와 규칙 - 업비트 투자자보호센터, 8월 14, 2025에 액세스, <https://m.upbitcare.com/academy/advice/40>
12. 이더리움 기반의 ERC20 토큰 만들기 - 니르바나 블로그, 8월 14, 2025에 액세스, <https://ihpark92.tistory.com/35>
13. ERC-20 토큰 설명 - 고팍스 아카데미, 8월 14, 2025에 액세스, <https://academy.gopax.co.kr/erc-20-tokeun-seolmyeong/>
14. ERC-20 코드 살펴보기(feat. OpenZeppelin) - 안수빈의 블로그, 8월 14, 2025에 액세스, <https://ansubin.com/erc20/>
15. ERC 20 - OpenZeppelin Docs, 8월 14, 2025에 액세스, <https://docs.openzeppelin.com/contracts/2.x/api/token/erc20>
16. [그게 뭔가요] 블록체인 개발자라면 꼭 알아야하는 이더리움 토큰 표준 ..., 8월 14, 2025에 액세스, <https://byline.network/2023/08/16-307/>
17. 이더리움 가장 합리적으로 구매하기 - 가스비 계산법 [2023년] - BeinCrypto Korea, 8월 14, 2025에 액세스, <https://kr.beincrypto.com/learn-kr/buy-ethereum-gas-fee/>
18. Eth 가스는 어떻게 작동하나요? 이더리움 가스 수수료 설명 - BitKan.com, 8월 14, 2025에 액세스, <https://bitkan.com/ko/learn/eth-%EA%B0%80%EC%8A%A4%EB%8A%94-%EC%96%B4%EB%96%BB%EA%B2%8C-%EC%9E%91%EB%8F%99%ED%95%98%EB%82%98%EC%9A%94-%EC%9D%B4%EB%8D%94%EB%A6%AC%EC%9B%80-%EA%B0%80%EC%8A%A4-%EC%88%98%EC%88%98%EB%A3%8C-%EC%84%A4%EB%AA%85-30514>
19. 721과 ERC - 1155 - 생각하는 개발자 - 티스토리, 8월 14, 2025에 액세스, <https://com789.tistory.com/27>
20. ERC-20 지갑 주소 얻는 방법 - Cryptomus, 8월 14, 2025에 액세스, <https://cryptomus.com/ko/blog/how-to-get-erc-20-wallet-address>
21. ERC-20이란 무엇입니까? 이더리움 토큰 표준 가이드 - Blade 지갑 서비스, 8월 14, 2025에 액세스, <https://bladewallet.io/ko/blog/what-is-erc-20-a-guide-to-the-ethereum-token-standard/>
22. 메타마스크는 무엇이며 어떻게 안전하게 사용할 수 있나요? | NordVPN, 8월 14, 2025에 액세스, <https://nordvpn.com/ko/blog/what-is-metamask/>
23. ERC-20 토큰이란? 장단점, 채굴 가능 여부까지! - 브런치, 8월 14, 2025에 액세스, <https://brunch.co.kr/@gapcha/162>
24. ERC20 토큰 관리, 8월 14, 2025에 액세스, <https://support.ledger.com/ko/article/4404389645329-zd>
25. 내 이더리움 ERC20 토큰 예치금이 보이지 않습니다. - Ledger Support, 8월 14, 2025에 액세스, <https://support.ledger.com/ko/article/4402543134993-zd>
26. Metamask 체인 및 토큰 추가 가이드. 안녕하세요? 드디어 메타마스크 가이드의 마지막 시간입니다! | by SEOBINA WAVE | Medium, 8월 14, 2025에 액세스, <https://medium.com/@seobina_/metamask-%EC%B2%B4%EC%9D%B8-%EB%B0%8F-%ED%86%A0%ED%81%B0-%EC%B6%94%EA%B0%80-%EA%B0%80%EC%9D%B4%EB%93%9C-9cb6559af617>
27. 메타마스크 토큰 추가하기 | Loyalty20 Rewards Programs - Little Blockchain Lab., 8월 14, 2025에 액세스, <https://wooriapt.github.io/Loyalty-Programs/2018/09/03/Metamask-ADD-Tokens.html>
28. 나만의 코인 만들기(ERC-20) 실습편 #비트코인 #이더리움 #코인 #토큰 - YouTube, 8월 14, 2025에 액세스, <https://www.youtube.com/watch?v=GLHMdTiOde8>
29. Solidity 기초 (2) : ERC-20 스마트 컨트랙트 배포하기 | by Kevin Hong - Medium, 8월 14, 2025에 액세스, <https://medium.com/hy-block/solidity-%EA%B8%B0%EC%B4%88-2-erc-20-%EC%8A%A4%EB%A7%88%ED%8A%B8-%EC%BB%A8%ED%8A%B8%EB%9E%99%ED%8A%B8-%EB%B0%B0%ED%8F%AC%ED%95%98%EA%B8%B0-ab2c302557d5>
30. 이더리움 지갑 주소: 정의 및 생성 방법 • 블로그 Cryptomus, 8월 14, 2025에 액세스, <https://cryptomus.com/ko/blog/a-step-by-step-guide-on-how-to-get-your-ethereum-wallet-address>
31. 이더스캔: 이더리움 네트워크를 구성하는 링크 조사하기 - Phemex, 8월 14, 2025에 액세스, <https://phemex.com/ko/academy/what-is-etherscan>
32. ETH 또는 토큰 전송 방법 | 1inch.io - 도움말 센터, 8월 14, 2025에 액세스, <https://help.1inch.io/ko/articles/5172778-eth-%EB%98%90%EB%8A%94-%ED%86%A0%ED%81%B0-%EC%A0%84%EC%86%A1-%EB%B0%A9%EB%B2%95>
33. kr.beincrypto.com, 8월 14, 2025에 액세스, <https://kr.beincrypto.com/learn-kr/buy-ethereum-gas-fee/#:~:text='%EA%B0%80%EC%8A%A4(Gas)'%EB%9E%80,%EB%8A%94%200.000000001ETH%EC%99%80%20%EA%B0%99%EC%8A%B5%EB%8B%88%EB%8B%A4.>
34. 이더리움 가스에 대한 이해: Gas Price, Gas Limit, Block Gas Limit | by 조상연 - Medium, 8월 14, 2025에 액세스, <https://playdev.medium.com/%EC%9D%B4%EB%8D%94%EB%A6%AC%EC%9B%80-%EA%B0%80%EC%8A%A4%EC%97%90-%EB%8C%80%ED%95%9C-%EC%9D%B4%ED%95%B4-gas-price-gas-limit-block-gas-limit-161268a5fc54>
35. 이더리움 가스는 무엇이고, 어떻게 계산할까?, 8월 14, 2025에 액세스, <https://m.upbitcare.com/academy/research/22>
36. 이더리움 가스 요금: Gwei와 Crypto Gas 이해하기 - Plisio, 8월 14, 2025에 액세스, <https://plisio.net/ko/blog/gwei-and-gas-fueling-the-ethereum-network>
37. How to use EtherScan. 이더스캔 활용 방법 | by BOSagora - Medium, 8월 14, 2025에 액세스, <https://medium.com/bosagora/kor-eng-%EC%9D%B4%EB%8D%94%EC%8A%A4%EC%BA%94-%ED%99%9C%EC%9A%A9-%EB%B0%A9%EB%B2%95-how-to-use-etherscan-ae69e593bf4a>
38. What is Etherscan and how to use it? - Coinbase, 8월 14, 2025에 액세스, <https://www.coinbase.com/learn/crypto-glossary/what-is-etherscan-and-how-to-use-it>
39. How do I find my transaction hash? - OpenSea Help Center, 8월 14, 2025에 액세스, <https://support.opensea.io/en/articles/8867103-how-do-i-find-my-transaction-hash>
40. 트랜잭션 해시 또는 ID(TxHash/TxID)란 무엇이며 어떻게 찾나요? - Cryptomus, 8월 14, 2025에 액세스, <https://cryptomus.com/ko/blog/what-is-a-transaction-hash-or-id-txhashtxid-and-how-to-find-it>
41. What is a Transaction Hash (Txn hash)? - Etherscan Information Center, 8월 14, 2025에 액세스, <https://info.etherscan.com/what-is-a-transaction-hash-txhash/>
42. Viewing Transactions on Etherscan, 8월 14, 2025에 액세스, <https://info.etherscan.com/viewing-transactions-on-etherscan/>
43. 트랜잭션 해시(TXID)에 대한 오해 - 브런치, 8월 14, 2025에 액세스, <https://brunch.co.kr/@nujabes403/15>
44. How to check an Ethereum transaction - Cointelegraph, 8월 14, 2025에 액세스, <https://cointelegraph.com/news/how-to-check-an-ethereum-transaction>
45. Etherscan: 무엇이며 어떻게 사용하는가 - Plisio, 8월 14, 2025에 액세스, <https://plisio.net/ko/blog/etherscan-what-it-is-and-how-to-use-it>
46. What is Etherscan? How to Look Up a Transaction | Tangem Blog, 8월 14, 2025에 액세스, <https://tangem.com/en/blog/post/the-anatomy-of-a-transaction/>
47. 탈중앙 금융(DeFi)에서 이자 농사란 무엇일까요? - 고팍스 아카데미, 8월 14, 2025에 액세스, <https://academy.gopax.co.kr/taljungang-geumyung-defi-eseo-ija-nongsaran-mueosilggayo/>
48. 디지털자산의 분류, 개념 및 주요 예시 l 거버넌스 토큰, 유틸리티 토큰 - 투이컨설팅, 8월 14, 2025에 액세스, <https://www.2e.co.kr/news/articleView.html?idxno=303386>
49. 탈중앙 거래소(DEX)란 무엇인가요? - 고팍스 아카데미, 8월 14, 2025에 액세스, <https://academy.gopax.co.kr/taljungang-georaeso-dex-ran-mueosingayo/>
50. DeFi 강의 및 실습, 8월 14, 2025에 액세스, <https://heungno.net/wp-content/uploads/2012/08/%EC%9B%8C%ED%81%AC%EC%83%B5-%EB%B0%9C%ED%91%9C%EC%9E%90%EB%A3%8C_%EA%B0%95%EC%9D%98-%EB%B0%8F-%EC%8B%A4%EC%8A%B5_rev1.pdf>
51. 그래서 어디에 쓰는 거라고? — DeFi | by 김인근 | CURG - Medium, 8월 14, 2025에 액세스, <https://medium.com/curg/%EA%B7%B8%EB%9E%98%EC%84%9C-%EC%96%B4%EB%94%94%EC%97%90-%EC%93%B0%EB%8A%94-%EA%B1%B0%EB%9D%BC%EA%B3%A0-defi-b1d324b3a097>
52. '유동성 스테이킹'의 모든 것 - 네이버 프리미엄콘텐츠, 8월 14, 2025에 액세스, <https://contents.premium.naver.com/digitalasset/digitalassetpro/contents/240119111530871oe>
53. 유동성 스테이킹의 모든 것, 8월 14, 2025에 액세스, <https://contents.premium.naver.com/digitalasset/digitalassetpro/contents/241002172337868tt>
54. ERC-20이란: 블록체인에서 스마트 계약 이해하기 | Deriv Blog, 8월 14, 2025에 액세스, <https://deriv.com/ko/blog/posts/what-is-erc-20>
55. The ERC-20 Token Standard - Base Documentation, 8월 14, 2025에 액세스, <https://docs.base.org/learn/token-development/erc-20-token/erc-20-standard>
56. 이더리움에서 스마트 계약의 토큰 승인 및 권한을 취소하는 방법 - Ledger Support, 8월 14, 2025에 액세스, <https://support.ledger.com/ko/article/8700644160925-zd>
57. ERC-1155란 무엇인가요? - 고팍스 아카데미, 8월 14, 2025에 액세스, <https://academy.gopax.co.kr/d/>
58. ERC-1155 란? - 생각하는 개발자 - 티스토리, 8월 14, 2025에 액세스, <https://com789.tistory.com/26>