

주요정보 요약

Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.

코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Ethereum
홈페이지	https://www.wbtc.network/
참고문헌 (백서, Docs 등)	https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf

1. 프로젝트 정보

WBTC의 개요

이더리움 블록체인 기반의 ERC-20의 토큰은 이더리움 생태계 내 디지털 토큰이 중요한 자산 클래스로 떠오르고 있습니다. 해당 토큰들은 총 발행량, 소유자, 발행, 빠른 컨펌 시간, 거래 세부 정보 및 스마트 컨트랙트 실행에 대한 투명성을 제공하는 블록체인과 이더리움의 모든 장점을 활용합니다. 이더리움 블록체인상의 토큰들은 다양한 기능을 수행할 수 있습니다. 이러한 토큰의 가격은 이를 담보하는 자산의 가격을 반영하므로 "스테이블코인"으로도 불립니다. 자산 담보형 토큰은 주로 두 가지 방식으로 발행됩니다.

알고리즘 기반: 이더리움의 일부 토큰은 수요와 공급을 스마트 컨트랙트를 통해 조절하여 토큰 가격을 특정 법정화폐에 맞추는 메커니즘을 따릅니다. 대표적인 예로는 Dai, Basis, Carbon, NuBits 등이 있습니다.

중앙화 방식: 자산이 특정 조직에 보관되고, 이 조직은 준비금 증명을 공개합니다. Tether, True USD, USDC(USD), Digix(금), Globcoin(다양한 법정화폐 구성), AAA Reserve(국채) 등이 이에 해당합니다.

래핑된 토큰은 중앙화 모델을 따르지만, 한 기관에만 의존하지 않고 네트워크 내에서 다양한 역할을 수행하는 기관 컨소시엄에 의존합니다. 해당 문서는 확장성, 신뢰, 규제, 거버넌스 문제를 해결하며 자산 담보형 토큰을 발행하기 위한 프레임워크를 제안합니다. 첫 번째 래핑 토큰으로는 비트코인(BTC)을 담보로 하는 ERC-20 토큰을 발행하며, 이를 "Wrapped BTC(WBTC)"라 명명합니다. WBTC는 중앙화 솔루션(USD)과 달리 완전하게 계정 처리가 되며, BTC 체인에서 준비금 증명이 게시됩니다.

WBTC 사용 시 추가적인 유틸리티/결제 토큰이 필요하지 않으며, 블록체인 수수료 외의 전송 수수료는 없습니다. WBTC는 단순한 연합형 거버넌스 모델을 사용하며, 사용 편의성을 높이는 데 중점을 둡니다.

WBTC의 활용

자산의 토큰화는 다음과 같은 이점을 제공합니다.

거래 속도 증가

이더리움 블록은 약 15초마다 생성되며, 5분 이내에 거래의 취소 불가능성에 대해 상당한 신뢰를 가질 수 있습니다. 이 속도는 비트코인, 금, 법정화폐 등 많은 자산의 네이티브 거래와 비교하여 빠릅니다.

중개자 수 감소

블록체인 자산의 주요 이점 중 하나는 중개자 없이 거래가 가능하다는 점입니다. 이는 원자적 스왑, 탈중앙화 거래소 프로토콜, 라이트닝/레이든 스타일 채널을 통해 실현할 수

있습니다.

보안성 강화

토큰화는 사용자가 자산의 개인 키를 완전히 제어할 수 있게 해줍니다. 키를 보유하고 싶지 않은 사용자는 보안에 중점을 둔 커스터디를 통해 거래소로부터 상호 의존 리스크를 줄일 수 있습니다.

사용자 편의성

ERC-20 표준은 다수의 기관과 Dapp에서 채택되어, 사용자가 다양한 거래소, 지갑, Dapp에서 토큰화된 자산을 처리할 수 있도록 합니다. 사용자는 24시간 빠르게 토큰을 이동할 수 있습니다.

투명성 향상

총 토큰 수, 토큰 생성 및 제거 거래, 토큰 보유자 수, 전송 규칙 등을 누구나 블록체인 익스플로러에서 확인할 수 있습니다. 이 수준의 투명성은 법정화폐, 상품, 주식 등에서는 일반적으로 제공되지 않습니다.

탈중앙화 거래소 및 Dapp에서의 유동성

현재 중앙화 거래소에서 ERC20 거래는 대부분 BTC로 이루어지며 ETH가 아닙니다. 대부분의 탈중앙화 거래소는 ETH/토큰 거래만 제공하고 BTC/토큰 거래는 제공하지 않습니다. 래핑된 토큰은 이러한 격차를 해소하고 탈중앙화 거래소에서 더 많은 유동성을 제공합니다. 또한, 다른 탈중앙화 애플리케이션/프로토콜(펀드, 대출 결제 등) 역시 BTC 토큰을 통해 증가된 유동성의 혜택을 받을 수 있습니다. WBTC는 비트코인에 스마트 컨트랙트의 편리함을 가져옵니다.

법정화폐 기반 토큰의 혜택

법정화폐로 담보된 토큰은 거래자가 가격 변동에 대한 걱정 없이 암호화폐로 자금을 보유할 수 있는 안전한 방법을 제공합니다. 이는 법정화폐를 직접 전송할 수 없는 중앙화 및 탈중앙화 거래소 모두에 특히 유용합니다. 법정화폐 기반 토큰은 암호화폐가 전통 금융을 대체할 수 있는 세상을 약속합니다. 특히, 전자상거래에서 구매자와 판매자가 환율이나 세금(미국의 경우 구매 시점에서 계산되는 양도소득세)에 대한 걱정 없이 사용할 수 있습니다.

암호화폐 간 상호운용성

오늘날 증가하는 다양한 암호화폐는 각기 다른 통화 교환 측면에 초점을 맞추고 있습니다. 이러한 측면에는 거래 처리량, 프라이버시, 저렴한 거래 수수료, 스마트 컨트랙트 기능, 노드/채굴자 분산화 등이 포함됩니다. 래핑된 프레임워크는 비트코인 같은 다른 암호화폐를 이더리움에서 나타내고, 이를 통해 이더리움 블록체인의 모든 기능을 활용할 수 있게 합니다. 예를 들어, 초기 코인 공개(ICO)를 래핑된 비트코인 토큰으로 직접 자금을 조달하고 이를 입금 시 발행하는 것도 가능합니다. 미래에는 중앙화 거래소와 기타 암호화폐를 수용하는 기관들이 다양한 암호화폐 노드를 유지할 필요 없이 이더리움 상에서 개발할 수 있게 될 것입니다.

온체인 정책 집행 방법

토큰화는 온체인에서 정책을 집행할 수 있는 방법을 제공합니다. 온체인 정책 집행은 규칙을 더 투명하게 하고, 단일 기관에 의존하지 않고 이를 관리합니다. 자산의 유형에 따라 자산 전송이나 거래에 규칙이 필요할 수 있습니다. 예를 들어, 증권에는 화이트리스트, 보유 기간, 신원 관리가 요구될 수 있습니다.

WBTC의 주요 문제점

신뢰성

자산 담보형 토큰은 일반적으로 자산을 보유한 기관에 대한 신뢰를 요구합니다. 이는 운영에서 신뢰를 최소화하고자 하는 암호화폐의 기본 원칙과 상충될 수 있습니다. 여기서 해결해야 할 주요 질문들은 다음과 같습니다.

- 자산 보유자는 기존 법적 체계에서 자산을 보유할 권한이 있는가?
- 커스터디안이 임의로 토큰을 생성할 수 있는가?
- 커스터디안은 보유 중인 자산에 대한 소유 증명을 어떻게 제공하는가?

규제

자산 담보형 토큰의 커스터디안은 자산을 보유하기 위한 라이선스를 필요로 합니다. 이 라이선스는 자산의 유형과 커스터디안이 위치한 지역적 관할권에 따라 달라질 수 있습니다. 커스터디안은 1:1 담보가 부족할 경우 시스템 전체가 약화될 수 있으므로, 주기적으로 준비금을 증명해야 합니다. 또한, 자산 담보형 토큰과 관련된 사용자에게는 KYC(고객 신원 확인)과 AML(자금세탁 방지) 제한이 적용됩니다. 이러한 규제는 토큰의 구매, 상환 또는 전송 시 적용되어야 합니다.

거버넌스

시스템에 여러 이해관계자가 있을 경우, 토큰의 변경 사항을 어떻게 처리할지에 대한 거버넌스 문제가 발생합니다. 대부분의 자산 담보형 토큰은 토큰을 관리하는 규칙/스마트 컨트랙트의 변경을 자산 커스터디안에게 전적으로 의존합니다. 일반적으로 ICO의 경우, 토큰 발행자가 프로토콜 변경에 대한 완전한 통제권을 가집니다. DAICO(탈중앙화 자율 ICO)와 같이 사용자에게 투표권을 부여하는 사례도 있지만, 낮은 투표 참여율이라는 문제가 존재합니다.

2. 토큰 이코노미

토큰 발행 관련 주체

커스터디안: 자산을 보유하는 기관이나 주체로, WBTC의 경우 BitGo가 이 역할을 맡습니다. 커스터디안은 토큰 민팅(발행)을 위한 키를 보유합니다.

머천트: 래핑된 토큰이 발행되거나 소각되는 기관이나 주체입니다. 머천트는 래핑된 토큰의 유통에 핵심적인 역할을 하며, WBTC의 경우 초기 머천트로 Kyber와 Republic Protocol이 참여합니다. 각 머천트는 새로운 래핑 토큰의 민팅과 소각을 시작할 수 있는 키를 보유합니다.

사용자: 래핑된 토큰의 보유자로, 이더리움 생태계 내의 다른 ERC20 토큰처럼 래핑된 토큰을 전송하고 거래할 수 있습니다.

WBTC DAO 멤버: 스마트 컨트랙트 변경과 커스터디안 및 머천트 추가/제거는 멀티시그(Multi-Signature) 컨트랙트를 통해 관리됩니다. 이 멀티시그 컨트랙트의 키 보유자는 WBTC DAO의 구성 기관들로 이루어집니다.

커스터디안은 자산을 머천트와 교환하여 래핑된 토큰으로 전환합니다. 이는 민팅(토큰 생성)과 소각(토큰 공급 감소)의 두 가지 유형의 거래로 이루어지며, 이러한 거래는 모두 블록 익스플로러에서 공개적으로 조회 가능합니다. 초기 교환 이후 머천트는 사용자와의 거래를 위해 일정량의 래핑 토큰을 유지합니다. 이중 단계 민팅 프로세스는 민팅과 소각이 시간이 많이 소요되는 점을 보완하여, 사용자가 래핑된 토큰을 더 빠르게 받을 수 있도록 돕습니다.

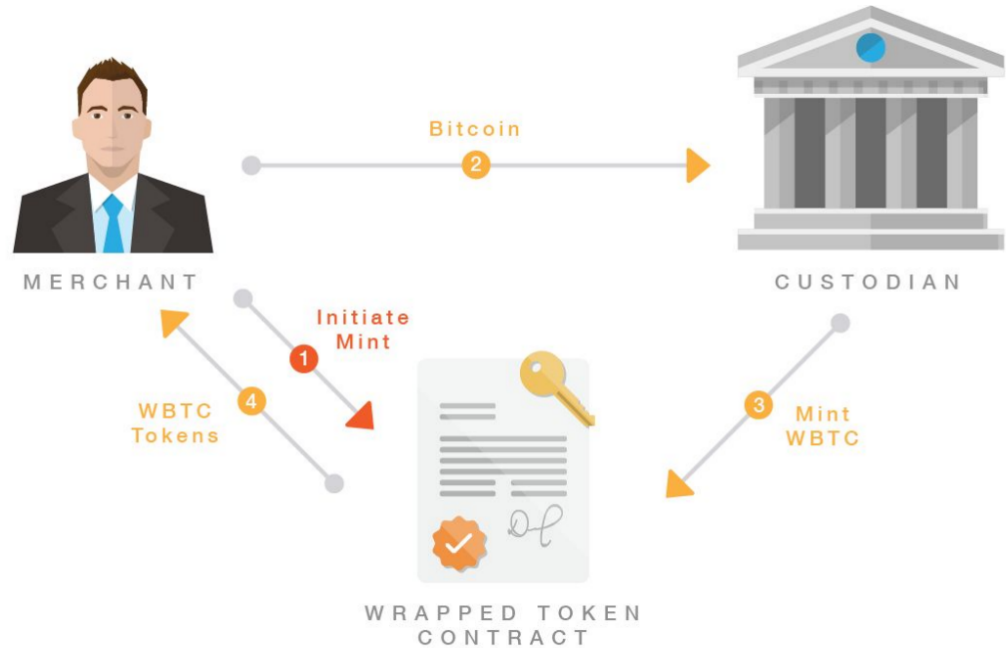
커스터디안 지갑 설정

커스터디안은 모든 머천트를 위한 풀 지갑을 보유해야 합니다. 이 지갑은 커스터디안이 제어하는 멀티시그 방식으로 운영되며, 온체인에서 화이트리스트에 등록된 머천트 주소로만 전송할 수 있습니다. 모든 민팅과 소각 거래는 커스터디안에게 제출된 후 48시간 내에 완료될 것으로 예상됩니다. 여러 커스터디안이 있을 경우, 하나의 지갑이 모든 대기

중인 래핑 토큰을 상환하기에 충분한 자금을 보유하지 못할 수도 있습니다.

민팅

민팅은 새로운 래핑 토큰을 생성하는 과정입니다. 래핑 프레임워크 내에서 민팅은 커스터디안이 수행해야 하지만, 머천트가 이를 "시작"해야 합니다. 민팅은 사용자와 직접적인 관련이 없으며, 머천트와 커스터디안 간의 일련의 거래로 이루어집니다.



출처 : 랩트 비트코인 백서

WBTC 민팅 이벤트 순서

머천트는 이더리움 체인에서 자신의 주소로 WBTC를 민팅하도록 커스터디안에게 권한을 부여하는 거래를 시작하고, BTC를 커스터디안에게 전송합니다. 커스터디안은 BTC 거래의 6회 확인을 기다린 후, 이더리움 체인에서 X개의 새로운 WBTC 토큰을 민팅하는 거래를 생성합니다.



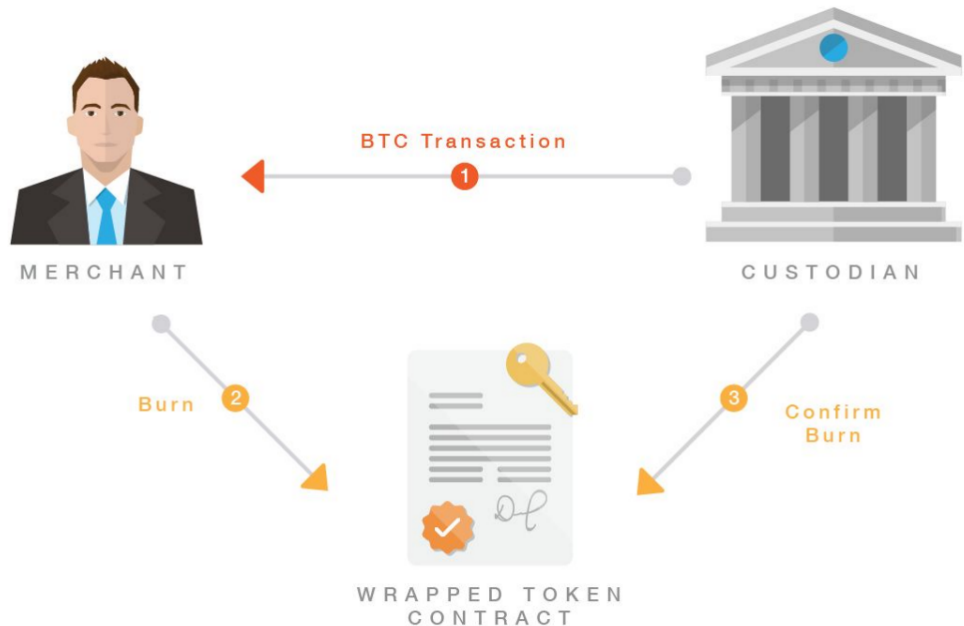
출처 : 랩트 비트코인 백서

사용자가 WBTC 토큰을 받는 이벤트 순서

사용자는 머천트에게 래핑된 토큰을 요청하고, 머천트는 필요한 AML, KYC 절차를 수행하여 사용자로부터 신원 정보를 확인합니다. 이후 사용자와 머천트는 원자적 스왑을 수행하거나 신뢰할 수 있는 거래소를 통해 거래를 완료하여, 머천트는 비트코인을 받고 사용자는 WBTC를 받게 됩니다.

소각 (Burning)

소각은 WBTC 토큰을 BTC로 상환하는 행위로, 오직 머천트 주소만 래핑된 토큰을 소각할 수 있습니다. 이를 위해 컨트랙트에서 'burn' 함수를 호출하여 이더리움 체인에서 소각할 토큰의 양을 입력합니다. 이로 인해 머천트의 WBTC 잔액이 차감되고 WBTC의 공급량이 감소합니다.



출처 : 랩트 비트코인 백서

WBTC 토큰 소각 이벤트 순서

머천트는 WBTC 토큰을 소각하는 소각 거래를 생성하고, 커스터디안은 ETH 거래의 25회 블록 확인을 기다린 후 머천트의 비트코인 주소로 X BTC를 전송합니다. 이후 커스터디안은 소각 요청이 완료되었음을 표시하는 이더리움 거래를 실행합니다.

사용자가 비트코인을 받는 이벤트 순서

사용자는 머천트에게 토큰 상환을 요청하고, 머천트는 필요한 AML, KYC 절차를 수행하여 사용자로부터 신원 정보를 확인합니다. 이후 사용자와 머천트는 원자적 스왑을 수행하거나 신뢰할 수 있는 거래소를 통해 거래를 완료하여, 사용자는 비트코인을 받고 머천트는 WBTC 토큰을 받게 됩니다.

온체인 전송 제한

토큰의 특성에 따라 전송 제한이 있을 수 있으나, WBTC의 경우 전송 제한이 없습니다.

거버넌스

래핑된 토큰 컨트랙트는 멀티시그(Multisig) 컨트랙트를 통해 관리되며, 멤버를 추가/제거하려면 DAO 멤버들의 서명이 필요합니다. 모든 커스터디안과 머천트는 DAO 멤버가 되지만, 다른 기관들도 커스터디안이나 머천트 역할 없이 멤버로 포함될 수 있습니다. 컨트랙트에서는 “M of N” 서명 방식을 사용하며, 여기서 M은 멀티시그 컨트랙트에서 필요한 서명의 수를, N은 전체 멤버 수를 나타냅니다. M과 N 값은 보안성과 멤버 추가/제거의 용이성을 고려하여 멤버 간 상호 합의에 따라 결정됩니다.

수수료

사용자 간 WBTC 전송에는 네트워크 수수료 외의 추가 비용이 없습니다. 네트워크 내 다양한 주체들이 수수료를 얻을 수 있는 방법은 다음 3가지입니다.

- **커스터디안 수수료:** 커스터디안은 머천트가 래핑된 토큰을 민팅하거나 소각할 때 수수료를 받습니다.
- **머천트 수수료:** 사용자가 자산과 교환하여 래핑된 토큰을 받을 때 해당 거래를 담당하는 머천트가 수수료를 받습니다.
- **사이드체인 거래 수수료:** 주로 사이드체인의 스팸을 방지하기 위한 목적으로 부과되며, 사이드체인에서 노드를 운영하는 모든 기관에 균등하게 분배됩니다.

커스터디안과 머천트 간의 계약

토큰의 민팅 및 소각 과정은 사용자와 무관하게 신뢰할 수 있는 기관들 간에 이루어집니다. 머천트는 사용자의 신원 정보를 안전하게 보관해야 하며, 커스터디안은 분기별로 보유 자산의 세부 사항을 공개하고, 민팅/소각 업무를 신속하게 수행해야 합니다. 이 기준을 충족하지 못할 경우 네트워크에서 제외될 수 있습니다.

네트워크 내 여러 커스터디안이 존재할 수 있지만, 이는 네트워크의 리스크를 증가시킬 수 있습니다. 향후에는 각 기관이 멀티시그 지갑의 키를 보유하여 커스터디 역할을 공유하는 모델도 가능하지만, 민팅/소각/감사 과정에 더 많은 협력과 시간이 필요하게 됩니다. 커스터디안 중 한 곳에서 보안 침해가 발생할 경우 신뢰가 손상되어 대규모 출금 사태로 이어질 수 있습니다. 반면, 머천트에서의 보안 문제는 모든 토큰이 여전히 커스터디안에 의해 담보되므로 영향이 덜 심각하지만, KYC/AML 사용자 데이터 유출로 이어질 수 있습니다.

가상자산 소개

WBTC(래핑된 비트코인)는 비트코인을 이더리움 네트워크에서 ERC-20 토큰으로 전환한 자산으로, 비트코인의 가치를 유지하면서 이더리움의 스마트 컨트랙트 기능을 활용할 수 있게 해줍니다. WBTC는 중앙화된 커스터디안이 실제 비트코인을 보유하고, 이를 토대로 발행되며, 분기별 감사와 투명한 온체인 기록을 통해 1:1 담보 비율을 보장합니다. 이를 통해 사용자들은 비트코인을 이더리움 생태계의 Dapp 및 DeFi 서비스에서 유동적으로 사용할 수 있습니다.

발행량 및 유통량계획

WBTC의 발행량 및 유통량 계획은 높은 투명성을 유지하기 위해 대시보드와 각 블록체인 스캐너에서 실시간으로 확인할 수 있습니다. 대시보드에서는 WBTC 네트워크의 주요 데이터와 함께 민팅 및 소각 상태, 커스터디안이 보유한 총 비트코인 수량, WBTC의 총 발행량, 사용 가능한 유통량을 한눈에 볼 수 있도록 구성되어 있습니다. 또한, 각 블록체인 스캐너를 통해 WBTC의 발행 및 유통 관련 거래 내역이 공개되며, 누구나 접근하여 블록체인에서 진행된 민팅과 소각 거래를 직접 검증할 수 있습니다.

ORDER BOOK

NETWORK		CUSTODY	
	34,234 WBTC		34,263 BTC (\$4,434,411 USD)
ACTION	DATE	MERCHANT	VALUE (WBTC)
	1/3/19 — 6:45:39	Kyber	312.95
	1/1/19 — 14:14:35	Kyber	92.00
	1/1/19 — 8:12:24	Republic Protocol	399.29
	12/31/18 — 23:01:47	Kyber	2,100.37
	12/30/18 — 12:15:51	Republic Protocol	50.50
	12/29/18 — 3:24:20	Republic Protocol	100.60
	12/29/18 — 1:59:01	Kyber	42.16
	12/27/18 — 17:04:54	Kyber	10.00
	12/25/18 — 14:45:31	Kyber	3.00
	12/21/18 — 2:01:45	Republic Protocol	14.20

⏪
⏩
Page 1 of 504
⏴
⏵

출처 : 랩트 비트코인 백서

3. 참고자료

WBTC의 현재 발행량

PROOF OF ASSETS



146,742.4539 WBTC

ERC20 Token Contract

CUSTODY



146,747.6965 BTC (\$10,613,770,751.23 USD)

On-chain Validation

The custodian performs audits on a regular basis to ensure transparency through publicly viewable and verifiable transactions. The Bitcoin addresses below are controlled by the custodian.

CUSTOMER Bitcoin ADDRESS	BALANCE AMOUNT
31uMgRj3bA+1Zzj1UyYfDT1Zvvc3gphg.	1,939.0430
31xk0u8H0ApkxXZTallz1Dr0DZV0aJwK	1,203.7981
31wR9NLr9WEL8oGQW8rEK5wd1gJ2uc8t	2,401.1433
31xdt6w0Xqg7Y1wvJ0PK9r+ycDj3dht1	1,206.0881
32Cw9GPw03w3wprnc7fPQC7gwC28Z8ev	1,204.5675
32Ver3t9feJgByNLF8ppgmNPFZ22C3Q	1,206.0881
32TKQYj3h1L4Uj3HfTYFLP8Pgy1W6dAC	2,303.7525
33PqQ026k0u0KvYb+zTFW3pRtLgJdrc	1,975.2522
33ghd5QC7BT7U8Rv48932x6A2L64LxrfJ	1,206.6918
34C7yq6wqW6d8Ed8D6aTjruZBavwtr	1,206.6376
34MPjw03L3u0wF7WbTUtWdLX2vYK1qg8t	1,204.5675
34QgWU758Wp4mZaf2anJ10KQJyVek7HqQ	1,206.0881
35T3+M6L83VAB7YvX0Mh0CB9qg.0C4v	1,206.6918
35LgpyY86tFKw0G0K7FpJ5BVChyL06f	1,206.6918
356kmttgjJSLndpVqgV8LcAP19cggpJ	1,654.3624

출처 : WBTC 대시보드

WBTC의 주요 파트너

PARTNERS

WBTC is a community-led project and its partners include merchants, custodians, exchanges, and DAO members.

PARTNER	ROLE	
BitGo	 DAO MEMBER  CUSTODIAN	▼
HIBTC	 EXCHANGE	▼
Switchoo	 EXCHANGE	▼
RadarRelay	 EXCHANGE	▼
Maker	 DAO MEMBER  MERCHANT	▼
Bamboo Relay	 EXCHANGE	▼
Loopring	 DAO MEMBER  MERCHANT	▼
GOPAX	 DAO MEMBER  MERCHANT  EXCHANGE	▼
Blockfolio	 DAO MEMBER	▼
Kyber	 DAO MEMBER  MERCHANT  EXCHANGE	GET WBTC ▼
Symbolic Capital Partners	 MERCHANT	▼
Uniswap	 EXCHANGE	GET WBTC ▼
DDEX	 DAO MEMBER  MERCHANT	▼
Nuo	 DAO MEMBER	▼

출처 : WBTC 대시보드

위험고지 안내 Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.