sBTC: 비트코인을 위한 무신뢰 양방향 페그 디자인

2022년 12월 14일

Translated by GM Chung | gm@despread.io

비트코인을 완전히 프로그래밍 가능하고 생산적인 자산으로 탈바꿈할 수 있다면, 비트코인은 탈중앙화 금융과 보다 안전한 웹3를 위한 중추가 될 수 있다. 비트코인 자산을 스마트 컨트랙트 안팎으로 자유롭게 이동하고 이때 사용한 계약을 신뢰 필요 없이 (trustlessly) 비트코인 블록체인에 쓸 (write)수 있다면, 이는 수천억 달러의 잠재 자본을 웹3 세상으로 끌어낼 것이다. 본 백서에서는 신뢰를 필요로 하지 않는 새로운 비트코인 페그 (novel trustless Bitcoin peg) 메커니즘을 제시한다. 이 무신뢰 페그 (trustless peg)를 사용하면 비트코인 레이어 상에 메인 비트코인 체인의 BTC와 1:1로 페깅된 BTC-페깅 (BTC-pegged) 자산을 발행할 수 있으며, 발행된 자산의 기능은 중앙화되거나 사전에 결정된 행위자에게 의존하지 않는다. 대신, 페그 메커니즘은 계속해서 변화하는 행위자들로 이뤄진 무허가 오픈-멤버십 (permissionless open-membership) 그룹에 의해 탈중앙화된 방식으로 작동되며, 이 행위자들은 경제적 인센티브를 받고 언제든지 페그 기능 기여를 시작 혹은 중단할 수 있다.

무신뢰 양방향 비트코인 페그 (Trustless two-way Bitcoin peg)는 지금까지 비트코인에 무신뢰 쓰기가 불가능했기 때문에 비트코인 생태계가 해결하지 못한 '성배 (holy grail)' 문제이다. 무신뢰 페그는 BTC를 중앙화된 엔터티에 위탁할 필요 없이 생산적인 자산으로 만들어주며 탈중앙화된 비트코인 대출, 비트코인 담보 스테이블코인 등 다양한 애플리케이션에 배포될 수 있다. 이더리움 상의 랩핑된 비트코인 자산 (wBTC)은 단일 커스터디안에게 맡겨지기에 비트코인 정신과는 위배되지만, 그럼에도 불구하고 사용량은 50~150억 달러에 이른다. 우리는 sBTC라 칭하는 비트코인-페깅 자산의 설계에 대해 서술하고자 한다. 이는 높은 성능과 탈중앙화된

보안을 제공하기 위해 스택스 비트코인 레이어와 비트코인 레이어1 간의 고유한 상호 작용을 사용해 구현한 무신뢰 페그 메커니즘이다.

비트코인은 가장 탈중앙화되고 안전하며 높은 내구력을 지닌 블록체인이다. BTC는 업계에서 찾아볼 수 있는 독특하고 가치 있는 자산이며, 비트코인 블록체인은 거래를 위한 단연 최고의 최종 정산 (settlement) 레이어이다. 비트코인의 베이스 레이어를 살펴보면 단순함과 탈중앙화를 위해 최적화되어있음을 찾아볼 수 있다 [8]; 비트코인은 설계상 상대적으로 느리며 기본적으로 정교한 애플리케이션 구축을 위해 필요로 하는 완전 표현형 스마트 컨트랙트를 제공하지 않는다. 때문에 보다 빠르고 정교한 애플리케이션은 베이스 레이어 외부에서 구축되어야 한다. 비트코인 레이어는 필요에 따라 비트코인 체인과 상호 작용하고 베이스 레이어 외부에서 높은 성능과 고급 기능을 제공할 수 있다. (이때 '비트코인 레이어'는 레이어1 외부의 기능 레이어를 의미하는 용어로, 정의에 따라 레이어2, 사이드체인 [6] 개념 등이 포함된다.) 비트코인 레이어가 제공하는 기능의 예로 빠른 결제 (Lightning), 자산 발행 (Liquid) 그리고 스마트 컨트랙트 (Stacks 및 RSK)가 있다.

이상적인 비트코인 레이어는 다음과 같은 세 가지 특징이 필요하다:

1. 개발자들이 탈중앙화된 방식으로 정교한 애플리케이션을 구축하도록 도와주는, 글로벌 원장을 갖춘 완전 표현형 스마트 컨트랙트.

2. 안전하고 무신뢰 방식으로 프로그래밍을 통한 비트코인 쓰기를 사용하여 BTC를 레이어 안팎으로 쉽게 이동하는 기능.

3. 베이스 레이어 (비트코인) 보안의 100%가 뒷받침되는 높은 보안을 갖춘 트랜잭션.

비트코인 레이어는 지금까지 눈에 띄는 진전을 이뤄왔지만, 2022년 현존하는 비트코인 레이어에는 몇 제한 사항이 존재한다: 라이트닝 (Lightning)은 전체 스마트 컨트랙트나 (불변 기록을 위한) 글로벌 원장이 존재하지 않으며, 리퀴드 (Liquid)와 RSK는 페그 연합 (federated pegs)이 존재하나 비트코인 정산 과정이 없고, 초기 버전의 스택스 (Stacks)에는 무신뢰 비트코인 페그가 없다. 반대로, 현재의 이더리움 레이어는 ETH가 앞서 언급한 세 가지 특징을 모두 갖추고 있으며 근래 사용자와 자본이 크게 증가했다. 이더리움의 경우 다양한 레이어가 주로 확장성을

위해 사용되지만, 비트코인의 경우 베이스 레이어의 제한된 기능을 감안했을 때 레이어의 중요성은 더욱 클 수 밖에 없다; 즉 비트코인 레이어는 확장성과 새로운 기능 모두를 필요로 한다.

sBTC 작업을 통해 이상적인 비트코인 레이어 구축에 한층 가까워질 수 있다. 사용자는 비트코인 레이어에서 전체 스마트 컨트랙트에 접근할 수 있을 뿐만 아닌 탈중앙화된 방법으로 레이어 안팎으로 BTC를 쉽게 이동할 수 있다. 이때, 레이어 트랜잭션은 비트코인 레이어1 보안으로 100% 보호된다. 무신뢰 페그 메커니즘은 비트코인 경제 성장을 빠르게 가속시켜줄 비트코인 애플리케이션의 새로운 시대를 열어줄 것이다.

본 백서에 소개된 sBTC 무신뢰 페그를 고유하게 만들어주는 특징은 다음과 같다:

- **개방형 및 탈중앙화** (Open and decentralized): 페그는 사전에 결정된 연합 혹은 중앙화된 집단이 아닌, 계속해서 변화하는 서명자들로 이뤄진 오픈-멤버십 집단에 의해 유지 관리된다.

- **검열 저항성** (Censorship resistant): 서명자 선택, 페그-아웃 요청 등 페그 관련 작업은 비트코인 메인 체인에서 발생하며 비트코인의 검열 저항성을 따른다. 즉, 스택스 레이어 상에 있는 외부 행위자는 관련 작업을 검열할 수 없다.

- **저렴한 페그 인/아웃** (Cheap peg in/out): 임계값 서명자는 스택스 레이어 합의로부터 발생한 BTC 보상을 인센티브로 받으며, 이는 추가적인 페그 수수료를 도입할 필요 없이 참여를 위한 강력한 경제적 인센티브로 작용한다.

- **온-체인 비트코인 오라클** (On-chain Bitcoin oracle): 비트코인 레이어1 상에서 온체인으로 구현된 고유한 가격 오라클을 사용하므로 페그 작업을 위해 외부 오라클에 의존하지 않는다.

- **비트코인 보안** (Bitcoin security): 스택스 레이어와 페그 상태는 비트코인 레이어1과 함께 자동으로 포크 (fork)되고, 100% 비트코인 완결성과 함께 비트코인 레이어1에서 발생한 모든 트랜잭션을 자동으로 정산 (settle)하여, 강력한 보안을 보장한다.

- **상업적 발전 가능성** (Commercially viable): 실제 참여 데이터에 따라 최근 스택스 합의에 락업된 자본을 감안했을 때 sBTC가 수억에서 수십억 달러의 유통량에 도달 가능하며, 이는 충분히 sBTC가 상업적으로 발전 및 확장 가능하다.

레이어 안팎으로 BTC의 무신뢰 이동을 가능하게 하는 것 외에도, 페그 메커니즘을 통해 레이어 상의 스마트 컨트랙트를 무신뢰 방식으로 비트코인에 쓸 수 있다. **비트코인 쓰기 기능** (Bitcoin write functionality)은 개발자를 위한 주요 신규 기능으로 무신뢰 페그를 통해 BTC를 프로그래밍하여 비트코인 주소로 전송할 수 있는 스마트 컨트랙트를 구축할 수 있다.

1 무신뢰 비트코인 페그

스마트 컨트랙트는 보안 및 성능상의 이유로 비트코인 베이스 레이어에서 실행해서는 안 된다; 베이스 레이어는 단순함을 유지해야 한다. 우리는 스택스 블록체인 레이어를 사용한 무신뢰 오픈-멤버십 비트코인 페그 메커니즘을 제시한다: BTC는 비트코인 메인 체인에 락업하고 BTC와 가치가 1:1로 페깅된 sBTC라 불리는 동일한 수량의 파생 자산을 스택스 레이어에 발행한다. 스마트 컨트랙트는 sBTC를 사용하여 실행 가능하며 원하는 경우 sBTC를 다시 BTC로 되돌릴 수 있다 (즉, sBTC를 소각하고 동일한 양의 BTC가 비트코인 체인에 자동으로 릴리즈된다). 스마트 컨트랙트는 프로그래밍을 통해 sBTC (BTC 페그)를 BTC 주소로 전송할 수 있다. 이는 비트코인 메인 체인 외부 컨트랙트를 프로그래밍하여 비트코인 메인 체인에 효과적으로 쓸 수 있음을 의미하며, 즉 "비트코인 쓰기 (Bitcoin write)" 문제를 해결할 수 있다.

본 백서를 읽는다면 나카모토 (Nakamoto) 릴리즈 및 비트코인 완결성 (finality)을 사용하여 최신 보안 모델을 다루고 있는 최신 버전의 **스택스 백서** [4]를 참고하길 바란다.

sBTC 접근 방식은 스마트 컨트랙트를 통해 비트코인을 금전적 자산으로 사용하게 해주고 동시에 스택스 레이어에서 보다 빠르고 저렴한 거래를 할 수 있다. 이미 구현되어 있는 BTC 파생 페깅 자산은 다음과 같다: 이더리움의 wBTC, RSK의 R-BTC, 리퀴드의 L-BTC. 하지만 이러한 자산의 경우 페그는 중앙화된 커스터디안 혹은 신뢰를 필요로 하는 엔터티 연합에 의해 관리되고 위임된다. sBTC는 신뢰를 필요로 하지 않는 페깅된 BTC 자산으로, 페그가 잘 유지되도록 명확한 경제적 인센티브가 있는 무허가 (permissionless)이자 탈중앙화 (decentralized)되고 변화 (dynamic)하는 참여자로 구성된 집단에 의해 관리된다.

무신뢰 비트코인 페그는 BTC를 중앙화된 엔터티에 위탁하지 않고 컨트랙트를 통해 배포하여 수익 창출을 위한 생산적인 자산으로 만들고자 한다. 이를 통해 스마트 컨트랙트에 신뢰를 필요 없이 배포되는 수천억 달러의 BTC를 가져옴으로써 탈중앙화 비트코인 대출,

비트코인 담보 스테이블코인 등 비트코인 보유자가 바라던 무신뢰 방식과 탈중앙화된 보안을 갖춘 애플리케이션을 실현하고자 한다.

sBTC의 무신뢰 페그는 스택스 레이어의 고유한 특징 및 스택스와 비트코인 간 연결을 통해 가능하다:

- 스택스 레이어에는 고유한 합의 프로토콜인 전송 증명 (PoX, Proof of Transfer)이 존재하며, 이는 비트코인의 작업 증명 (PoW) 프로토콜을 활용함과 동시에 sBTC를 지원한다. PoX에서 스태커 (Stacker)는 자본을 락업하고 페그-아웃 트랜잭션에 임계값 서명 작업을 수행하면 보상으로 BTC를 받을 수 있다. 스택스 채굴자는 BTC를 사용하여 스택스 블록을 채굴하고, 사용된 BTC는 스태커에게 보상으로 분배된다. 이는 **성공적인 페그를 위한 인센티브-호환 경제적 보장**이 가능하다: 스택스 채굴자는 캐노니컬 (canonical) 포크에서 채굴하는 것이 인센티브와 호환되며, 스태커는 페그를 충실히 유지하는 것이 항상 가장 높은 수익성으로 이어진다.

- 스태커는 이미 코어 합의 프로토콜로부터 보상을 받기 때문에, 정상 작동 중 BTC를 안팎으로 페깅하더라도 **사용자는 "랩핑 수수료 (wrapping fees)"를 지불할 필요가 없다**; 즉 프로토콜 보상이 경제적 인센티브를 제공한다. (wBTC의 경우와 같이) 보관 시스템의 랩핑 수수료가 높아지기 때문에 이는 중요한 이점으로 작용한다.

- 스택스에는 포크 위험이 없다. **스택스 레이어는 비트코인 메인 체인과 자동으로 "함께 포크"한다.** 즉, 비트코인이 포크되면 스택스도 이에 따라 포크한다. 이는 비트코인이 포크되거나 재구성 (reorganize)되더라도 페그 작업, 페그 지갑 및 스태커 세트 변경으로 인한 영향이 스택스 체인 (해당 스택스 포크)에 반영됨을 의미한다. 이 작업은 해당 포크의 sBTC 상태와 일치하는 경우에만 특정 스택스 포크에 반영된다. 그 결과 채굴과 스태킹 모두 오픈-멤버십이지만, 포크로 인해 페그가 손상되지 않는다. 따라서 스태커는 포크로 인해 돈을 잃지 않고 포크는 사용자의 BTC 안전에 위험을 초래하지 않는다. 이는 비트코인으로 포크하지 않는 이더리움 [7]과 같은 체인에 페깅된 BTC 자산에는 해당되지 않는다: 또한 비트코인 재구성 (reorg)은 랩핑된 BTC의 상태를 캐노니컬 비트코인 포크와 일치하지 않게 할 수 있으므로, 별도의 개입이 필요하다.

- **스태커라 불리는 임계값 서명자 세트는 시스템 활성을 유지하고 작업에 대한 BTC 보상**을 통해 페그-아웃 요청에 서명하고 인센티브를 받는다. 스택스 합의 참여를 통한 BTC 보상은 스택스 레이어의 고유한 특징이다.

- 스택스 상의 컨트랙트는 비트코인 트랜잭션을 읽고 처리할 수 있기 때문에 임계값 서명자 세트는 비트코인 트랜잭션을 통해 선출된다. 이는 스택스 채굴자가 스태커 선출을 검열할 수 없음을 의미한다. 마찬가지로 BTC 페그-아웃 요청도 비트코인 트랜잭션을 통해 브로드캐스트되며 스택스 채굴자는 수익 손실 없이는 이러한 요청을 무시할 수 없다.

- 이 시스템은 스태커의 BTC 지불금을 활성 복구 메커니즘으로 사용한다. 스태커가 적시에 페그-아웃 요청에 서명하지 못한 경우 일부 BTC 지불금이 페그-아웃 요청을 이행하기 위해 사용된다.

sBTC 설계는 오늘날 수억 달러 상당의 BTC를 sBTC 유통량으로 확장하고 잠재적으로 향후 수백억 달러 상당의 sBTC 유통을 이룰 수 있기 때문에 상업적으로 발전 가능하다. sBTC 공급 상한선은 락업된 STX 자본의 경제적 규모에 따라 결정되며, 이는 아래 내용에서 활성 보장(liveness guarantee)이라 설명한다. 스택스를 통해 구축된 애플리케이션의 경제가 성장하고 스택스 컨트랙트를 통해 더 많은 비트코인이 생산적이게 됨에 따라, sBTC 유통 한도는 점차 증가할 것이다.

sBTC 설계는 커스터디안 혹은 신뢰를 필요로 하는 중앙화된/연합된 당사자를 중개인으로 도입하지 않는다. 수십억 달러 상당의 BTC가 페그-인 시스템을 통해 스마트 컨트랙트에 사용되려면, 시스템에 중앙화된/연합된 신뢰가 존재하지 않는 것이 중요하다. 리퀴드 혹은 RSK와 같이 이전에 존재하던 비트코인을 위한 페그 시스템은 연합 구성원의 정직한 행동 보증에 있어 어떠한 담보 제공도 없이 그저 연합 신뢰에만 의존해야 했다. sBTC 시스템은 (a) 오픈-멤버십, 누구나 시스템에 쉽게 가입 가능하며 페그-아웃 트랜잭션의 서명자가 될 수 있으며 (b) 페그-아웃 서명자는 시스템 활성 유지를 위해 서명자에게 강력한 경제적 인센티브를 제공하는 BTC 가치보다 더 많은 담보를 락업해야 한다는 점에 있어 연합형 페그 시스템과 차별된다 (담보는 서명자가 보류 중인 모든 페그-아웃 요청을 처리할 때까지 해제되지 않는다).

새로운 sBTC를 발행하는 유일한 방법은 비트코인 메인 체인의 스크립트에 동일한 수량의 BTC를 예치하는 것이다. 시스템은 항상 1:1로 BTC:sBTC 비율을 유지하며 누구나 공개

시스템을 모니터링하여 1:1 비율이 유지되고 있는지 확인 가능하다. 이는 BTC 보유량에 대한 증거가 덜 투명한 wBTC와 같은 커스터디안의 접근 방식과는 다르다. 또한, sBTC의 비트코인 메인 체인의 비트코인 스크립트/지갑은 단일 엔터티 혹은 고정 연합과 비교했을 때 탈중앙화 되었으며 오픈-멤버십 그룹에 의해 관리된다. 임계값 서명자는 페그 활성 상태 유지를 위해 경제적 인센티브 즉, 페그-아웃 트랜잭션에 계속해서 서명한다.

sBTC 설계에는 페그 인/아웃 수수료가 포함되어 있지 않으며 (정상 작동 시), 사용자가 원하는 만큼 언제든지 시스템에 페그 인 및 아웃이 가능하다. 사용자는 페그 시스템 사용 시 각각의 비트코인 메인 체인 트랜잭션 수수료만 지불하면 된다. 이더리움의 wBTC와 같은 랩핑된 비트코인 설계에는 일반적으로 랩핑/언랩핑 기능에 대한 수수료가 존재한다. 이 수수료는 랩핑 기능을 수행하고 시스템을 유지 관리하는 커스터디안의 비즈니스 유지를 위해 필요로 한다. sBTC 설계는 서명자에 대한 인센티브로 스택스 합의로부터 발생한 BTC 보상을 사용하며 추가적인 페그 수수료 인센티브가 필요로 하지 않는다. 서명자에게는 높은 비율 (락업된 자본 기준 7-8% [3])의 인센티브가 제공되는 반면, 페그 인/아웃 기능은 사용자에게 무료로 유지된다 (BTC 수량에 관계없이 가스 수수료만 지불). 건전한 비율로 경제적 보안을 유지하기에 sBTC 유통량이 너무 높아지는 경우 안전한 마진 내 sBTC 유통량을 유지하기 위해 페그-인에 대한 수수료 구조가 도입된다. 이 주제에 대해서는 “sBTC 유통량” 세션에서 보다 상세히 다뤄진다.

2 sBTC 설계 세부 사항

sBTC 시스템은 캐노니컬 (즉, 기본 (main) 및 유효 (valid)) 스택스 포크에서 채굴과 인센티브 호환이 되도록 설계되었으며, 스태커가 높은 수익을 유지하는 행위는 항상 페그를 충실하게 유지하는 것이다. sBTC에는 두 가지 작동 모드가 존재한다: 일반 모드, 그리고 복구 모드. **일반 모드 (Normal Mode)**는 앞서 설명한 바와 같다: 사용자는 스태커의 락업한 STX 비율을 반영한 임계값 비율에 의해 제어되는 비트코인 체인의 페그 지갑/스크립트로 전송된 BTC를 보낸다. BTC가 이 지갑으로 전송될 때마다 (페그-인 작업) 동일한 수량의 sBTC가 발신자가 선택한 주소로 발행되어 1:1 페그를 유지한다. 유효한 페그-아웃 작업에서 스택커의 임계값 비율은 비트코인 메인 체인의 임계값-서명 게이트 트랜잭션을 통해 페그 지갑/스크립트에서 요청된

비트코인 주소로 원하는 수량의 BTC를 전송하여 페그-아웃을 실행한다. 그다음 프로토콜은 스택스 측에서 동일한 양의 sBTC를 소각한다.

일반 모드에서 어떠한 이유로 활성 실패 (BTC 손실 포함)가 발생하면 일정 수의 스태커가 다시 온라인 상태가 되어 서명 페그-아웃 요청을 재개할 때까지 시스템은 복구 모드로 전환된다. **복구 모드** (Recovery mode)에서 스태커가 획득한 PoX 지불금의 일부가 페그-아웃 요청을 이행하도록 리디렉션되어 스태커가 다시 온라인 상태가 되지 않더라도 결국 모든 미결제 상태의 페그-아웃 요청이 이행된다. 일반 모드 대비 느리지만 복구 모드의 설계는 스택스 레이어가 살아 있고 PoX 채굴이 계속해서 이뤄지는 이상 사용자의 BTC는 되찾을 수 있도록 보장된다. 복구 모드는 스태커가 적시에 페그-아웃 요청을 이행하도록 하는 경제적 인센티브 역할을 수행하며, 그렇지 않을 경우 BTC 보상을 잃게 된다. 복구 모드를 통해 sBTC의 전체 유통량을 복구하는 것은 PoX로부터 발생한 BTC 보상 크기에 따라 결정되기 때문에 매우 느린 과정이 될 수 있다.

sBTC 설계의 주요 안전 가정은 스태커가 악의적으로 행동하여 얻을 수 있는 것보다 훨씬 더 많은 돈을 잃을 수 있다는 점을 감안했을 때 스태커에게 경제적으로 합리적인 선택지는 항상 페그를 이행하는 것이다. 또한 페그에 대한 공격을 시도하기 위해 70%의 서명 임계값 수준을 달성해야 하며 이는 수많은 탈중앙화된 참가자들이 결탁하거나 타협해야 함을 의미한다.

일반 및 복구 모드의 설계는 스택스 채굴자, 스태커 그리고 사용자에 대한 인센티브를 신중하게 고려해야 한다. 페그 운영이 캐노니컬 스택스 포크에서 채굴과 인센티브 호환이 유지되도록 하기 위해, 나카모토 릴리즈 제안 [4]에는 스택스 레이어 메인넷 출시와 함께 2021년 출시된 PoX 합의 알고리즘에 대한 중요 업데이트가 포함되어 있다.

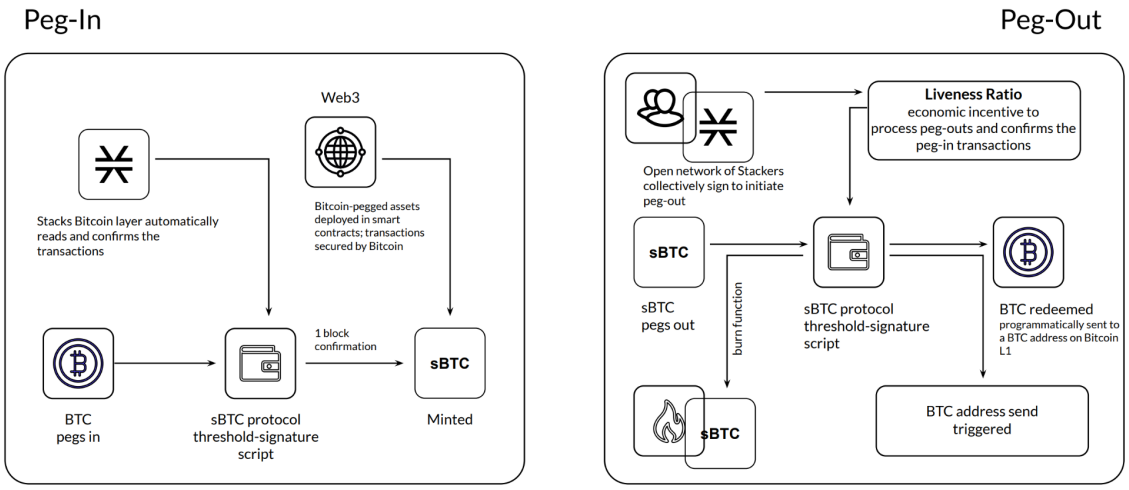

그림 1: sBTC 페그-인 및 페그-아웃 작업

PoX를 사용한 sBTC 설계에서 **스태커는** STX가 락업된 각 보상 사이클 동안 **PoX 보상을 받고 BTC 스크립트/지갑을 공동으로 (collectively) 유지하기 위해 적극적으로 작업을 수행해야 한다**. 이 지갑은 페그-아웃 요청을 위해 사용되며, 스태커가 적시에 이를 수행하지 못하면 STX 토큰이 락업된 상태를 유지하고 모든 페그-아웃 요청이 이뤄질 때까지 PoX 보상을 받지 못한다. 대신, 이들의 PoX 보상은 페그-아웃 요청 이행으로 리디렉션된다.

sBTC 출시와 함께 **모든 스택킹 관련 트랜잭션과 모든 페그 트랜잭션은 비트코인 트랜잭션 형태로 비트코인 체인을 통해 브로드캐스트 되어야 한다**. 그 이유는 관련 작업이 모든 잠재적인 스택스 포크로부터 이뤄져야하기 때문이다. 때문에 스택스 채굴자는 누군가가 스태킹에 참여하고 페그 참여자가 되는 것을 검열할 수 없다. 대신 스택스 채굴자가 새로운 스택스 블록을 생성하면, 비트코인으로부터 브로드캐스트되는 페그 및 스태킹 작업이 가능한 모든 포크에 자동으로 포함된다. 이는 채굴자가 스태킹 및 sBTC 활동을 무시하는 블록을 생성하는 것을 방지하며, 때문에 이를 수행하지 못한 블록은 새로운 합의 규칙에서 유효하지 않게 된다.

또한 sBTC 설계를 통해 스택스는 주요 보안 예산 업그레이드를 받게 되며, 이때 임의 길이의 포크는 제거되고 스택스 트랜잭션은 150 블록 후 비트코인 완결성을 따르게 된다. 이는 **비트코인 완결성 (일반적으로 24시간 이내)에 도달하는 모든 스택스 레이어 작업이 스택스 레이어를 통해 포크될 수 없음**을 의미한다; 트랜잭션을 변경하는 유일한 방법은 150 깊이 (depths) 이상에 대해 매우 비싸고 비실용적인 비트코인의 심층 재구성을 시도하는 것이다. 또한 7 깊이의 스택스 포크는 대부분 스택스 채굴력 (mining power)과 대부분의 스태킹 서명을 필요로 하므로, 이러한 포크를 구현하기는 어려울 것이다. 마지막으로 비트코인 완결성으로 인해 PoX 앵커 블록의 기록은 절대 포크되지 않을 것이다. 복구 모드를 올바르게 구현하기 위해선 이러한 새로운 특징을 필요로 한다.

sBTC 출시와 함께 스택스 채굴자 집단과 이들이 커밋할 최소 BTC 금액은 다음 스택스 블록을 채굴하기 전 미리 알 수 있게 된다. 이를 위해 **스택스 레이어는 각 채굴자가 다음 비트코인 블록에 사용할 BTC 수량을 추가로 커밋하도록 요구하게 한다**. 만약 이들의 다음 블록-커밋에 정확한 금액이 커밋되지 않으면, 블록 커밋은 무효된다. 우리는 이를 블록 사전-커밋 (pre-commit)이라 한다. 또한 블록 사전-커밋은 패스트 블록 (fast blocks) 기능을 가능하게 한다. 패스트 블록은 스택스 채굴자 집단이 오픈-멤버십을 유지한채 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) 패스트 블록을 생성할 수 있다.

2.1 임계값 서명 지갑

스택스를 위한 비-수탁 비트코인 페그 설계의 핵심은 비트코인 메인 체인에서 유지 관리되는 임계값 서명 기반 지갑/스크립트이다. 지갑 자금은 임계값 서명 메커니즘에 의해 제어된다. 주어진 사이클 (일반적으로 2주)에서의 잠재적 서명자는 PoX 합의에 참여하기 위해 STX를 (무허가 방식으로) 락업한 스태커로, 해당 사이클 동안 페그-아웃 서명 작업을 수행하고 BTC 보상을 받는다. 페그 지갑 스크립트에서 서명자의 서명 파워 (signing power)는 PoX에 락업된 자본에 따라 상대적으로 결정된다. 유효한 서명에는 높은 임계값이 적용된다: 페그 지갑 스크립트에서 BTC 자금을 성공적으로 이동하려면 페그 아웃 트랜잭션에 70% 이상의 서명 권한이 필요로 한다. 또한 이는 페그 지갑을 공격하려면 스태커의 70%가 악의적으로 결탁하고 경제적으로 비합리적이어야 하며, 적어도 30%의 스태킹 파워에 대한 정직한 페그 지갑의 자금에는 피해를 줄 수 없다. 스태킹 파워와 스태커는 매 스태킹 사이클 (일반적으로 2주)마다 변경될 수 있기 때문에, 스태킹 사이클마다 고유한 스크립트/지갑이 사용된다.

스태커가 비트코인 트랜잭션을 통해 자본을 락업할 때 트랜잭션에 서명 비트코인 퍼블릭 키 (signatory Bticoin public key)를 포함한다. 이때 포함되는 퍼블릭 키는 PoX 컨트랙트에 등록되며, (스태킹 사이클 시작 시) PoX 앵커 블록이 채굴될 때 모든 스태커의 퍼블릭 키가 PoX 보상 세트의 일부로 발표된다. 서명 퍼블릭 키 (Signatory public key)는 결정적 방식 (deterministic manner)으로 합쳐져 스태킹 사이클을 위한 페그 지갑 주소를 생성할 수 있다. 각 스태커는 매 사이클마다 고유한 서명 퍼블릭 키를 갖는다 (서명 키는 여러 사이클에서 재사용 가능한 스태커의 BTC 보상 주소와 다르다).

스태킹 사이클이 종료되면 스태커는 다음 사이클의 페그 지갑 주소를 알게 되며, 페그 활성 유지를 위해 프로토콜 규칙의 일부로 현재 만료된 페그 지갑 주소에서 새로운 페그 지갑 주소로 남아 있는 모든 BTC를 전송해야 한다. 페그 지갑은 경제적 보안 (economic security)을 활용한다: 스태커는 페그 지갑의 BTC 가치보다 200% 더 많은 자본을 락업해야하며, 페그 활성

상태를 계속 유지하고 모든 페그-아웃 요청 및 지갑 로테이션이 완료될 때까지 스태커들의 BTC 보상 지급이 보류되며 자본은 합의에 락업된 상태를 유지한다.

페그 설계에 있어 중요한 것은 주어진 사이클 동안 어떠한 이유로 서명자의 70% 임계값을 충족할 수 없는 경우 (예를 들어, 서명자가 장기간 오프라인 상태이거나 트랜잭션 서명을 거부하는 경우)를 위한 백업 메커니즘이다. 현재 제안은 특정 수의 블록이 통과한 뒤 자동으로 활성화되는 사이클 지갑에 명시적인 백업 스크립트를 인코딩하는 것이다. 한 접근 방식은 백업으로 낮은 수준에서 임계값을 충족할 수 있는지 확인하기 위해 복구에 대한 70% 임계값을 점진적으로 낮추는 것이다. 또 다른 제안은 이전 스태킹 사이클의 서명자를 활용하여 특정 시간 이후 페그-아웃에 서명할 수 있도록 하는 것이다. 백업 스크립트 구성 및 선택 규칙에 관한 자세한 내용은 이곳 [2]에 설명되어 있다.

sBTC 설계, 페그-인 및 페그-아웃 작업, PoX 합의 알고리즘과의 상호 작용, 일반 및 복구 모드, 서명자 선택 및 백업 등 관련한 자세한 프로토콜 스펙은 SIP-21 [2]을 통해 확인할 수 있다. 본 백서에서는 세부적인 프로토콜 사양보다 더 높은 수준의 설계에 중점을 두고 있다.

2.2 sBTC 유통량

sBTC는 비트코인 메인체인에서 BTC를 1:1로 락업하고 발행된다. 이론적으로 sBTC의 유통량은 스크립트/지갑에 예치된 총 BTC 수량과 같아야 한다. 그러나 설계 인센티브를 호환 가능하게 유지하기 위해 우리는 sBTC의 최대 유통량에 엄격한 제한을 두고 있다: sBTC의 총 유통량은 스태킹에 참여한 STX 자본 가치의 일정 수준을 초과할 수 없다 (기본값으로 60%). 예를 들어, $200M 상당의 STX가 스태킹에 락업되어 있는 경우 sBTC의 최대 유통량은 $120M이 될 수 있다. sBTC 페그 가치는 STX에 따라 결정되지 않는다 (페그 값은 비트코인 메인 체인에 락업된 BTC로부터 파생됨). 그러나 페그 활성 및 인센티브 호환성은 올바른 인센티브를 보장하기 위해 sBTC의 유통량 대비 락업된 STX의 가치가 충분히 높은지에 따라 좌우된다.

sBTC는 다음과 같은 특징이 있다:

- 경제적 보안 특성에 영향을 미치기 위해선 공격자는 서명자의 70% 이상을 공격해야 한다. 스택스 채굴자는 페그-아웃을 유발하거나 무시할 수 없다. 궁극적으로 페그 및 스태커 세트 유지 관리에 필요한 모든 프로토콜 작업은 비트코인 체인으로부터

브로드캐스트 됨으로써 보장 및 달성된다; 이렇게 비트코인에서의 스택스-관련 작업은 다음 스택스 블록에서 처리되므로 모든 후속 스택스 포크에서 유효하다. 따라서 스택스 채굴자는 이 작업을 무시할 수 없다. 또한 BTC 페그-아웃은 sBTC 보유자의 유효한 요청에 대한 응답으로만 발생된다. 마지막으로, 페그-아웃 요청은 요청을 시작한 스택스 트랜잭션이 비트코인 완결성에 도달해야 완료된다. 즉, 트랜잭션은 비트코인 해시 파워로 100% 보호되며 스택스 레이어 채굴자는 이를 재정렬 (reorder)하거나 되돌릴 수 없다.

- 임의 수량의 BTC 페그-아웃은 스태커와 채굴자 모두 BFT로 작동하는 경우 약 24시간 이내 완료된다. 이는 시스템의 정상적인 기능으로, 150 블록 내로 유효 금액에 대한 페그-아웃이 자동으로 이행된다.

- 대다수의 BFT 채굴자가 정직한 한, 페그 시스템과 스택스 체인은 계속해서 활성을 유지한다. 다수의 스태커가 트랜잭션에 서명하지 않거나 오프라인 상태를 유지하면 시스템이 복구 모드로 전환되어, 페그-아웃이 계속해서 이뤄지나, 매우 느리게 진행된다. 그러나 이론적으로 모든 스태커가 악의적인 경우에도 모든 페그-아웃 요청은 결국 이행된다. 왜냐하면 스태커는 블록 생산에 관여하지 않으며 복구 모드 메커니즘이 존재하기 때문이다.

2.3 탈중앙화 온-체인 비트코인 오라클

PoX 프로토콜은 BTC/STX 가격 페어 정보를 비트코인 온-체인에서 탈중앙화된 방식으로 직접 가져올 수 있으며, 외부 오라클이 필요하지 않다는 고유한 특징을 갖고 있다. 이는 외부 오라클이 중앙화 및 공격을 위한 잠재적 벡터가 될 수 있기 때문에 설계에 있어 잠재적인 공격 루트를 제거했다. BTC/STX 가격 피드는 스택스 합의에 의해 소비되고 영향을 줄 수 있기 때문에 시스템은 중앙화 요소가 없을수록 강력해진다. 때문에 합의에서 외부 오라클 입력 (input)을 피하는 것이 안전하다. BTC/STX 가격 페어에 대한 탈중앙화 비트코인 오라클 피드를 사용하면 합의 프로토콜이 외부 오라클로부터의 영향 없이도 스택스 레이어 합의에 sBTC를 심도 있게 통합할 수 있다.

2.4 활성 비율

프로토콜에는 유통 중인 sBTC와 락업된 STX 비율 값을 기반으로 sBTC 유통량에 대한 제한을 설정할 수 있으며, 이를 활성 비율 (Liveness ratio)이라 한다. 활성 비율이 60%인 경우, 1억 달러 상당의 STX가 락업되어 있을 때 프로토콜은 sBTC 유통을 6천만 달러 이하로 유지하는 것을 목표로 한다. 활성 비율이 설정한 제한을 초과하면 더 많은 페그-아웃이 발생하고 비율이 다시 낮아질 때까지 (혹은 활성 비율이 증가할 때까지) 프로토콜에 의해 페그-인이 일시적으로 비활성화된다. 활성 비율은 온-체인 투표를 통해 설정 가능하다. 페그의 경제적 보안은 활성 비율 값이 낮을수록 높고 활성 비율이 증가하면 감소한다. 활성 비율은 STX의 가치가 BTC 대비 하락하면 활성 비율을 유지하기 위해 sBTC의 유통량도 감소해야 한다. 사용자는 락업된 자본의 상태를 독립적으로 모니터링하고 필요에 따라 sBTC를 페그-아웃할 수 있다. 페그 지갑은 높은 활성 비율 (예를 들어 90%)에서도 계속 작동 가능하며, 이는 스태커/서명자가 서로 결탁하여 페그 지갑으로부터 잠재적으로 훔칠 수 있는 자본보다 더 많은 자본이 락업되어 있기 때문이다.

2.5 네트워크 부트스트래핑

sBTC 최대 유통량은 애플리케이션 성장을 위해 생태계 초기에 제한을 둘 수 있다. 대출 풀, AMM (Automated Market Makers) 등 비트코인 애플리케이션이 상용화를 이뤄내기 위해선 높은 비트코인 유동성을 필요로 한다. sBTC 유통량이 수천만 달러 혹은 수억 달러로 낮아진다면 sBTC를 사용하는 애플리케이션에 부트스트래핑 문제가 발생할 수 있다. 또한 대출 프로토콜과 같은 특정 애플리케이션은 사용자가 시장 움직임에 따라 추가 담보를 예치하도록 요구할 수 있기 때문에 사용자는 적시에 추가 담보를 제공할 수 있어야 한다; 활성 비율이 높아지면 잠재적인 페그-인 일시중지 현상이 일어나 이러한 시나리오에서 문제가 될 수 있다. 이러한 부트스트래핑 문제는 스택스 네트워크의 사용량이 증가하고 합의에 더 많은 자본이 락업되어 수십억 달러 혹은 수백업 달러로 sBTC 유통량이 증가해야 감소할 것이다.

우리는 sBTC 유통이 가능한 많을 수 있도록 네트워크 초기에 높은 활성 비율을 적용할 것을 제안한다. 활성 비율은 온-체인 투표를 통해 설정할 수 있으며, 우리는 향후 몇 년 동안 스택스 네트워크가 성장함에 따라 활성 비율이 잠재적으로 낮아질 것으로 예상한다. 즉, 시간이 지남에 따라 페그의 경제적 보안이 증가해야 함을 의미한다 (활성 비율이 낮아짐).

또한 sBTC를 보안하기 위해 수탁 혹은 연합 비트코인 자산도 스택스 레이어에 사용할 수 있다. 실제로, Tokensoft와 Anchorage의 수탁형 비트코인 자산인 xBTC는 2022년 현재 스택스 레이어 상에 존재한다. xBTC와 같은 수탁 자산 및 애플리케이션 개발자가 구축한 연합 비트코인 자산도 아토믹 스왑 [1,5]을 사용하여 사용자에게 추가적인 유동성과 선택지로 제공할 수 있다. 연합 자산과 sBTC의 주요 차이점은 (a) 활성 인센티브로 락업된 STX 자본이 없고 (b) 연합 구성원이 일반적으로 폐쇄적이고 신뢰를 필요로 하는 집단이며 오픈-멤버십이 아니라는 점에 있어, 이는 탈중앙화된 서명자 집합으로 구성된 sBTC와는 확연히 차별된다. 연합 혹은 수탁 자산에는 경제적 보안이 존재하지 않으며 경제적 보안은 연합 혹은 커스터디안의 신뢰로 대체된다.

연합 혹은 수탁 자산은 사용자에게 추가적인 선택지와 유동성을 제공할 수 있지만, 우리의 본연의 작업과는 중요하지 않으며 우리는 무신뢰 페그에 집중할 예정이다. sBTC 유통량이 수십억 혹은 수백억 달러에 달하게 되면, sBTC를 통해 비트코인 앱을 상용화할 수 있을 정도의 충분한 유동성이 뒷받침될 것이다.

2.6 무신뢰 및 연합 비트코인 파생상품의 차이점

비트코인 페그 시스템의 경우 합의에 락업된 STX와 같은 추가 자산 없이는 sBTC와 같은 무신뢰 접근 방식을 이뤄낼 수 없다. sBTC는 보다 탈중앙화되고 경제적 보안을 갖춘 오픈-멤버십 서명자 집합을 보유하고 있다. 즉, 서명자에게 경제적으로 합리적인 길은 항상 페그 활성을 유지하는 것이다. 반면 (Liquid와 같은) 연합된 페그 사용자는 연합을 신뢰해야지만 연합 구성원의 오작동에 대한 경제적 위험은 존재하지 않으며, 오직 평판 위험만 존재한다. 우리는 무신뢰 sBTC 접근 방식이 우수하다고 굳게 믿는다.

sBTC와 연합 페그 간 비교를 통해 경제적 인센티브와 STX 토큰의 필요성을 알 수 있다. 스택스 레이어 원장을 보호하고 유지하기 위한 인센티브로 사용되는 것 외에도 STX 자산은 무신뢰 비트코인 페그 활성화에 있어 중요하다. STX와 같은 추가 자산이 없다면, 연합 혹은 수탁 설계만 택할 수 있다. 비트코인 커뮤니티에는 비트코인 외 새로운 자산에 있어 거리감이 존재한다. 이는 비트코인 외 다른 암호화폐 자산이 시장에서 발생하는 불협화음과 위험성을 고려했을 때 이해할 수 있다. 우리의 설계는 애플리케이션 개발자가 원하는 경우 연합형 페그를

구축하고 사용할 수 있도록 허용하지만, 핵심 합의 프로토콜은 무신뢰 페그에만 초점을 두고 있다. 무신뢰 페그는 별도의 STX 자산이 있기 때문에 가능하다. 우리는 탈중앙화 및 무신뢰 시스템이 연합 설계보다 장기적으로 우수하다고 믿으며, 특히 네트워크가 초기 부트스트래핑 단계를 통과하면 sBTC 유통량이 수십억에서 수백업 달러에 도달하여 사용자에게 충분한 유동성을 제공할 수 있을 것이다.

3 결론

수천억 달러의 비트코인 자본을 잠금 해제하는 것은 아직 미개척된 황야와 같다. 비트코인 레이어는 BTC용 탈중앙화 금융 및 애플리케이션을 활성화할 수 있지만 주요 제한 사항이 존재한다. 아직도 사용자가 완전히 신뢰를 필요로 하지 않는 방식으로 비트코인 레이어에서 실행되는 스마트 컨트랙트 안팎으로 BTC를 이동할 방법은 존재하지 않는다. 이는 비트코인 페그-아웃 문제라 불리며 약 10년이라는 시간 동안 비트코인 '성배' 문제로 다뤄졌다; 아직까지 연합/중앙화된 접근 방식만 존재한다.

본 백서에서는 무신뢰 양방향 비트코인 페그 시스템을 제시한다. 고정 연합 혹은 멀티시그 지갑 연합이 사용자의 신뢰를 요구로 했던 이전 접근 방식과 달리, sBTC라는 새로운 접근 방식은 오픈-멤버십과 변화하는 서명자 집합을 통해 경제적 보안을 제공할 것이다. 또한 사용자는 BTC를 비트코인 레이어 안팎으로 이동할 때 수수료를 지불하지 않으며 동적 서명자 집합은 합의 프로토콜로부터 작업에 대한 보상을 BTC로 받을 수 있다.

우리는 이번 작업을 통해 이상적인 비트코인 레이어를 구축하는 데 한 발짝 더 가까워졌다. 사용자는 레이어에서 전체 스마트 컨트랙트에 접근 가능해져을 뿐만 아닌 트랜잭션이 베이스 레이어 보안의 100%로 보호되는 동안 탈중앙화된 방식으로 레이어 안팎으로 자산을 쉽게 이동할 수 있다. sBTC는 비트코인 경제를 빠르게 성장시켜줄 비트코인 애플리케이션의 새로운 시대를 가져올 것이다.

참고문헌

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

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

[3] Stacking stats. https://stacking.club/cycles/all.

[4] Stacks: A bitcoin layer for smart contracts, Dec 2022. https://stx.is/nakamoto.

[5] 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.

[6] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timon, and Pieter Wuille. Enabling Blockchain Innovations with Pegged Sidechains. White paper, Blockstream, 2014. https://blockstream.com/sidechains.pdf.

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

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