

비트코인 스테이킹:

지분증명 경제를 보호하기 위해 2,100만 비트코인을 활용하다

바빌론 팀*

버전 1.0: 2023-07-13

초록

지분증명(PoS) 체인은 자본에 의해 보안이 유지되지만, 자본은 매우 고비용일 수 있습니다. 비트코인은 작업증명(PoW) 체인이지만 동시에 6,000억 달러 규모의 자산이며, 그 대부분은 유휴 자본입니다. 우리는 비트코인 보유자가 유휴 비트코인을 스테이킹함으로써 PoS 체인의 보안을 강화하고 그 과정에서 수익을 얻을 수 있는 *비트코인 스테이킹* 개념을 제안합니다.

우리는 비트코인 보유자가 자신의 비트코인을 PoS 체인으로 브리징하지 않고도 신뢰 없이 스테이킹할 수 있으며, 동시에 체인에 *완전한* 슬래시 가능한 보안 보장을 제공하는 비트코인 스테이킹 프로토콜을 제안합니다. 이 프로토콜은 스테이킹 해제(unbonding)를 빠르게 수행할 수 있어 비트코인 보유자에게 유동성을 극대화합니다. 또한 이 프로토콜은 다양한 PoS 합의 알고리즘 위에 플러그인 형태로 모듈화되어 설계되었으며, 이를 기반으로 리스테이킹 프로토콜(restaking protocol)을 구축할 수 있는 원시 수단을 제공합니다.

본 문서에서는 다수의 스테이커와 다수의 PoS 체인으로 확장 가능한 시스템 아키텍처를 제안하며, 비트코인을 스테이킹한 바빌론 체인이 제어 평면 역할을 수행하여 비트코인과 PoS 체인 간의 동기화를 담당합니다. 비트코인 스테이킹은 비트코인의 새로운 중요한 사용 사례를 가능하게 하며, 비트코인과 지분증명 경제의 통합을 향한 의미 있는 발걸음입니다.

1 지분증명 보안은 자본을 필요로 한다

지난 몇 년간 블록체인 산업은 작업증명(PoW)에서 지분증명(PoS)으로 시빌 저항 메커니즘을 전환하는 흐름을 보여주었습니다. 이 트렌드를 대표하는 사건은 2022년 9월의 머지(Merge), 즉 이더리움이 PoW에서 PoS 합의로 마이그레이션한 일입니다. PoW 블록체인이 어려운 수학 퍼즐을 푸는 채굴자에 의해 보호되는 반면, PoS 블록체인은 스테이킹을 하는 검증자에 의해 보호됩니다. 검증자의 스테이크는 위반 행위 시 슬래시될 수 있는 *예치금* 역할을 합니다. 슬래시 가능성은 PoW 체인에는 없는 기능이며, 이는 이더리움이 PoW에서 PoS로 전환한 주요 동기 중 하나입니다 [18].

보안 스테이크의 시가총액이 클수록 체인을 공격하는 데 더 큰 비용이 들고, 그만큼 체인의 경제적 보안도 강해집니다. 따라서 PoW 체인이 *작업*에 의해 보안되는 반면, PoS 체인은 *자본*에 의해 보안됩니다.

이러한 자본은 특히 소규모 체인이나 초기 부트스트랩 단계에 있는 체인의 경우 유치하기 어렵습니다. 이러한 자본을 유치하기 위해서는 높은 수익률을 제공해야 하며, 이를 위해 높은 인플레이션율이 필요합니다. 예를 들어, 60개 이상의 애플리케이션 특화 체인으로 구성된 Cosmos 생태계에서는 연간 인플레이션율이 20%에서 100%에 이르는 경우가 흔합니다. 이처럼 높은 인플레이션은 장기적으로...

* *문의: contact@babylonchain.io. 본 라이트페이퍼는 Babylon 팀, ZeroSync의 Robin Linus, Common Prefix 및 임페리얼 칼리지의 Orfeas Stefanos Thyfronitis Litos 간의 협업으로 작성된 기술 논문 [9]을 바탕으로 하고 있습니다.*

시간이 지나며 인플레이션율이 감소함에 따라 보안성과 유틸리티 사이의 긴장은 더욱 심화됩니다.

2 비트코인: 6,000억 달러 규모의 자산

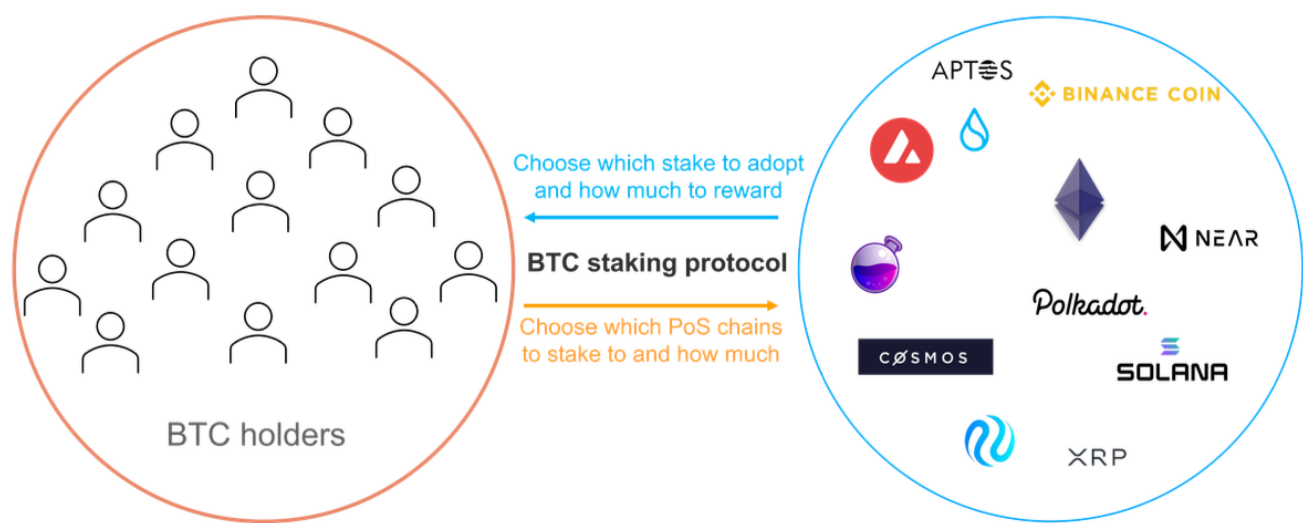
PoS로의 전환에도 불구하고, 현재 기준 전체 크립토 자산의 절반 이상을 차지하는 가장 큰 크립토 자산인 비트코인은 여전히 PoW 체인에 의해 보호되고 있습니다. PoS 자산과 비교할 때, 비트코인 자산은 몇 가지 중요한 차이점을 가집니다:

1. **담보화되지 않음.** 비트코인은 작업에 의해 보호되기 때문에, 비트코인 자산 자체는 비트코인 체인을 보호하는 데 사용되지 않습니다. 반면, 각 PoS 자산은 자신의 체인을 보호하기 위해 사용됩니다.
2. **더 유향 상태임.** 대부분의 비트코인 자산은 유향 상태에 있으며 활용되지 않습니다. DeFi 대출이나 보안 스테이킹 등 수익을 창출하는 활동은 대부분 PoS 체인에서 발생하기 때문에, 비트코인이 수익을 얻기 위해서는 다른 체인으로 *브리징* 되거나 제3의 중앙화 커스터디 기관에 예치되어야 합니다. 그러나 이러한 브릿지와 중앙화 커스터디는 많은 비트코인 보유자에게 너무 위험한 것으로 간주됩니다. 예를 들어, 가장 규모가 큰 래핑된 비트코인 자산 중 하나인 WBTC는 시가총액이 50억 달러도 되지 않으며, 전체 비트코인 시가총액의 일부 소수점 수준에 불과합니다.
3. **더 탈중앙화됨.** 비트코인은 가장 오래된 블록체인이기 때문에, 토큰 보유자의 구성은 아마도 가장 탈중앙화되어 있습니다. 채굴자, 초기 수용자 및 개발자, 프로젝트 창립자, 개인 투자자, 기관 투자자, 거래소 등 다양한 주체들이 존재합니다. 반면, 많은 PoS 체인의 자산은 프로젝트 초기 단계에서 초기 투자자, 창립자 및 팀 구성원, 재단 등에 집중되어 있습니다. 이러한 자산 집중은 자산이 스테이킹되어 네트워크를 검증할 때 네트워크를 중앙집중화 위험에 노출시킵니다.
4. **더 낮은 변동성.** 비트코인은 가장 큰 크립토 자산으로서, 대부분의 PoS 자산에 비해 변동성이 현저히 낮습니다. PoS 자산의 변동성은 PoS 체인의 보안성에 중대한 문제를 야기할 수 있는데, 그 이유는 보안성이 스테이킹된 자산의 시가총액에 직접적으로 연동되기 때문이며, 자산 가치가 급락하면 공격자가 공격을 감행할 기회를 제공하게 됩니다.

3 비트코인 스테이킹

이러한 속성들을 고려할 때, 왜 비트코인을 스테이킹하여 PoS 체인의 보안을 돕는 데 활용하지 않겠습니까? *비트코인 스테이킹*이라는 개념이 본 연구의 중심입니다.

비트코인 스테이킹은 양면 시장(two-sided marketplace)입니다 (그림 1). 한쪽에는 보안을 필요로 하며 그에 대한 수익을 지불할 의사가 있는 PoS 체인들이 있습니다. 다른 한쪽에는 자본을 보유하고 그 자본으로 수익을 얻고자 하는 비트코인 보유자들이 있습니다. *비트코인 스테이킹 프로토콜*은 이러한 양면 시장을 구현하는 *보안 공유 프로토콜*입니다. 훌륭한 비트코인 스테이킹 프로토콜은 PoS 체인 소비자에게는 강력한 보안 보장을 제공하고 (그래야 수익을 지급할 유인이 생기므로), 비트코인 보유 제공자에게도 강력한 보안 보장을 제공해야 합니다 (그래야 스테이킹할 유인이 생기므로).



[그림 1: 비트코인 스테이킹은 양면 시장이다.]

4 바빌론 비트코인 스테이킹 프로토콜: 보안 속성

우리는 여기서, 범용 PoS 소비자 체인과 함께 사용할 수 있는 비트코인 스테이킹 프로토콜을 제안하며, 이 프로토콜은 다음 세 가지 중요한 보안 속성을 가집니다:

1. **완전 슬래시 가능한 PoS 보안.** 안전성 위반이 발생할 경우, 전체 비트코인 스테이크의 1/3이 슬래시되는 것이 보장됩니다. 전체 비트코인 스테이크의 2/3가 정직하게 PoS 프로토콜을 따르기만 하면, 해당 PoS 체인은 생존성을 유지합니다.
2. **스테이커 보안.** 각 비트코인 스테이커는 PoS 프로토콜을 정직하게 따르기만 하면 자금을 인출하거나 언본드(unbond)할 수 있는 권리가 보장됩니다.
3. **스테이커 유동성.** 스테이킹된 비트코인의 언본딩은 사회적 합의(social consensus) 없이도 안전하고 빠르게 수행되는 것이 보장됩니다.

속성 1은 프로토콜을 위반한 참여자는 슬래시된다는 것을 의미합니다. 속성 2는 프로토콜을 위반하지 않은 참여자만이 스테이크를 잃는다는 것을 의미합니다. 이 두 속성을 함께 보면, 부테린과 그리피스가 주장한 바와 같이 [18], 완전한 슬래시 가능성을 갖춘 PoS 보안의 골드 스탠더드를 충족함을 알 수 있습니다. 실제로, 완전한 슬래시 가능성은 PoS 이더리움의 중심 설계 목표이며 [19], Cosmos SDK 체인, Polygon, BNB Chain 등 여러 PoS 블록체인 구축에 널리 사용되는 합의 엔진인 Tendermint의 중심 설계 목표이기도 합니다 [13, 15].

실제로 속성 2는 독립형 PoS 프로토콜보다도 더 강력합니다: 모든 다른 스테이커가 부정직하더라도, 스테이커는 여전히 언본드할 수 있습니다. 본 비트코인 스테이킹 프로토콜에서는 인출 검열이 불가능합니다. 따라서 본 프로토콜은 *신뢰 없는 스테이킹 (trustless staking)*을 제공합니다.

PoS 이더리움이나 Cosmos SDK 체인과 같은 독립형 PoS 체인들은 수 주에 이르는 긴 언본딩 기간을 겪는데, 이는 장거리 공격 (long range attack)을 방지하기 위한 사회적 합의(social consensus) 사용 때문입니다 [16, 21, 12, 22]. 장거리 공격은 PoS 체인의 근본적인 "nothing-at-stake" 공격 벡터입니다. 반면, 우리 비트코인 스테이킹 프로토콜에서는 스테이크 분포가 비트코인 체인에 유지되므로 이러한 장거리 공격에 면역입니다. 우리는 스테이킹 프로토콜을 적절히 설계함으로써 속성 3이 달성 가능함을 보입니다.

5 도전 과제

우리는 비트코인 스테이킹에 대해 두 가지 기본 접근 방식을 고려하며, 각 방식은 고유의 도전 과제를 갖습니다.

1. **PoS 체인으로의 브리징.** 비트코인 스테이킹의 한 가지 접근은 먼저 비트코인을 비트코인 체인에서 소비자 PoS 체인으로 브리징한 후, 그곳에서 슬래싱 규칙을 적용하는 것입니다. 이 접근은 PoS 체인에 슬래시 가능한 보안(속성 1)을 제공할 수 있지만, 근본적인 한계는 브리징 솔루션 자체의 보안에 있습니다. 현재 대부분의 비트코인 브리지는 중앙화 커스터디(예: wBTC의 Bitgo) 또는 멀티시그 브리징 위원회를 신뢰하는 방식에 기반하고 있습니다. (자세한 논의는 섹션 9.8 참조.) 이상적인 비트코인 브리징조차도 목적지 체인의 스테이커를 신뢰해야 한다는 점에서, 브리징 솔루션만으로는 속성 2, 즉 신뢰 없는 스테이킹(trustless staking)을 달성할 수 없습니다.
2. **비트코인 체인에서의 원격 스테이킹.** 브리징을 피하기 위한 대안적 접근 방식은 *원격 스테이킹(remote staking)*입니다. 즉, 스테이킹된 비트코인을 비트코인 체인의 계약에 락업(lock)하고, 소비자 PoS 체인에서 프로토콜 위반이 발생했을 때 해당 스테이크를 슬래시하는 방식입니다. 이 접근은 Eigenlayer의 이더리움 리스테이킹 프로토콜 [36], Cosmos 생태계의 메쉬 시큐리티 [11, 4]와 같은 보안 공유 솔루션에서 사용됩니다. 이들 환경에서는 보안 제공 체인(즉, 보안의 출처)이 튜링 완전한 스마트 컨트랙트 레이어를 가지고 있습니다. 따라서 소비자 체인에서 보안 제공 체인으로 위반 증거를 전송하고, 스마트 컨트랙트를 통해 슬래싱을 수행하는 것이 기술적으로 용이합니다.

하지만, 우리 설정에서 보안 제공 체인은 비트코인이며, 비트코인은 스마트 컨트랙트를 지원하지 않고 표현력이 제한된 스크립팅 언어만 제공합니다. 따라서 비트코인이 비트코인 체인에 남아 있음으로써 신뢰 없는 스테이킹(속성 2)은 확보되지만, 이제 핵심 도전 과제는 어떻게 슬래싱을 구현하여 속성 1, 즉 완전 슬래시 가능한 PoS 보안을 달성할 것인가입니다.

우리의 비트코인 스테이킹 프로토콜은 원격 스테이킹 접근을 따르며, 스마트 컨트랙트의 부재를 고급 암호 기술, 합의 프로토콜 혁신, 비트코인 스크립트 언어의 최적 활용을 결합하여 극복합니다. 이러한 기술적 세부사항을 설명하기에 앞서, 먼저 스테이커의 여정을 따라가며 비트코인 스테이킹 프로토콜의 고수준 기능을 살펴보겠습니다.

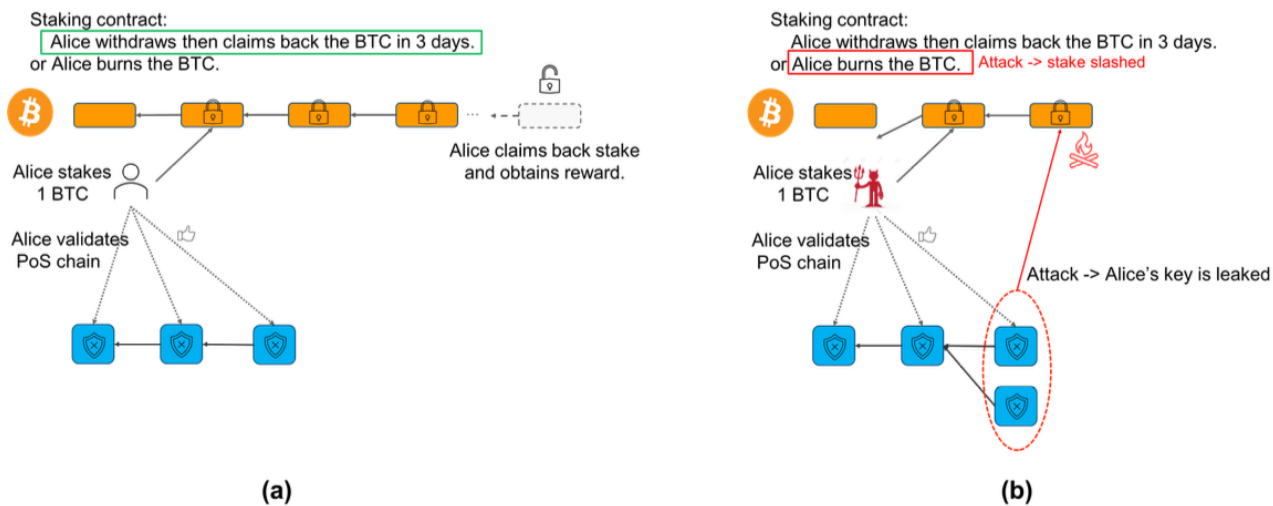
6 비트코인 스테이커의 여정

앨리스는 1 비트코인을 보유하고 있으며, 이를 PoS 체인에 스테이킹하고자 합니다. 먼저 그녀는 스테이킹 트랜잭션을 비트코인 체인에 전송하여 비트코인을 셀프 커스터디 볼트에 락업함으로써 스테이킹 계약에 진입합니다. 이 비트코인은 두 가지 방법 중 하나로만, 앨리스의 개인 키를 사용하여 잠금 해제할 수 있습니다:

1. 앨리스가 언본딩 트랜잭션을 발행하면, 비트코인은 3일 후에 언락되고 앨리스에게 반환됩니다.
2. 앨리스가 슬래싱 트랜잭션을 발행하면, 비트코인은 소각 주소(burn address)로 전송됩니다.

이 스테이킹 트랜잭션이 비트코인 체인에 등장하면, 앨리스는 자신의 키를 사용해 블록에 서명함으로써 PoS 체인의 검증을 시작할 수 있습니다. 검증 활동 중에는 두 가지 경로가 존재합니다.

첫 번째는 **정상 경로(happy path)**입니다 (그림 2(a)). 앨리스가 프로토콜을 정직하게 따르고, 스테이킹을 해제하고자 할 때 비트코인 체인에 언본딩 트랜잭션을 전송하여 언본딩 요청을 합니다 (그림 2(b)).



[그림 2: 비트코인 스테이커의 여정: (a) 정상 경로 - 앨리스는 스테이킹하고, PoS 체인을 검증하며, 언본딩 요청을 하고 3일 후 언스테이킹함; (b) 비정상 경로 - 앨리스는 스테이킹 후 PoS 체인에서 안전성 위반을 저지르고, 비트코인이 소각됨.]

언본딩 트랜잭션이 비트코인 체인에 포함되면, 앨리스의 PoS 체인에서의 검증 역할은 중단되고, 3일이 지나면 인출 요청이 승인되어 1 비트코인이 앨리스에게 반환됩니다. PoS 체인은 또한 앨리스에게 보상도 지급합니다.

두 번째는 **비정상 경로(unhappy path)**입니다 (그림 2(b)). 이 경우 앨리스가 악의적인 행동을 하여 PoS 체인에서 이중지불(안전성) 공격에 가담합니다 (그림 2(c)). 이 경우, 스테이킹 프로토콜은 앨리스의 개인 키가 공개되도록 보장합니다. 이제 누구나 앨리스인 척하며 슬래싱 트랜잭션을 비트코인 체인에 전송할 수 있으며, 앨리스의 1 비트코인을 소각할 수 있습니다. 이 비정상 경로의 존재는 안전성 위반이 슬래시 가능성을 보장하며, 모든 참여자가 정상 경로를 유지하려는 동기를 갖게 만듭니다.

7 기술 구성 요소

다음은 섹션 6에서 설명한 프로토콜 기능을 가능하게 하고, 섹션 5에서 논의된 도전 과제를 극복할 수 있게 해주는 핵심 기술 요소들입니다. 자세한 내용은 향후 발표될 정식 논문 [9]에 포함될 예정입니다.

7.1 비트코인 커버넌트(covenant) 에뮬레이션을 통한 스테이킹 계약

비트코인에는 스마트 컨트랙트 레이어가 존재하지 않기 때문에, 스테이킹 계약은 비트코인 스크립트로 작성된 UTXO 트랜잭션의 형태로 표현되어야 합니다 [10]. 각 UTXO 트랜잭션은 UTXO 집합에서 자금을 사용하며, 비트코인 스크립트는 자금 사용 조건을 지정할 수 있는 소수의 오퍼코드(opcode)를 제공합니다. 스테이킹 계약은 다음 네 가지 트랜잭션으로 구성됩니다:

- **스테이킹 트랜잭션:** 입력은 스테이커의 비트코인 주소이며, 출력은 다음 두 가지 방법 중 하나로 소비될 수 있습니다:
 - **언본딩 트랜잭션:** 상대적인 락 타임(relative lock time)이 경과한 후 스테이커가 출력을 사용할 수 있도록 허용합니다. 언본딩 시간 측정에 사용되는 상대 락 타임은 `OP_CHECKSEQUENCEVERIFY` 오퍼코드로 구현할 수 있습니다 [10];

개별 검증자 v 는 다음과 같은 두 개의 상이한 투표를 게시해서는 안 됩니다.

$\langle v, s_1, t_1, h(s_1), h(t_1) \rangle$ 그리고 $\langle v, s_2, t_2, h(s_2), h(t_2) \rangle$

다음 중 하나라도 만족하는 경우:

I. $h(t_1) = h(t_2)$.

즉, 하나의 타겟 높이에 대해 두 개의 서로 다른 투표를 게시해서는 안 됩니다.

또는

II. $h(s_1) < h(s_2) < h(t_2) < h(t_1)$.

즉, 자신의 다른 투표 범위 내에서 투표해서는 안 됩니다.

[그림 2: 캐스퍼의 두 계율(Casper Commandments). 이 계율 중 하나라도 위반한 검증자는 자신의 예치금을 슬래시당합니다.]

[그림 3: 캐스퍼의 슬래싱 조건. 출처: [18].]

- **슬래싱 트랜잭션:** 출력 자금을 즉시 소각 주소(소비 불가능한 출력)로 전송할 수 있도록 허용합니다.
- **언스테이킹 트랜잭션:** 상대적 타임락이 만료된 후, 언본딩 트랜잭션의 출력을 사용할 수 있습니다.

스테이킹 계약은 트랜잭션의 출력이 특정 방식으로만 소비되도록 제한하는 *비트코인 커버넌트(covenant)*의 한 예입니다 [25, 26]. 커버넌트는 `OP_CHECKTEMPLATEVERIFY` [8]라는 비트코인 스크립트 오퍼코드를 통해 구현할 수 있으며, 이는 향후 비트코인 스크립트 업그레이드에 포함될 것으로 제안된 기능입니다. 업그레이드 이전에도 커버넌트를 에뮬레이션하기 위한 다양한 방법이 제안되었습니다. 본 연구의 주요 혁신 중 하나는 거의 신뢰 없는 형태의 새로운 커버넌트 에뮬레이션 방식입니다. 자세한 내용은 [9]를 참조하십시오.

7.2 책임 있는 주장과 파이널리티 장치를 활용한 자동 슬래싱

비트코인에는 스마트 컨트랙트가 없기 때문에, 단순히 안전성 위반 증거를 전송하고 비트코인이 그것을 처리해주시기를 기대할 수 없습니다. 대신, 본 프로토콜은 슬래싱으로 직접 연결될 수 있는 증거, 즉 스테이커의 개인 키를 전송하는 방식을 허용합니다. 안전성 위반이 발생할 때마다 스테이커의 개인 키가 유출되도록 보장하기 위해 우리는 다음 두 가지 개념을 결합합니다: (a) 암호학에서의 책임 있는 주장(accountable assertions) [32], (b) 블록체인 합의에서의 파이널리티 장치(finality gadgets) [18, 27, 28].

추출 가능한 일회성 서명(Extractable One-Time Signatures, EOTS)은 동일한 개인 키로 서로 다른 두 메시지를 서명하면 해당 개인 키가 유출될 수 있는 서명 방식입니다. EOTS는 동일한 비트코인을 이중 지불하는 경우처럼 동일성 위반(equivocation)을 처벌하는 일반적인 방법으로 제안되어 왔습니다 [32]. 하지만, 합의 프로토콜의 슬래싱 조건은 단순한 동일성 위반보다 훨씬 복잡합니다. 예를 들어, 캐스퍼(Casper) [18], 즉 PoS 이더리움 프로토콜의 슬래싱 모듈에는 두 가지 슬래싱 조건 세트가 존재합니다 (그림 3). 첫 번째 조건은 동일한 높이의 블록 두 개를 서명하는 것으로 동일성 위반에 해당하지만, 두 번째 조건은 더 복잡하며

단순한 동일성 위반으로 표현될 수 없습니다.

유사하게, 텐더민트(Tendermint)에서도 두 가지 슬래싱 조건 세트가 존재합니다. 하나는 동일 라운드 및 동일 높이에서 블록 두 개를 서명하는 것이며, 다른 하나는 소위 망각 공격(amenia attack)에서 기인하는 조건으로, 역시 동일성 위반으로 직접 표현될 수 없습니다 [14].

우리는 기본 합의 프로토콜의 서명 방식은 변경하지 않되, 베이스 합의 프로토콜이 블록을 파이널라이즈한 이후 추출 가능한 일회성 서명(EOTS)을 사용하여 추가 서명 라운드를 삽입하는 방식으로 이 문제를 우회합니다.

블록은 기본 프로토콜에 의해 파이널라이즈될 뿐만 아니라 전체 스테이크의 2/3 이상이 EOTS로 서명한 경우에만 진정으로 파이널라이즈된 것으로 간주됩니다. 이 추가 서명 라운드는 일종의 *파이널리티 장치(finality gadget)*로 해석될 수 있으며, EOTS 파이널리티 장치라고 부를 수 있습니다 [27]. 이 수정된 프로토콜에서 안전성 위반이 발생하면, 전체 스테이크의 1/3 이상이 EOTS를 사용하여 동일한 높이의 두 블록에 서명한 것으로 나타납니다 [9]. 이로 인해 해당 스테이커들의 개인 키가 추출됩니다. 또한, EOTS 서명 방식은 비트코인에서 사용되는 서명 알고리즘인 슈노르(Schnorr) 서명으로 구현될 수 있습니다. 따라서 추출된 개인 키는 슬래싱 트랜잭션을 소비하는 데 사용할 수 있습니다.

이러한 파이널리티 장치 기반 솔루션의 매우 중요한 장점은 그 *모듈성(modular nature)*입니다. 즉, 어떤 BFT 합의 프로토콜 위에서도 기본 프로토콜을 변경하지 않고 사용할 수 있다는 것입니다. 이는 본 기술이 특정 PoS 체인에 종속되지 않도록 만들어 줍니다.

7.3 비트코인 타임스탬핑을 통한 빠른 언본딩

PoS 체인에서 네이티브 스테이킹이 있는 경우, 언본딩 시간은 매우 깁니다 (예: Cosmos Hub는 3주). 이는 장거리 공격(long-range attack)을 방어하기 위해 사회적 합의(social consensus)가 필요하기 때문입니다. 공격자가 언본딩 이후 대체 포크를 구축하는 장거리 공격은 비용이 거의 들지 않습니다. 반면, 비트코인과 같은 PoW 체인에서는 장거리 공격이 매우 높은 비용을 요구하는데, 이는 기존의 가장 긴 체인을 대체할 긴 포크를 만들기 위해 막대한 에너지가 필요하기 때문입니다. 우리 비트코인 스테이킹 프로토콜에서는 언본딩 요청이 비트코인 체인에 제출되므로, 해당 트랜잭션을 체인에서 제거하는 비용은 막대하게 됩니다. 이는 본 프로토콜에서 언본딩이 사회적 합의 없이도 빠르게 진행될 수 있음을 시사합니다.

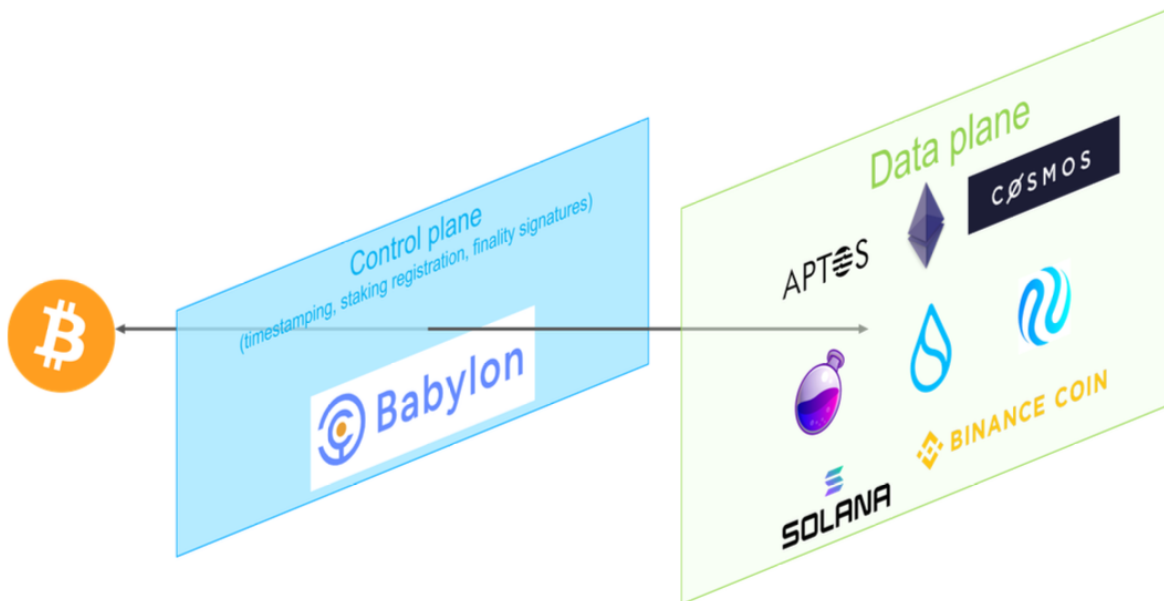
그러나 한 가지 문제는, 스테이크 분포는 비트코인 체인에 보존되지만, 블록에 대한 투표는 PoS 체인에서 이루어진다는 점입니다. 공격자는 PoS 체인의 진행을 늦춤으로써 오래된 스테이커 집합이 블록을 검증하게 만들 수 있습니다. 이는 곧 공격자가 비트코인 체인에서는 언스테이킹을 한 후에도 여전히 PoS 체인에서 투표 권한을 가지게 되어, PoS 체인에서 포크를 일으킬 수 있다는 것을 의미합니다. 비록 스테이커의 개인 키가 유출되더라도, 이미 언스테이킹이 완료되었기에 슬래시하기에는 너무 늦습니다.

이러한 공격을 방지하고 빠른 언본딩을 가능하게 하려면, PoS 체인은 비트코인 체인과 긴밀히 동기화되어야 합니다. 이를 위해 *비트코인 타임스탬핑(Bitcoin timestamping)*이라는 기술을 사용할 수 있습니다. 이 방식에서는 PoS 블록 해시와 해당 블록에 투표한 스테이커 집합이 비트코인 체인에 기록됩니다. 흥미롭게도, 이 비트코인 타임스탬핑 기술은 PoS 체인의 네이티브 스테이킹에서도 안전하고 빠른 언본딩을 가능하게 하는 데 유용하며, 외부 신뢰로서 비트코인을 활용할 수 있게 합니다 [35]. 우리는 이 기술을 비트코인 스테이킹 프로토콜의 빠른 언본딩을 가능하게 하기 위한 방식으로 재해석하고 있습니다.

8 시스템 아키텍처

앞서 설명한 원시 구성 요소들을 바탕으로, 비트코인 스테이킹 프로토콜의 핵심 인프라는 비트코인과 PoS 체인 사이의 제어 평면(control plane)입니다 (그림 4). 이 제어 평면은 다음과 같은 주요 기능들을 담당합니다:

- 비트코인 네트워크와의 동기화를 위해 PoS 체인에 비트코인 타임스탬핑 서비스를 제공합니다;
- 마켓플레이스로 작동하여 비트코인 스테이크와 PoS 체인을 매칭시키고, EOTS 키 등록 및 갱신 등 스테이킹 및 검증 관련 정보를 추적합니다;
- PoS 체인의 파이널리티 서명을 기록합니다;



[그림 4: 제어 평면과 데이터 평면으로 구성된 시스템 아키텍처]

한편, 각 PoS 체인의 검증자들은 일반적인 합의 프로토콜에서처럼 블록을 생성하고 검증하는 것 외에도, 파이널리티 장치에 대해 파이널리티 서명을 수행합니다. 이들 검증자들은 함께 아키텍처의 데이터 평면(data plane)을 운영합니다.

제어 평면(control plane)은 탈중앙화, 보안성, 검열 저항성 및 확장성을 보장하기 위해 하나의 체인으로 구현됩니다. 예를 들어, 비트코인 네트워크의 제한적이고 고비용인 블록 공간은 모든 PoS 체인이 직접 타임스탬프를 기록하는 데에는 지속 가능성과 확장성이 부족하여, 비트코인 스테이킹의 채택을 저해합니다. 이 문제를 해결하기 위해 바빌론 팀은 안전한 비트코인 타임스탬핑 프로토콜을 설계하고, 이를 Cosmos-SDK 기반의 바빌론 체인으로 구현했습니다. 이 체인은 표준 IBC(인터블록체인 커뮤니케이션) 프로토콜을 통해 여러 Cosmos SDK 체인에 대한 효율적인 타임스탬프 집계를 가능하게 합니다. 이 체인은 2023년 2월에 최초로 출시되었으며, 테스트넷은 다양한 분야의 30개 이상의 Cosmos SDK 체인과 통합되었습니다 (그림 5).

이로써 바빌론 체인이 제어 평면 역할을 하고, 비트코인과 데이터 평면(즉, PoS 체인) 간의 상호작용을 가능하게 하는 3계층 아키텍처가 완성됩니다. 이 아키텍처는 네트워크 효과를 유도하고 상호운용성의 잠재력도 제공합니다. 예를 들어, 바빌론 체인 상에서 두 PoS 체인의 파이널리티 상태를 기반으로, 체인 간 교차 거래(cross-PoS-chain transaction)를 정산하는 것이 가능해질 수 있습니다.

9 관련 연구

9.1 크로스체인 스테이킹, 리스테이킹, 메쉬 보안

모든 기존 PoS 체인은 해당 체인의 원장에 보관된 네이티브 자산에 의해 보안이 유지됩니다. 예를 들어, PoS 이더리움은 ETH에 의해 보호되고, Cosmos Hub는 ATOM에 의해, BNB 체인은 BNB에 의해 보호됩니다. 그러나 네이티브 토큰만 사용하는 경우, PoS 체인의 경제적 보안성은 해당 네이티브 토큰의 시가총액에 의해 상한이 제한됩니다. 대신에 또는 추가로 PoS 체인 위에서 *외부 암호 자산(remote crypto asset)*을 스테이킹함으로써, 스테이킹된 총 시가총액을 증가시켜 체인의 보안성을 향상시킬 수 있습니다. 블록체인 산업에서 최근 부상하고 있는 접근 방식은 *크로스체인 스테이킹(cross-chain staking)*이라 부를 수 있습니다. 이 방식은 스테이킹된 외부 자산이 자체 체인에 그대로 존재하지만, 보안 제공 대상 체인의 우선 검증인(preferred validator)을 위한 스테이킹 계약에 자산이 락업됩니다.



[그림 5: 31개의 IBC 지원 체인과 연결된 비트코인 타임스탬핑 테스트넷]

이 스테이킹된 자산은 검증자가 슬래시 가능한 위반 행위를 했을 때에만 슬래시됩니다. 이는 Cosmos 생태계를 위해 제안된 *메쉬 보안(mesh security)* 개념의 핵심 아이디어였습니다 [11, 4]. 하나의 Cosmos 앱체인(제공 체인)의 자산은 *크로스 스테이킹*되어 다른 Cosmos 앱체인(소비 체인)의 보안을 도울 수 있습니다. 이 크로스 스테이킹 프로토콜은 다시 Eigenlayer의 이더리움 리스테이킹 개념 [36]에서 영감을 받았습니다. 여기서는 PoS 이더리움에서 이미 스테이킹된 ETH를 다시 스테이킹하여, 데이터 가용성 계층, 브리지, 오라클 서비스 등 *적극적 검증 시스템(AVS: Actively Verified Systems)*이라 불리는 미들웨어를 보호합니다. 이러한 프로젝트들과 함께, 암호 자산이 자산 고유의 체인 이외의 체인이나 서비스를 보호하는 데 사용되는 일반화된 형태의 PoS가 등장하고 있습니다.

우리의 비트코인 스테이킹 프로토콜은 크로스체인 스테이킹 프로토콜의 한 예로 볼 수 있지만, Cosmos 메쉬 보안 및 이더리움 리스테이킹과는 두 가지 중요한 차이점이 존재합니다. 첫째, 이더리움 리스테이킹과 Cosmos 메쉬 보안에서는 자산이 이미 제공 체인의 보안을 위해 스테이킹되어 있습니다. 반면, 비트코인은 비트코인 자산 자체가 아니라 PoW에 의해 보호되므로, 비트코인 자산은 담보화되지 않은 상태입니다. 이는 리스테이킹으로 인해 발생할 수 있는 과잉 레버리지 리스크를 줄여줍니다 [17, 36]. 둘째, 비트코인에는 스테이크 슬래싱을 구현할 스마트 컨트랙트가 존재하지 않습니다. 대신, 우리는 비트코인 스크립트 언어를 최적화하여 활용하고 고급 암호학적 메커니즘을 사용하여 동일한 목적을 달성합니다.

9.2 책임성과 슬래시 가능성

많은 PoS 체인의 중요한 특성 중 하나는, 프로토콜 위반자를 입증 가능한 방식으로 책임지게 만들 수 있는 능력입니다 [18, 20, 33]. 이 특성은 PoW 체인에는 존재하지 않는데, 이는 채굴자들이 온체인 신원을 가지고 있지 않기 때문입니다. 실제로 **책임 있는 안전성(accountable safety)**, 즉 전체 스테이크의 1/3을 검증자들이 안전성 위반 시 책임을 지도록 만드는 능력은 PoS 이더리움의 설계에서 중심적인 요소입니다 [18, 20].

하지만 책임성(accountability)과 온체인 슬래싱(on-chain slashing) 사이에는 간극이 존재합니다. 즉, 프로토콜 위반 증거를 사용하여 실제로 위반자의 스테이크를 온체인에서 몰수하는 과정에 어려움이 있습니다. 특히, 안전성 위반의 경우 전체 검증자 중 1/3 이상이 이미 악의적이며, 위반 증거가 체인에 포함되어 슬래싱 효과를 발휘하는 것을 검열할 수 있습니다. 이러한 경우, 위반자를 슬래시하고 검증자 집합에서 제거하며, 나머지 정직한 검증자들이 체인을 재시작하기 위해 복잡한 사회적 합의 과정이 오프체인에서 발생해야 합니다 [35]. 이에 반해, 우리의 비트코인 스테이킹 프로토콜은 이러한 문제를 겪지 않습니다. 왜냐하면 비트코인 스테이크는 PoS 체인이 아닌 비트코인 체인에 존재하며, PoS 체인에서 안전성 위반이 발생하면 자동으로 슬래시되기 때문입니다.

9.3 책임 있는 주장과 Stakechain

동일성 위반(equivocation)을 처벌하기 위해 추출 가능한 일회성 서명을 사용하는 일반적인 개념은 [32]에서 시작되었습니다. 해당 연구에서는 분산 프로토콜에서 참여자가 **책임 있는 주장(accountable assertion)**을 하려면, 먼저 비트코인 체인에 자금을 타임락해야 한다고 제시합니다. 동일한 맥락에서 두 가지 상이한 주장을 할 경우, 해당 참여자의 개인 키가 유출되며, 누구나 이 키를 사용해 예치금을 회수할 수 있습니다. [24]는 이 개념을 바탕으로 비트코인으로 뒷받침되는 지분증명(PoS) 사이드체인을 제안합니다.

하지만 이 PoS 프로토콜은 블록체인의 각 높이에서 단일 투표 단계만을 포함합니다. 이는 안전성 위반을 명확하게, 동일한 높이에서 두 블록에 대한 동일성 위반으로 모델링할 수 있게 해주지만, 공격자가 매우 적은 지분만 가지고 있어도 프로토콜이 정지되는 문제가 있습니다. 반면, 알려진 BFT 프로토콜 설계는 모두 **다단계 투표(multiple phases of voting)**를 포함하여 생존성을 보장합니다. 우리의 접근은 새로운 PoS 프로토콜을 설계하려는 것이 아니라, 기존의 PoS 합의 프로토콜과 함께 사용되는 부가적인 파이널리티 장치로서 비트코인 스테이킹 프로토콜을 제안합니다. 이는 기반 합의 프로토콜이 생존해 있는 한 전체 프로토콜의 생존성을 보장하며, 동시에 슬래시 가능성을 제공하는데, 이는 EOTS를 사용해 파이널리티 장치에 서명할 때, 모든 안전성 위반이 동일한 높이의 블록에 대한 동일성 위반으로 해석될 수 있기 때문입니다. 또한, [32]에서 제안된 예치 계약은 고정 기간(fixed-term) 예치만 허용하는 반면, 우리는 유연성을 갖춘 접근 방식을 취합니다.

9.4 파이널리티 장치

광의적으로 볼 때, 파이널리티 장치는 기존의 합의 프로토콜 위에 오버레이되는 추가 프로토콜로서, 추가적인 보안 속성을 제공합니다. 최초의 파이널리티 장치는 Casper FFG [18]이며, 이는 가장 긴 체인 프로토콜 위에서 사용되어 네트워크 분할 시 안전성을 보장합니다 (가장 긴 체인 프로토콜은 기본적으로 이 속성을 갖지 못함). 또 다른 파이널리티 장치는 Polkadot에서 사용되는 GRANDPA입니다 [34]. PoS 이더리움의 비콘 체인 합의 프로토콜인 Gasper [19]는 LMD(Latest Message Driven) GHOST 프로토콜 위에 Casper FFG를 파이널리티 장치로 활용합니다. 하지만 [27]은 Gasper가 생존성(liveness) 공격에 취약하다는 것을 보여줍니다. 보안성이 형식적으로 입증된 최초의 파이널리티 장치는 snap-and-chat 프로토콜입니다 [27]. [28]에서 제안된 책임성 장치는 가장 긴 체인 프로토콜에 책임성 속성을 추가할 수 있게 합니다. 우리 비트코인 스테이킹 프로토콜의 EOTS 파이널리티 장치는 이와 유사한 철학을 따릅니다. 이는 기존 BFT 합의 프로토콜에 비트코인 스테이크의 슬래시 가능성 속성을 추가합니다.

9.5 비트코인 머지 마이닝

머지 마이닝(merge mining)은 2010년 사토시 나카모토가 고안한 최초의 비트코인 보안 공유 기술입니다. 이 기술은 최초의 비트코인 사이드체인인 Namecoin을 보호하는 데 사용되었으며, 현재 머지 마이닝을 통해 지원되는 가장 큰 비트코인 사이드체인은 Rootstock입니다 [5]. 머지 마이닝 기술을 활용하면, 비트코인 채굴자는 추가 에너지 소비 없이 동시에 비트코인과 다른 PoW 체인을 함께 채굴할 수 있습니다. 하지만 보안 공유 프로토콜로서의 머지 마이닝은 “*Nothing-at-Stake*” 문제에 직면해 있습니다. 즉, 원칙적으로 채굴자가 비트코인 체인을 정직하게 채굴하는 동시에 사이드체인을 공격할 수도 있다는 것입니다. 비트코인이 채굴자의 주요 수익원인 상황에서는, 사이드체인에서의 악의적인 행위를 억제할 유인이 충분하지 않을 수 있습니다. 반면, 비트코인 스테이킹은 모든 것이 위험에 처한 상태입니다: PoS 체인에서 악의적인 행위는 슬래시될 수 있습니다. 따라서, 비트코인 스테이킹은 머지 마이닝보다 훨씬 강력한 보안 공유 기술입니다.

9.6 비트코인 타임스탬핑

비트코인의 보안을 공유하는 또 다른 기술은 타임스탬핑(timestamping)입니다 [35]. 이 방법은 PoS 블록의 해시와 서명을 트랜잭션 형태로 비트코인 체인에 제출하고 기록하는 방식입니다. 이로 인해 PoS 블록에 추가적인 순서 계층이 부여되어, 포크 발생 시 블록 간 우선순위를 정할 수 있습니다. 이 기술은 바빌론 비트코인 타임스탬핑 테스트넷의 핵심이 됩니다. 비트코인은 트랜잭션 확정에 시간이 오래 걸리기 때문에, 이러한 타임스탬프를 안전하게 기록하는 과정은 느릴 수밖에 없습니다. 따라서, 비트코인 타임스탬핑은 장거리 공격(long-range attack)과 같은 장기 보안에 효과적입니다. 반면, 비트코인 스테이킹은 PoS 체인의 경제적 보안을 강화하여 단기 공격에 대한 방어를 제공합니다. 더불어 앞서 설명했듯이, 비트코인 타임스탬핑은 비트코인 스테이킹 프로토콜의 필수 구성 요소로서, PoS 체인과 비트코인 간의 동기화 역할을 수행합니다.

9.7 프로오브트랜스퍼와 Stacks

Stacks [7]는 PoX(Proof-of-Transfer) 합의 메커니즘을 개발했습니다. 이 메커니즘에서는 채굴자들이 비트코인을 비트코인 체인의 특정 주소로 전송함으로써 다음 블록 제안자가 되기 위해 경쟁하며, 전송 금액이 많을수록 선택 확률이 높아집니다. 이는 지분 증명(Proof-of-Stake) 프로토콜과는 근본적으로 다른 메커니즘이며, 따라서 슬래시 가능성과 스테이커 보안성 같은 속성은 Stacks의 PoX에는 적용되지 않습니다.

그럼에도 불구하고, Stacks의 스마트 컨트랙트가 비트코인 자산에 접근할 수 있도록 하기 위해, Stacks는 sBTC라는 합성 비트코인 토큰을 민트하고 소각하는 방법을 제안합니다. 이는 STX 토큰을 스테이킹한 “Stackers”라 불리는 참여자들에 의해 보안됩니다 [6]. Stackers는 70% 임계값 서명 그룹으로 작동하며 두 가지 역할을 수행합니다: 1) sBTC의 민팅과 상환, 2) 이미 파이널리티가 확정된 Stacks 원장에 대한 포크 승인. 따라서, sBTC 브리지는 전체 스택커의 30% 이상이 정직하면 안전하며, 70% 이상이 정직하게 서명하면 생존성도 확보됩니다. 우리의 접근 방식의 주요 장점은, 비트코인을 브리징하지 않고도 스테이킹을 가능하게 한다는 점입니다. 브리징된 토큰의 총 락업 자산 가치에 의해 보안성이 제한되는 기존 브리징 모델과 대비됩니다.

Stacks와 비교했을 때, 우리의 비트코인 스테이킹 프로토콜은 비트코인을 소비하지 않으며, 보안 위반이 없는 한 비트코인은 그대로 보존됩니다. 이는 자산을 보안 목적으로 보다 효율적이고 확장 가능하게 활용할 수 있게 합니다.

9.8 비트코인 브리징

광의적으로 볼 때, 현재 비트코인 브리지는 세 가지 범주로 분류할 수 있습니다: 중앙화 방식, 담보 기반 방식, 사이드체인 기반 방식이며, 여기에 하드웨어 솔루션을 통한 잠재적 보안 강화가 추가될 수 있습니다. 본 논의에서는 아톰릭 스왑(atomic swaps)은 제외하는데, 이는 사용성, 지연 시간, 유동성 공급 측면의 도전 과제로 인해 기존의 비트코인 브리지에서 채택되지 않았기 때문일 수 있습니다.

중앙화 브리지는 사용자들이 신뢰하는 중앙화된 주체에 의해 운영되며, 대표적인 예는 중앙화 거래소입니다. 사용자는 해당 거래소에 비트코인 또는 타 체인의 래핑된 비트코인을 입금하고, 지원되는 체인 중 하나로 출금할 수 있습니다. 예를 들어, 바이낸스 사용자는 자신의 비트코인을 바이낸스 계정에 입금한 후, BNB 체인 상의 래핑된 비트코인 토큰으로 출금할 수 있습니다. 또 다른 예는 wBTC이며, 여기서 Bitgo가 네이티브 비트코인의 커스터디 역할을 수행합니다 [37]. 이러한 솔루션은 중앙화된 주체가 악의적 행

동을 하지 않거나, 공격받았을 경우 사용자에게 충분한 보상을 제공할 것이라는 강한 신뢰 가정에 기반합니다.

Interlay는 과잉담보된 볼트를 통해 비트코인을 풀카달 생태계로 가져오는 솔루션입니다. 이 볼트는 비트코인을 수령하고 이를 기반으로 래핑된 비트코인을 생성하는 peg-in과, 래핑된 비트코인을 소각하고 네이티브 비트코인을 반환하는 peg-out 기능을 제공합니다 [23]. 여기서 핵심 트레이드오프는 보안성(예: 볼트가 비정상적으로 작동해 비트코인을 탈취할 경우를 대비한 높은 담보 비율)과 수용량(브리징할 수 있는 비트코인의 양은 담보 총액 및 담보 비율에 의해 제한됨) 사이에 존재합니다. 마찬가지로, Stacks가 Nakamoto 업그레이드 [7]에서 제안한 sBTC [6]는 스테킹된 STX 토큰 보유자 집단이 비트코인과 Stacks 체인의 sBTC 토큰 간 peg-in과 peg-out을 수행하는 역할을 맡습니다.

대안적으로, **Nomic**은 텐더민트 기반 체인으로, 비트코인을 nBTC로 브리징한 후 이를 IBC(인터블록체인 통신 프로토콜) [3]을 통해 Osmosis 및 기타 Cosmos 존에서 사용할 수 있도록 합니다 [29]. 이와 같은 브리징 솔루션의 한계는, 브리징된 토큰의 전체 보안이 Nomic 체인의 보안에 의존하며, Nomic 토큰의 총 스테이킹 가치에 의해 느슨하게 상한이 결정된다는 점입니다. 유사하게, Rootstock은 그들의 채굴자들이 비트코인 라이트 클라이언트를 실행하고, 이를 통해 네이티브 비트코인과 해당 체인에서의 합성 비트코인 토큰 간 peg-in 및 peg-out을 수행합니다 [5, 31]. 아래에서 설명할 하드웨어 기반 보안을 제외하면, 이러한 래핑된 비트코인의 보안성은 Rootstock의 PoW 체인의 보안성과 동일한 수준에 머뭅니다.

추가적으로, Rootstock의 비트코인 페깅 메커니즘인 PowerPeg [31]은 보안 하드웨어를 활용하여 비트코인 페깅의 보안을 강화합니다. 유사한 하드웨어 기반 보안 강화는 Avalanche의 비트코인 브리지에도 적용되며, 여기서는 Intel SGX가 사용됩니다 [2]. 런타임에서 코드 무결성을 검증할 수 있다면, 하드웨어 루트 오브 트러스트의 사용은 이러한 브리지의 공격 표면을 이론적으로 줄일 수 있습니다. 그러나 다음과 같은 실질적인 소프트웨어 보안 고려사항이 적용됩니다: a) 보안 하드웨어 내부에서 실행되는 브리징 로직이 외부 소스로부터 얻은 중요한 정보에 의존하는 경우, 브리지의 보안은 외부 컴포넌트의 보안 수준에 종속됩니다; b) 보안 하드웨어 내부 코드에 존재하는 취약점이 악용될 경우, 하드웨어가 제공하는 보안 강화는 무력화될 수 있습니다.

앞서 언급했듯이, 기존 비트코인 브리지의 핵심 리스크 중 하나는, 래핑된 비트코인 토큰이 비트코인보다 훨씬 낮은 보안 수준의 체인에 의해 보호되면서도 상환 가능한 구조라는 점입니다. 다행히도, 외부 체인과 시스템을 보호하기 위한 비트코인 스테이킹을 구현하는 데 있어, 우리는 락업된 비트코인의 완전한 전송 가능성을 요구하지 않습니다. 우리가 제안하는 비트코인 스테이킹 스킴은 락업된 비트코인의 소비 행위를 오직 안전성 위반에 대한 슬래싱으로 제한함으로써, 기존 브리지들의 보안성과 수용량 문제를 우회합니다. 그 결과, 본 스킴은 섹션 4에서 서술한 바와 같은 강력한 안전성 보장을 제공합니다.

10 결론

비트코인은 최초의 블록체인이며, 여전히 시가총액 기준으로 가장 큰 블록체인입니다. 그러나 가치 저장 수단 외의 유틸리티는 작은 블록 공간, 높은 지연 시간, 제한된 프로그래밍 가능성 때문에 제한되어 왔습니다. 특히, 사이드체인이나 기타 레이어 2 프로젝트를 구축하여 비트코인을 확장하고 그 활용 사례를 넓히려는 기존 시도들은 대량의 비트코인을 해당 체인으로 브리징할 수 없는 제약에 가로막혔습니다. 이러한 브리지는 보안성, 수용량, 또는 그 둘 모두에 의해 제한을 받습니다.

우리의 연구는 비트코인 자산에 대한 새롭고 중요한 사용 사례를 제시합니다: PoS 세계에 보안을 제공하는 스테이킹. 우리는 적어도 이 사용 사례에 있어, 비트코인 자산을 다른 체인으로 브리징하지 않고도 PoS 체인에 완전한 경제적 보안을 제공할 수 있음을 보여주었습니다. 이를 실현하기 위한 가장 큰 도전 과제는, 비트코인 체인에 스마트 컨트랙트가 없음에도 불구하고 모든 안전성 위반을 원격으로 슬래시하는 능력을 확보하는 것입니다. 우리는 다음 네 가지 개념을 하나의 프로토콜로 통합하여 이를 달성했습니다:

1. 동일성 위반 시 개인 키를 유출시키는 책임 있는 주장(*accountable assertions*),
2. 모든 안전성 위반을 책임 있는 주장에 대한 동일성 위반으로 변환하는 *파이널리티 장치*(*finality gadgets*),
3. 개인 키 유출 시 자금 소각을 강제하는 *비트코인 커버넌트 에뮬레이션*(*Bitcoin covenant emulation*),
4. 언스테이킹 이전에 슬래싱 트랜잭션이 소비될 수 있도록 보장하는 *비트코인 타임스탬핑*(*Bitcoin timestamping*).

우리의 설계는 모듈화되어 있으며, 모든 PoS 합의 프로토콜 위에서 사용할 수 있습니다. 본 비트코인 스테이킹 프로토콜을 구현하기 위해 비트코인의 소프트 포크나 하드 포크는 필요하지 않습니다.

오디널(Ordinals)과 같은 새로운 사용 사례와 함께, 비트코인은 최근 일종의 르네상스를 겪고 있습니다. 우리는 비트코인 스테이킹이라는 사용 사례가 이 르네상스에 더욱 동력을 불어넣고, 막대한 비트코인 자산에 대한 다른 신뢰 없는(trustless) 사용 사례를 찾으려는 노력을 자극할 것이라 믿습니다.

비트코인에서 일어나는 일은 비트코인에 머무른다.

11 감사의 말

이 라이트페이퍼는 Babylon 팀, ZeroSync의 Robin Linus, Common Prefix 및 임페리얼 칼리지의 Orfeas Stefanos Thyfronitis Litos 간의 협업에서 비롯된 것입니다. 우리는 2023년 Bitcoin Miami에서 Robin Linus를 만나 그의 Stakechain 연구에 대해 들었습니다. 당시 우리는 이미 비트코인 스테이킹에 대해 집중적으로 연구하고 있었기에, 함께 힘을 합쳐 본 작업을 완성하게 되었습니다.

참고문헌

- [1] Akash networks. <https://akash.network/>. Accessed: 2023-07-10.
- [2] How does the avalanche bridge™ work? <https://support.avax.network/en/articles/6349640-how-does-the-avalanche-bridge-work>.
- [3] Inter-blockchain communication protocol. <https://ibcprotocol.org/>.
- [4] Mesh security. <https://github.com/osmosis-labs/mesh-security>
- [5] Rsk. <https://www.rsk.co/>. Accessed: 2021-11-3.
- [6] sbtc: Design of a trustless two-way peg for bitcoin. <https://stx.is/sbtc-pdf>
- [7] Stacks: A bitcoin layer for smart contracts. <https://stx.is/nakamoto>.
- [8] Bip 119: OP_CHECKTEMPLATEVERIFY, 2023. <https://github.com/bitcoin/bips/blob/master/bip-0119.media.wiki>
- [9] Bitcoin staking. 진행 중., 2023.
- [10] Script, 2023.
- [11] Sunny Aggarwal. Mesh Security 강연, Cosmoverse 2022. <https://youtu.be/2ZZBK09-iRs?t=4937>
- [12] Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, Vassilis Zikas. Ouroboros Genesis: 동적 가용성을 갖는 합성형 지분증명 블록체인. *컴퓨터 및 통신 보안 컨퍼런스 (CCS '18)*, ACM, 2018, pp. 913–930.
- [13] Ethan Buchman. *Tendermint: 블록체인 시대의 비잔틴 장애 허용*. 박사학위 논문, 캐나다 퀘베프대학교, 2016.
- [14] Ethan Buchman 외. 텐더민트 재조명: 설계 상의 트레이드오프, 책임성, 실제 사용 사례. *DSN (부록)*, IEEE, 2022, pp. 11–14.
- [15] Ethan Buchman, Jae Kwon, Zarko Milosevic. BFT 합의에 대한 최신 소문. *arXiv preprint arXiv:1807.04938*, 2018.
- [16] Vitalik Buterin. 지분증명: 약한 주관성을 사랑하게 된 계기, 2014.
- [17] Vitalik Buterin. 이더리움 합의에 과부하를 주지 마라. https://vitalik.ca/general/2023/05/21/dont_overload.html, 2023년 5월.
- [18] Vitalik Buterin, Virgil Griffith. Casper: 친근한 파이널리티 장치. *arXiv:1710.09437*, 2019.
- [19] Vitalik Buterin 외. GHOST와 Casper의 결합. *arXiv:2003.03052*, 2020.
- [20] Vitalik Buterin 외. GHOST와 Casper의 결합. *arXiv preprint arXiv:2003.03052*, 2020.
- [21] Phil Daian, Rafael Pass, Elaine Shi. Snow White: 견고한 재구성 가능 합의 및 안전한 지분증명 응용. *금융 암호학 및 데이터 보안 컨퍼런스 (FC '19)*, Springer, 2019, pp. 23–41.
- [22] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, Constantinos Patsakis. 지분증명 프로토콜의 장거리 공격에 대한 조사. *IEEE Access*, 7:28712–28725, 2019.
- [23] Interlay Labs. Interlay v2: 비트코인 금융, 언뱅크드, 2023년 2월. <https://gateway.pinata.cloud/ipfs/QmWp62gdLssFpAoG2JgK8sy3m3rTRUa8LyzoSY8ZFisYNB>

- [24] Robin Linus. Stakechain: 비트코인으로 뒷받침된 지분증명, 2021년 12월. <https://coins.github.io/stakechains.pdf>
- [25] Gregory Maxwell. SCIP 서명을 이용한 Coincovenants — 웃기지만 나쁜 아이디어, 2013. <https://bitcointalk.org/index.php?topic=278122.0>
- [26] Malte Moser, Ittay Eyal, Emin Gün Sirer. 비트코인 커버넌트. *금융 암호학 컨퍼런스*, 2015.
- [27] Joachim Neu, Ertem Nusret Tas, David Tse. Ebb-and-flow 프로토콜: 가용성과 파이널리티 딜레마에 대한 해결책. *보안 및 프라이버시 심포지엄(S&P '21)*, IEEE, 2021.
- [28] Joachim Neu, Ertem Nusret Tas, David Tse. 가용성과 책임성 딜레마 및 이를 해결하기 위한 책임성 장치. *금융 암호학 컨퍼런스*, 2022.
- [29] Nomic. Nomic 비트코인 브리지. <https://www.nomic.io/>
- [30] Greg Osouri, dam Bozanich. AKT: Akash Network 토큰 마이닝 경제학, 2020년 1월. <https://ipfs.io/ipfs/QmdV52bF7j4utynJ6L11RgG93FujiUmBHij7pRD6NjUt6B/>
- [31] Rootstock. Powpeg: 가장 안전하고, 허가가 필요 없으며, 검열 불가능한 비트코인 페그 구축. <https://dev.rootstock.io/rsk/architecture/powpeg/>
- [32] Tim Ruffing, Aniket Kate, Dominique Schröder. 거짓말쟁이여, 비트코인을 잃어라! — 동일성 위반을 비트코인 몰수로 처벌하는 방식. *제22회 ACM 컴퓨터 및 통신 보안 컨퍼런스 (CCS '15)*, ACM, 2015, pp. 219–230.
- [33] Peiyao Sheng, Gerui Wang, Kartik Nayak, Sreeram Kannan, Pramod Viswanath. BFT 프로토콜 포렌식. *CCS*, ACM, 2021, pp. 1722–1743.
- [34] Alistair Stewart, Eleftherios Kokoris-Kogias. GRANDPA: 비잔틴 파이널리티 장치. *arXiv:2007.01560*, 2020.
- [35] Ertem Nusret Tas, David Tse, Fisher Yu, Sreeram Kannan, Mohammad Ali Maddah-Ali. 비트코인 기반 지분증명 보안 강화: 가능한 것과 불가능한 것들. *IEEE 보안 및 프라이버시 심포지엄*, IEEE, 2023.
- [36] EigenLayer 팀. EigenLayer: 리스테이킹 콜렉티브. <https://docs.eigenlayer.xyz/overview/whitepaper/>
- [37] WBTC. 래핑된 비트코인(wBTC). <https://wbtc.network/>