시트레아(CTR)

주요내용설명서(국문백서)

Korean White Paper

2026년 6월 9일

Disclaimer

본 번역본은 2026년 6월 9일 기준의 시트레아(Citrea) Docs 및 블로그 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.

빗썸

프로젝트 소개

시트레아(Citrea)는 롤업[1]입니다. 시트레아는 정기적으로 비트코인 네트워크에 배치 증명[2]을 제출합니다. 이 증명에는 각 배치에 대한 상태 차이도 포함되어 있어 배치의 시작부터 끝까지 발생한 모든 상태 변화를 비트코인 데이터를 읽는 사람이라면 누구나 확인할 수 있습니다. 시트레아 풀 노드[3]는 이러한 상태 차이를 읽어 비트코인에서 직접 상태를 재구성할 수 있습니다. 아주 작은 암호학적 약정[4]만 게시되어 해당 데이터만으로는 상태를 재구성하는 것이 불가능한 사이드체인[5]과는 구별되는 지점입니다.

시트레아는 비트코인을 데이터 가용성[6] 레이어로 활용하며, 비트코인은 이 시스템의 유일한 신뢰 기준 역할을 합니다. 비트코인 네트워크가 안전하게 유지되는 한 시트레아의 상태 데이터는 언제든 접근 및 재구성이 가능합니다.

타입 2 zkEVM[7]

시트레아는 EVM과 호환됩니다. 개발자는 표준 EVM 도구들을 사용하여 솔리디티[8]로 스마트 컨트랙트[9]를 작성하고 배포할 수 있습니다. 시트레아는 대량의 zkEVM 트랜잭션을 오프체인에서 처리합니다. 그리고 이렇게 처리된 트랜잭션들을 바탕으로 배치 단위의 간결한 스타크[10] 증명을 생성합니다(이 증명은 이후 스나크[11] 증명으로 한 번 더 래핑[12]됩니다). 최종 완성된 증명은

[1] Rollup
[2] Batch proof
[3] Full node
[4] Commitment
[5] Sidechain
[6] Data availability (DA)
[7] Zero-knowledge Ethereum virtual machine
[8] Solidity
[9] Smart contract
[10] STARK (Scalable Transparent ARgument of Knowledge)
[11] SNARK (Succinct Non-interactive ARgument of Knowledge)
[12] Wrapping

비트코인 네트워크에 직접 게시되며, 이를 통해 클라이언트는 인스크립션[13]과 유사한 데이터 포맷 내에서 해당 배치의 유효성을 쉽게 검증할 수 있습니다.

시트레아의 통화: 비트코인(BTC)

시트레아는 BTC를 자체 통화로 사용합니다. 혼란을 방지하고 온/오프램프[14] 사용자 경험을 개선하기 위해 시트레아 내의 네이티브 BTC는 '시트레아 비트코인(Citrea Bitcoin)', 줄여서 cBTC로 부릅니다.

비트코인 확장에 최적화된 시트레아

별도의 실행 레이어인 시트레아는 비트코인 및 이더리움과 비교하여 다른 특성을 갖습니다. 독립적인 실행 레이어로서 시트레아는 비트코인의 베이스 레이어보다 더 높은 처리량, 더 풍부한 스마트 컨트랙트 기능, 더 낮은 수수료를 제공합니다. 이와 동시에 완결성[15]은 여전히 비트코인 네트워크에 고정(앵커링)됩니다.

구분	시트레아	이더리움	비트코인
실행	zkEVM	EVM	비트코인 스크립트[16]
확정[17]	비트코인	이더리움	비트코인
데이터 가용성	비트코인(상태 차이 기록)	이더리움	비트코인
수수료 및 통화	BTC(cBTC)	ETH	BTC

[13] Inscription

[14] On/off-ramp

[15] Finality

[16] Script

[17] Settlement

시트레아의 신뢰 최소화 네이티브 양방향 페그[18]: 클레멘타인(Clementine)

클레멘타인은 비트VM[19]을 기반으로 작동하는 시트레아의 신뢰 최소화 양방향 페그 메커니즘입니다. 이 시스템은 재귀적(반복 압축)으로 증명된 시트레아의 배치 증명을 경량 클라이언트[20] 증명 형태로 사용합니다. 이를 통해 비트코인 네트워크에서도 비트VM을 활용해 낙관적(옵티미스틱) 방식의[21] 영지식 증명[22] 검증이 이루어지도록 지원합니다.

클레멘타인은 1-of-N(N명 중 1명)의 신뢰 가정을 바탕으로 하기에 신뢰가 최소화된 구조를 갖습니다. 즉, 브리지[23] 검증인 그룹 중 단 한 명의 주체만 정직하게 행동하더라도 그 누구도 브리지에 페깅된 BTC를 탈취할 수 없음을 의미합니다.

비즈니스 모델

클레멘타인: 신뢰 최소화 비트코인 브리지

기존의 비트코인 브리지들은 대개 신뢰 기반 멀티시그나 아예 별개의 체인 및 합의 구조에 의존합니다. 이는 사용자들에게 과반수가 정직할 것이라는 정직한 다수[24] 가정을 강요하게 만들며, 결과적으로 경제적 활동이 비트코인 본연의 네트워크에서 멀어지게 하는 문제를 낳습니다.

클레멘타인은 비트VM2를 기반으로 하는 신뢰 최소화 솔루션입니다. 비트VM2는 비트코인 네트워크에 어떠한 변경이나 소프트 포크[25]를 가하지 않고도 비트코인상에서 직접 영지식 증명을 낙관적으로 검증할 수 있게 해주는 혁신적인 방식입니다.

---

[18] Peg

[19] BitVM (Bitcoin virtual machine)

[20] Light client

[21] Optimistic

[22] ZK Proof

[23] Bridge

[24] Honest-majority

[25] Soft fork

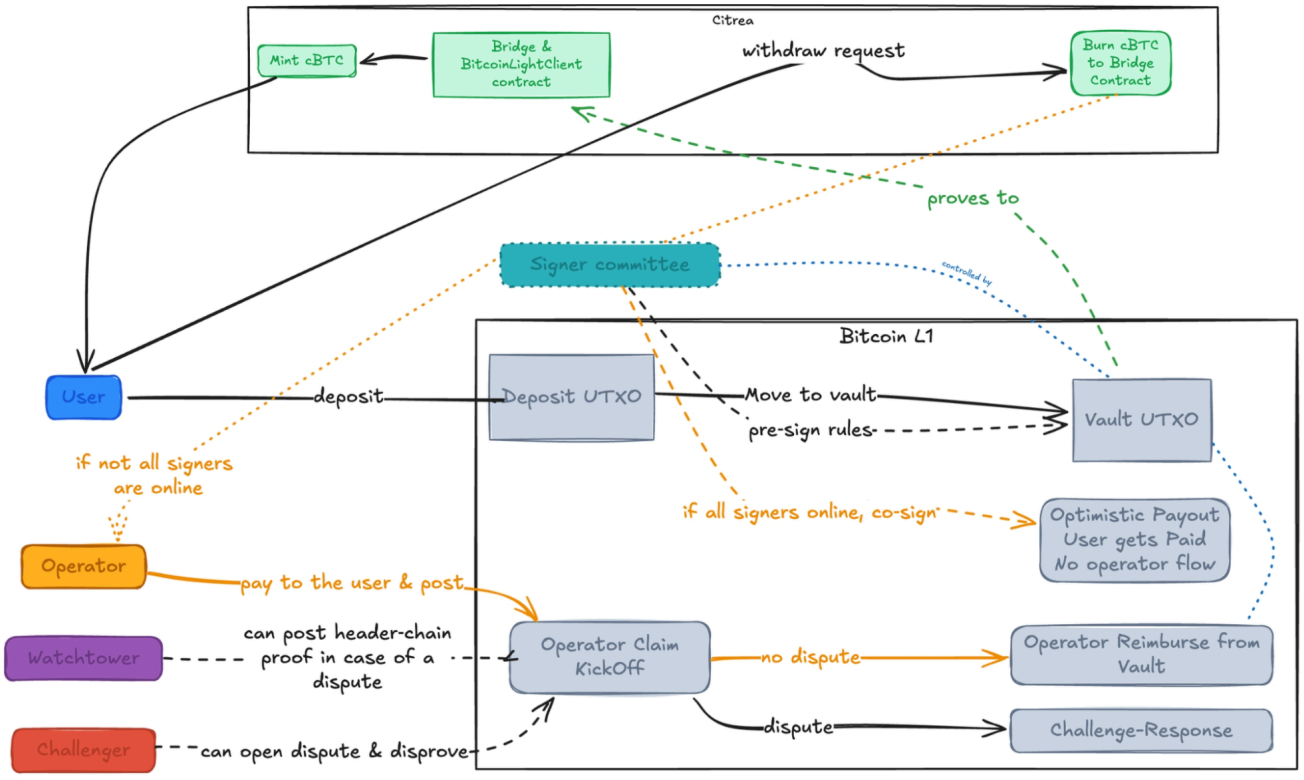
비트VM2를 사용하면 다음과 같은 작업이 가능합니다.

- 비트코인 네트워크상에서 영지식 증명이 올바른지 검증할 수 있습니다.
- 만약 제출된 증명이 올바르지 않다면, 이를 판별하고 비트코인 네트워크상에서 직접 제재(조치)를 취할 수 있습니다.

비트VM2의 지원을 통해 클레멘타인은 자산의 안전성을 비트코인상에서 유지하고 페그아웃(자산 출금)[26] 시 요구되는 신뢰 수준을 '1-of-N 정직성(N명 중 1명만 정직하면 됨)'으로 낮추어 궁극적인 신뢰 최소화를 달성합니다.

- 단 한 명의 정직한 서명자(Signer)만 있어도 자산이 사전에 승인된 지출 경로로만 이동하도록 보장할 수 있습니다.
- 단 한 명의 정직한 감시자(Watchtower)만 있어도 잘못된 비트코인 체인에 기록된 부당한 자금 인출 시도를 차단할 수 있습니다.
- 단 한 명의 합리적인 이의 제기자(Challenger)만 있어도 잘못된 연산 결과를 증명해 내고 악의적인 운영자(Operator)가 걸어둔 담보금을 회수할 수 있습니다.

1-of-N 정직성 가정이 유지되는 한 네트워크 멈춤 현상이나 악의적인 탈취 시도가 발생하더라도 시스템 내 자산은 안전합니다.



[클레멘타인 브리지 구조]

[26] Peg-out

클레멘타인 브리지가 원활하게 작동하려면 5가지 핵심 역할군이 필요합니다.

- 사용자: 페그인(BTC를 예치하여 시트레아의 자체 자산인 cBTC 발행)[27] 및 페그아웃(시스템 컨트랙트를 통해 cBTC를 소각하고 비트코인 네트워크로 BTC 출금) 절차를 시작하는 주체입니다.
- 서명자: 허용된 지출 규칙에 사전 서명하는 n명으로 구성된 위원회입니다. 이들은 비트코인의 커버넌트(조건부 지출 제한)[28]와 유사한 기능을 구현합니다. 즉, 자금은 클레멘타인이 승인한 경로로만 이동할 수 있으며 만약 서명자들이 정해진 시간 내에 사용자의 예치금을 볼트[29]로 옮기지 못하면 해당 자금은 사용자에게 반환됩니다.
- 운영자: 사용자에게 BTC를 선지급하여 비트코인 네트워크로의 빠른 출금을 돕고, 이후 누구도 사기나 악의적 의도를 증명하지 못하면 브리지 볼트에서 환급을 청구하는 주체입니다. 만약 운영자의 악의적인 행동이 적발될 경우 클레멘타인은 이의 제기 절차를 시작합니다. 경제적 안전성을 보장하기 위해 운영자는 프로토콜에 언제든 삭감[30]될 수 있는 보증금(약 2 BTC)을 예치해야 합니다.
- 감시자: 시트레아와 비트코인 네트워크 양쪽을 모두 모니터링하는 주체입니다. 운영자의 악의적인 의도가 감지되어 이의 제기 트랜잭션이 발생하면 감시자는 누적 작업 증명[31]이 포함된 압축된 비트코인 헤더 체인 증명[32]을 제출할 책임이 있습니다.
- 이의 제기자: 이의 제기 트랜잭션을 발생시키고 감시자가 제출한 헤더 체인 증명을 활용하여 운영자에게 자신의 행동이 정당했음을 증명하도록 강제하는 주체입니다.

자금 이동 방식

- 페그인 (BTC → cBTC)
    - 1단계(사용자 예치): 사용자는 두 가지 지출 경로가 인코딩된 탭루트[33] 주소로 10 BTC를 전송합니다.
        - 브리지 경로: 모든 서명자의 서명이 있고 위트니스 스크립트[34]에 사용자의 EVM 주소를 인스크립션한 경우에만 지출할 수 있습니다.

[27] Peg-in

[28] Covenant

[29] Vault

[30] Slashing

[31] Proof of work (PoW)

[32] Header-chain proof

[33] Taproot

[34] Witness script

        - 환불 경로: 브리지가 200 비트코인 블록이 생성되는 동안 아래 설명된 2단계 절차를 수행하지 않으면 타임락(OP_CSV) 이후 사용자가 자금을 다시 가져갈 수 있습니다. 이 타임아웃 기능은 2단계가 진행되지 않을 경우 자금이 네트워크에 묶이는 것을 방지합니다.
    - 2단계(볼트로 BTC 이동): 서명자들은 예치금을 브리지가 허용한 출구로만 지출할 수 있는 볼트 UTXO(미사용 트랜잭션 출력값)[35]로 이동시키는 트랜잭션에 서명합니다.
        - 이 볼트 이동(MovetoVault) 트랜잭션은 사전 서명된 트랜잭션과 뮤시그[36] 방식의 다중 서명 결합을 통해 커버넌트와 유사한 기능을 구현합니다. 단 한 명의 서명자만 정직하게 행동하더라도 자금은 반드시 사전에 서명된 경로만 따라 이동해야 합니다.
    - 3단계 (시트레아에서 발행): 볼트 이동 트랜잭션이 비트코인 네트워크에서 성공적으로 최종 확정(6컨펌 이상)되면 시트레아의 브리지 시스템 스마트 컨트랙트가 비트코인 경량 클라이언트 스마트 컨트랙트를 사용하여 해당 트랜잭션의 유효성을 검증합니다. 검증이 완료되면 컨트랙트는 사용자의 시트레아 주소(예치 단계에서 연동된 주소)로 10 cBTC를 발행합니다.
- 페그아웃 (cBTC → BTC)

  시트레아에서 비트코인 네트워크로 브리징하는 과정(시트레아의 cBTC를 비트코인의 BTC로 변환하는 작업)은 몇 가지 단계를 거쳐 처리됩니다.

  먼저, 사용자는 safeWithdraw 함수를 호출하여 브리지 시스템 스마트 컨트랙트를 통해 시트레아 상의 cBTC를 소각해야 합니다. 그런 다음, 사용자는 자신의 BTC 주소와 출금 수량이 포함된 지급 트랜잭션 템플릿을 사용하여 브리지의 운영자들에게 출금을 요청합니다. 이 특수한 템플릿은 사전에 서명된 트랜잭션으로, 실행을 위해서는 운영자가 제공하는 추가적인 UTXO 입력값이 필요합니다.

  사용자가 cBTC를 소각한 후에는 크게 두 가지 시나리오가 전개됩니다.
    - 페그아웃 시나리오 1: 이상적인 상황

      운영자들에게 어떠한 악의적인 의도도 없다면 자금 지급은 다음 두 가지 방식 중 하나로 완료됩니다.
        - n명의 서명자를 통한 낙관적 지급(Optimistic Payout): 모든 서명자가 온라인 상태라면 굳이 운영자가 나서지 않아도 서명자들이 직접 서명하여 사용자의 주소로 BTC를 전송할 수 있습니다. 이는 참여자 전원의 서명이 필요한(n-of-n) 일반적인 다중 서명 전송과 똑같이 작동하며 시스템에서는 이를 낙관적 지급이라고 부릅니다.
        - 운영자 지급(Operator Payout): 서명자 중 단 한 명이라도 12시간 이상 오프라인 상태일 경우 앞서 설명한 낙관적 지급은 완료될 수 없습니다. 그러나 이러한 상황에서도 사용자에 대한 자금 지급은

[35] Unspent transaction output

[36] Musig

보장되어야 하므로 운영자 그룹 중 한 명이 개입하여 사용자로부터 지급 템플릿을 확보합니다. 그런 다음 운영자는 해당 템플릿에 자신의 입력값을 추가하고 지급 트랜잭션을 네트워크에 전파합니다. 이 템플릿은 비트코인의 특수 서명 방식[37]을 사용합니다. 이를 통해 사용자의 출력값(수령 자금)은 안전하게 고정되며 동시에 어떠한 운영자든 해당 트랜잭션에 자금을 조달할 수 있습니다.

사용자 입장에서는 앞서 언급된 두 트랜잭션(낙관적 지급 또는 운영자 지급) 중 하나라도 최종 확정되면 출금이 완료된 것입니다.

만약 운영자 지급을 통해 자금 지급이 완료되었다면, 운영자는 비트코인 네트워크에 있는 브리지 볼트에서 자금을 환급받아야 합니다. 이 과정은 다음과 같이 진행됩니다.

- 운영자는 비트코인 네트워크에 청구 트랜잭션(KickOff)을 전파하여 환급을 요청합니다.
- 이로 인해 이의 제기 기간이 시작됩니다. 정해진 기간(예: 정상적인 상황의 경우 1.5일) 동안 아무도 이의를 제기하지 않으면 운영자는 타임락이 만료되어야만 잠금이 해제되는 NoChallenge라는 또 다른 트랜잭션을 전파할 수 있습니다. 운영자는 이 NoChallenge 트랜잭션을 사용하여 자금을 최종 환급받습니다.

- 페그아웃 시나리오 2: 분쟁 및 이의 제기 상황

만약 운영자가 존재하지 않는 출금 건에 대해 환급을 청구하는 등 악의적인 시도를 할 경우 프로토콜은 감시자와 이의 제기자가 주도하는 분쟁 해결 단계에 진입하며 다음과 같은 절차를 거칩니다.

1. 이의 제기 시작: 이의 제기자는 운영자의 악의적인 KickOff 트랜잭션을 감지하고 비트코인 네트워크에 이의 제기 트랜잭션을 전파하여 분쟁의 시작을 알립니다.
2. 감시자 트랜잭션 전파: 감시자는 운영자가 기존을 초과하는 작업 증명을 가진 비공개 비트코인 포크를 악의적으로 구성하지 못하도록 충분한 대기 시간을 거칩니다. 이후, 누적 작업 증명이 포함된 현재의 최종 확정된 정식 비트코인 헤더 체인 증명을 네트워크에 제출합니다.
3. 이의 제기 및 응답 절차: 이제 운영자는 자신의 환급 청구가 정당함을 방어해야 합니다. 이를 위해 운영자는 자신이 속한 체인이 감시자가 제출한 증명보다 더 많은 작업 증명을 가지고 있으며 시트레아에서 출금한 사용자에게 실제로 자금을 지급한 트랜잭션이 포함되어 있음을 입증하는 비트코인 zk스나크 경량 클라이언트 증명을 제출해야 합니다.
    a. 운영자가 정직할 경우: 일정 시간을 기다린 후 올바른 경량 클라이언트 증명을 제출함으로써 이의 제기자를 상대로 승리하고 자금을 환급받을 수 있습니다. 운영자의 증명에 요구되는 유일한 조건은 감시자의 증명보다 더 많은 누적 작업 증명을 포함하는 것입니다.

[37] SIGHASH_SINGLE|ANYONECANPAY

b. 운영자가 악의적일 경우: 해시레이트[38]의 물리적 한계로 인해 더 많은 작업 증명이 포함된 유효한 경량 클라이언트 증명을 결코 만들어낼 수 없습니다. 따라서 유효하지 않은 증명을 제출하거나 정당한 지급 내역을 증명하지 못하여 결국 분쟁에서 패배하게 됩니다.
    - 이 분쟁 해결 단계에서는 비트VM이 핵심적으로 활용됩니다. 복잡한 연산 자체는 오프체인에서 실행되지만 실행 과정의 그 어떠한 단계라도 온체인(비트코인 네트워크)상에서 이의를 제기하고 완벽하게 검증할 수 있습니다.

실행 환경

시트레아 VM(Citrea VM)은 비트코인 네트워크 위에서 구동되며 cBTC를 네이티브 토큰[39]으로 사용하는 EVM 동등성[40]을 갖춘 VM입니다. 개념적으로 EVM은 가상자산 생태계에서 가장 오랜 기간 검증을 거친 성숙한 VM입니다. EVM은 결정론적인[41] 스택 기반 VM으로, 안전하게 격리된 환경에서 스마트 컨트랙트를 효율적으로 실행하는 데 탁월한 성능을 발휘합니다.

시트레아는 이러한 EVM의 강력한 기능을 그대로 물려받으면서도 이를 한 단계 발전시켜 자체적인 zkEVM 형태로 구현해 냈습니다. zkEVM은 VM의 전체 실행 과정을 수학적으로 증명할 수 있도록 만든 특수한 형태의 EVM입니다. 시트레아의 zkEVM은 타입 2로 분류됩니다. 이는 완전한 EVM 동등성을 제공함과 동시에 zk스타크를 기반으로 확장 가능하고 신뢰 최소화된 증명 시스템을 갖추고 있음을 의미합니다. 시트레아 zkEVM은 리스크제로[42]를 사용하여 구축되었습니다.

시트레아만의 차별화된 특징

타입 2 zkEVM인 시트레아는 이더리움이나 다른 EVM 기반 블록체인들과 비교했을 때 다음과 같은 차별화된 특징을 가집니다.

[38] Hash rate

[39] Native token

[40] EVM-equivalent

[41] Deterministic

[42] RISCZero

- 자체 통화는 BTC: 시트레아 네트워크 내의 가스비[43] 결제 및 송금에는 신뢰 최소화 방식으로 비트코인과 1:1 연동된 자산인 cBTC가 사용됩니다. 이는 단순한 ERC-20[44] 토큰이 아니며, (비트코인의 8자리가 아닌) 18자리 소수점을 지원하는 네이티브 자산입니다.
- 블록 생성 시간 및 가스 한도: 시트레아의 블록 생성 시간은 2초이며 블록당 가스 한도는 1,000만입니다.
- 레이어1 수수료: 시트레아는 상태 변화 값을 비트코인 네트워크에 기록하기 때문에 근본적인 데이터 가용성 비용이 발생하며, 이는 사용자에게 레이어1 수수료로 청구됩니다. 레이어1 수수료는 트랜잭션이 종료될 때 해당 주소의 잔고에서 차감되며, l1FeeRate*diffSize 공식으로 계산됩니다. 레이어1 수수료를 지불할 잔고가 부족하면 트랜잭션은 실패합니다.
    - 레이어1 수수료율: 상태 변화 값의 바이트[45]당 웨이[46] 비용으로 현재 비트코인 네트워크의 수수료 시장 상황을 반영하여 산출됩니다.
    - 상태 변화 크기: 압축된 상태 변화 값의 크기(바이트 단위)입니다.
- EVM 버전 및 조정 사항: 시트레아는 이더리움의 펙트라[47] 버전 EVM을 지원하되 다음과 같은 조정 사항을 적용했습니다.
    - 시트레아에서는 EIP-4844[48]와 KZG 프리컴파일[49]을 지원하지 않습니다. 0x0A 주소를 호출할 경우 일반적인 외부 소유 계정[50]처럼 동작합니다.
    - EIP-2935: 시트레아에서는 지원하지 않습니다.
- 추가 프리컴파일: 펙트라 버전에 더해 시트레아는 secp256r1(스마트 기기 및 패스키에 널리 쓰이는 표준 암호 방식) 및 슈노르[51] 서명 검증을 위한 두 가지 추가 프리컴파일을 제공합니다.
- 머클 트리[52]: 시트레아는 상태 관리를 위해 기존의 패트리샤[53] 머클 트리 대신 젤리피시[54] 머클 트리를 사용합니다.

---

[43] Gas fee

[44] Ethereum Request for Comments-20

[45] Byte

[46] Wei

[47] Pectra

[48] Ethereum Improvement Proposal-4844

[49] Precompiles

[50] Externally owned account (EOA)

[51] Schnorr

[52] Merkle tree

[53] Patricia

[54] Jellyfish

- 시스템 스마트 컨트랙트: 시트레아에는 시스템 수준의 작업에 최적화된 특수한 시스템 스마트 컨트랙트들(BitcoinLightClient, Bridge, FeeVault)이 존재합니다.

시트레아 USD: ctUSD

ctUSD는 단기 미국 국채와 현금을 기반으로 1:1 가치가 연동되는 미국 달러 기반 스테이블코인[55]입니다. 범용 스테이블코인 플랫폼인 M0의 기술을 기반으로 하며, 미국 최고 수준의 엄격한 컴플라이언스[56] 체계를 갖춘 글로벌 가상자산 결제 선도 기업 문페이[57]가 발행합니다. 파트너십을 통해 ctUSD는 곧 시행될 미국 지니어스 법안[58]의 가이드라인을 준수하도록 설계되었으며, 미국(뉴욕주 제외)을 비롯해 전 세계 160개국 이상(캐나다 및 유럽경제지역(EEA) 제외)의 사용자가 이용할 수 있습니다.

ctUSD: 문페이 인프라를 활용한 비트코인 통합 유동성

ctUSD는 비트코인 생태계의 네이티브 스테이블코인을 목표로 합니다. 비트코인 애플리케이션에 필수적인 기반 유동성을 공급할 뿐만 아니라 온체인 비트코인 담보와 오프체인 법정화폐 시스템을 가장 간편하게 연결하도록 설계되었습니다.

ctUSD는 비트코인과 그 생태계 발전의 가장 고질적인 과제였던 '규제를 준수하는 네이티브 통합 스테이블코인 유동성에 대한 글로벌 접근성' 문제를 해결합니다.

ctUSD는 다음의 강점을 바탕으로, 비트코인 사용자와 애플리케이션 생태계에 자본 효율성이 뛰어난 온체인 시장을 조성합니다.

- 풍부한 네이티브 유동성: 시트레아 네트워크에서 ctUSD를 직접 발행함으로써 외부 브리지 해킹 위험을 원천 차단하고 체계적으로 관리되는 준비금을 통해 언제든 1:1 상환이 가능하도록 보장합니다. 이러한 설계적 강점은 ctUSD가 시트레아 생태계의 기축 스테이블코인으로 자리매김하는 핵심 기반이 됩니다. 또한 DEX 및 머니 마켓[59]에서 가장 널리 쓰이는 기준 자산[60]으로 기능하도록 설계되었습니다.

---

[55] Stablecoin

[56] Compliance

[57] MoonPay

[58] GENIUS Act

[59] Money market

[60] Quote asset

- 출시와 동시에 확보되는 광범위한 유통망: ctUSD는 3,000만 명 이상의 인증된 사용자를 보유한 문페이 네트워크와 결합합니다. 기존 문페이 사용자는 별도의 KYC(고객 확인)[61] 절차 없이 즉시 서비스를 이용할 수 있으며, 비자·마스터카드·애플페이·구글페이·페이팔 등을 통해 실시간 매수·매도가 가능합니다(지역별 지원 여부 상이).

ctUSD 컴플라이언스 프레임워크 및 준비금

문페이가 발행하는 ctUSD는 도입 예정인 지니어스 법안의 실행 지침을 준수하며, 단기 미국 국채와 현금을 통해 전액 담보됩니다. 문페이는 미국 송금업 면허[62]와 엄격한 컴플라이언스 기준을 바탕으로 규제 준수를 최우선 가치로 삼는 스테이블코인 프레임워크를 제공합니다.

높은 수준의 소비자 보호를 실현하기 위해 모든 준비금 자산은 토큰 보유자의 권익 보호를 목적으로 별도 수탁 관리됩니다. 해당 준비금은 문페이의 고유 자산으로 간주되지 않으며 오직 사용자의 상환 요청을 충당하는 목적으로만 전용됩니다. ctUSD의 담보 자산은 문페이의 유동적이고 투명한 준비금 관리 아키텍처를 통해 운용됩니다.

토크노믹스

시트레아(CTR) 자체에는 투표 권한이 없습니다. 사용자는 CTR을 스테이킹[63]하여 xCTR을 받게 되며, xCTR은 양도 불가능한 토큰으로 시트레아 거버넌스 트레저리[64]와 시트레아 네트워크에 대한 거버넌스 권한을 부여합니다.

- 스테이킹: CTR을 스테이킹하면 xCTR을 받을 수 있으며, 언스테이킹[65]에는 90일의 대기 기간이 존재
- 거버넌스: xCTR 보유자는 트레저리 자금 배분, 위원회 선출, 네트워크 운영 등에 대해 투표 가능
- 이중 트레저리 구조: 거버넌스 트레저리(xCTR 보유자가 관리) 및 재단 트레저리(연구 개발, 보조금, 운영)
- 고정 발행량: CTR 총발행량은 100억 개이며 인플레이션[66] 없음

[61] Know your customer
[62] Money Transmitter License
[63] Staking
[64] Treasury
[65] Unstaking
[66] Inflation

총발행량

CTR의 총발행량은 100억 개로 고정되어 있습니다.

항목	수치
총발행량	10,000,000,000 CTR
출시 시점의 락업[67] 해제된 발행량	34.83%
출시 시점의 유통량	12%

락업 해제된 발행량(unlocked supply)과 실제 유통량(circulating supply)의 차이는 락업 해제 이후 실제 시장 내 유입 여부입니다.
인센티브 및 트레저리 물량(25.16%)은 스마트 컨트랙트에 락업되어 있으며, xCTR 보유자의 거버넌스를 통해서만 해제될 수 있습니다. 생태계 성장 및 연구 개발(22.83%) 물량은 재단이 보유하고 있으며, 런칭 초기 거버넌스 탈중앙화를 지원하기 위한 스테이킹 및 위임에 주로 활용됩니다. 해당 물량 역시 실제 시장에서 유통되는 물량은 아닙니다. 따라서 출시 시점 기준 실제 유통량으로 집계되는 것은 초기 청구 물량(12%)뿐입니다.

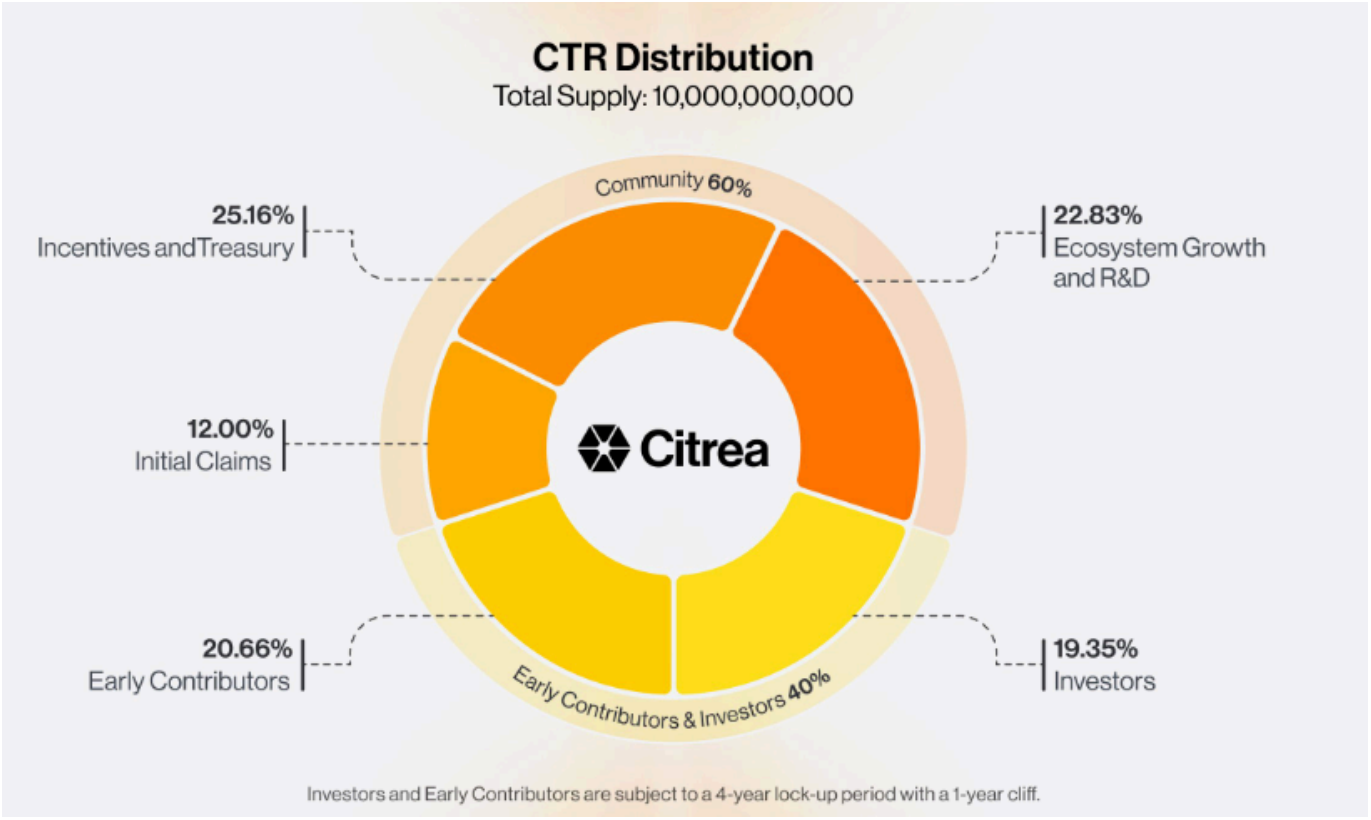
분배

카테고리	할당	락업 계획
초기 청구	12%	제네시스 에어드랍 및 기타 토큰 생성 이벤트[68] 관련 활동을 통해 배포되며, 이전 커뮤니티 세일 활동도 포함
인센티브 및 트레저리	25.16%	xCTR 보유자 거버넌스를 통해 관리되며, 게이지 시스템(gauge system), 생태계 인센티브, 위원회 또는 서비스 제공자 보상 등에 사용

[67] Lockup

[68] Token generation event (TGE)

생태계 성장 및 연구 개발	22.83%	출시 시점에 전체 언락[69]되며, 연구 개발, 개발자 지원, 생태계 확장 및 운영을 위한 전략적·장기적 배치에 활용
투자자	19.35%	1년 클리프[70] 이후 4년에 걸쳐 점진적으로 언락
초기 기여자	20.66%	1년 클리프 이후 4년에 걸쳐 점진적으로 언락



[CTR 토큰 분배 (총: 10,000,000,000개)]

[69] Unlock

[70] Cliff

로드맵

향후 계획: 게이지 시스템

게이지 시스템은 모든 것을 연결하는 엔진입니다.

거버넌스 논의를 거치고 시스템이 활성화되면, xCTR 보유자는 에포크[71]마다 투표를 통해 거버넌스 트레저리의 유동성을 특정 풀 및 애플리케이션으로 분배할 수 있게 됩니다. 이는 단순한 보상 분배가 아니라 경쟁 기반의 자본 조정 메커니즘입니다.

- 보상 강화: 자신이 투표한 풀에 유동성을 공급하는 활발한 투표자는 더 큰 보상을 받을 수 있습니다. 이를 통해 디파이 거버넌스 측면에서 강력한 참여 동기를 부여합니다.
- xCTR 득표를 위한 애플리케이션 간 경쟁: 각 애플리케이션에서는 인센티브, 파트너십, 자체 CTR 트레저리를 활용해 유동성을 유치합니다.
- 투표로 인한 xCTR 수요 촉진: 보상 분배에 관여하는 유일한 방법은 xCTR을 활용하는 것이기 때문에 투표 주기마다 CTR 스테이킹 수요가 증가하게 됩니다.

게이지 시스템은 CTR을 핵심 거버넌스 토큰에서 전체 네트워크의 엔진으로 바꿔 놓습니다. 프로토콜, 유동성 공급자, 투표자는 모두 에포크가 진행될 때마다 자본 분배 효율이 더욱 높아지는 선순환 구조에 참여하게 되며 매개변수 및 활성화 일정은 거버넌스를 통해 결정됩니다.

시트레아 제품 로드맵

시트레아는 대규모의 BTC 자본 시장을 실현하기 위한 탄탄한 제품 로드맵을 갖고 있습니다. 제품의 주요 초점은 수익 창출 및 볼트 선택지를 확대하고 시트레아의 성장하는 비트코인 생태계에 더 많은 사용자가 참여할 수 있도록 접근성을 향상하는 것입니다. 생태계 제품 외에도 탈중앙화를 위한 인프라 개선 등이 로드맵에 포함되어 있습니다.

[71] Epoch

BTC 구조화 상품[72]

시트레아는 다양한 볼트 및 BTC 수익 창출 기회를 형성하는 데 집중합니다. 그 일환으로 눈[73], 키록[74], 모포와 같은 최고의 자산 운용가 및 프로토콜과 협업하여 기관을 위한 수익 창출 서비스를 제공하고 있으며, 서비스 중인 3개의 볼트(키록 cBTC 볼트, 눈 cBTC 볼트, 모포 ctUSD 볼트)에는 이미 상당한 규모의 cBTC와 ctUSD가 예치되어 있습니다.

향후 시트레아는 ctUSD와 cBTC를 중심으로 볼트 아키텍처를 공격적으로 확장하여 수익 기회를 확장해 나갈 계획입니다. 주요 기관 파트너 및 디파이 전문가와의 협업을 통해 시트레아의 제품들에 풍부하고 통합된 유동성이 갖춰져 성숙하고 안전하며 확장성이 뛰어난 BTC 중심 금융 시장을 실현하는데 일조할 것으로 기대됩니다.

주력 제품: 시트레아 게이트웨이(Citrea Gateway) – 생태계 발견 플랫폼

시트레아는 비트코인 경제를 확장하면서도 사용자가 수익 기회를 찾는 과정에서 파편화된 프로토콜들 사이를 이리저리 헤매게 하지는 않을 생각입니다. 시트레아 게이트웨이는 전체 생태계를 투명하고 편리하게 탐색할 수 있도록 도와주는 통합 생태계 발견 플랫폼으로서 설계되고 있습니다. 시트레아 게이트웨이를 활용하면 별개의 애플리케이션들을 일일이 방문해야 하는 것이 아니라 단일 통합 인터페이스를 통해 최적의 수익 기회를 발견하고, 기본적인 프로토콜 위험 프로파일[75]을 평가하며, 여러 BTC 자본 시장에 즉각적으로 자본을 배치할 수 있습니다.

복잡한 참여 과정을 없애는 것이 목적인 시트레아 게이트웨이는 차세대 비트코인 경제에 참여하기 위한 이상적인 시작점이 되어줄 것입니다.

주력 제품(미발표)

현재 활발하게 개발 중인 세 번째 주력 제품은 전체 가상자산 생태계, 특히 비트코인 분야에서 널리 인식되고 있으나 늘 충족되지는 못하고 있는 핵심적인 시장 수요를 목표로 삼습니다. 비트코인의 특성에 맞춰 구현되어 오랜 시간 해결되지 못했던 근본적인 문제를 해결해줄 제품입니다. 추후 적절한 시기에 더 자세한 내용을 공유하도록 하겠습니다.

[72] Structured product

[73] Noon

[74] Keyrock

[75] Risk profile