

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Stacks
홈페이지	https://www.stacks.co/
참고문헌 (백서, Docs 등)	https://docs.stacks.co/

1. 프로젝트 정보

스택스(Stacks)는 스마트 계약을 위한 비트코인 레이어(Bitcoin layer)로 스마트 계약과 탈중앙화 애플리케이션이 무신뢰 방식으로 비트코인을 자산으로 사용하고 비트코인 블록체인에 트랜잭션을 정산(settle)할 수 있도록 해줍니다. 2021년 초에 출시된 초기 버전의 스택스는 트랜잭션의 비트코인 정산, 비트코인 트랜잭션에 대응할 수 있는 안전한 계약 언어 클라리티(Clarity), BTC와의 자산 아톰릭 스왑을 도입했습니다. 스택스의 다음 주요 제안 업그레이드인 나카모토(Nakamoto) 릴리즈(2023년 예상)는 비트코인 레이어로서 스택스의 기능을 강화해 주는 중요한 기능을 담고 있습니다: (a) BTC를 레이어 안팎으로 이동하고 비트코인 쓰기를 위한 무신뢰 양방향 비트코인 페그, (b) 비트코인 완결성에 의해 보호되는 트랜잭션, (c) 빠른 거래 및 블록 타임입니다. 이 기능이 완료되면 스택스 레이어는 비트코인을 무신뢰 방식으로 완전히 프로그래밍 가능한 자산으로 만들어주게 됩니다. 이를 통해 수천억 달러의 수동적인 비트코인 자산을 생산적인 자산으로 탈바꿈시키고, 탈중앙화 애플리케이션으로 비트코인을 가져오고, 비트코인을 보다 안전한 웹3를 위한 중추로 만들어줄 것입니다.

나카모토 릴리스

비트코인은 가장 탈중앙화되고 안전하며 내구성이 뛰어난 블록체인입니다. BTC는 독특하고 강력하며 그리고 가장 널리 보유된 자산으로, 비트코인 블록체인은 거래를 위한 단연 최고의 최종 정산(settlement) 레이어입니다. 따라서 탈중앙화와 내구성을 극대화하고자 하는 애플리케이션은 BTC를 자산으로 사용하고 비트코인 블록체인에서 최종 정산을 수행해야 합니다. 그러나 본연의 특성을 보존하기 위해 비트코인 블록체인은 설계상 느리고, 미니멀(minimal)하며, 변화에 강합니다. 예를 들어, 비트코인은 기본적으로 완전 표현형 스마트 계약이나 빠른 성능을 제공하지 않기 때문에 정교한 애플리케이션을 직접 구축할 수 없습니다. 따라서 BTC는 수동적인 자산으로 남아 있으며, 대신 대부분의 애플리케이션은 이더리움 및 기타 레이어1 블록체인에 구축되나, 이러한 체인들의 네이티브 자산은 BTC보다 강력하지 않습니다. 비트코인 레이어(Bitcoin layers)는 비트코인 레이어1을 수정할 필요 없이 기능을 확장하고 비트코인의 성능을 향상시킬 수 있습니다. 빠른 결제 (Lightning) 및 일반적인 스마트 계약 (Stacks 및 RSK)를 예시로 들 수 있습니다. 변화에 있어 보수적인 비트코인은 정산 레이어로서 FedWire 그리고 인터넷 프로토콜로서 TCP/IP와 비교 가능합니다: 추가적인 기능과 혁신은 더 높은 수준의 레이어에서 구축되나, 그 베이스는 여전히 단순하고 안정적입니다.

비트코인 레이어는 완전 표현형 스마트 컨트랙트, 높은 성능 혹은 보다 강화된 개인정보 보호를 필요로 하는 정교한 애플리케이션을 가능하게 합니다.

스마트 컨트랙트를 위한 스택스 레이어에는 다음과 같은 고유한 혁신이 있습니다:

S – Secured by the entire hash power of Bitcoin / 비트코인의 전체 해시 파워에 의한 보안 (비트코인 완결성).

T – Trust-minimized Bitcoin peg mechanism; write to Bitcoin / 신뢰를 최소화한 비트코인 페그 메커니즘; 비트코인 쓰기.

A – Atomic BTC swaps and assets owned by BTC addresses / 아토믹 BTC 스왑 및 비트코인 주소를 사용한 자산 소유.

C – Clarity language for safe, decidable contracts / 안전하고 결정 가능한 컨트랙트를 위한 클라리티(Clarify) 언어.

K – Knowledge of full Bitcoin state; read from Bitcoin / 전체 비트코인 상태에 대한 식별력; 비트코인 읽기.

S – Scalable, fast transactions that settle on Bitcoin / 비트코인에 정산되는 확장 가능하고 빠른 트랜잭션.

나카모토 릴리스의 핵심 구성 요소는 비트코인 완결성과 빠른 거래이며, 다른 속성들은 이미 스택스에 있습니다. 보다 구체적으로, 스택스의 나카모토 릴리스는 다음과 같습니다.

비트코인 보안: 스택스 트랜잭션에 대해 비트코인 완결성을 가능하게 합니다; 스택스 레이어에서 발생한 트랜잭션은 비트코인 전체 해시 파워에 의해 보호됩니다. 즉, 이러한 거래를 되돌리기 위해서는 공격자가 비트코인을 재구성(reorg)해야 합니다. 이 모든 거래는 비트코인 상에 정산되며 비트코인 완결성을 갖습니다. 또한 스택스 레이어는 비트코인과 함께 포크되므로, 스택스의 모든 상태는 자연적으로 비트코인 포크를 따릅니다.

신뢰를 최소화한 비트코인 페그: 새로운 탈중앙화 비-수탁형 비트코인 페깅 자산인 sBTC를 도입하여 거래 상대방 위험을 최소화하면서 비트코인 페깅 자산을 사용해 스마트 컨트랙트를 훨씬 빠르고 저렴하게 실행할 수 있습니다. 또한 스택스 레이어의 컨트랙트는 중앙화된 폐쇄형 주체에 의존할 필요 없이 페그-아웃 트랜잭션을 통해 비트코인에 기록할 수 있습니다.

아토믹 스왑과 자산: 이미 스택스를 통해 아토믹 BTC 스왑이 가능하며, 비트코인 주소를 사용하여 스택스 레이어에 정의된 자산을 소유하고 이동할 수 있습니다. 대표적으로 매직 스왑 및 카타마란 스왑은 비트코인 레이어1의 BTC와 이미 스택스 상에 존재하는 자산 간의 무신뢰 아토믹 스왑입니다. 또한, 사용자가 비트코인 주소를 사용하여 STX, 스테이블코인 및 NFT와 같은 스택스 레이어 자산을 소유할 수 있으며 경우에 따라 비트코인 레이어1 트랜잭션을 사용하여 전송할 수 있습니다. sBTC가 작동하기 위해서는

나카모토 릴리스가 필요하지만 sBTC 자체는 나카모토 릴리스에 포함되지 않으며 별도의 백서에 설명되어 있습니다.

클래러티 언어: 증명 가능한 스마트 계약을 위한 안전하고 결정 가능한 언어인 클래러티를 지원합니다. 클래러티를 사용하면 개발자는 계약을 실행하기 전에도 수학적 확실성을 가지고 계약이 무엇을 할 수 있고 무엇을 할 수 없는지 알 수 있습니다. 탈중앙화 페그 계약은 클래러티 언어의 안전성의 이점을 누릴 수 있습니다. 특히, 클래러티 WASM은 클래러티 가상머신에 대한 변경 사항으로 실행 시간이 크게 단축되고 러스트와 솔리디티 개발자가 스택스에서 스마트 계약을 작성할 수 있는 잠재적인 경로를 제공합니다. 그러나 이 작업은 나카모토 릴리스의 일부가 아닙니다.

비트코인 상태 식별력: 전체 비트코인 상태에 대한 식별이 가능합니다; 비트코인 거래 및 상태 변경을 신뢰할 수 없이 읽을 수 있고 비트코인 거래로 인해 유발되는 스마트 계약을 실행할 수 있습니다. 비트코인 읽기 기능은 무엇보다도 비트코인 레이어1에 락업된 BTC와 일치하도록 무신뢰 페그 상태를 유지하는데 도움을 줍니다.

확장 가능하고 빠른 트랜잭션: 비트코인 블록 사이의 더 빠른 스택스 레이어 블록 그리고 여러 메커니즘을 도입하여 높은 성능과 확장성을 제공합니다. 또한 서브넷과 같은 확장성 레이어는 메인 스택스 레이어와 다른 성능과 탈중앙화 사이에서 다른 절충점을 만들 수 있습니다.

사용자가 비트코인 레이어 안팎으로 BTC를 쉽게 이동하고 레이어의 스마트 계약이 비트코인 상태를 무신뢰로 읽고 쓸 수 있게 된다면 수천억 달러의 잠재적인 비트코인 자산을 탈중앙화 비트코인 대출, 비트코인 담보 스테이블코인 등의 애플리케이션에 배포할 수 있습니다. 이 모든 애플리케이션은 비트코인의 세계적인 수요를 증가시켜 비트코인의 가치와 유틸리티를 높일 수 있습니다. 비트코인 레이어의 애플리케이션의 활동이 증가하면 비트코인 블록 공간의 수요 증가와 함께 비트코인 채굴자의 수익 증가로 이어질 수 있으며, 향후 비트코인 코인베이스 인센티브가 트랜잭션 수수료로 대체되어야 하기에 이는 비트코인의 보안에 도움이 될 수 있습니다. 무신뢰 쓰기과 무신뢰 비트코인 페그가 포함된 스택스 나카모토 릴리스는 비트코인 경제 성장을 위한 중요한 단계가 될 것입니다.

비트코인의 작업 증명(PoW)에서 영감을 받은 스택스 레이어의 합의 프로토콜인 전송증명(Proof of Transfer, PoX)은 에너지 효율적이며 PoW 에너지를 재활용합니다. 무신뢰 페그의 설계는 PoX 합의와 통합되어 있기에 가능합니다. 스택스 레이어의 네이티브 토큰(STX)은 PoX 합의에 필수적입니다. STX는 (a) 스택스 채굴자가 비트코인 레이어1 외부에서 스택스 레이어 글로벌 원장을 유지하도록 장려하고 (b) sBTC 무신뢰 페그에 대한 활성 보장 및 페그 메커니즘에 참여하는 임계값 서명자에 대한 인센티브를 제공하는 데 필요합니다. 네이티브 토큰이 없는 비트코인 페그에 대한 기존 접근 방식은 무허가형 오픈-시스템을 지원할 수 없으며 커스터디언을 사용하거나 잘 알려진 연합

구성원의 신뢰로 대체하고 있습니다.

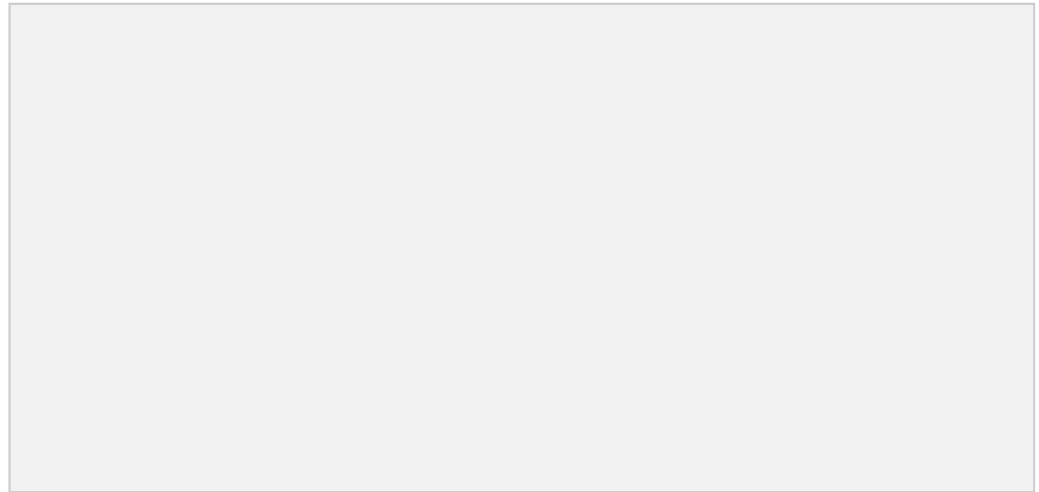
sBTC

sBTC 시스템은 표준(즉, 기본 및 유효) 스택스 레이어 포크에서 채굴과 인센티브 호환이 되도록 설계되었으며, 스택커의 가장 수익성 있는 행동 과정은 항상 페그를 충실히 유지하는 것입니다. sBTC에는 두 가지 작동 모드가 존재합니다: 일반 모드와 복구 모드입니다. 일반 모드는 앞서 설명한 대로 사용자는 스택커의 락업한 STX 비율을 반영한 임계값 비율에 의해 제어되는 비트코인 체인의 페그 지갑/스크립트로 전송된 BTC로 보냅니다. BTC가 이 지갑으로 전송될 때마다(페그-인 작업) 동일한 수량의 sBTC가 발신자가 선택한 주소로 발행되어 1:1 페그를 유지합니다. 유효한 페그-아웃 작업에서 스택커의 임계값 비율은 비트코인 메인 체인의 임계값-서명 게이트 트랜잭션을 통해 페그 지갑/스크립트에서 요청된 비트코인 주소로 원하는 수량의 BTC로 전송하여 페그-아웃을 실행합니다. 그다음 프로토콜은 스택스 측에서 동일한 양의 sBTC를 소각합니다.

일반 모드에서 어떠한 이유로 활성 실패 (BTC 손실 포함)가 발생하면 일정 수의 스택커가 다시 온라인 상태가 되어 서명 페그-아웃 요청을 재개할 때까지 시스템은 복구 모드로 전환됩니다. 복구 모드에서 스택커가 획득한 PoX 지불금의 일부가 페그-아웃 요청을 이행하도록 리디렉션되어 스택커가 다시 온라인 상태가 되지 않더라도 결국 모든 미결제 상태의 페그-아웃 요청이 이행됩니다. 복구 모드의 설계는 일반 모드보다 상당히 느리지만 스택스 레이어가 살아있고 PoX 채굴이 계속해서 이루어지는 이상 사용자의 BTC를 회수할 수 있도록 보장합니다. 복구 모드는 스택커가 페그-아웃 요청을 적시에 이행할 수 있는 경제적 인센티브로 작용하며, 그렇지 않으면 BTC 보상을 잃기 시작합니다. 복구 모드를 통해 sBTC의 전체 유통량을 복구하는 것은 PoX로부터 발생한 BTC 보상 크기에 따라 결정되기 때문에 매우 느린 과정이 될 수 있습니다.

sBTC 설계의 주요 안전 가정은 스택커가 악의적으로 행동하여 얻을 수 있는 것보다 훨씬 더 많은 손실을 볼 수 있다는 점을 감안할 때, 경제적으로 합리적인 선택은 항상 페그를 이행하는 것입니다. 또한, 70%의 임계 서명 수준은 수많은 탈중앙화된 참가자들이 결탁하거나 타협해야 함을 의미합니다.

일반 모드와 복구 모드의 설계는 스택스 채굴자, 스택커 그리고 사용자에 대한 인센티브를 신중하게 고려해야 합니다. 페그 운영이 캐노니컬 스택스 포크에서 채굴과 인센티브 호환이 유지되도록 하기 위해, 나카모토 릴리스 제안에는 스택스 레이어 메인넷 출시와 함께 2021년 출시된 PoX 합의 알고리즘에 대한 중요 업데이트가 포함되어 있습니다.



PoX를 사용한 sBTC 설계에서 스택커는 STX가 락업된 각 보상 사이클 동안 PoX 보상을 받고 BTC 스크립트/지갑을 공동으로 유지하기 위해 적극적으로 작업을 수행해야 합니다. 이 지갑은 페그-아웃 요청을 위해 사용되며, 스택커가 적시에 이를 수행하지 못하면 STX 토큰이 락업된 상태를 유지하고 모든 페그-아웃 요청이 이뤄질 때까지 PoX 보상을 받지 못합니다. 대신, 이들의 PoX 보상은 페그-아웃 요청 이행으로 리디렉션됩니다.

sBTC 출시와 함께 모든 스택킹 관련 트랜잭션과 모든 페그 트랜잭션은 비트코인 트랜잭션 형태로 비트코인 체인을 통해 브로드캐스트되어야 합니다. 그 이유는 관련 작업이 모든 잠재적인 스택스 포크로부터 이뤄져야 하기 때문입니다. 때문에 스택스 채굴자는 누군가가 스택킹에 참여하고 페그 참여자가 되는 것을 검열할 수 없습니다. 대신 스택스 채굴자가 새로운 스택스 블록을 생성하면, 비트코인으로부터 브로드캐스트되는 페그 및 스택킹 작업이 가능한 모든 포크에 자동으로 포함됩니다. 이는 채굴자가 스택킹 및 sBTC 활동을 무시하는 블록을 생성하는 것을 방지하며, 때문에 이를 수행하지 못한 블록은 새로운 합의 규칙에서 유효하지 않게 됩니다.

sBTC 설계를 통해 스택스는 주요 보안 예산 업그레이드를 받게 되며, 이때 임의 길이의 포크는 제거되고 스택스 트랜잭션은 150 블록 후 비트코인 완결성을 따르게 됩니다. 이는 비트코인 완결성(일반적으로 24시간 이내)에 도달하는 모든 스택스 레이어 작업이 스택스 레이어를 통해 포크될 수 없음을 의미합니다; 트랜잭션을 변경하는 유일한 방법은 150 깊이(depths) 이상에 대해 매우 비싸고 비실용적인 비트코인의 심층 재구성을 시도하는 것입니다. 또한 7 깊이의 스택스 포크는 대부분 스택스 채굴력(mining power)과 대부분의 스택킹 서명을 필요로 하므로, 이러한 포크를 구현하는 데 어려움이 가중됩니다. 마지막으로 비트코인 완결성으로 인해 PoX 앵커 블록의 기록은 절대 포크되지 않을 것입니다. 복구 모드를 올바르게 구현하기 위해선 이러한 새로운 특징이 필요합니다.

sBTC 출시와 함께 스택스 채굴자 집단과 이들이 커밋할 최소 BTC 금액은 다음 스택스 블록을 채굴하기 전 미리 알 수 있게 됩니다. 이를 위해 스택스 레이어는 각 채굴자가 다음 비트코인 블록에 사용할 BTC 수량을 추가로 커밋하도록 요구하게 됩니다. 만약 이들의

다음 블록-커밋에 정확한 금액이 커밋되지 않으면, 블록 커밋은 유효하지 않습니다. 이를 블록 사전-커밋(pre-commit)이라고 합니다. 또한 블록 사전-커밋은 패스트 블록(fast blocks) 기능을 가능합니다. 패스트 블록은 스택스 채굴자 집단이 오픈-멤버십을 유지한 채 누구나 참여 가능하지만, 생성될 특정 비트코인 블록에 있어 채굴자 집단은 미리 알려져 있고, 이 채굴자 집단은 BFT-스타일 쿼럼 서명 알고리즘(BFT-style quorum signing algorithm)을 사용하여 두 비트코인 정산 사이 (5초마다) 패스트블록을 생성할 수 있습니다.

2. 토큰 이코노미

가상자산 소개

STX 토큰은 스택스 2.0 블록체인의 네이티브 토큰입니다. 이는 단순 거버넌스 혹은 투기 목적의 토큰이 아닌, 아래에서 설명하는 스택스 비트코인 레이어의 합의 메커니즘의 핵심으로, 다음 두 가지 주요 목표에 필수적입니다: (i) (비트코인과 같이) 초기 트랜잭션 수수료가 원장을 유지하기에 충분하지 않기 때문에 “새로운 블록 보조금(new block subsidy)”으로써 스택스 블록 채굴을 장려합니다, (ii) 활성 인센티브이자 경제적으로 안전한 탈중앙화 비트코인 페그의 기반 역할을 합니다. 스택스 레이어는 자체적인 고유 자산을 가지고 있지 않지만, 비트코인의 성장을 돕고 비트코인과 경쟁하지 않습니다.

스택스 레이어는 스택스와 비트코인 레이어를 모두 활용하는 새로운 합의 메커니즘인 전송 증명(PoX, Proof of Transfer)을 위해 STX와 BTC에 의존하고 있습니다. PoX는 비트코인 작업 증명(PoW) 합의와 비슷한 정신을 따릅니다: 비트코인 PoW 채굴자가 전기를 사용하여 BTC를 보상받는 것과 같이, 스택스 PoX 채굴자는 (이미 생성된) BTC를 사용하여 STX를 보상으로 받습니다. PoW와 마찬가지로 PoX는 나카모토 방식의 단일-리더 선출 방식을 사용합니다: PoX 채굴자는 단순히 BTC를 사용하여 입찰하고, 입찰가-가중치가 반영된 임의 확률에 따라 리더로 선출될 수 있습니다. 리더 선출은 비트코인 체인에서 이루어지며 새로운 블록은 스택스 레이어에 기록됩니다. 이러한 방식으로 PoX는 비트코인 채굴자가 이미 수행한 작업을 재활용하고, 추가적인 전기 에너지를 소비하지 않습니다: 스택스 노드가 BTC를 사용하여 입찰하기 위해 일반적인 랩톱/컴퓨터 운영 비용만 필요로 합니다.

발행량 및 유통량계획

채굴자는 민팅한 블록에 대해 보상을 받습니다.

보상은 다음과 같습니다:

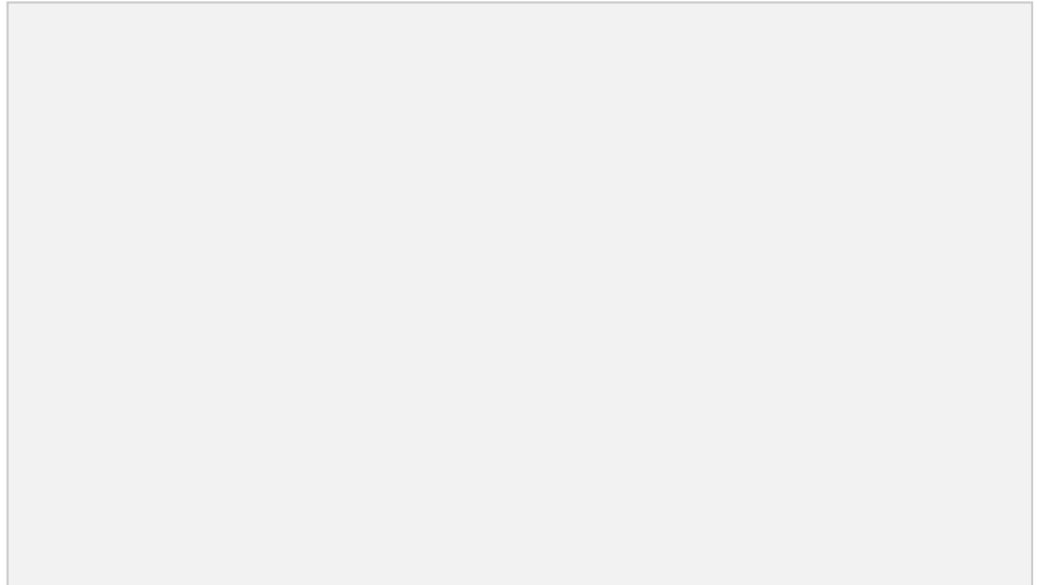
채굴 첫 4년 동안 블록당 1000 STX가 분배됩니다.

이후 4년 동안 블록당 500 STX가 분배됩니다.

이후 4년 동안 블록당 250 STX가 분배됩니다.

이후에는 블록당 125 STX가 무기한 분배됩니다.

이러한 "반감기"는 비트코인 반감기와 동기화됩니다.



3. 참고자료

- [1] <https://stx.is/nakamoto>
- [2] <https://assets.stacks.co/sbtc.pdf>
- [3] <https://docs.stacks.co/stacks-101/mining>
- [4] <https://www.stacks.co/roadmap-neww>

