스택스: 스마트 컨트랙트를 위한 비트코인 레이어

무신뢰 비트코인 페그 및 비트코인 완결성이 포함된 나카모토 릴리즈

2022년 12월 14일

Translated by GM Chung | gm@despread.io

스택스 (Stacks)는 스마트 컨트랙트를 위한 비트코인 레이어 (Bitcoin layer)이다; 스택스를 사용하면 스마트 컨트랙트와 탈중앙화 애플리케이션이 무신뢰 방식으로 비트코인을 자산으로 사용하고 비트코인 블록체인에 트랜잭션을 정산 (settle)할 수 있다. 2021년 초에 출시된 초기 버전의 스택스는 트랜잭션의 비트코인 정산, 비트코인 트랜잭션에 반응 가능한 안전한 컨트랙트 언어 클래러티 (Clarity), BTC와의 자산 아토믹 스왑을 도입했다. 스택스의 다음 주요 제안 업그레이드인 나카모토 (Nakamoto) 릴리즈 (2023년 예상)는 비트코인 레이어로서 스택스의 기능을 강화해 주는 중요한 기능을 담고 있다: (a) BTC를 레이어 안팎으로 이동하고 비트코인 쓰기를 위한 무신뢰 양방향 비트코인 페그, (b) 비트코인 완결성에 의해 보호되는 트랜잭션, (c) 비트코인 블록 사이 빠른 트랜잭션. 이 기능이 완료되면 스택스 레이어는 비트코인을 무신뢰 방식으로 완전히 프로그래밍 가능한 자산으로 만들어주게 된다. 이를 통해 수천억 달러의 수동적인 비트코인 자본을 생산적인 자산으로 탈바꿈하고, 탈중앙화 애플리케이션으로 비트코인을 가져오고, 비트코인을 보다 안전한 웹3를 위한 중추로 만들어줄 것이다.

비트코인은 가장 탈중앙화되고 안전하며 높은 내구력을 지닌 블록체인이다. BTC는 독특하고 강력하며 그리고 가장 널리 보유된 자산으로, 비트코인 블록체인은 거래를 위한 단연 최고의 최종 정산 (settlement) 레이어이다. 따라서 탈중앙화와 내구력을 극대화하고자 하는 애플리케이션은 BTC를 자산으로 사용하고 비트코인 블록체인에서 최종 정산을 수행해야 한다. 그러나 본연의 특성을 보존하기 위해 비트코인 블록체인은 설계상 느리고, 미니멀

(minimal)하며, 변화에 강하다. 예를 들어, 비트코인은 기본적으로 완전 표현형 스마트 컨트랙트나 빠른 성능을 제공하지 않기 때문에 정교한 애플리케이션을 직접 구축할 수 없다. 따라서 BTC는 수동적인 자산으로 남아있다. 이에 대부분의 애플리케이션이 이더리움 및 기타 레이어1 블록체인에 구축되나, 이러한 체인들의 네이티브 자산은 BTC보다 강력하지 않다.

비트코인 레이어 (Bitcoin layers)는 비트코인 레이어1을 수정할 필요 없이 기능을 확장하고 비트코인의 성능을 향상시킬 수 있다. 빠른 결제 (Lightning) 및 일반적인 스마트 컨트랙트 (Stacks 및 RSK)를 예시로 들 수 있다. 변화에 있어 보수적인 비트코인은 정산 레이어로서 FedWire 그리고 인터넷 프로토콜로서 TCP/IP와 비교 가능하다: 추가적인 기능과 혁신은 더 높은 수준의 레이어에서 구축되나, 그 베이스는 여전히 단순하고 안정적이다. 비트코인 레이어는 완전 표현형 스마트 컨트랙트, 높은 성능 혹은 보다 강화된 개인정보보호를 필요로 하는 정교한 애플리케이션을 가능하게 한다.

스마트 컨트랙트를 위한 스택스 레이어에는 다음과 같은 고유한 혁신이 있다:

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 클래러티 (Clarity) 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.

무신뢰 비트코인 페그 (**sBTC 백서 참고** [6]), 빠른 트랜잭션 및 비트코인 완결성은 나카모토 릴리즈를 위해 제안되었으며, 그 외 특징들은 이미 스택스에 존재한다. 이 혁신에 대해 자세히 살펴보면, 스택스의 나카모토 릴리즈는 다음과 같다:

- **비트코인 보안** (Secured by Bitcoin): 스택스 트랜잭션을 위한 비트코인 완결(finalization)을 가능하게 한다; 150 비트코인 블록 혹은 약 하루의 확인(confirmations)이 이뤄지면, 스택스 레이어에서 발생한 트랜잭션은 비트코인 전체 해시 파워에 의해 보호된다. 즉, 이러한 거래를 되돌리기 위해선 공격자가 비트코인을 재구성(reorg)해야 한다. 이 모든 거래는 비트코인 상에 정산되며 비트코인 완결성을 갖는다. 또한 스택스 레이어는 비트코인과 함께 포크하므로, 스택스의 모든 상태는 자연적으로 비트코인 포크를 따르게 된다.

- **신뢰를 최소화한 비트코인 페그** (Trust-minimized Bitcoin peg): 새로운 탈중앙화 비-수탁형 비트코인-페깅 자산인 sBTC를 도입하며, 스마트 컨트랙트를 통해 안전성 손실 없이 비트코인-페깅 자산을 빠르고 저렴하게 사용할 수 있다. 또한 이는 스택스 레이어 상의 컨트랙트가 페그-아웃 트랜잭션을 통해 비트코인에 무신뢰 쓰기를 가능하게 한다.

- **아토믹 스왑 및 자산** (Atomic swaps and assets): 이미 스택스를 통해 아토믹 BTC 스왑이 가능하며, 비트코인 주소를 사용하여 스택스 레이어에 정의된 자산을 소유하고 이동할 수 있다. 대표적으로 매직 스왑 [2] 및 카타마란 스왑 [8]은 비트코인 레이어1의 BTC와 이미 스택스 상에 존재하는 자산 간의 무신뢰 아토믹 스왑이다. 또한 사용자는 비트코인 주소를 사용하여 STX, 스테이블코인 및 NFT와 같은 스택스 레이어 자산을 소유할 수 있으며 경우에 따라 비트코인 레이어1 트랜잭션을 사용하여 전송할 수 있다.

- **클래리티 언어** (Clarity language): 완전 표현형 스마트 컨트랙트를 위해 안전하고 결정 가능한 언어인 클래리티 (Clarity)를 지원한다. 클래리티를 사용하는 개발자는 컨트랙트를 실행하기 전 계약 실행 가능 여부를 확실하게 알 수 있다 [1]. 무신뢰 페그 컨트랙트는 클래리티 언어의 안정성을 활용 가능하다. 2022년 12월 기준 스택스 레이어에 배포된 클래리티 컨트랙트는 5,000건이 넘는다 [4].

- **비트코인 상태 식별력** (Knowledge of Bitcoin state): 전체 비트코인 상태에 대한 식별이 가능하다; 비트코인 트랜잭션 및 상태 변화를 무신뢰로 읽을 수 있으며 비트코인 트랜잭션에 의해 트리거되는 스마트 컨트랙트를 실행할 수 있다. 비트코인 읽기 기능은

무엇보다 비트코인 레이어1에 락업된 BTC와 일치하도록 무신뢰 페그 상태를 유지하는 데 도움을 준다.

- **확장 가능하고 빠른 트랜잭션** (Scalable, fast transactions): 비트코인 블록 사이 더 빠른 스택스 레이어 블록 그리고 여러 메커니즘을 도입하여 높은 성능과 확장성을 제공한다. 또한 서브넷과 같은 확장성 레이어는 메인 스택스 레이어의 탈중앙화를 성능과 맞교환함으로써 차별점을 이뤄내며, 다른 프로그래밍 언어 및 실행 환경도 지원 가능하다 (예를 들어, 이더리움의 솔리디티 (Solidity) 및 EVM을 지원하여, 모든 이더리움 스마트 컨트랙트가 비트코인 페깅 자산을 사용하고 비트코인 체인에 정산할 수 있다).

사용자가 비트코인 레이어 안팎으로 BTC를 쉽게 이동하고 레이어의 스마트 컨트랙트가 비트코인 상태를 무신뢰로 읽고 쓸 수 있게 된다면 수천억 달러의 잠재적인 비트코인 자본을 탈중앙화 비트코인 대출, 비트코인 담보 스테이블코인 등의 애플리케이션에 배포할 수 있다. 이 모든 애플리케이션은 비트코인의 세계적인 수요를 증가시켜 비트코인의 가치와 유틸리티를 높일 수 있다. 비트코인 레이어의 애플리케이션 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 있다. 무신뢰 쓰기와 무신뢰 비트코인 페그가 포함된 스택스 나카모토 릴리즈는 비트코인 경제 성장을 위한 중요한 단계가 될 것이다.

비트코인의 작업 증명 (PoW)에서 영감을 얻은 스택스 레이어의 합의 프로토콜인 전송 증명 (PoX)은 에너지 효율적이며 PoW 에너지를 재활용한다. 무신뢰 페그의 설계는 PoX 합의와 통합되어 있기에 가능하다. 스택스 레이어의 네이티브 토큰 (STX)은 PoX 합의에 있어 필수적이다. STX는 (a) 스택스 채굴자가 비트코인 레이어1 외부에서 스택스 레이어 글로벌 원장을 유지하도록 장려하고, (b) sBTC 무신뢰 페그 활성 보장과 페그 메커니즘에 참여하는 임계값 서명자에게 인센티브를 제공하는데 필요하다. 네이티브 토큰이 없는 비트코인 페그에 대한 이전 접근 방식은 무허가형 오픈-시스템을 지원할 수 없으며 커스터디안을 사용하거나 잘 알려진 연합 구성원의 신뢰로 대체하고 있다.

지금까지 스택스 비트코인 레이어 프로젝트는 탈중앙화에 확실한 초점을 두고 공시 및 투명성에 있어 법적 준수를 잘 따라왔다. STX는 미국 역사상 최초로 SEC로부터 인증받은 토큰

오퍼링을 통해 일반 대중에게 배포되었다. 이 프로젝트는 2021년 1월 스택스 메인넷 출시 이전 완전히 탈중앙화되었다. 현재 탈중앙화된 생태계는 30개 이상의 독립 엔터티로 구성되어 있다.

1 비트코인 레이어

신뢰의 탈중앙화는 블록체인의 주요 혁신이자 약속이다. 2022년 암호화폐 세계에서 발생한 최근의 실패는 중앙화된 엔터티로부터 발생했으며 "신뢰할 수 있는" 중앙화된 중개자에 의존하지 않는 시스템의 중요성이 더욱 강조되었다. 비트코인은 가장 안전하고 내구성이 있으며 가치 있는 블록체인이다; 이는 가치 저장소로서 '캐즘을 넘어서고 (crossed the chasm)'있다. 비트코인은 인플레이션이 없으며 전례 없는 비-수탁형 소유권을 갖춘 견고한 '하드 머니 (hard money)'이다. 또한 비트코인 블록체인은 가장 탈중앙화되었으며 검열에 강하고 불변하며 내구성이 뛰어난 블록체인이기 때문에 트랜잭션을 위한 최고의 결제 레이어이다.

그러나 비트코인은 설계상 상대적으로 느리고 미니멀하며 이러한 강력한 특징을 그대로 지키기 위해 변화에 있어 보수적이다. 비트코인의 평균 블록 생성 시간은 약 10분으로, 초당 5-7건의 트랜잭션 밖에 처리하지 못한다 [12]. 또한 비트코인은 자체 특징을 활용할 수 있는 프로그래밍 가능한 스마트 컨트랙트 및 정교한 애플리케이션을 기본적으로 지원하지 않는다. 그 결과 비트코인은 생산적인 자산이 아닌 수동적인 자산으로 남아있다. 매력적이고 고유한 특징에도 불구하고 가치 저장 및 자금 이동 외 애플리케이션을 위한 플랫폼으로 사용되고 있지 않는다.

비트코인 레이어는 앞서 언급한 문제를 해결하고자 한다. **비트코인 레이어는 비트코인 블록체인을 수정할 필요 없이 기능과 성능을 확장한다.** 자산 발행을 위한 리퀴드 (Liquid), 빠른 결제를 위한 라이트닝 (Lightning), 스마트 컨트랙트를 위한 스택스 (Stacks) 및 RSK와 같이 오늘날 다양한 비트코인 레이어가 개발 및 진전을 이루고 있다. 예를 들어 라이트닝은 결제 확장을 위한 비트코인 레이어로, 신뢰를 최소화한 방식으로 더 빠르고 저렴한 결제를 가능하게 한다. 결제는 P2P 채널을 통해 오프체인에서 이뤄지며 채널이 닫힐 때 비트코인 메인 체인에서 (비트코인 트랜잭션을 통해) 최종적인 순 정산이 이뤄진다. 라이트닝과 같은 P2P 레이어는 가상 머신과 같이 일반적인 컴퓨팅을 위한 글로벌 상태 혹은 실행 환경은 제공하지 않는다.

그러나 수많은 애플리케이션이 스마트 컨트랙트와 완전한 실행 환경을 필요로 한다. 이는 글로벌 상태와의 개인 대 개인 (P2P) 상호 작용이 아닌 글로벌을 필요로 하며, 비트코인 메인 체인에서 비트코인 스크립트와 탭루트가 제공하는 것 이상으로 보다 완전한 표현 능력을 갖춘 스마트 컨트랙트를 필요로 한다. 완전-표현형 스마트 컨트랙트가 필요한 애플리케이션으로 AMM (Automated Market Maker), 유동성 풀, 탈중앙화 NFT 마켓플레이스, 탈중앙화 도메인 등이 있으며 그 외에도 아직 발견되지 않은 애플리케이션이 다수 있다. 따라서 스마트 컨트랙트를 통해 비트코인을 자산으로 사용하고 비트코인 블록체인을 최종 정산 레이어로 사용할 수 있도록, 스마트 컨트랙트를 지원하는 비트코인 레이어를 갖는 것은 필수적이다.

1.1 스마트 컨트랙트를 위한 비트코인 레이어

완전-표현형 스마트 컨트랙트를 사용하면 개발자가 원하는 모든 유형의 애플리케이션 로직을 구축할 수 있다. 이러한 스마트 컨트랙트는 상태 및 (컴파일 여부와 관계없이) 코드에 대한 글로벌 액세스 접근 가능성 및 영구 저장소 (persistent storage)를 필요로 한다. 비트코인 블록체인은 임의의 컨트랙트 퍼블리싱 및 복잡한 컨트랙트 상태 저장을 허용하지 않기 때문에 컨트랙트 로직 및 상태는 비트코인 레이어1 외부에서 저장 및 실행되어야 한다. 스마트 컨트랙트는 수정이 불가능해야 하므로 수정 불가능한 글로벌 원장, 즉 별개의 블록체인에 퍼블리싱 되어야 한다.

비트코인 생태계 내 광범위하게 완전-표현형 스마트 컨트랙트를 가능하게 만들기 위한 기존의 시도는 사이드체인 접근법에 초점이 맞춰졌었다. 사이드체인은 RSK 및 리퀴드와 같은 스마트 컨트랙트를 지원하는 일종의 비트코인 레이어이다. 사이드체인에서 BTC는 BTC와 가치가 1:1로 페깅된 파생 자산을 사용하여 타 블록체인 (사이드체인)에 “페그-인 (pegged-in)”한다. 스마트 컨트랙트는 타 블록체인에서 실행되며 페깅 자산의 비트코인 블록체인과의 상호 작용은 많지 않다. BTC는 요구에 따라 비트코인 블록체인에 “페그 아웃 (pegged out)” 할 수 있다. 비트코인과의 유일한 접점은 페그-인 및 페그-아웃 작업을 통해 이뤄지며 병합 채굴 (merged-mining) 접근 방식은 비트코인의 채굴력 (mining power)을 활용한다. 일반적으로 사이드체인의 스마트 컨트랙트는 비트코인 트랜잭션과 BTC가 상호 작용하지 않는다; 비트코인 블록체인에는 관련한 기록이 존재하지 않는다. 이는 비트코인 트랜잭션과 직접 상호 작용하고 비트코인 레이어1에서 트랜잭션을 해결 가능한 라이트닝과 같은 비트코인 레이어2와 다르다. 2022년 현재 어떠한 비트코인 사이드체인도 무신뢰 오픈-멤버십

비트코인 페그-아웃을 구현하지 못했다. 2022년 현재 비트코인 생태계의 사이드체인 (리퀴드, RSK 등)은 오픈-멤버십 비트코인 페그-아웃을 구현하지 못했으며, 이를 위해 잘 알려진 연합, 신뢰할 수 있는 엔터티 혹은 중앙화된 커스터디안에 의존하고 있다. 코스코스 (Cosmos) 생태계의 Nomic은 초기 단계의 탈중앙화된 비트코인 브릿지/페그를 구현했다. tBTC [5] 및 renBTC와 같은 프로젝트는 이더리움 기반 비트코인 페깅 자산에 탈중앙화된 접근 방식을 시도했고, 최근 renBTC는 연합 설계 모델로 전환 중에 있다.

RSK는 블록 생성 및 합의를 위해 병합 채굴을 사용하며, 리퀴드는 잘 알려진 엔터티 연합 (known federation of entities)을 사용한다. 병합 채굴을 사용하는 사이드체인의 보안은 얼마나 많은 비트코인 채굴자가 사이드체인을 채굴하느냐에 따라 결정된다. 모든 채굴자가 이를 택한다면 사이드체인은 매우 안전할 수 있다. 하지만 일부의 참여만 이뤄지거나 혹은 일부만 참여하는 기간 동안 소수의 비트코인 채굴자가 사이드체인을 쉽게 공격할 수 있기 때문에 안전을 위협받을 수 있다 (예를 들어, Namecoin 체인은 오랜 기간 동안 이러한 공격 위험에 노출되어 있었다 [ref]). 스마트 컨트랙트 체인을 채굴하는 것은 비트코인을 채굴하는 것과는 다르다. 왜냐하면 이는 단순 해시 (hash)를 해결하는 것뿐만 아닌 임의의 컨트랙트 (프로그램)를 실행하고 훨씬 더 많은 양의 데이터와 로직을 처리해야 하기 때문이다. 비트코인 사이드체인에서 지금까지 경험하지 못한 높은 스마트 컨트랙트 트래픽이 발생하면 이는 채굴자에게 매력적이지 않을뿐더러 비트코인 채굴의 탈중앙화를 감소시킬 수 있다. 따라서 **스마트 컨트랙트 레이어를 채굴하기 위해 비트코인 채굴자에게 의존하는 것은 장기적으로 좋은 아이디어가 아니다.**

1.2 스마트 컨트랙트를 위한 비트코인 레이어의 바람직한 특성

BTC를 자산으로 사용하고 비트코인 블록체인에 정산되는 범용적인 스마트 컨트랙트를 위해 비트코인 레이어를 어떻게 구현해야 할까? 먼저 비트코인이 (이더리움처럼) 스마트 컨트랙트를 기본적으로 지원하는 시나리오를 확인해보겠다. 컨트랙트는 비트코인 체인, 즉 글로벌 원장에 코드와 상태를 저장한다. 또한 이는:

1. 비트코인 전체 해시 파워로 보호되는 원장이 있으며,
2. 일반적인 비트코인 트랜잭션에 의해 실행되도록 트리거되며,

3. 탈중앙화되고 신뢰할 수 없는 방식으로, 즉 고정된 엔터티 집단에 의존할 필요 없이 비트코인 블록체인에 서명된 트랜잭션을 작성 (브로드캐스트)하고,

4. 트랜잭션이 비트코인 체인에 정산되도록 하여 다른 비트코인 트랜잭션과 마찬가지로 모든 스마트 컨트랙트 및 트랜잭션 기록을 무신뢰 방식으로 누구나 검증 가능하며,

5. 비트코인 포크 대상이 되어야 한다 (즉, 비트코인 체인이 포크되면 (a) 캐노니컬 (canonical) 비트코인 포크에서 종료되는 컨트랙트 및 트랜잭션만 유효하며, (b) 비트코인 포크로 인한 결과로 컨트랙트 및 트랜잭션이 비트코인과 일치하지 않아야 한다.).

이는 바람직한 특성이지만 우리는 비트코인이 허용하는 것보다 더 높은 트랜잭션 처리량과 더 낮은 트랜잭션 컨펌 대기 시간을 달성할 수 있는 메커니즘을 원한다. 앞서 설명한 네티이브 비트코인 스마트 컨트랙트의 특성과 사이드체인 접근 방식을 비교해보면, 다음과 같은 특성을 충족하지 않음을 확인할 수 있다:

1. 모든 비트코인 채굴자가 사이드체인도 채굴하지 않는 이상, 비트코인 레이어 혹은 해당 스마트 컨트랙트는 비트코인의 전체 해시 파워에 의해 보호되지 않으며,

2. 현재의 사이드체인 구현에서의 스마트 컨트랙트는 일반적인 비트코인 트랜잭션에 의해 트리거될 수 없고,

3. 비트코인 트랜잭션을 쓸 수 있지만, 무신뢰 방식이 아닌 연합된 페그 방식이며,

4. 페그 작업 외 이뤄지는 트랜잭션이 비트코인 체인에 정산되지 않고 완전히 분리되어 있기에 트랜잭션 정산을 비트코인에서 확인할 수 없고,

5. 체인과 비트코인 간 긴밀한 지속 관계가 없어 비트코인과 함께 포크하지 않기 때문에 비트코인 포크를 대부분 인지할 수 없다.

사이드체인이 페그 작업 외 비트코인과 독립적으로 작동하는 것은 비트코인의 속도에 크게 제약 받지 않고 더 높은 트랜잭션 처리량과 더 낮은 대기 시간이 적용될 수 있으나, 트랜잭션이 비트코인 블록체인에 정산되지 않는다. **스택스 비트코인 레이어는 네이티브 비트코인 스마트 컨트랙트의 바람직한 특성에 최대한 근접하게끔 설계되었으나 높은 성능도 갖추고 있다.** 아래

내용에는 스마트 컨트랙트를 위한 스택스 비트코인 레이어를 소개하고 네이티브 비트코인 스마트 컨트랙트의 이상적인 특성과 관련하여 어떻게 작동하는지 살펴보도록 하겠다.

2 스택스 비트코인 레이어

스택스 (Stacks)는 기존 사이드체인과는 다른 유형의 스마트 컨트랙트를 위한 비트코인 레이어로, 비트코인과 보다 긴밀하고 지속적인 연결이 되어 있다. 스택스 레이어는 애플리케이션과 스마트 컨트랙트가 BTC를 자산 혹은 화폐로 사용하고 트랜잭션을 비트코인 메인 체인에 정산할 수 있도록 한다. **스택스 레이어는 BTC를 수동적인 자산이 아닌 생산적인 자산으로 전환시키고 애플리케이션이 다양한 영역에서 중앙화 요소 없이 신뢰 약속 (promise of trust)을 수행 가능하게 하여 비트코인 경제를 성장시키는 것을 목표로 한다.** RSK 및 리퀴드와 같은 사이드체인과 마찬가지로 스택스 레이어는 자체 글로벌 원장 및 실행 환경을 갖추고 있으며, 이를 통해 스마트 컨트랙트를 지원하고 추가적인 트랜잭션을 발생시키더라도 비트코인 블록체인에 부담을 주지 않는다. 그러나 스택스 레이어는 네이티브 비트코인 스마트 컨트랙트의 이상적인 특성 대부분을 갖추고 있기 때문에 매우 독특하다. 또한 아래 설명될 패스트 블록 (fast blocks), 무신뢰 페그 (trustless peg) 및 서브넷 (subnets)을 통해 더 높은 성능의 메커니즘을 제공한다.

RSK 및 리퀴드와 달리 **스택스에는 자체 네이티브 자산 (STX)이 존재한다.** 이는 단순 거버넌스 혹은 투기 목적의 토큰이 아닌, 아래에서 논의할 스택스 비트코인 레이어의 합의 메커니즘을 위한 핵심으로, 다음 두 가지 주요 목표를 위해 필수적이다: (i) (비트코인과 같이) 초기 트랜잭션 수수료가 원장을 유지하기에 충분하지 않기 때문에 "새로운 블록 보조금 (new block subsidy)"으로써 스택스 블록 채굴을 장려한다, (ii) 경제적으로 안전한 무신뢰 비트코인 페그의 기반이자 활성 인센티브 역할을 한다. 추후 살펴보겠지만 자체 네이티브 자산이 존재함에도 불구하고, 스택스 레이어는 비트코인의 성장을 돕고 비트코인과 경쟁하지 않는다.

스택스 레이어는 스택스와 비트코인 레이어를 모두 활용하는 **새로운 합의 메커니즘인 전송 증명 (PoX, Proof of Transfer)**을 위해 STX와 BTC에 의존하고 있다. PoX는 비트코인의 작업 증명 (PoX) 합의와 비슷한 정신 (spirit)을 따른다: 비트코인 PoW 채굴자가 전기를 사용하여 BTC를 보상 받는 것과 같이, 스택스 PoX 채굴자는 (이미 생성된) BTC를 사용하여 STX를 보상 받는다. PoW와 마찬가지로 PoX는 나카모토 (Nakamoto) 방식의 단일-리더 선출 (single-leader

election) 방식을 사용한다: PoX 채굴자는 단순히 BTC를 사용하여 입찰하고, 입찰가-가중치가 반영된 임의 확률에 따라 리더로 선출될 수 있다. 리더 선출은 비트코인 체인에서 이뤄지며 새로운 블록은 스택스 레이어에 쓰여진다. 이러한 방식으로 **PoX는 비트코인 채굴자가 이미 수행한 작업을 재활용하고**, 추가적인 전기 에너지를 소비하지 않는다: 스택스 노드가 BTC를 사용하여 입찰하기 위해 일반적인 랩톱/컴퓨터 운영 비용만 필요로 한다.

PoW와 마찬가지로, PoX는 무허가형 (permissionless)이다: BTC를 사용하고자 하는 누구나 스택스 채굴자가 될 수 있다. 또한 모든 STX 보유자는 PoX 합의에 참여하기 위해 자신의 STX를 락업할 수 있으며 ("스태킹"이라 부른다), 무신뢰 비트코인 페그에 서명자로 참여하는 것과 같이 시스템을 위해 유용한 작업을 수행하고 비트코인 보상을 받을 수 있다. 비트코인 정신에 따라, 스태커는 시스템을 위한 긍정적 기여에 보상을 받고 부적절한 행위에 있어 불이익을 줌으로써 행위를 억제할 수 있다 (그러나 지분 증명 (PoS, Proof of Stake) 시스템과 달리 '슬래싱 (slashed)'이 일어나지 않는다). 마지막으로, PoX 합의의 본질은 BTC와 STX 간 가격 비율이 온체인에 지속적으로 기록되고 사용할 수 있다는 것에 있으며, 이는 온-체인 비트코인 가격 오라클 역할을 한다. 이는 페그 백서에 설명한 바와 같이 외부 오라클의 필요성을 제거하여 무신뢰 페그에 유용하게 사용할 수 있다.

스택스는 스택스 메인 레이어와 무신뢰 비트코인 페그를 위해 이더리움의 솔리디티 (Solidity) 보다 **안전한 언어인 클래러티 (Clarity)를 사용한다**. 클래러티는 결정 가능 (Not Turing-complete)한 언어이다. 즉, 프로그램이 수행할 작업을 코드 자체를 통해 확실하게 확인 가능하며 코드 정확성은 소프트웨어를 통해 확인 가능하다. 클래러티는 컴파일된 언어가 아닌 인터프리터 기반 (interpreted) 언어이므로, 스마트 컨트랙트의 소스 코드를 사람이 직접 블록체인에서 확인 가능하며, 추가적인 실행 안정성을 제공하기 위해 사후-조건 (post-conditions)이 존재한다.

스택스 레이어를 통해 개발자는 이더리움, 솔라나, 아발란체 등 타 스마트 컨트랙트 플랫폼에서 구축 가능한 모든 종류의 애플리케이션을 구축할 수 있으며, BTC를 자산/화폐로 사용하고 발생하는 트랜잭션을 비트코인 블록체인에 정산할 수 있다. 이는 클래러티 가상머신 (Clarity VM)의 클래러티 혹은 아래 설명되는 서브넷을 사용하여 EVM 혹은 다른 가상 머신의 솔리디티 혹은 다른 언어로 이 작업을 수행할 수 있다. 또한 사용자는 기본적으로 비트코인 체인에서 직접 스테이블코인 및 NFT와 같은 자산을 BTC와 교환할 수 있다.

이 세션의 남은 파트에서는, 먼저 앞서 논의한 네이티브 비트코인 스마트 컨트랙트의 특성과 관련하여 스택스 레이어가 어떻게 평가될 수 있는지 알아보고, 더 높은 성능을 제공하는 방법에 대해 알아보고자 한다. 우리는 스택스가 네이티브 토큰을 통해 어떻게 비트코인을 돕는지 논의할 것이다. 그다음 무신뢰 양방향 비트코인 페그에 대해 조금 더 자세히 알아보고 (보다 자세한 설명은 sBTC 문서를 통해 확인 가능하다) 새로운 릴리즈에서의 스택스 체인의 보안 및 포크 규칙에 대해 논의할 것이다. 마지막으로 성능 및 다목적성을 위한 추가 기능으로 서브넷, EVM 호환성 및 ZK 롤업 가능성에 대해 알아보도록 하겠다.

2.1 스택스와 '네이티브 비트코인' 스마트 컨트랙트

스택스 레이어는 비트코인의 네이티브 스마트 컨트랙트의 모든 특성을 제공할 수 있다:

- **비트코인 완결성 및 보안:** 스택스 블록은 약 하루 정도의 확인 과정을 통해 비트코인 완결성을 갖는다; 즉, 스택스는 비트코인 블록체인과 비트코인의 전체 해시 파워에 의해 보호된다 (스택스 채굴기 뿐만이 아니며, 이는 병합 채굴과는 다르다). 완결성을 갖게 되면, 스택스 레이어는 포크를 허용하지 않기 때문에 스택스 트랜잭션을 재구성하기 위해서는 심층 재구성 (deep reorg) 공격으로 비트코인을 성공적으로 공격해야 하지만, 이는 매우 비싸고 논리적으로 이뤄내기 어렵다. 스택스 블록은 비트코인 블록에 기록되기 때문에 스택스 블록 관련 정보는 블록이 생산되기 전 비트코인 블록체인에서 공개적으로 확인 가능하며, 이러한 이유로 공격 및 재구성을 쉽게 감지하고 대응할 수 있어 히든 블록 공격 (hidden block attack)을 비트코인보다 훨씬 어렵게 만든다.

- **비트코인 트랜잭션에 의해 트리거되는 스마트 컨트랙트:** 스택스 레이어의 스마트 컨트랙트는 비트코인 상태를 읽을 수 있고 표준 비트코인 트랜잭션에 의해 트리거될 수 있다. 이는 스택스 노드가 비트코인 노드를 실행하고, 비트코인 상태를 열심히 읽고 인덱싱하기 때문이다.

- **비트코인 쓰기:** sBTC 비트코인 페그 메커니즘은 **무신뢰 방식으로 비트코인 트랜잭션을 비트코인 체인에 기록할 수 있다.** 스택스 또한 애플리케이션이 비트코인 체인에서 직접 BTC를 배포할 수 있도록 한다; 예를 들어, 사용자는 스택스 레이어에서 BTC와

스테이블코인과 같은 다른 자산 간에 무신뢰 아토믹 스왑을 수행할 수 있다. 더 빠른 성능을 위해 스택스 레이어는 **1:1로 페깅된 BTC의 무신뢰 비-수탁형 페그-아웃 및 페그-인을 지원한다**: BTC는 스택스 레이어에 페깅할 수 있고, 스마트 컨트랙트 및 그 외 작업은 스택스 레이어에서 빠르게 작동할 수 있으며, 비트코인 메인 체인에 페깅을 되돌릴 수 있다. 리퀴드의 L-BTC 및 RSK의 R-BTC와 같은 사이드체인의 파생 자산과 달리, 페그-아웃을 위해 고정된 연합 혹은 멀티시그 하드웨어 지갑 연합에 의존하지 않는다. 스택스 합의 프로토콜과 통합된 방식을 사용함으로써 오픈-멤버십 집단으로 이뤄진 서명자를 통해 경제적 보안을 이뤄낸다. sBTC와 함께 패스트 블록 및 서브넷을 사용하면 비트코인 블록체인에서 BTC를 직접 사용하는 것보다 스마트 컨트랙트를 통해 더 짧은 대기 시간과 더 높은 처리량으로 처리 가능하다.

- 비트코인 정산 및 확인 (Settlement and verification on Bitcoin). 모든 스택스 레이어 스마트 컨트랙트 및 트랜잭션 해시는 **비트코인 블록체인에 정산된다**. 이는 스택스의 PoX 합의 프로토콜 작동에 의한 필연적인 결과로, 합의 과정의 일부이다.

- 비트코인과의 포크 (Forking with Bitcoin). PoX 프로토콜은 스택스 레이어에 비트코인과 함께 포크한다는 바람직한 특성을 제공한다. 비트코인 포크는 스택스 레이어에 자연스럽게 적응하고 "순조롭게" 이뤄진다. 캐노니컬 스택스 체인은 항상 캐노니컬 비트코인 체인에서 찾아볼 수 있으며 스마트 컨트랙트, 트랜잭션 및 페그는 비트코인 포크가 발생하더라도 자동으로 동기화되고 손상되지 않는다. 이러한 특성으로 인해 제안된 스택스 원장의 모든 버전은 모든 포크를 담고 있는 비트코인 메인 체인을 확인하여 완전히 독립적으로 검증될 수 있으며, 이를 통해 추가적인 보안 및 연속성을 갖춘 레이어를 제공할 수 있다. 즉, 사용자는 비트코인 노드를 실행하기만 하면 스택스의 포크 이력이 올바른지 개별적으로 확인할 수 있다.

무신뢰 비트코인 페그는 네이티브 비트코인 스마트 컨트랙트가 이뤄낼 수 있는 것보다 훨씬 더 높은 성능을 가능하게 한다. 더 빠른 스택스 레이어에서 실행되는 스마트 컨트랙트를 통해 빠른-확인과 지연시간이 낮은 블록 (여전히 BTC를 자산으로 사용하고 비트코인 체인에 최종 정산이 됨)을 제공 가능할 뿐만 아닌 수천 건의 스택스 트랜잭션을 단일 해시로 묶어 비트코인에서 처리할 수 있다.

2.2 비트코인과의 시너지 vs 경쟁

스택스 비트코인 레이어는 근본적인 방식으로 비트코인에 의존한다. 동시에 자체 토큰 (STX)을 갖고 있다는 이유로 비트코인에서 가치를 빼앗아온다는 주장도 있다. 이는 ETH 및 비트코인과 경쟁하는 다른 토큰에 해당될 수 있지만, 스택스 레이어의 STX는 비트코인과 경쟁하기 보다 비트코인 생태계를 성장시키는 데 도움을 주기에 해당되지 않는다.

우리는 앞서 STX 토큰이 단순 거버넌스 혹은 투기 목적의 토큰이 아닌 스택스 비트코인 레이어의 합의 메커니즘에 사용되며, 다음 두 가지 주요 기능을 위해 필수적이라 언급했다: (i) (비트코인과 같이) 초기 트랜잭션 수수료가 원장을 유지하기에 충분하지 않기 때문에 새로운 블록 보조금으로써 스택스 블록 채굴을 위한 인센티브를 제공하고, (ii) 경제적으로 안전한 무신뢰 비트코인 페그의 기반이자 활성 인센티브 역할을 한다.

따라서 토큰은 비트코인을 생산적으로 만들어주는 비트코인 애플리케이션 및 기타 스마트 컨트랙트 애플리케이션을 구축하고 성장시키는 데 있어 필수적이다. 이러한 애플리케이션은 **비트코인 수요를 증가시키고 비트코인을 더욱 가치 있게 만들어준다**. 또한 스택스 레이어를 사용하는 비트코인 애플리케이션 및 활동은 **비트코인 채굴자에게 더 높은 수수료를 가져다주며**, 크게 다음과 같이 두 가지 방법이 있다: (a) 애플리케이션은 비트코인 체인에서 수많은 트랜잭션을 발생시키고, 동시에 수수료가 사용되며, (b) 스택스 채굴 및 비트코인 정산은 결과적으로 많은 BTC 트랜잭션과 함께 높은 수수료를 발생시킨다. 특히 비트코인 채굴자를 위한 트랜잭션 수수료 인센티브는 갈수록 중요해지고 있는데, 이는 비트코인 코인베이스 보상 (혹은 '새로운 블록 보조금')이 4년마다 '비트코인 반감기'로 인해 줄어들어 비트코인 채굴자들이 트랜잭션 수수료에 더 많은 의존을 하기 시작했기 때문이다. 그리고 비트코인을 통해 탈중앙화 애플리케이션이 가능해지면 사용자가 비트코인과 경쟁하는 다른 체인 및 암호화폐를 사용해야 할 이유가 줄어들 것이다.

스택스 프로젝트는 비트코인 생태계 구축에 있어 오랜 경력을 가진 개발자와 컴퓨터 과학자들로부터 시작되었다 (일부 스택스 초기 개발자들은 온-체인 비트코인 프로토콜을 기반으로 가장 많이 사용된 초기 OP-RETURN [11]을 구축했다).

2.3 탈중앙화된 무신뢰 양방향 비트코인 페그

비트코인 레이어에서 실행되고 BTC를 자산으로 사용하는 스마트 컨트랙트는 비트코인 상태를 읽을 수 있을 뿐만 아닌 수정 (modify)도 가능해야 한다. 이는 외부 소프트웨어를 통해 개인 키를 사용한 비트코인 트랜잭션 서명이 관리되어야 함을 의미한다. “비트코인 쓰기 (Bitcoin write)”는 (외부) 스마트 컨트랙트로부터 실행된 트랜잭션을 통해 이뤄지기 어렵다. 또한 이러한 방식은 비트코인 체인에서 모든 개별 트랜잭션 및 상태 업데이트를 처리하는 것이 매우 느리며 트랜잭션이 완료될 때까지 많은 시간을 기다려야 한다. 성능을 위해 비트코인 상 전송되는 트랜잭션과 완료까지의 기다림을 줄여야 한다.

페깅 비트코인 자산은 이러한 문제 해결을 목표로 한다. 사용자는 비트코인 체인의 “페그 지갑”에 일정 수량의 BTC를 락업하고 동일한 수량의 페깅 자산을 다른 체인/레이어에 발행한다 (“페그-인”). 발행된 페깅 자산은 (자체 상태를 유지하는) 해당 레이어에서 스마트 컨트랙트를 통해 자주 사용할 수 있으며, 이를 통해 해당 레이어의 상태를 더 높은 성능으로 수정할 수 있다. 원하는 경우 일정 수량의 자산을 소각하고 동일한 수량의 BTC를 비트코인으로부터 돌려받을 수 있다. 즉, 페그 지갑에서 락업 해제되어 지정된 비트코인 주소로 전송된다 (“페그-아웃”). 페그-아웃은 “비트코인 쓰기”를 구현하며 이 전체 구조는 성능을 크게 향상시킬 수 있다.

서명 관리로 인해 페그-아웃은 굉장히 까다로운 작업이다. 이더리움의 wBTC, RSK의 R-BTC, 리퀴드의 L-BTC와 같은 페깅 자산은 타 블록체인 및 비트코인 레이어에서 구현된다. 그러나 이 모든 자산의 페그는 중앙화된 커스터디안 혹은 (멀티시그를 사용하여) 비트코인 페그-아웃 트랜잭션에 서명하는 신뢰할 수 있고 허가된 엔터티 연합에 의해 위임되고 관리된다. 이더리움의 wBTC는 단일 커스터디안에게 위탁되어 비트코인 정신을 위배함에도 불구하고 사용량은 50~150억 달러에 이른다. 이렇게 많은 수량의 BTC (예를 들어 수천억 달러)를 중앙화된 커스터디안 혹은 연합에 의존해서는 안된다.

sBTC는 BTC에 1:1로 페깅된 스택스 비트코인 레이어의 무신뢰 페깅 비트코인 자산으로, 관리를 위해 중앙화되거나 혹은 미리 결정된 엔터티에 의존하지 않는다. 대신 페그 유지 관리에 자유롭게 참여 가능하며 계속해서 변화하는 엔터티로 구성된 무허가 오픈-멤버십 그룹에 의해 탈중앙화된 방법으로 유지 관리된다. 그리고 이들은 페그 유지에 있어 명확한 경제적 인센티브가 주어진다. 이 엔티티는 STX를 락업하거나 “스택 (Stack)”하고 페그-아웃 서명 및 기타 합의에

중요한 작업을 수행하는 PoX 합의 프로토콜의 스태커로; 작업에 대한 댓가로 스태킹한 STX에 비례하여 BTC를 보상받는다. 무신뢰 페그는 스택스 합의 프로토콜 (전송 증명 혹은 PoX)에 통합되며 필요한 인센티브 엔지니어링을 위해 PoX 및 네이티브 STX 토큰에 의존한다. 이러한 무신뢰 비트코인 페그는 해결되지 않은 '성배 (holy grail)' 문제였지만, 이제 sBTC를 통해 BTC를 중앙화된 엔터티에 위탁하지 않고도 스마트 컨트랙트를 통해 생산적인 자산으로 만들 수 있으며, 비트코인 보유자들이 바라던 탈중앙화 대출, 비트코인 기반 스테이블코인 등 고성능의 무신뢰 탈중앙 보안을 갖춘 애플리케이션에 배포될 수 있다.

누구나 스택스 채굴자로 참여할 (혹은 되지 않을) 수 있는 것처럼 누구나 스태커가 될 (혹은 되지 않을) 수 있다. 즉, 누구나 페그-아웃 서명자가 될 수 있다. 올바른 페그-아웃에 서명하고 부합한 페그-아웃에 서명하지 않는 스태커의 정직한 행동은 스태킹된 STX가 담보 역할을 하며 BTC가 인센티브로 보상된다. 이 프로토콜은 성공적인 원장 및 페그를 위한 인센티브 호환 경제 보증을 제공한다: 스택스 채굴자의 경우 캐노니컬 포크에서 채굴하는 것이 항상 인센티브와 호환되며, 스태커의 경우 페그를 충실히 유지하는 것이 항상 가장 높은 수익성을 가져온다. 비트코인의 PoW 정신에 따라, 스태커는 시스템에 긍정적인 기여를 하고 보상을 받을 수 있으며 부적절한 행동에는 경제적 불이익을 받음으로써 행동을 억제당한다 (그러나 지분 증명 시스템과 달리 '슬래싱 (slashed)'이 일어나지 않는다).

페그-아웃은 임계값 서명 메커니즘을 사용한다: 스태킹된 STX의 70%에 해당하는 스태커가 페그-아웃에 서명하는 한 활성이 유지되며, 스태킹된 STX의 최소 31%에 해당하는 스태커가 잘못된 페그-아웃에 서명하지 않는 한 안전이 유지된다 (BTC를 도난당할 수 없으며 쉽게 감지된다). 인센티브 호환성을 감안했을 때 페그 지갑을 공격하기 위해서는 많은 스태커가 악의적으로 결탁하고 경제적으로 비합리적인 행동을 해야 한다. 임의 수량에 대한 페그-아웃은 약 24시간 내로 이행되며, 무신뢰 아토믹 스왑을 통해 BTC/sBTC 페어에 대한 빠른 스왑을 진행할 수 있다. STX 토큰은 무허가 환경에서 sBTC 비트코인 페그를 보호하는 경제적 보장에 있어 필수적이다. 네이티브 토큰이 없는 기존의 사이드체인 (RSK, 리퀴드)에서는 무허가, 무신뢰 페그를 지원할 수 없으며 중앙화된 연합 접근 방식에 의존해야 한다. 스태킹 인센티브는 페그를 유지하는 스태커를 보상하기 때문에 **sBTC는 사용자가 "랩핑 수수료 (wrapping fees)"를 지불할 필요가 없다는 점**이 wBTC를 포함한 다른 페깅 자산과의 주요 차별점이다.

또한 무신뢰 페그는 스택스 비트코인 레이어의 모든 특징과 이점을 상속한다.

2.4 보안 및 포크 규칙

스택스 레이어는 나카모토 릴리즈와 함께 **보안 모델에 대한 주요 업그레이드가 진행된다**. 지금의 스택스는 비트코인과 별도의 보안 예산을 갖고 있다. 이 보안 예산은 스택스 채굴자가 소비한 BTC 자본으로 정의된다. 나카모토 출시와 함께 거의 모든 스택스 체인의 기록이 스택스 채굴 예산과는 관계없이 비트코인 완결성을 갖게 된다: **스택스 레이어는 마지막 150 블록을 제외하고 비트코인 채굴력의 100%로부터 불변성이 보장된다**. 구체적으로 말하자면, 스택스 레이어 블록은 약 150 블록의 확인이 진행되면 (포크와 함께) 비트코인 완결성을 따르게 되며, 150 블록 미만의 블록만 다른 보안 예산을 갖게 된다. 최신 블록의 보안 예산의 경우 채굴자가 사용한 BTC로 시작하여 블록 경과에 따라 스태커가 락업한 자본 (오늘날 수억 달러 상당)이 더해질 것이다. 따라서 스택스 보안의 단계별 기능은 다음과 같다:

- 포크는 6회 정도의 확인 범위 내에서 자유롭게 허용되며, 이는 거래소 및 사람들이 비트코인 블록 완결을 위해 기다리는 시간이다. 이러한 포크는 비트코인의 포크와 같이 가치 있으며, 진행 중인 경쟁 포크를 방지하기 위한 메커니즘이 제공된다.

- 최근 기록 (150 블록 이내)을 공격하려면, 예를 들어 스택스 레이어에 51% 공격을 실행하려면, 공격자는 포크가 공격을 수행하기 위해 상당수의 채굴력과 70%의 스태커를 필요로 한다. 스태커는 비트코인 체인에서 악의적인 행위가 일어나지 않는 한 포크를 허용하지 않는다 (악의적인 행위는 스택스의 비트코인 체인에 대한 초기 및 지속적인 가시성을 통해 미리 인지할 수 있으며 이에 따라 경고될 수 있다). 따라서 스태커의 70% 이상을 해당 포크에 동의시키는 것은 매우 어려운 일이며 이를 위해 수억 달러의 자본을 필요로 한다: 스태커는 스택스 레이어에서 발생하는 악의적인 행위를 극복하기 위해 설계된 포크만을 허가한다.

- 지금까지 스택스 레이어의 대부분의 블록 (약 150 블록 (약 하루) 이상 확인된 블록)은 비트코인 완결성을 따르고 비트코인 해시 파워의 100%에 의해 보호된다. 스택스 기록을 공격하려면 (예를 들어 1일 이상 지난 거래를 변경하려면) 공격자는 비트코인을 심층 재구성 (deep reorg)해야 하며, 이는 비트코인의 해시 파워와 비트코인 채굴의 탈중앙화 정도를 고려했을 때 매우 어려운 일이다.

이 새로운 보안 모델은 스택스 레이어의 주요 업그레이드로, 병합 채굴 (merged mining) 혹은 연합 설계 (federated design) 방식과는 크게 차별된다. 스택스의 포크 규칙은 일반적으로 포크 가능성을 최소화하기 위해 설계되었으며, 채굴자는 특정 공격에 대한 대응으로 체인을 복구하기 위해 특정 조건 하에 포크를 생성할 수 있도록 유연성을 갖추고 있다. 보다 구체적으로 스택스 레이어는 다음 규칙을 따른다:

- 패스트 블록은 두 정산 블록 사이에서 순차적으로 하나씩 생성되며 포크하지 않는다. 순차적으로 생성된 M 크기의 패스트 블록은 다음 정산 스택스 블록 (settlement Stacks block)에 정산된다. 정산 블록을 채굴한 채굴자는 순차적으로 생성된 길이 0에서 M까지의 모든 패스트 블록을 포함할 수 있지만, 모든 정산 블록에 있어 고려해야 할 패스트 블록은 단 하나이다. 정산 블록 채굴자는 가장 긴 패스트 블록을 포함하면 경제적 인센티브를 받는다. 즉, 채굴자는 정산 블록을 채굴할 때 가장 길고 유효한 패스트 블록을 담아야 한다. 정산 블록 채굴자가 더 짧은 패스트 블록을 정산한다면 이는 채굴자가 돈을 버리는 행위이다.

- 포크 규칙은 정산 블록에만 적용되며, 정산 블록에는 순차적으로 생성된 패스트 블록이 포함되어 있다. 즉, 정산 블록은 순차적으로 하나씩 생성된 패스트 블록의 모든 트랜잭션을 패키징하는 것이라 볼 수 있다.

- 만약 (a) 스택스 정산 블록이 150 비트코인 블록 확인이 이뤄지고 (b) 해당 스택스 블록에서 정산된 sBTC 페그-아웃 요청이 성공적으로 스태커에 의해 처리되면, 해당 스택스 정산 블록과 모든 상위 블록은 항상 캐노니컬 스택스 포크에 포함된다. 즉, 스택스 블록은 “완결성”을 갖추게 되며, 이 두 가지 조건이 충족되는 즉시 캐노니컬 포크로부터 포크될 수 없다. 완결성을 갖춘 블록의 모든 상위 블록도 자동으로 완결성을 갖게 된다 (상위 블록에 sBTC 페그-아웃 요청이 없는 경우에도). 완결성을 갖춘 스택스 정산 블록은 비트코인 완결성을 갖추게 된다. 즉, 완결성을 갖춘 스택스 블록의 체인 기록을 수정하는 유일한 방법은 비트코인의 심층 재구성을 수행하는 것뿐이다. 완결성을 갖춘 정산 블록 내 정산된 모든 패스트 블록도 완결성을 갖게 된다. 스택스 레이어의 어떠한 행위도 완결성을 갖춘 스택스 블록체인을 수정할 수 없다.

- 완결성을 갖춘 스택스 블록에서 스택스 포크를 할 수 있는 한 가지 예외의 경우가 존재한다: 가장 마지막으로 완결성을 갖춘 블록, 즉 마지막으로 처리된 페그-아웃 요청이 포함된 블록은 대다수의 스태커 (70% 이상)가 명시적으로 권한을 부여한 경우 새로운 포크를 위해 사용할 수 있다. 이렇게 스택스 블록에서 포크를 생성할 수 있는 권한을 "스태커 블레싱 (Stacker blessing)"이라 한다.

- 주어진 시간 동안 시스템 내 스태커 블레싱은 아예 발생하지 않거나 최대 한번 일어날 수 있다. 스태커 블레싱은 무시하고 넘어갈 수 있으나 활성화되는 경우 블레싱을 사용한 포크가 캐노니컬 포크가 되면 사라진다.

- 채굴자는 깊이 (depth) 6 이하의 스택스 블록을 상위 블록으로 사용하여 자유롭게 새로운 포크를 생성할 수 있다. 채굴자는 이러한 포크를 시작하기 위해 스태커로부터 명시적인 "블레싱 (blessing)"을 받지 않는 한, 깊이 7의 스태스 블록부터 가장 마지막 완결성을 갖춘 블록까지는 상위 블록으로 사용하여 포크를 만들 수 없다. 채굴자는 (스태커 블레싱이 포함된 마지막 완결성을 갖춘 블록을 제외하고) 완결성을 갖춘 블록에서 절대 포크를 만들 수 없다.

포크 규칙을 요약하면 다음과 같다:

1. 스택스 패스트 블록: 포크가 일어나지 않는다.

2. 스택스 정산 블록 깊이 1-6: 채굴자는 이 블록을 사용하여 포크를 자유롭게 생성할 수 있다.

3. 스택스 정산 블록 깊이 7-마지막 완결성을 갖춘 블록이 "동결"시: 채굴자는 블록을 "동결 해제 (unfreeze)"하기 위해 스태커 블레싱을 통해서만 포크 할 수 있다.

4. 그 외 다른 포크는 허용되지 않는다. 즉, 모든 완결성을 갖춘 블록 (마지막 완결성을 갖춘 블록 제외)은 스택스 포크의 상위 블록으로 사용할 수 없다.

일반적으로 사용자는 6 정산 블록보다 깊은 포크를 만나보기 힘들다. 이는 체인이 공격을 받고 스태커를 통해 정직한 채굴자가 체인을 건강한 상태로 복구하는 매우 드문 경우이다. 사실상 이러한 공격은 거의 불가능하다. 위의 단계 (2)은 대부분의 거래소가 트랜잭션 최종 확인을 위해

최소 6회의 정산 확인을 요구하므로 보안 예산과는 무관하다. 비트코인은 6 블록 내 포크가 가능하기 때문에 중요한 트랜잭션의 경우 7회 이상의 정산 확인을 기다려야 한다. 위의 단계 (3)는 대다수의 채굴력과 락업된 스태킹 자본에 따라 보안 예산이 결정된다. 이는 오늘날 수억 달러 규모이다. 위의 단계 (4)은 100% 비트코인 보안이며 가장 강력한 보안이 보장된다. 이는 스택스 레이어 체인 기록에 있는 대부분의 블록에 대한 보안 예산이다. 즉, 스택스 원장의 대부분이 비트코인 메인 체인의 해시 파워로부터 보호된다.

3 스택스 메인 레이어의 성능

2021년 초기 버전의 스택스 레이어는 비트코인과 동일한 속도로 블록을 생성하며, 이는 예측이 불가능하고 느리다 (평균 10분마다 블록 생성). 2023년 출시를 목표로 하는 나카모토 릴리즈의 스택스 레이어는 두 비트코인 블록 사이 패스트 블록을 도입하며, 이는 약 5초마다 새로운 블록을 생성한다. 비트코인 메인 체인에서 이뤄지는 트랜잭션 정산은 여전히 비트코인 블록 속도를 따르지만, 스택스 블록은 대기 시간이 훨씬 짧고 예측 가능하다.

이더리움, 솔라나, 아발란체 등 대부분의 최신 스마트 컨트랙트 레이어1은 지분 증명 (PoS, Proof-of-Stake) 기반 메커니즘을 사용하여 포크 허용 없이 빠른 블록을 생성한다. PoS 접근 방식은 본질적으로 중앙화된 세력이나 하드 포크 없이 특정 실패로부터 복구가 불가능하다는 단점이 존재하나, 이러한 체인은 일반적으로 짧은 대기 시간의 블록 생산이 가능하고 애플리케이션 사용자는 단 몇 초 안에 이뤄지는 트랜잭션 확인을 누릴 수 있다. 반면에 비트코인 작업 증명의 블록 생성은 해시 함수의 임의성을 고려할 때 본질적으로 예측이 불가능하며, 비트코인은 네트워크에 연결된 노드로 블록을 전파하기 위해 충분한 시간을 허용하여 탈중앙화를 최적화했기 때문에 느리다. 또한 비트코인은 포크를 허용하고 네트워크가 단기 포크를 해결할 수 있도록 충분한 시간을 제공한다.

스택스 레이어는 애플리케이션 사용자에게 **비트코인 완결성이 보장되는 빠른 트랜잭션**을 제공하는 것을 목표로 한다. 스택스 블록이 몇 초 만에 생성되므로 사용자는 빠른 확인이 가능하며, 스택스 레이어의 모든 트랜잭션은 결국 백그라운드에서 비트코인에 정산되고 완결성을 갖춰 비트코인 해시 파워 100%로부터 혜택을 받게 된다.

핵심 아이디어는 스택스가 PoX 합의의 고유한 특성을 사용할 수 있다는 것으로, PoX를 통해 스택스와 비트코인 글로벌 원장에 접근할 수 있다. 비트코인 원장에 대한 공개 입찰 프로세스를 통해, 다음 비트코인 블록까지 스택스 블록을 채굴할 수 있는 스택스 채굴자 그룹이 선출된다 (비트코인 평균 블록 시간 10분, 약 120 스택스 블록). 채굴자 세트가 선출되면, 채굴자는 BTC 입찰가에 따라 가중치가 부여된 BFT-스타일 쿼럼 서명 (BFT-style quorum signing)을 사용하여 5초마다 스택스 블록을 생성하고, 이는 **비트코인 블록 사이 시간으로부터 스택스 레이어 대역폭을 분리해준다**. 새로운 채굴자는 모든 비트코인 블록의 스택스 채굴자 세트에 가입할 수 있으며, 이는 스택스 채굴의 오픈-멤버십 특성을 유지시켜 준다.

따라서 나카모토 릴리즈의 스택스 레이어에는 다음과 같이 두 가지 유형의 블록이 존재한다:

- **패스트 블록** (Fast blocks)은 스택스 채굴자의 BFT-스타일 쿼럼 서명 메커니즘을 통해 5초마다 생성된다. 패스트 블록은 새로운 트랜잭션 및 컨트랙트 호출을 포함할 수 있으며 N+1 번째 패스트 블록은 N 번째 패스트 블록 상태를 기반으로 순차적으로 하나씩 패스트 블록을 생성할 수 있다.

- **정산 블록** (Settlement blocks)은 모든 비트코인 블록에서 생성된다. 정산 블록은 새로운 트랜잭션을 포함하지 않고 비트코인 체인에서 순차적으로 생성된 최신의 패스트 블록들만 정산한다. 정산 블록 채굴자들은 비트코인 정산을 위해 가장 긴 패스트 블록을 포함하고 경제적 인센티브를 받는다.

정산 블록 사이 생성되는 패스트 블록은 포크가 허용되지 않는다. 포크는 앞서 언급된 포크 규칙에 따라 정산 블록 수준에서만 허용된다.

3.1 서브넷을 통한 고성능 및 다용성

스택스 비트코인 레이어는 더 높은 성능과 다용성 그리고 보안을 위해 추가적인 기능을 제공한다. 앞서 설명한 성능 메커니즘에도 불구하고 스택스 레이어는 낮은 대기 시간이나 높은 네트워크 처리량 대신 비트코인과 같이 탈중앙화에 최적화되어 있다: 원격으로 노트북 및 인터넷 연결을 사용하는 사용자는 스택스 및 비트코인 풀 노드를 실행할 수 있어야 한다. 그러나 메인 스택스 체인은 **고성능 '서브넷** (Subnets)'을 위한 코디네이팅 레이어 (coordinating layer) 역할도 한다.

또한 서브넷은 스마트 컨트랙트도 지원하며 메인 스텍스 체인이나 다른 서브넷과는 달리 탈중앙화와 성능 간의 절충안을 이뤄낼 수 있다. 게다가 개별 서브넷은 다양한 프로그래밍 언어 및 실행 환경에서 스마트 컨트랙트를 지원할 수 있다. 아래에서 자세히 설명하는 바와 같이, 서브넷은 보안의 이점을 살리기 위해 클래러티 및 클래러티 VM을 지원할 수 있으며, 다른 서브넷을 통해 이더리움의 솔리디티 언어 및 EVM **호환성** 혹은 이더리움 가상 머신과의 호환성을 지원하여 통합 및 개발 용이성을 누리고, 기존의 모든 솔리디티 스마트 컨트랙트를 활용하여 BTC를 자산으로 사용하고 비트코인 블록체인에 정산할 수 있다.

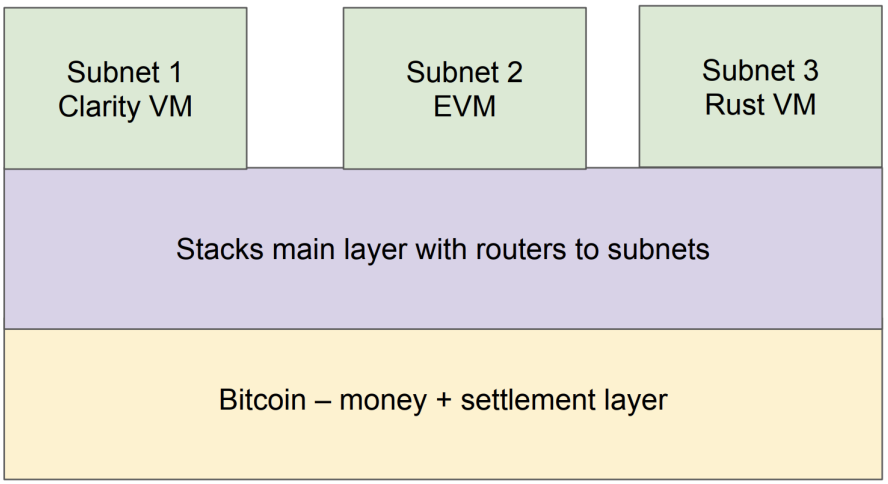

그림 1: 서브넷 및 다양한 VM을 통한 확장성

서브넷은 스택스 비트코인 레이어를 위한 확장성 및 실행 프레임워크이다. 성능 측면에서 애플리케이션은 낮은 대기 시간, 높은 처리량 및 폭발적인 트랜잭션 볼륨을 필요로 하는 상황(예를 들어 NFT 발행)에 따라 각자 필요로 하는 요구 사항이 존재할 수 있다. 서브넷은 스택스 비트코인 레이어를 통해 비트코인 블록체인에서 트랜잭션을 계속 정산함과 동시에, 실행 레이어에서 탈중앙화를 낮추는 대신 높은 처리량을 달성할 수 있도록 설계되어 있다. 빠른 속도와 높은 처리량 (TPS로 측정)을 갖춘 레이어1 스마트 컨트랙트 체인은 고성능 채굴 노드와 데이터센터급 대역폭을 요구하기 때문에 채굴에 있어 다소 중앙화된 모습을 보이고 있다.

스택스 아키텍처는 코어 레이어와 서브넷을 통해 애플리케이션 개발자와 사용자가 탈중앙화되고 처리량이 낮은 실행 (스택스 메인 레이어) 혹은 중앙화되었지만 처리량이 높은 실행 (서브넷) 중 선택할 수 있도록 한다. 서브넷의 채굴자/오퍼레이터는 데이터센터 노드와 같이

채굴자 세트 간 높은 네트워크 대역폭을 요구할 수 있으며, 높은 성능을 위해 서브넷 채굴자 세트를 화이트리스트에 추가할 수 있다.

서브넷은 자산 저장이 아닌 실행을 위해 사용된다. 고성능의 서브넷을 통해 개발자와 사용자는 필요에 따라 높은 처리량을 선택한 뒤 자신이 희망할 때 자산을 코어 스택스 레이어로 출금할 수 있다. 이러한 자산으로 STX 혹은 비트코인-페깅 sBTC 등이 있다. 개념 자체는 비트코인과 스택스 레이어 간의 페깅 BTC 자산을 위한 프레임워크와 유사하다.

또한 서브넷은 동일 혹은 다른 서브넷에 배포를 하여, 다양한 실행 환경을 지원할 수 있다. 예를 들어, 게임 애플리케이션을 별도의 서브넷에 배포할 수 있으며, 이를 통해 나머지 애플리케이션 트래픽으로부터 게임 애플리케이션 네트워크 로드만 분리할 수 있다. 우리는 모듈식 레이어와 서브-네트워크 확장이 확장성을 위한 최선의 길이라 믿는다. 이와 관련하여 우리의 접근 방식은 아발란체의 서브넷 개념과 폴카닷의 파라체인 개념과 유사하다고 말할 수 있다. 하지만 스택스 서브넷의 애플리케이션은 비트코인의 완결 정산 및 보안의 혜택을 받으며, 서브넷에 배포된 스마트 컨트랙트가 네이티브 비트코인 트랜잭션에 의해 트리거 될 수 있도록 비트코인 (스택스 코어 레이어와 같은)과 긴밀하게 통합되어 있고, 스택스 레이어에서 sBTC를 사용하여 비트코인 메인 체인에 쓰기를 트리거 할 수 있다는 점이 차별화된다.

3.2 향후 작업: 비트코인 롤업 및 스택스 레이어

비트코인을 위한 ZK 롤업 (영지식 롤업, ZK rollups)은 흥미로운 연구 분야를 제시하고 있다. 잠재적으로 소프트 포크와 같이 비트코인을 일부 변경함으로써 향후 비트코인 롤업을 활성화시킬 수 있다 [ref]. 전체 실행 환경과 비트코인보다 더 빠른 업그레이드 속도를 갖춘 스택스 레이어는 비트코인 롤업 및 부정 증명 (fraud proofs)과 같은 확장성 기술을 실험하기에 좋은 장소를 제공할 수 있다. 스택스 레이어에 퍼블리싱된 롤업 혹은 부정 증명은 관련 트랜잭션/데이터가 비트코인 완결성에 도달함에 따라 비트코인 해시 파워 100%로부터 이점을 얻을 수 있다. 또한 스택스 레이어는 비트코인 블록체인에 정산됨과 동시에 롤업에 필요한 모든 데이터를 위한 스토리지 레이어 역할을 할 수 있다.

비트코인에 페깅된 sBTC를 사용하는 것을 포함하여, 스택스 레이어 자체에 롤업 및 부정 증명을 배포할 수 있다. 실제로 스택스 레이어를 위한 아비트럼 (Arbitrum) 스타일 부정 증명 프로토타입 구현에 대한 작업이 진행 중이다 [ref]. 무신뢰 비트코인 자산 sBTC는 이러한 롤업 및

부정 증명 시스템과 함께 사용할 수 있으므로, 사용자는 sBTC를 통해 비트코인을 자산으로 사용함과 동시에 롤업 및 부정 증명 (예를 들어, 개인정보보호 및 확장성)의 이점도 누릴 수 있다. 비트코인이 지금까지 신중하고 변경 사항에 대한 채택 속도가 느렸기 때문에 단기적으로 향후 2~3년 동안은 비트코인 블록체인에 직접 롤업을 적용하는 것보다 스택스 레이어를 통한 롤업이 보다 실용적일 것이다. 그러나 장기적으로 보았을 때 비트코인 체인의 BTC 대신 (혹은 추가로) 스택스 레이어에서 sBTC를 통해 롤업을 사용하는 것이 더 유익할 수 있다. 그 이유는 바로 MEV (Maximal Extractable Value) 및 데이터 스토리지 때문이다.

롤업의 MEV 인센티브를 착취하려면 비트코인 수준보다 스택스 롤업의 스택스 레이어 (최소 6 블록까지)에서 트랜잭션 재정렬 (reorderings)/재조직 (reorgs)을 수행하는 것이 더욱 경제적이다. 비트코인 롤업을 직접 사용하면, MEV 인센티브를 비트코인 수준에서 직접 처리해야하므로, 현재 단순한 모습을 보여주고 있는 비트코인의 채굴 인센티브가 보다 복잡해질 수 있다. 예를 들어 스택스 레이어가 sBTC와 함께 롤업을 사용하는 경우 MEV 인센티브나 잠재적인 공격이 비트코인 블록체인에 노출되지 않을 수 있다.

롤업 데이터를 저장하기 위해 메인 비트코인 체인의 크기를 늘리는 것보다 스택스와 같은 외부 레이어를 사용하는 것이 좋다. 롤업 및 부정 증명은 비교적 초기 단계에 있지만 비트코인의 흥미로운 영역으로 남아 있다. 이에 스택스 커뮤니티와 개발자는 sBTC 및 비트코인 완결성을 사용한 스택스 롤업을 이뤄내기 위해 연구 및 프로토타이핑에 집중하고 있다.

4 결론

나카모토 릴리즈를 통해, 스택스 비트코인 레이어는 비트코인을 자산으로 사용하고 비트코인 블록체인에서 트랜잭션의 최종 정산을 수행 가능한 스마트 컨트랙트 및 탈중앙화 애플리케이션을 도입하고자 한다. 스택스는 비트코인의 보안과 내구성을 해칠 필요 없이 생산적인 자산으로 탈바꿈해 주며 탈중앙화 비트코인 대출 및 비트코인 기반 스테이블코인 등 광범위한 애플리케이션을 가능하게 한다. 스택스 레이어를 사용한 애플리케이션은 사람들이 비트코인을 화폐로 사용하고, 비트코인 블록체인을 신원 혹은 애플리케이션 데이터를 위한 정산처로 사용할 수 있다. 이는 비트코인보다 덜 안전한 대체 레이어1 블록체인 및 암호화폐 자산에 대한 사용자의 필요성을 줄여줄 것이다.

스택스 비트코인 레이어의 핵심 요소는 (a) 비트코인 해시 파워 100%로 보호되는 트랜잭션 (비트코인 완결성), (b) 새로운 무신뢰 비트코인 페그, sBTC, (c) 아토믹 BTC 스왑 및 비트코인 주소를 통한 자산 소유, (d) 안전한 프로그래밍 언어, 클래러티, (e) 비트코인 상태 읽기 및 쓰기, (f) 비트코인에 정산되는 확장 가능하고 빠른 트랜잭션이다. 또한 스택스의 PoX 합의는 비트코인과 함께 포크되며 개방형 프로토콜을 위한 긍정적 기여에 BTC를 인센티브로 보상한다.

무신뢰 페그는 약 10년 동안 해결하지 못한 비트코인의 '성배' 문제로, 기존에 존재하던 페그는 커스터디안과 같은 중앙화된 메커니즘과 경제적 보안 없이 잘 알려진 연합의 신뢰에만 의존해 왔다. 스택스의 sBTC 페그는 BTC 및 인센티브 엔지니어링에 1:1로 뒷받침되어 있어 비트코인 수준의 경제적 보안을 사용할 수 있으며, 서명자를 위한 오픈-멤버십을 통해 무신뢰 페그 시스템을 활성화한다. 무신뢰 페그는 안전, 인센티브 호환성 및 활성을 위해 PoX 합의, 비트코인 완결성 및 BTC 보상과 같은 스택스 레이어의 여러 특징에 의존하고 있다. 스택스 레이어만의 고유한 특성이 없었더라면, sBTC와 같은 무신뢰 비트코인 페깅 자산은 상업적으로 실현 불가능하고 인센티브 호환을 이루지 못했을 것이다.

또한 스택스 레이어는 낮은 대기 시간을 위해 패스트 블록 그리고 높은 처리량을 위해 서브넷을 제공한다. 서브넷은 이더리움 가상머신 혹은 EVM의 솔리디티 언어와 같이 다른 언어 및 실행 환경에서 실행되는 스마트 컨트랙트를 가능하게 하며, 앞으로 친숙한 통합 및 개발이 허용됨과 동시에 비트코인을 화폐로 사용하고 비트코인 블록체인을 통한 정산이 가능해질 것이다.

참고문헌

[1] Clarity: A decidable language for smart contract. https://clarity-lang.org/.

[2] Magic protocol for atomic swaps with BTC and Stacks. https://magicstx.gitbook.io/magic-protocol/overview/magic-protocol.

[3] SIP-21 Improvement Proposal. https://github.com/stacksgov/sips/pull/113.

[4] Stacks on chain: State of the network. https://stacksonchain.com/dashboards/State-of-the-Network/16.

[5] tBTC: A Decentralized Redeemable BTC-backed ERC-20 Token. https://docs.keep.network/tbtc/index.pdf.

[6] sBTC: A decentralized two-way peg for bitcoin, Dec 2022. https://stx.is/sbtc-pdf.

[7] Muneeb Ali. Trust-to-Trust Design of a New Internet. PhD thesis, Princeton University, 2017. https://www.cs.princeton.edu/research/techreps/TR-003-17.

[8] Muneeb Ali. Bitcoin DeFi is here: A deep dive into trust-less swaps, 2021. https://www.hiro.so/blog/bitcoin-defi-is-here-a-deep-dive-into-trust-less-swaps.

[9] Vitalik Buterin. A next-generation smart contract and decentralized application platform. Technical report, 2014. https://ethereum.org/en/whitepaper/.

[10] John Light. Validity rollups on bitcoin, 2021. https://bitcoinrollups.org/.

[11] Jude Nelson, Muneeb Ali, Ryan Shea, and Michael J Freedman. Extending existing blockchains with virtualchain. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)*, Chicago, IL, June 2016.

[12] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Tech report, 2009. https://bitcoin.org/bitcoin.pdf.