

# 테더(Tether)

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

## 테더 (Tether)

## 테더: 비트코인 블록체인의 법정화폐

### 초록 (Abstract)

법정화폐로 담보된 디지털 토큰은 개인과 기관이 익숙한 회계 단위를 사용하면서도, 견고하고 탈중앙화된 방식으로 가치를 교환할 수 있도록 한다. 블록체인의 혁신은 감사 가능한 암호학적으로 보호된 전 세계 원장을 제공하는 것이다. 자산 담보형 토큰 발행자와 기타 시장 참여자는 블록체인 기술과 내장된 합의 시스템을 활용하여 익숙하고 변동성이 낮은 통화 및 자산으로 거래할 수 있다.

책임성을 유지하고 환율의 안정성을 보장하기 위해, 우리는 ‘테더(tether)’라는 암호화폐 토큰과 그에 대응하는 실물 자산인 법정화폐 간에 **1:1 준비금 비율**을 유지하는 방법을 제안한다. 이 방법은 비트코인 블록체인, **Proof of Reserves(준비금 증명)** 및 기타 감사 방식을 활용하여 발행된 토큰이 언제나 전액 담보 및 예치되어 있음을 증명한다.

## 목차 (Table of Contents)

- [테더](#)
- [테더: 비트코인 블록체인 위의 법정화폐](#)
  - [초록](#)
- [목차](#)

- 서론
- 기술 스택 및 프로세스
  - 테더 기술 스택
- 자금 흐름 프로세스
- 준비금 증명 프로세스
- 구현상의 취약점
- 주요 응용 사례
  - 거래소 대상
  - 개인 사용자 대상
  - 가맹점 대상
- 향후 혁신
- 결론
- 부록
  - 감사상의 결함: 거래소 및 지갑
- 기존 법정화폐 폐깅 시스템의 한계
- 시장 리스크 사례
- 법률 및 컴플라이언스
- 용어 해설
- 참고문헌

# 서론 (Introduction)

세상에는 사람들이 가치 저장 수단, 거래 매개체 또는 투자 대상으로 자유롭게 선택하는 다양한 자산이 존재한다. 우리는 비트코인 블록체인이 이러한 자산을 거래하고 저장하며 회계 처리하는 데 더 나은 기술이라고 믿는다. 대부분의 추정치에 따르면 전 세계 부의 총량은 약 250조 달러에 이르며[1], 그중 대부분은 은행이나 유사한 금융 기관에 의해 보유하고 있다. 이러한 자산이 비트코인 블록체인으로 이전되는 것은 비례적으로 매우 큰 기회를 의미한다.

비트코인은 “신뢰가 아닌 암호학적 증거에 기반한 전자 결제 시스템으로, 서로 거래를 원하는 두 당사자가 신뢰할 수 있는 제3자 없이 직접 거래할 수 있도록 한다.”[2]라는 개념으로 만들어졌다. 비트코인은 **탈중앙화 디지털 화폐(암호화폐)**라는 새로운 형태의 디지털 화폐를 창조했다<sup>1</sup>.

암호화폐의 주요 장점으로서는 낮은 거래 비용, 국경 없는 전송 및 변환 가능성, 신뢰 불필요한 소유 및 교환, 가명성(pseudo-anonymity), 실시간 투명성, 그리고 기존 은행 시스템 문제로부터의 면역성 등이 있다 [3].

현재 암호화폐의 주류 활용이 제한적인 이유로는 **가격 변동성**, **대중의 기술 이해 부족**, **비기술적 사용자에게 불편한 사용성** 등이 일반적으로 언급된다.

자산 연동형 암호화폐(Asset-pegged cryptocurrency) 개념은 2012년 1월 J.R. Willett이 저술한 **마스터코인(Mastercoin) 백서**[4]를 통해 비트코인 커뮤니티에서 처음으로 대중화되었다<sup>2</sup>.

오늘날 우리는 BitAssets, Ripple, Omni, Nxt, NuShares/Bits 등과 같은 프로젝트에서 이러한 개념이 구현되는 것을 볼 수 있다.

모든 비트코인 거래소 및 지갑(예: Coinbase, Bitfinex, Coinapult)은 이미 사용자가 특정 암호화폐의 변동성을 회피하기 위해 이를 법정화폐, 금, 기타 자산으로 교환할 수 있는 유사한 서비스를 제공하고 있다. 나아가, 기존의 거의 모든 금융 기관이나 결제 제공자 역시 법정화폐(또는 자산) 보유를 허용함으로써 유사한 서비스를 제공하고 있다.

이 백서에서는 **오픈소스, 암호학적으로 안전하며 분산 원장 기술을 사용하는 소프트웨어를 통해 법정화폐 가치를 저장하고 전송하는 응용 사례**에 초점을 맞춘다 — 즉, 진정한 암호화폐적 형태의 법정화폐 연동 모델이다.

성공적인 암호화폐의 목표는 신뢰의 필요성을 완전히 제거하는 것이지만, 앞서 언급한 모든 구현체들은 신뢰할 수 있는 제3자에 의존하거나 기술적, 시장적, 절차적 한계를 가진다<sup>3</sup>.

---

<sup>1</sup> 용어 정의는 [용어 해설](#) 참조

<sup>2</sup> 그러나 Dr. Szabo의 BitGold 제안[5] 이후부터 논의되어 왔다.

<sup>3</sup> 부록의 [기존 법정화폐 페깅 시스템의 한계](#) 참조

우리의 솔루션에서, 법정화폐 연동형 암호화폐는 “**테더(Tether)**”라 불린다.

모든 테더는 초기<sup>4</sup>에 비트코인 블록체인 상의 **Omni Layer 프로토콜**을 통해 발행되며, 암호화폐 토큰 형태로 존재한다.

유통 중인 각 테더 단위는 홍콩에 기반한 **Tether Limited**가 예치한 해당 법정화폐 단위로 **1:1 비율**(예: 1 USDT = 1 USD)로 담보된다.

테더는 Tether Limited의 이용 약관에 따라 법정화폐로 상환 또는 교환 가능하며, 사용자가 원할 경우 동등한 시가의 비트코인으로 교환할 수도 있다.

한 번 발행된 테더는 비트코인이나 다른 암호화폐처럼 자유롭게 전송, 저장, 지불 등에 사용될 수 있다.

예치된 법정화폐는 암호화폐의 속성을 획득하며, 그 가격은 영구적으로 해당 법정화폐의 가치에 연동된다.

우리의 구현은 다른 법정화폐 연동형 암호화폐 대비 다음과 같은 이점을 가진다:

- 테더는 **비트코인 블록체인 위에 존재**하므로, 검증되지 않은 ‘알트코인’ 블록체인이나 폐쇄형 중앙 데이터베이스 위에서 동작하지 않는다.
- 테더는 **비트코인처럼 사용 가능**하며, 즉 P2P, 가명성, 탈중앙화, 암호학적으로 안전한 환경에서 작동한다.
- 테더는 **상점, 거래소, 지갑 등과 쉽게 통합 가능**하며, 비트코인이나 다른 암호화폐와 동일한 방식으로

적용된다.

- 테더는 **Omni Layer** 프로토콜의 특성을 계승하며, 여기에는 탈중앙화 거래소, 브라우저 기반 오픈 소스 지갑 암호화, 비트코인 기반의 투명성·책임성·다자간 보안 및 보고 기능이 포함된다.
- **Tether Limited**는 단순하지만 효과적인 **Proof of Reserves** 방식을 사용하여, 준비 자산의 수탁자로서의 대조 위험을 크게 줄인다.
- 테더의 발행 및 상환은 가격 또는 유동성 제약을 받지 않는다. 사용자는 원할 때 언제든지 빠르고 낮은 수수료로 테더를 사고팔 수 있다.
- 테더는 시장 리스크<sup>5</sup>(블랙 스완, 유동성 위기 등)에 노출되지 않는다. 준비금은 1:1로 유지되며 시장 변동에 의존하지 않는다.
- 테더의 1:1 담보 구조는 복잡한 담보화나 파생 전략에 비해 비전문 사용자에게도 직관적으로 이해 가능하다.

언제든지 우리의 준비금 계좌에 보유된 법정화폐 잔액은 유통 중인 테더 수량 이상으로 유지된다.

이 단순한 구조는 **Proof of Reserves(준비금 증명)** 프로세스를 가장 신뢰성 있게 지원하며, 이는 유통 중인 테더와 준비금 내 실물 화폐 간의 가격 패리티를 유지하는 핵심이다.

이 백서에서는 거래 및 준비금의 투명성을 입증하는 증거<sup>6</sup>를 제시한다.

---

<sup>4</sup> 향후 Ripple, Nxt 등과 같은 비트코인 2.0 프로토콜도 지원될 예정이다.

<sup>5</sup> 부록의 [시장 리스크 사례](#) 참조

<sup>6</sup> [준비금 증명 프로세스](#) 섹션 참조

현재 지갑 감사는 신뢰도가 매우 낮다(예: Proof of Solvency[6] 방식의 결함). 따라서 우리는 거래소와 지갑이 사용자 자금의 수탁을 테더를 통해 우리에게 위탁(outsource) 하도록 제안한다.

사용자는 Tether.to(웹 지갑)를 통해 테더를 직접 구매할 수 있으며, Bitfinex와 같은 테더 지원 거래소를 통해 입출금 수단으로 사용할 수 있다.

또한 Ambisafe, Holy Transaction, Omni Wallet 등 **Omni Layer** 지원 지갑을 통해 테더를 송금 및 보관할 수도 있다.

그 외의 거래소, 지갑, 가맹점들도 전통적인 법정 결제 수단을 대체하는 형태로 테더 통합을 논의하기를 권장한다.

우리는 우리의 구현이 완전한 탈중앙화 모델은 아님을 인식하고 있다<sup>7</sup>.

Tether Limited가 준비 자산의 중앙 수탁자 역할을 수행해야 하기 때문이다(다만 유통 중인 테더 자체는 탈중앙화된 디지털 화폐이다).

그러나 우리는 이 구현이 미래의 혁신을 위한 기초를 마련하고, 약점을 보완하며, 새로운 상품과 서비스를 위한 견고한 플랫폼을 구축하고, 장기적으로 비트코인 블록체인의 성장과 활용도를 강화할 것이라고 믿는다.

이러한 향후 혁신에는 다음이 포함된다:

- 사용자 및 가맹점 간 모바일 결제 기능 제공
- 다수의 탈중앙화된 주체(예: 복수의 거래소) 간 즉각적 또는 준실시간 법정화폐 가치 전송

- 스마트 컨트랙트 및 다중서명 기능 도입을 통한 보안성, 준비금 증명 절차 개선 및 신규 기능 구현

# 기술 스택 및 프로세스 (Technology Stack and Processes)

유통 중인 각 테더는 홍콩에 기반한 **Tether Limited**가 보유한 준비금 내 해당 법정화폐의 동등한 금액과 **1:1 비율로 담보된다**.

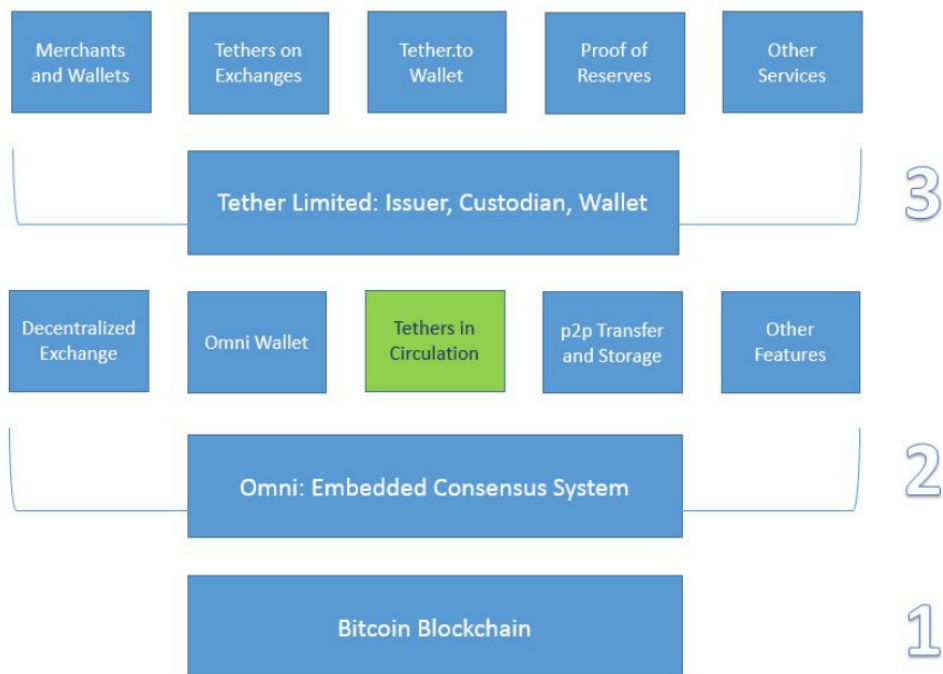
우리는 담보 자산의 수탁자로서 그 자산에 대해 책임을 지는 **신뢰받는 제3자** 역할을 수행한다.

이러한 리스크는 단순한 구현을 통해 완화되며, 이는 법정화폐와 암호화폐 양쪽의 감사 절차 복잡성을 줄이는 동시에 보안성, 검증 가능성, 투명성을 강화한다.

## 테더 기술 스택 (Tether Technology Stack)

이 스택은 3개의 계층과 다양한 기능으로 구성되어 있으며, 아래 다이어그램을 통해 가장 잘 이해할 수 있다.

7 [구현상의 취약점](#) 섹션 참조



각 계층은 다음과 같다.

### 1. 첫 번째 계층은 비트코인 블록체인이다.

테더의 거래 원장은 **내장 합의 시스템(embedded consensus system)**인 **Omni**를 통해 메타

데이터 형태로 비트코인 블록체인에 내장되어 있다.

## 2. 두 번째 계층은 Omni Layer 프로토콜이다.

Omni는 다음과 같은 기능을 수행하는 기초 기술이다.

a) 비트코인 블록체인에 내장된 메타데이터로 표현된 디지털 토큰을 **발행(Grant, create)** 하거나 **폐기(Revoke, destroy)** 한다. 여기서 토큰은 법정화폐에 연동된 디지털 토큰, 즉 테더이다.

b) **Omnichest.info**(예: Omni 자산 ID #31은 TetherUSD를 나타냄)와 **Omnicores API**를 통해 테더의 유통 현황을 추적 및 보고한다.

c) 사용자가 다음 환경에서 테더 및 기타 자산/토큰을 거래하고 보관할 수 있도록 한다.

i) **P2P, 가명성(pseudo-anonymous), 암호학적으로 안전한 환경**

ii) **오픈소스, 브라우저 기반, 암호화된 웹 지갑(Omni Wallet)**

iii) **다중서명(multi-signature) 및 오프라인 콜드스토리지 지원 시스템**

## 3. 세 번째 계층은 Tether Limited이며, 다음과 같은 주요 기능을 수행하는 사업 주체이다.

a) 법정화폐 예치를 수락하고 이에 상응하는 테더를 발행한다.

b) 법정화폐 인출을 실행하고 이에 상응하는 테더를 소각한다.

c) 유통 중인 모든 테더를 담보하는 법정화폐 준비금을 수탁한다.

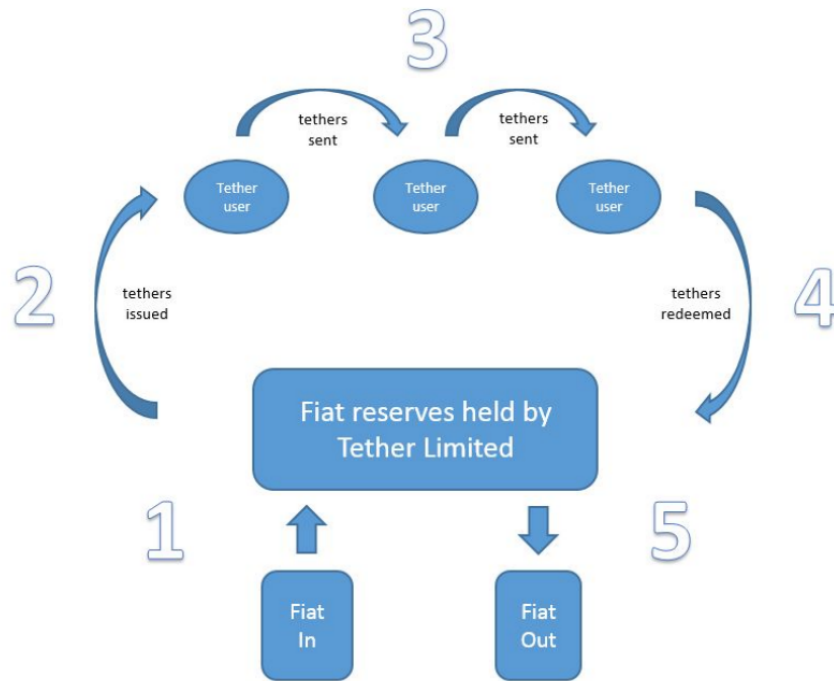
d) 준비금 증명(Proof of Reserves) 및 기타 감사 결과를 공개적으로 보고한다.

e) 기존 비트코인/블록체인 지갑, 거래소, 가맹점과의 통합을 시작 및 관리한다.

f) **Tether.to** 웹 지갑을 운영하며, 사용자가 테더를 송금, 수신, 저장, 전환할 수 있도록 한다.

# 자금 흐름 프로세스 (Flow of Funds Process)

테더의 생애주기는 다섯 단계로 구성되며, 아래 다이어그램을 통해 가장 잘 이해할 수 있다.



**1단계** – 사용자가 법정화폐를 **Tether Limited**의 은행 계좌에 입금한다.

**2단계** – **Tether Limited**가 테더를 발행하고 사용자의 테더 계좌에 입금한다. 테더가 유통에 들어간다.  
사용자가 입금한 법정화폐 금액 = 발행된 테더 금액 (예: 10,000달러 입금 → 10,000 tetherUSD 발행).

**3단계** – 사용자는 테더를 사용해 거래한다<sup>8</sup>.  
사용자는 **P2P 오픈소스, 가명성, 비트코인 기반 플랫폼**을 통해 테더를 전송, 교환, 저장할 수 있다.

**4단계** – 사용자가 **Tether Limited**에 테더를 예치하고 이를 법정화폐로 상환받는다.

**5단계** – **Tether Limited**가 테더를 소각하고 사용자의 은행 계좌로 법정화폐를 송금한다.

사용자는 위 과정 외에도 거래소나 다른 개인을 통해 테더를 취득할 수 있다.  
한 번 유통에 들어간 테더는 개인과 기업 간 자유롭게 거래될 수 있다.  
예를 들어, 사용자는 Bitfinex를 통해 테더를 구매할 수 있으며, 곧 더 많은 거래소에서도 지원될 예정이다.

이 자금 흐름 다이어그램이 전달하고자 하는 핵심 개념은, **Tether Limited**만이 테더를 발행(생성)하거나 소각(유통에서 제거) 할 수 있다는 것이다.  
이 메커니즘이 시스템의 **지급 능력(solveny)**을 유지하는 핵심 절차이다.

# 준비금 증명 프로세스 (Proof of Reserves Process)

지급 능력 증명(Proof of Solveny), 준비금 증명(Proof of Reserves), 실시간 투명성(Real-Time Transparency) 등의 개념은 암호화폐 업계 전반에서 점점 더 주목받고 있다.

현재의 거래소 및 지갑 감사 방식은 매우 신뢰성이 낮다.

비트코인 생태계에서는 **해킹, 부실 운영, 명백한 사기**로 인한 지급 불능 사례가 여러 차례 발생했다.

따라서 사용자는 거래소 선택 시 신중해야 하며, 이용 중에도 지속적인 경계심을 유지해야 한다.

그럼에도 불구하고 숙련된 사용자조차 이러한 위험을 완전히 제거할 수는 없다.

특히 **트레이더나 기업 사용자처럼 거래소에 상당한 법정화폐 잔액을 유지해야 하는 사용자**는 항상 제3자 보관(counterparty) 리스크를 감수해야 한다.

결론적으로, 현재의 거래소 및 지갑 감사 프로세스는 충분히 신뢰할 수 없다고 본다.

이들은 수탁자나 거래소가 실제로 지급 능력을 보유하고 있는지를 보장하지 못한다.

Merkle Tree 접근법[6]과 같은 개선 시도가 있었으나, 여전히 주요한 결함<sup>9</sup>이 남아 있다.

테더의 **Proof of Reserves** 구조는 혁신적이다.

그 이유는 **유통 중인 전체 테더(부채)가 언제나 동일한 금액의 법정화폐(자산)로 완전 담보됨을 입증하는 절차를 단순화**하기 때문이다.

---

<sup>8</sup> 주요 응용 사례 섹션의 테더 사용 이점 참조

<sup>9</sup> 감사상의 결함: 거래소 및 지갑 섹션 참조

우리의 구성에서, 유통 중인 각 **tetherUSD**는 준비금 내 보유 중인 **1달러**를 나타낸다(즉, 1:1 비율).

따라서 특정 시점에서 유통 중인 모든 테더의 합계가 준비금 내 보유된 USD 잔액과 정확히 동일할 경우, 시스템은 완전한 지급 능력을 갖춘 것으로 본다.

테더는 비트코인 블록체인 위에 존재하므로, 언제든지 유통 중인 테더의 수량과 회계 검증은 **기술적으로 명확하고 검증 가능하다**.

이에 대응하는 USD 총액은 **은행 잔액 공개 및 주기적 전문 감사**를 통해 증명된다.

아래는 이 구현의 세부 설명이다.

- **Tether Limited는 모든 테더를 Omni Layer 프로토콜을 통해 발행한다.**

Omni는 비트코인 블록체인 위에서 작동하므로, 모든 발행·상환·유통 중인 테더와 그 거래 이력은 **Omnichest.info** 도구를 통해 공개적으로 감사 가능하다.

- TetherUSD의 Omnichest 자산 ID는 **#31**이다.

- 링크: <http://omnichest.info/lookupsp.aspx?sp=31>

- 이 자산 ID로 발행된 총 테더 수를 **TUSDissue**,

- 상환된 총 테더 수를 **TUSDredeem**,

- 특정 시점 유통 중인 총 테더 수를 **TUSD**라 하면,

- $TUSD = TUSDissue - TUSDredeem$

- TUSD는 위 링크에서 “Total Property Tokens”로 표시된다.

- **Tether Limited는 테더 구매/상환을 위한 은행 계좌를 운영한다.**

- 총 입금액을 **DUSDdepo**,

- 총 출금액을 **DUSDwithd**,

- 은행 계좌의 달러 잔액을 **DUSD**라 하면,

▪  $DUSD = DUSDdepo - DUSDwithd$

- 발행된 각 테더는 동등한 법정화폐 단위로 완전히 담보된다 (1 tetherUSD = 1 USD).

위의 암호화폐 및 법정화폐 회계 과정을 결합하면, 테더 시스템의 “지급 능력 방정식(Solvency Equation)”은 다음과 같이 표현된다.

◦  $TUSD = DUSD$

◦ 비트코인 블록체인에 기록된 모든 테더 발행 및 상환은 은행 계좌의 입금 및 출금과 1:1로 대응된다.

◦ TUSD의 검증 가능성은 블록체인에 기반하며,  
DUSD의 검증 가능성은 다음 절차에 기반한다:

- 웹사이트의 **Transparency** 페이지에서 은행 잔액을 공개한다.
- 전문 감사인이 정기적으로 은행 잔액 및 금융 내역서를 검증, 서명, 공개한다.

사용자는 아래와 같은 투명성 페이지(Transparency Page)에서 이 정보를 확인할 수 있다.



명확히 하기 위해, 우리는 **Tether 시스템**<sup>10</sup>과 **Tether.to 웹 지갑** 간의 Proof of Reserves 개념이 다르다는 점을 밝힌다.

이 백서에서는 주로 **Tether 시스템 전체**, 즉 유통 중인 모든 테더에 대한 Proof of Reserves에 초점을 맞춘다.

반면, **Tether.to**는 폐쇄형 코드 및 중앙 서버 기반의 소비자 지향 웹 지갑이다.

이 지갑의 Proof of Reserves 절차는 본문에서 다른 시스템 수준의 방식과 본질적으로 다르다.

우리는 **Tether.to** 지갑을 위한 **PoR 기반 투명성 솔루션** 배포를 계획하고 있다.

이는 현재 존재하는 시스템 중 가장 발전된 PoR 모델이 될 것이며, 부록<sup>11</sup>에서 언급된 거의 모든 문제를 해결할 것이다.

물론 사용자는 개인 키를 직접 관리하거나 Omni Wallet을 이용해 테더를 안전하게 보관할 수도 있다.

## 구현상의 취약점 (Implementation Weaknesses)

우리의 구현이 완전히 **신뢰 불필요한(trustless)** 암호화폐 시스템을 즉시 실현하지는 못한다는 점을 이해하고 있다.

그 주요 이유는 사용자가 **Tether Limited**와 그에 연계된 **기존 은행 기관(legacy banking institution)**을 신뢰해야만 준비금 자산의 수탁자로 인정할 수 있기 때문이다.

그러나 거의 모든 거래소와 지갑(법정화폐나 USD를 보유하는 경우) 역시 동일한 약점을 안고 있다.

즉, 이러한 서비스를 사용하는 사용자들은 이미 유사한 리스크에 노출되어 있다.

아래는 우리의 접근 방식에서 발생할 수 있는 취약점들을 요약한 것이다.

- Tether Limited가 **파산할 수 있다**
- **은행이 지급 불능(파산)** 상태가 될 수 있다
- **은행이 자금을 동결하거나 몰수할 수 있다**
- **우리가 준비금을 유용할 수 있다**
- **리스크가 단일 실패 지점(single point of failure)**으로 재증앙화될 수 있다

---

<sup>10</sup> 용어 해설 참조

<sup>11</sup> 감사상의 결함: 거래소 및 지갑 참조

거의 모든 디지털 자산 거래소와 지갑(법정화폐를 보유하는 경우)이 이미 이러한 문제에 직면하고 있음을 주목해야 한다.

따라서 이와 같은 서비스를 사용하는 사용자들은 이미 동일한 리스크를 감수하고 있다.

아래에서는 각 문제에 대해 우리가 취하고 있는 대응 방안을 설명한다.

### **Tether Limited가 파산할 수 있다**

이 경우 법인인 Tether Limited는 파산하겠지만, **고객 자금은 안전하게 보호되며 모든 테더는 계속 상환 가능하다.**

비트코인 관련 보안 침해 사고의 대부분은 은행 계좌가 아니라 **암호화폐 자체를 목표로** 발생했다.

테더는 비트코인 블록체인 위에 존재하므로, 개인은 **개인 키를 직접 보관함으로써** 테더를 안전하게 저장할 수 있다.

### **은행이 지급 불능 상태가 될 수 있다**

이 리스크는 기존 금융 시스템의 모든 사용자와 거래소 운영자가 공통적으로 직면하는 문제다.

현재 Tether Limited는 **대만의 Cathay United Bank 및 Hwatai Bank**에 계좌를 보유하고 있으며, 양 은행 모두 **테더의 비즈니스 모델을 명확히 이해하고 수용 가능하다고 판단**하고 있다.

또한, **다른 관할권에서도 추가 은행 파트너십을 구축**하여 이 리스크를 더욱 완화하고 있다.

### **은행이 자금을 동결하거나 몰수할 수 있다**

우리가 거래하는 은행은 비트코인의 성격을 잘 이해하고 있으며,

비트코인 관련 사업체에 대해 **전 세계적으로 은행 서비스를 제공하는 주요 기관들**이다.

또한 우리가 따르는 **KYC(고객확인제도) 및 AML(자금세탁방지)** 절차는 해당 은행이 현재 거래하는 다른 디지털 자산 거래소들과 동일한 수준으로 운영된다.

그들은 우리가 **관련 법규를 완전히 준수하고 있음<sup>12</sup>**을 확인해 주었다.

### 우리가 준비금을 유용할 수 있다

Tether Limited의 **법인 정관(corporate charter)**은 공개되어 있으며<sup>12</sup>, **사업자 명단, 위치, 평판** 또한 투명하게 공개되어 있다. 은행 계좌의 소유권은 법적으로 법인 정관에 구속되며, 모든 입출금 거래에는 추적 가능한 기록이 남고, **엄격한 내부 통제 정책**에 따라 관리된다.

### 리스크가 단일 실패 지점으로 재중앙화될 수 있다

이 문제를 해결하기 위한 몇 가지 아이디어를 보유하고 있으며, 곧 공개될 **블로그 및 제품 업데이트를 통해 구체적인 방안을 공유할 예정**이다. 이 문제는 다양한 방법으로 접근 가능하지만, 현재의 초기 구현은 향후 버전에서 이러한 혁신을 실현하기 위한 **올바른 방향성**을 제시하고 있다. 우리가 선택한 플랫폼 구조를 통해 **중앙화 리스크를 “토큰의 발행과 상환”이라는 단일 기능으로 제한**했으며, 그 외 시스템의 모든 측면은 **탈중앙화 방식으로 운영**된다.

---

<sup>12</sup> [법률 및 컴플라이언스](#) 섹션 참조

<sup>13</sup> 각주 #10과 동일

## 주요 응용 사례 (Main Applications)

이 섹션에서는 비트코인 및 블록체인 생태계 전반과 전 세계 사용자들에게 테더가 가지는 주요 응용 사례를 요약하고 논의한다.

우리는 테더의 수혜 대상을 **거래소(Exchanges)**, **개인(Individuals)**, **가맹점(Merchants)**의 세 그룹으로 구분한다.

모든 그룹에 공통되는 주요 이점은 다음과 같다.

- 비트코인의 속성을 다른 자산 클래스에 부여
- 변동성이 적고 익숙한 회계 단위 제공
- 전 세계 자산이 비트코인 블록체인으로 이전

## 거래소 대상 (For Exchanges)

거래소 운영자들은 기존 금융 시스템을 통한 법정화폐의 입출금이 복잡하고, 위험하며, 느리고, 비용이 많이 든다는 점을 잘 알고 있다.

이에는 다음과 같은 문제가 포함된다.

- 거래소에 적합한 결제 서비스를 식별해야 함
  - 거래 취소 불가능성, 사기 방지, 수수료 최소화 등 고려 필요

- API가 없는 은행과의 시스템 통합
- 규제 준수, 보안, 신뢰 구축을 위한 은행과의 지속적 협의
- 소액 송금 시 과도한 비용 발생
- 국제 송금 시 3~7일의 결제 지연
- 불리한 환전 수수료

테더를 도입함으로써 거래소는 위와 같은 문제를 해소하고 다음과 같은 추가적인 이점을 얻을 수 있다.

- 기존 은행이나 결제 업체 대신 **암호화 기반 법정화폐(crypto-fiat)** 를 입출금 및 보관 수단으로 활용
  - 사용자가 거래소로 법정화폐를 더 자유롭게, 빠르게, 저렴하게 이동 가능
- **법정화폐 수탁 리스크를 Tether Limited에 위탁**하고, 거래소는 암호화폐만 관리
- 플랫폼에 다른 테더 기반 법정화폐 거래쌍을 손쉽게 추가 가능
- 고객 자산을 **순수 암호화폐 방식(멀티시그, 콜드/핫 월렛, HD 월렛 등)** 으로 안전하게 관리
  - 감사 또한 완전한 암호화 환경 내에서 더 쉽고 안전하게 수행 가능
- **비트코인으로 가능한 모든 거래소 기능은 테더로도 가능**

거래소 이용자는 거래소 내 법정화폐 보유가 얼마나 위험한지 잘 알고 있다.

지급 불능 사례가 증가함에 따라 그 위험은 현실적이다.

앞서 언급했듯, **테더를 사용하는 것이 거래소 내에 법정화폐를 직접 보유하는 것보다 상대적으로 적은 카운터 파티 리스크**에 노출된다.

또한, 테더를 보유함으로써 얻을 수 있는 추가적인 이점은 다음 섹션에서 다룬다.

## 개인 사용자 대상 (For Individuals)

현재 전 세계에는 다양한 유형의 비트코인 사용자가 존재한다.

매일 수익을 추구하는 트레이더, 장기 보유를 원하는 투자자, 신용카드 수수료 회피나 프라이버시를 중시하는 기술 친화적 소비자,

철학적으로 새로운 금융 패러다임을 추구하는 사용자, 전 세계로 송금을 보다 효율적으로 수행하려는 사용자,

처음으로 금융 서비스 접근성을 얻는 개발도상국 사용자, 새로운 기술을 창조하려는 개발자 등 다양하다.

이러한 모든 개인에게 테더는 다음과 같은 방식으로 유용하게 사용될 수 있다.

- **중개자 없이, 가명성 하에 USD/법정화폐 가치를 전송**
- **개인 키를 직접 보관함으로써 USD/법정화폐 가치를 콜드 스토리지로 보존**
- **거래소 내 법정화폐 보유 리스크 회피 – crypto-fiat 형태로 쉽게 입출금 가능**
- **법정화폐를 보관하기 위해 별도의 은행 계좌를 개설할 필요 없음**
- **비트코인과 연동된 애플리케이션을 손쉽게 확장하여 테더 지원 추가 가능**

- 개인이 비트코인으로 할 수 있는 모든 것은 테더로도 가능

## 가맹점 대상 (For Merchants)

가맹점은 결제보다 비즈니스 운영 자체에 집중하길 원한다.

그러나 여전히 전 세계의 많은 소상공인 및 대형 사업체는 글로벌하고 저비용이며 보편적인 결제 솔루션의 부재로 어려움을 겪고 있다.

가맹점은 더 나은 대안을 필요로 한다. 테더는 다음과 같은 방식으로 이를 해결할 수 있다.

- 상품의 가격을 비트코인 대신 USD/법정화폐 기준으로 표시 (변동 환율 및 결제창 문제 해소)
- 비트코인을 USD/법정화폐로 변환하는 과정과 그에 따른 수수료 및 절차 제거
- 차지백(결제 취소) 방지, 수수료 절감, 프라이버시 강화
- 법정화폐-암호화폐 혼합 기능을 활용한 새로운 서비스 제공
  - 예: 마이크로 팁핑, 기프트 카드 등
- 가맹점이 비트코인으로 할 수 있는 모든 것은 테더로도 가능

## 향후 혁신 (Future Innovations)

- 다중서명(Multi-sig) 및 스마트 컨트랙트(Smart Contracts)
- 지급 능력 증명(Proof of Solvency) 혁신

## 결론 (Conclusion)

테더(Tether)는 오늘날 존재하는 최초의 비트코인 기반 법정화폐 연동형 암호화폐이다. 테더는 가장 안전하고 검증된 퍼블릭 블록체인인 비트코인 네트워크를 기반으로 한다. 모든 테더는 1:1 비율로 전액 준비금으로 보유되며, 시장 요인이나 유동성 제약에 영향을 받지 않는다. 테더는 단순하고 신뢰할 수 있는 Proof of Reserves 메커니즘을 구현하고 있으며, 정기적인 전문 감사를 받는다. 또한, 우리의 은행 네트워크, 규제 준수 체계, 법적 구조는 테더 발행자이자 준비금 수탁자로서의 안전한 기반을 제공한다. 우리 팀은 비트코인 생태계 내외의 숙련되고 평판 있는 기업가들로 구성되어 있다. 우리는 암호화폐 업계 내 기존 사업체(거래소, 지갑, 가맹점 등)와의 통합을 지속적으로 추진하고 있다. 현재 이미 Bitfinex, HolyTransaction, Omni Wallet, Poloniex, C-CEX 등과 통합되어 있으며, 앞으로 더 많은 파트너가 추가될 예정이다. 자세한 정보를 원한다면 언제든지 연락해 주길 바란다.

## 부록 (Appendix)

# 감사상의 결함: 거래소 및 지갑 (Audit Flaws: Exchanges and Wallets)

다음은 기술 기반<sup>14</sup> 거래소 및 지갑 감사에서 발견된 현재의 주요 결함들을 요약한 것이다.

**Merkle Tree[6] 접근법**에서는 사용자가 자신의 잔액(사용자의 리프, leaf)이 거래소의 부채 선언 (Merkle 해시로 표현된 사용자 잔액 데이터베이스)에 정확히 포함되었는지를 직접 검증해야 한다. 이 방식은 충분한 수의 사용자가 자신의 계정이 트리에 포함되었음을 검증하고, 포함되지 않은 경우 이를 보고할 때에만 올바르게 작동한다. 그러나 한 가지 잠재적 위험은 **거래소 데이터베이스 운영자가 실제 부채 총액을 반영하지 않는 해시값을 생성할 수 있다는 점**이다.

---

<sup>14</sup> 전문 감사인을 고용하지 않고 기술적 방법으로만 감사를 수행하는 경우를 의미함

이 경우 거래소는 **불완전한 데이터베이스를 해싱하여 부채 규모를 실제보다 축소시켜**, 외부 검증자에게 지급 능력이 있는 것처럼 보이게 만들 수 있다. 다음은 부정 행위를 저지르는 거래소가 특정 계정을 데이터베이스에서 제외하는 대표적 시나리오들이다.

- **“비트더스트(Bitdust)” 계정:**  
활동이 거의 없거나 비활성화된 계정들은 사용자가 자신의 잔액 불일치를 확인하거나 신고할 가능성이 낮다.  
그러나 이러한 장기 미사용 계정들이 전체 거래소 부채의 상당 비율을 차지할 수도 있다.
- **“공모 고래(Colluding Whales)” 공격:**  
대규모 비트코인 트레이더들이 여러 거래소에서 시장을 움직이는 사례가 존재한다.  
이러한 트레이더들은 주문을 신속히 실행하기 위해 대형 거래소에 상당한 자본금을 예치해야 한다.  
종종 이들은 자신이 신뢰하는 거래소를 선택하며, 해킹이나 유동성 위기가 발생하더라도 **자금 인출 우선권을 확보할 수 있다고 믿는다**.  
이런 상황에서 거래소와 트레이더가 **해시 계산 전 데이터베이스에서 고래 계정을 제외하기로 공모할 가능성**이 있다.
- **“키 임대(Key Rental)” 공격:**  
악의적인 거래소는 감사를 통과하기 위해 자신이 실제로 소유하지 않은 비트코인의 **개인 키를 임대**받을 수 있다.  
이렇게 하면 대차대조표상 자산이 늘어난 것처럼 보이지만, 이는 단순히 빌린 자금일 뿐이다.  
마찬가지로 거래소는 일시적으로 **법정화폐를 차입**하여 동일한 효과를 낼 수도 있다.
- 그 외에도 본 문서에서 다루지 않은 공격 벡터가 존재한다.

## 통계적 유의성 확보(보고의 완전성):

위의 세 가지 공격 벡터 외에도, 데이터베이스가 조작되었더라도 충분한 수의 사용자가 잔액 검증을 수행하지 않으면 부정이 감지되지 않을 수 있다.

모든 사용자의 100%가 자신의 잔액을 검증할 확률은 거의 0에 가깝다.

따라서 감사자는 **표본 추출 빈도, 표본 크기, 데이터 특성 등에 근거해 데이터베이스의 유효성을 통계적으로 판단해야 한다.**

현재로서는 거래소에 문제가 발생했을 때 사용자가 법적으로 보상을 받을 방법이 거의 없다.

예를 들어, **Mt.Gox가 운영을 중단했을 때**, 많은 사용자가 자신의 계정 잔액을 **캡처, 서명 메시지 등으로 독립적으로 기록하지 않았기 때문에**,

법 집행 기관에 해당 거래소의 부채(I.O.U)가 실제로 존재했음을 입증하기 어려웠다.

결국 이러한 사용자는 거래소가 자체적으로 해시 트리나 원본 데이터베이스를 공개하길 기다리는 수밖에 없었다.

현재 제안된 감사 구조 역시 **미묘하지만 중요한 결함**을 내포하고 있다.

특히 기관 웹사이트에 게시되는 **데이터 보고(해시 트리)**는 사용자에게 어떠한 보장도 제공하지 않는다.

악의적인 거래소는 **사용자 그룹별로 서로 다른 상태나 잔액을 게시하거나, 사후적으로 데이터를 수정할 수도 있기 때문이다.**

따라서 이러한 데이터는 반드시 **비트코인 블록체인과 같은 안전한 브로드캐스트 채널을 통해 공개되어야 한다.**

#### **프라이버시 문제:**

자동화되거나 공개적인 감사 시스템이 채택되지 못하는 주요 장벽 중 하나는 **개인정보 보호(privacy)**이다.

개인정보 보호를 개선하기 위한 연구가 진행 중이지만 아직 완벽한 해결책은 없다.

사용자 기반의 부채 검증 시스템을 정확히 구축하려면, 사용자가 거래소 내 계정 잔액과 비트코인 주소를 보고해야 한다.

그러나 일부 사용자는 어떠한 보상이 주어지더라도 이를 공개하지 않을 것이므로,

**암호학적으로 안전한 프라이버시 보호와 데이터 보고의 양립**이 핵심 과제가 된다.

#### **시간 시계열(Time Series):**

Merkle Tree 해시는 특정 시점의 데이터베이스 스냅샷에 불과하다.

이 데이터베이스의 시간 시계열이 유지되지 않으면 **심각한 공격 벡터**가 열릴 수 있다.

또한, 사용자 보고 데이터의 시간 시계열 역시 **사기 사건의 이력과 패턴을 복원하는 데 필수적**이다.

#### **신뢰받는 제3자(Trusted Third Parties):**

현재까지의 모든 거래소 감사는 일정 수준의 **“평판 있는 제3자”** 검증에 의존해 왔다.

예를 들어, **Coinbase 감사[7]**에서는 **Andreas Antonopoulos**, **Kraken 감사[8]**에서는 **Stefan Thomas**가 검증을 수행했다.

만약 우리가 반드시 신뢰 가능한 제3자에 의존해야 한다면,

감사 표준 및 절차를 명확히 하여 **이러한 약점을 제도적으로 보완해야 한다.**

# 기존 법정화폐 연동 시스템의 한계 (Limitations of Existing Fiat-pegging Systems)

다음은 기존 법정화폐 페깅(fiat-pegging) 시스템에서 공통적으로 나타나는 단점과 한계를 정리한 것이다.

- **폐쇄형 소프트웨어와 중앙화된 데이터베이스에 기반한 시스템**으로, 본질적으로 Paypal이나 기존의 소매기관용 자산 거래/이체/보관 시스템과 다를 바 없다.
- **비트코인만큼 충분히 검증·테스트되지 않은 알트코인 블록체인에 의존하는 탈중앙화 시스템**.
- **헤징 파생상품(meta-asset), 효율적 시장 가설, 담보화(collateralization)** 등에 의존하는 페깅 프로세스. 이러한 구조에서는 유동성, 전송성, 보안성 등 다양한 문제가 발생할 수 있다.
- **수탁기관의 투명성 및 감사 부족** — 이는 암호화폐든, 법정화폐든, 혹은 기관의 내부 원장 데이터든 마찬가지다 (폐쇄형 및 중앙화된 데이터베이스와 동일한 문제).
- **기존 은행 시스템 및 제3자(은행 계좌 보유자)에 대한 의존** — 준비 자산의 이체 및 결제 메커니즘이 여전히 전통 금융 구조에 묶여 있다.

---

## 시장 리스크 사례 (Market Risk Examples)

**담보화(collateralization) 방식**에서는, 담보로 사용되는 자산의 가격이 페깅 대상 자산의 가격과 **반대 방향으로 움직일 경우 시장 리스크**가 발생한다.

이 경우 담보의 총가치가 발행된 자산의 총가치보다 낮아지며, 시스템이 지급 불능 상태에 빠질 수 있다.

이 리스크는 **담보 가격이 페깅 자산의 가격과 같아질 때 포지션을 청산(시장 매도)** 함으로써 완화된다.

이 방식은 전통 금융시장에서도 유동성이 높은 여러 자산군에서 유효한 접근법으로 평가된다.

그러나 글로벌 금융위기에서 보았듯이, 급격한 시장 변동으로 인해 **유동성 경색(liquidity crunch)** 이 발생하면 담보를 제때 청산하지 못해 손실이 발생할 수 있다.

암호화폐 시장은 규모가 작고 변동성이 크기 때문에, 이러한 현상이 발생할 가능성이 더 높다.

또한, 담보화 방식은 **페깅 자산을 생성하기 위해 충분한 담보 공급이 필요하다는 구조적 제약**을 가지므로, 유동성과 가격 형성의 한계가 존재한다.

---

파생상품(derivatives) 방식에서는, 자산의 가격을 고정하기 위해 **스왑(swap)**, **옵션(covered/naked options)**, **선물(futures)**, **선도(forwards)** 등 다양한 파생 전략을 사용한다. 각 전략은 고유한 장단점을 가지며, 여기서는 세부 논의는 생략한다. 요약하면, 이러한 파생 기반 페킹 구조 역시 담보화 방식과 유사한 **시장 리스크**를 내포하고 있다.

이 두 방법은 상호 배타적이지 않으며, 종종 **기존 금융기관의 거래·헤징·리스크 관리 구조에서 결합되어 사용**된다.

---

우리는 위의 접근법 중 일부 조합이 장기적으로는 자산 페킹을 위한 **안정적이고 신뢰 가능한 리스크 최소화 프로세스**로 발전할 가능성이 있다고 본다.

그러나 현재 시점에서는 이러한 방식이 **유동성과 가격 안정성을 보장하기 위한 현실적 대안**으로 보기 어렵다. 그 대신, 우리는 **준비금(reserve) 기반 접근법**이 산업 성장 과정에서 지속적으로 존재하며, 위의 방법들과 상호 보완적인 역할을 할 것이라 믿는다.

기술이 발전함에 따라, 우리는 100% 상환 보증 원칙을 유지하면서도 유익한 기술적 혁신을 적극 도입할 것이다.

---

## 법률 및 규제 준수 (Legal and Compliance)

**Tether Limited** (“Tether”)는 **홍콩 회사조례(Hong Kong Companies Ordinance)**에 따라 설립된 유한회사이며, **영국령 버진아일랜드(BVI)** 법에 따라 설립된 **Tether Holdings Limited**가 100% 지분을 보유하고 있다.

Tether는 **미국 재무부 산하 금융범죄단속네트워크(FinCEN)**에 **자금서비스사업자(MSB)**로 등록되어 있다.

(MSB 등록번호: **31000058542968**)

Tether는 미국 내 사용자 지원 강화를 위해 **미국 금융기관과의 제휴 관계를 구축 중**이다.

또한 Tether는 **RenRenBee Limited**와 **주-대리점(principal–agency) 계약**을 체결 중이다.

RenRenBee는 **홍콩 세관 및 소비세청(Hong Kong Customs and Excise Department)**으로부터

**자금서비스사업자(Money Services Operator)** 라이선스를 취득한 기업이다 (라이선스 번호: **13-09-01265**).

이 계약에 따라, RenRenBee는 **Tether의 대리인(agent)**으로서 **자금세탁방지(AML)** 및 **고객실사(CDD)** 절차를 수행한다.

이러한 구조를 통해, Tether는 미국법 및 홍콩의 자금세탁방지·테러자금조달방지 관련 법률에 부합하는 고객실사, 기록 보관, 보고 체계를 운영하고 있다.

현재 Tether Limited는 대만의 Cathay Bank와 Hwatai Bank에 계좌를 보유하고 있으며, 양 은행 모두 Tether의 비즈니스 모델이 법적·규제적 요건에 부합함을 확인하였다.

해당 은행들은 우리 프로세스에 만족하고 있으며, 계좌 개설 전 각 은행의 법무, 준법감시, 본사 검토 절차를 거쳤다.

이는 우리의 요청에 따른 절차였으며, 설립 초기부터 규제 준수 및 은행과의 신뢰 구축을 핵심 목표로 삼았다. 또한, 이들 은행은 이미 다른 비트코인 기반 비즈니스와도 협력 관계를 유지하고 있다.

---

## 용어 해설 (Glossary of Terms)

**디지털 통화(Digital currency):**

[Wikipedia 정의 참조.](#)

**암호화폐(Cryptocurrency) 또는 탈중앙화 디지털 화폐(Decentralized digital currency):**

오픈소스, 암호학적 보안, 분산 원장을 사용하는 모든 형태의 암호화폐.

참조: <http://en.wikipedia.org/wiki/Cryptocurrency>

**실물 화폐(Real-world currency), 법정화폐(Fiat currency) 또는 국가/주권 통화(National/Sovereign currency):**

위 정의의 암호화폐가 아닌 모든 형태의 통화.

**암호화폐 시스템(Cryptocurrency system):**

암호화폐의 존재를 가능하게 하는 소프트웨어와 프로세스의 집합.

**기존 금융 시스템(Legacy financial system):**

암호화폐 시스템이 아닌 모든 금융 시스템.

**유틸리티 기반 디지털 토큰(Utility-backed digital tokens, Dapps):**

가치 전송 기능 외에 응용 프로그램의 유용성에서 가치가 파생되는 탈중앙화 토큰.

**자산 담보형/페깅 암호화폐(Asset-backed/pegged cryptocurrency):**

실물 자산에 가격이 고정된(연동된) 암호화폐. 즉, “유틸리티 기반” 암호화폐가 아닌 형태.

**테더(Tether, Tethers):**

Tether Limited가 발행한 법정화폐 연동형 암호화폐의 단위.

**TetherUSD 또는 tUSD:**

Tether Limited가 발행한 암호화폐 기반 USD 단위.

## **TUSD:**

특정 시점에 유통 중인 모든 tUSD의 총합.

## **테더 시스템(Tether System):**

테더의 발행 및 운영을 가능하게 하는 전체 프로세스 및 기술적 인프라.

## **준비금 증명(Proof of Reserves):**

자산 담보형 탈중앙화 토큰 발행자가 모든 발행 토큰이 실제 준비 자산으로 완전 담보됨을 암호학적·수학적으로 증명하는 절차.

# **참고문헌 (References)**

- [1] [2012 Global Wealth Report](#)
- [2] [Bitcoin Whitepaper](#)
- [3] [Deloitte: Bitcoin – The New Gold Rush](#)
- [4] [Mastercoin Specification](#)
- [5] [Bit Gold by Nick Szabo](#)
- [6] [Proving Bitcoin Reserves](#)
- [7] [Coinbase Audit Review – Andreas Antonopoulos](#)
- [8] [Kraken Audit – 100% Bitcoin Reserve Proof](#)