비트코인 스테이킹(Bitcoin Staking): 2,100만 개의 비트코인을 활용해 지분증명 경제를 강화하다

Babylon Team
Version 1.0: 2023-07-13

Translated by DSRV

초록

지분증명(Proof-of-Stake, PoS) 체인은 자본에 의해 보안이 유지되지만, 보안을 위한 비용은 매우 비쌀 수 있습니다. 비트코인(Bitcoin)은 작업증명(Proof-of-Work, PoW) 체인이지만 동시에 6천억 달러 규모의 자산이며, 대부분이 유휴 상태로 남아 있습니다. 본 연구에서는 비트코인 스테이킹(staking)이라는 개념을 제안합니다. 이를 통해 비트코인 보유자는 유휴 비트코인을 스테이킹 하여 PoS 체인의 보안을 강화하고, 그 과정에서 이익을 얻을 수 있습니다. 또한, 비트코인 보유자가 PoS 체인으로 비트코인을 브릿징(bridging)하지 않고도 신뢰할 수 있게 스테이킹할 수 있는 비트코인 스테이킹 프로토콜을 제시합니다. 이 프로토콜은 스테이킹된 비트코인을 완전히 슬래싱(slashing)할 수 있게 하여 PoS 체인에 보안을 보장하며, 비트코인 보유자의 유동성을 극대화하기 위해 빠른 스테이킹 언본딩(unbonding)을 지원합니다. 또한, 이 프로토콜은 다양한 PoS 합의 알고리즘 위에서 작동할 수 있는 모듈형 플러그인으로 설계되었으며, 이를 바탕으로 리스테이킹(restaking) 프로토콜을 구축할 수 있는 기본 구조를 제공합니다. 많은 스테이커(staker)와 PoS 체인으로 확장할 수 있는 시스템 아키텍처도 제안되었으며, 비트코인을 스테이킹한 바빌론(Babylon) 체인이 제어 평면(control plane)으로 동작해 비트코인과 PoS 체인 간의 동기화를 담당합니다. 비트코인 스테이킹은 비트코인의 중요한 신규 활용 사례를 가능하게 하며, 비트코인과 PoS 경제를 통합하기 위한 중요한 진전을 가져옵니다.

1 지분증명(Proof-of-Stake) 보안은 자본이 필요하다

지난 몇 년 동안 블록체인 산업은 작업증명(Proof-of-Work, PoW)에서 지분증명(Proof-of-Stake, PoS)으로 시빌 공격 저항(sybil resistance) 메커니즘의 트렌드가 전환하는 것을 목격했습니다. 이러한 트렌드를 가져온 주요 사건 중 하나는 2022년 9월 이루어진 이더리움의 PoW에서 PoS로의 합의 알고리즘 전환인 “더 머지(The Merge)”입니다.

PoW 블록체인은 복잡한 수학적 문제를 해결하는 채굴자(miner)에 의해 보안이 유지되는 반면, PoS 블록체인은 스테이킹(staking)을 하는 검증자(validator)에 의해 보호됩니다. 검증자가 스테이킹하는 자본은 프로토콜을 위반할 경우 슬래싱(slashing)될 수 있는 보증금 역할을 합니다. 이 슬래싱 가능성은 PoW 체인에는 없는 특징으로, 이더리움이 PoW에서 PoS[18]로 전환한 주요 동기 중 하나입니다. 보안을 담당하는 스테이킹의 시가총액이 클수록 체인을 공격하는 데 드는 비용이 더 많이 들며, 이는 체인의 경제적 보안을 더욱 강하게 만듭니다. 따라서 PoW 체인은 작업에 의해 보호되지만, PoS 체인은 자본에 의해 보호됩니다.

그러나 이러한 자본을 확보하는 것은 특히 작은 체인이나 초기 단계의 체인에게 어려운 일입니다. 높은 수익을 제공하여 자본을 유치하기 위해 높은 인플레이션 비율이 요구됩니다. 예를들어, 60개 이상의 애플리케이션 전용 체인으로 구성된 코스모스(Cosmos) 생태계에서는 초기 연간 인플레이션 비율이 20%에서 100%까지 다양합니다. 이러한 높은 인플레이션은 체인의 장기적인 성장을 저해합니다. 높은 비용은 체인의 보안과 유용성간의 긴장을 야기합니다. 예를 들어, 체인의 인플레이션은 애플리케이션의 활성화를 지원하는 데 사용될 수도 있습니다.

코스모스 SDK 기반으로 분산 AI 컴퓨팅 플랫폼을 운영하는 아카시(Akash) [1] 체인은 이를 잘 보여주는 사례입니다. AKT 토큰의 초기 인플레이션 비율은 100%로, 보안과 고품질 컴퓨팅 하드웨어[30]를 제공하는

공급자에게 보상을 지급합니다. 시간이 지남에 따라 인플레이션 비율이 감소하면 보안과 유용성 간의 긴장은 더욱 심화됩니다.

2 비트코인(Bitcoin) - 6,000억 달러의 자산

PoS로의 전환이 이루어졌음에도 불구하고, 이 글을 작성하는 시점에서 전체 암호 자산의 절반 이상을 차지하는 가장 큰 암호 자산인 비트코인은 여전히 PoW 체인에 의해 보안이 유지되고 있습니다. PoS 자산과 비교했을 때 비트코인 자산은 다음과 같은 몇 가지 중요한 차이점이 있습니다:

1. 비구속 자산: 비트코인은 PoW에 의해 보호되기 때문에, 비트코인 자산 자체가 비트코인 체인을 보호하는 데 사용되지 않습니다. 반면, 모든 PoS 자산은 자신의 체인을 보호하기 위해 사용됩니다.

2. 더 많은 유휴 자산: 비트코인의 대부분은 유휴 상태로 남아 있으며, 활용되지 않습니다. PoS 체인의 자산은 디파이(DeFi) 대출이나 스테이킹과 같은 수익 창출 활동으로 사용되지만, 비트코인을 활용하려면 이를 다른 체인으로 브릿징(bridging)하거나 제3의 중앙화된 수탁사에 맡겨야 합니다. 그러나 이러한 브릿지와 중앙화된 수탁사는 많은 비트코인 보유자에게 높은 위험으로 여겨집니다. 예를 들어, 가장 큰 랩핑(wrapped) 비트코인 자산 중 하나인 wBTC는 시가총액이 비트코인 시가총액의 1%에도 미치지 못하는 50억 달러 이하에 불과합니다.

3. 더 분산화된 보유 구조: 비트코인은 가장 오래된 블록체인으로, 채굴자, 초기 사용자 및 개발자, 프로젝트 창립자, 개인 및 기관 투자자, 거래소 등 가장 분산화된 토큰 보유자 집합을 보유하고 있습니다. 반면, 많은 PoS 체인의 자산은 초기 투자자, 창립자 및 팀원, 재단에 집중되어 있는 경우가 많습니다. 자산이 네트워크를 검증하기 위해 스테이킹되면, 자산이 한곳에 집중되어 있을수록 네트워크가 중앙화될 위험이 커집니다.

4. 낮은 변동성: 비트코인은 시가총액이 가장 큰 암호 자산으로, 대부분의 PoS 자산보다 변동성이 훨씬 낮습니다. PoS 자산의 변동성은 PoS 체인의 보안에 큰 영향을 미칠 수 있습니다. 체인의 보안이 스테이킹된 자산의 시가총액에 직접적으로 의존하기 때문에 자산 가치가 급격히 하락하면 공격자가 체인을 공격할 기회를 제공할 수 있습니다.

3 비트코인 스테이킹(Bitcoin Staking)

이러한 특성을 고려할 때, 비트코인을 스테이킹하여 PoS 체인을 보호하는 데 활용하지 않을 이유가 있을까요? 이것이 바로 이 논문의 핵심인 비트코인 스테이킹입니다.

비트코인 스테이킹은 양면 시장(two-sided marketplace)입니다 (Figure 1). 한쪽에는 보안을 필요로 하며 이에 대한 보상으로 수익을 지불할 준비가 된 PoS 체인이 있습니다. 다른 한쪽에는 자본을 보유하고 이를 통해 수익을 얻고자 하는 비트코인 보유자가 있습니다. 비트코인 스테이킹 프로토콜은 이 양면 시장을 실현하는 보안 공유 프로토콜입니다.

좋은 비트코인 스테이킹 프로토콜은 소비자인 PoS 체인과 제공자인 비트코인 보유자 양쪽 모두에게 강력한 보안을 보장해야 합니다. PoS 체인이 보안 비용으로 수익을 지불할 의향을 가지려면 강력한 보안이 보장되어야하며, 비트코인 보유자가 스테이킹에 참여하려면 자산의 안전성과 수익성이 보장되어야 합니다.아

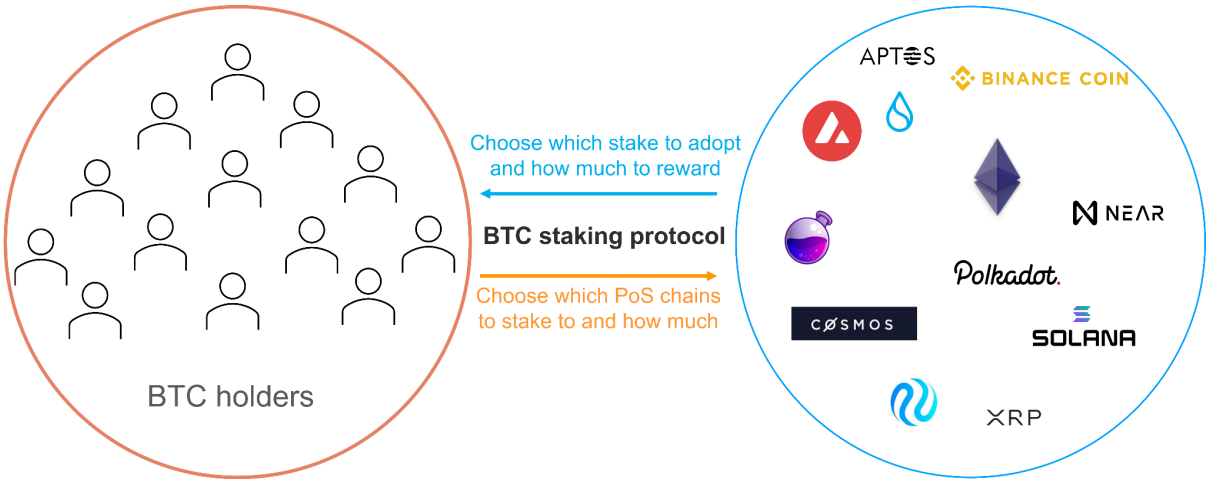

Figure 1. 비트코인 스테이킹은 양면 시장입니다.

4 바빌론(Babylon) 비트코인 스테이킹 프로토콜(Bitcoin Staking Protocol) - 보안 속성

본고에서는 기존의 PoS 체인과 함께 사용할 수 있는 비트코인 스테이킹 프로토콜을 소개합니다. 이 프로토콜은 세 가지 중요한 보안 특성을 가지고 있습니다.:

1. 완전 슬래싱 가능한 PoS 보안: 보안 위반이 발생하면 비트코인 스테이킹 금액의 1/3이 반드시 슬래싱 됩니다. 비트코인 스테이킹 금액의 2/3 이상이 정직하게 PoS 프로토콜을 따르면, PoS 체인은 정상적으로 작동합니다.

2. 스테이커(staker) 보안: 비트코인 스테이커는 PoS 프로토콜을 정직하게 따르면, 언제든 자신의 자금을 언본딩(unbonding)할 수 있습니다.

3. 스테이커 유동성: 스테이킹된 비트코인을 언본딩할 때, 사회적 합의(social consensus) 없이도 안전하고 빠르게 처리됩니다.

속성 1은 프로토콜을 위반한 참여자가 슬래싱 된다는 점을 강조하고, 속성 2는 오직 프로토콜을 위반한 참여자만 자산을 잃는다는 점을 명확히 합니다. 이 두 속성을 합치면, 비탈릭 부테린(Vitalik Buterin)과 버질 그리피스(Virgil Griffith)[18]가 제안한 PoS 보안의 금본위(gold standard)인 “완전 슬래싱 가능성(full slashability)”을 충족합니다. 완전 슬래싱 가능성은 PoS 이더리움(Ethereum) [19]과 텐더민트(Tendermint) [13, 15] 같은 PoS 블록체인 합의 엔진의 핵심 설계 목표입니다. 텐더민트는 코스모스 SDK 체인, 폴리곤(Polygon), BNB 체인 등 다양한 PoS 블록체인을 구축하는 데 널리 사용됩니다. 특히, 속성 2는 기존의 독립형 PoS 프로토콜보다 더 강력합니다. 다른 PoS 체인의 모든 스테이커가 악의적이라 해도, 정직한 스테이커는 여전히 자산을 안전하게 출금할 수 있습니다. 바빌론의 비트코인 스테이킹 프로토콜에서는 출금 제한(검열)이 불가능하여 신뢰가 필요 없는 스테이킹(trustless staking)제공합니다.

기존의 독립적인 PoS 체인(PoS 이더리움이나 코스모스 SDK 체인)은 몇 주에 달하는 긴 언본딩 시간이 필요합니다. 이는 PoS 체인에서 발생할 수 있는 근본적인 “위험부재(nothing-at-stake)" 공격 벡터인 롱레인지 공격(long-range attack) [16, 21, 12, 22]을 방어하기 위해 사회적 합의를 사용하기 때문입니다. 반면, 이 비트코인 스테이킹 프로토콜에서는 스테이킹된 비트코인이 비트코인 체인에 유지되므로, 이러한 롱레인지 공격에 면역이 됩니다. 올바르게 설계된 스테이킹 프로토콜을 통해 바빌론은 속성 3을 실현할 수 있음을 보여줍니다.

5 과제

본 연구에서는 비트코인 스테이킹을 위한 두 가지 기본적인 접근 방식을 고려하며, 각각의 방식에는 고유한 과제가 있습니다.

1. PoS 체인으로의 브릿징

비트코인 스테이킹에 대한 한 가지 접근 방식은 비트코인 체인에서 비트코인 보안의 소비자(consumer) PoS 체인으로 비트코인을 먼저 브릿징하고, 그곳에서 슬래싱 규칙을 적용하는 것입니다. 이 접근 방식은 속성 1,즉 PoS 체인에 슬래싱 가능한 보안을 제공할 수 있지만, 근본적인 한계는 브릿징 솔루션 자체의 보안에 있습니다. 대부분의 기존 비트코인 브릿지는 wBTC의 비트고(Bitgo)같은 중앙화된 수탁사나 다중 서명 브릿지 위원회를 신뢰하는 데 기반합니다. (더 자세한 내용은 섹션 9.8을 참조하십시오.) 심지어 이상적인 비트코인 브릿지조차도 대상 체인의 스테이커를 신뢰해야만 합니다. 따라서 브릿징 솔루션을 사용해서는 속성 2, 즉 신뢰가 필요 없는 스테이킹을 달성할 수 없습니다.

2. 비트코인 체인에서의 원격 스테이킹

비트코인을 브릿징하지 않고 활용할 수 있는 또 다른 접근 방식은 원격 스테이킹입니다. 이 방식은 비트코인 체인에 스테이킹된 비트코인을 컨트랙트(contract)로 잠그고, 소비자 PoS 체인에서 프로토콜 위반이 발생했을 때 스테이킹된 비트코인을 슬래싱하는 것입니다. 이 접근 방식은 아이겐레이어(Eigenlayer)의 이더리움 리스테이킹(restaking) 프로토콜[36]이나 코스모스 생태계의 메쉬 보안(mesh security)[11] [4]과 같은 보안 공유 솔루션에서도 사용됩니다. 이 두 사례에서 보안 제공자 체인(provider chain),즉 보안의 근원은 튜링 완전한 스마트 컨트랙트(smart contract) 계층입니다. 이는 보안 소비자 체인에서 보안 제공자 체인으로 프로토콜 위반 증거를 전송하고, 제공자 체인의 스마트 컨트랙트에서 슬래싱을 실행하는 작업을 기술적으로 간단하게 만듭니다. 그러나 바빌론의 설정에서 보안 제공자 체인은 비트코인입니다. 비트코인은 스마트 컨트랙트를 지원하지 않으며, 표현력이 제한된 스크립트 언어만 제공합니다. 따라서 비트코인이 비트코인 체인에 그대로 유지된다는 점에서 신뢰 없는 스테이킹(속성 2)을 달성할 수 있지만, 이제 남은 주요 과제는 속성 1, 즉 완전 슬래싱 가능한 PoS 보안을 실현하기 위해 슬래싱을 어떻게 수행할 것인지입니다.

바빌론의 비트코인 스테이킹 프로토콜은 원격 스테이킹 방식을 따르지만, 고급 암호학 기술, 합의 프로토콜 혁신, 그리고 비트코인 스크립트 언어의 최적화된 활용을 결합하여 스마트 컨트랙트의 부재라는 한계를 극복했습니다. 이 기술적 세부 사항을 살펴보기 전에, 스테이커의 여정을 통해 비트코인 스테이킹 프로토콜의 주요 기능을 간단히 소개하겠습니다.

6 비트코인 스테이커(Bitcoin Staker)의 여정

Alice는 1 비트코인을 보유하고 있으며, 이를 PoS 체인에 스테이킹하고자 합니다. 먼저, 그녀는 비트코인 체인에 스테이킹 트랜잭션을 전송하여 자신의 비트코인을 셀프 수탁 금고 역할을 하는 스테이킹 컨트랙트에 들어갑니다. 잠긴 비트코인은 Alice의 개인 키를 통해서만 아래 두 가지 방법 중 하나로 잠금 해제가 가능합니다:

1. Alice는 언본딩 트랜잭션을 실행하여 비트코인을 잠금 해제하고, 3일 후 비트코인을 반환받습니다.

2. Alice는 슬래싱 트랜잭션을 실행하여 비트코인을 소각 주소로 전송합니다.

스테이킹 트랜잭션이 비트코인 체인에 기록되면, Alice는 자신의 키를 사용하여 PoS 체인의 블록에 서명하여 검증 작업을 시작할 수 있습니다. 검증 작업 중 Alice는 두 가지 가능한 경로를 따르게 됩니다.

첫 번째, 긍정적인 경로(Happy Path, Figure 2(a))는 Alice가 정직하게 프로토콜을 따르는 경우입니다. Alice가 스테이킹을 중단하고자 할 때, 그녀는 비트코인 체인에 언본딩 요청 트랜잭션을 전송합니다(Figure 2(b)). 언본딩 트랜잭션이 비트코인 체인에 기록되면, Alice의 PoS 체인에서의 검증 작업은 중단되고, 3일 후 출금 요청이 승인되어 1 비트코인이 Alice에게 반환됩니다. 또한, PoS 체인은 Alice에게 보상을 지급합니다.

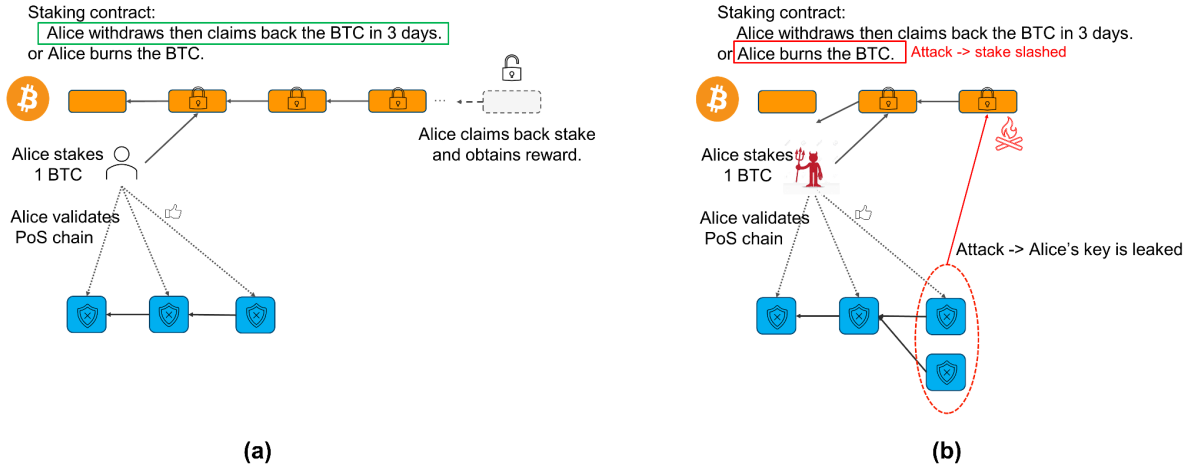

Figure 2:비트코인 스테이커의 여정: (a) 긍정적인 경로: Alice는 스테이킹, PoS 체인 검증, 언본딩 요청을 진행하고 3일 후 언스테이킹; (b) 부정적인 경로: Alice는 스테이킹 후 PoS 체인에서 안전 위반을 저지르고, 비트코인이 소각됨.

두 번째, 부정적인 경로(Unhappy Path, Figure 2(b))는 Alice가 악의적으로 행동하여 PoS 체인에서 이중 지불(double-spend)과 같은 안전 위반(safety violation)을 시도하는 경우입니다(Figure 2(c)). 이 경우, 스테이킹 프로토콜은 Alice의 개인 키를 공개합니다. 이제 누구나 Alice인 척하며 비트코인 체인에 슬래싱 트랜잭션을 전송할 수 있으며, 이는 Alice의 1 비트코인을 소각합니다. 이 부정적인 경로는 모든 안전 위반이 반드시 슬래싱된다는 점을 보장하며, 이를 통해 모든 참여자가 정직하게 프로토콜을 준수하도록 만듭니다.

7 기술 구성 요소

다음은 섹션 6에서 설명한 프로토콜 기능을 가능하게 하고, 섹션 5에서 언급된 과제를 극복하기 위한 핵심 요소들입니다. 구체적인 내용은 곧 발행될 정식 논문 [9]에서 확인할 수 있습니다.

7.1 비트코인 커버넌트 에뮬레이션(Bitcoin Covenant Emulation)을 통한 스테이킹 컨트랙트(Staking Contract)

비트코인에는 스마트 컨트랙트 계층이 없기 때문에, 스테이킹 컨트랙트는 비트코인 스크립트로 작성된 UTXO 트랜잭션 형태로 표현되어야 합니다. [10] 각 UTXO 트랜잭션은 UTXO 세트에서 자금을 소비하며, 비트코인 스크립트는 자금 소비 조건을 지정하기 위한 적은 수의 명령어(opcode)를 제공합니다. 스테이킹 컨트랙트에는 다음과 같은 4가지 트랜잭션이 포함됩니다:

- 스테이킹 트랜잭션, 입력은 스테이커의 비트코인 주소이며, 출력은 다음 두 가지 방법 중 하나로 사용할 수 있습니다:
  - 언본딩 트랜잭션, 상대적 잠금 시간(언본딩 시간을 측정)이 만료된 후 스테이커가 출력을 사용할 수 있습니다. 상대적 잠금 시간은 OP_CHECKSEQUENCEVERIFY [10] 연산자를 사용하여 구현할 수 있습니다.

AN INDIVIDUAL VALIDATOR ν MUST NOT PUBLISH TWO DISTINCT VOTES,

$$\langle \nu, s_1, t_1, \mathrm{h}(s_1), \mathrm{h}(t_1) \rangle \quad \text{AND} \quad \langle \nu, s_2, t_2, \mathrm{h}(s_2), \mathrm{h}(t_2) \rangle \ ,$$

SUCH THAT EITHER:

I. $\mathrm{h}(t_1) = \mathrm{h}(t_2)$.
Equivalently, a validator must not publish two distinct votes for the same target height.

OR

II. $\mathrm{h}(s_1) < \mathrm{h}(s_2) < \mathrm{h}(t_2) < \mathrm{h}(t_1)$.
Equivalently, a validator must not vote within the span of its other votes.

Figure 2: The two Casper Commandments. Any validator who violates either of these commandments gets its deposit slashed.

Figure 3: Casper의 슬래싱 조건 (그림 출처: [18])

- 슬래싱 트랜잭션, 출력을 즉시 소각 주소(사용 불가능한 출력)로 전송할 수 있습니다.

- 언스테이킹(unstaking) 트랜잭션, 언본딩 트랜잭션의 출력은 상대적 잠금 시간이 만료된 후 사용할 수 있습니다.

스테이킹 컨트랙트는 *비트코인 커버넌트(covenant)*[25] [26]의 예로, 트랜잭션 출력이 특정 방식으로만 사용되도록 제한하는 구조입니다. 커버넌트는 비트코인 스크립트의 향후 업그레이드에서 포함될 것으로 제안된 OP_CHECKTEMPLATEVERIFY[8] 연산자를 사용하여 구현할 수 있습니다.

업그레이드 이전에도 커버넌트를 에뮬레이션(emulation)하는 여러 방법이 제안된 바 있습니다. 본 연구의 혁신 중 하나는 신뢰가 필요 없는(trustless) 새로운 커버넌트 에뮬레이션 방식을 도입한 것입니다. 자세한 내용은 [9]를 참조하십시오.

7.2 책임 있는 주장(Accountable Assertions) 및 최종성 장치(Finality Gadgets)을 통한 자동 슬래싱(Auto Slashing)

비트코인에는 스마트 컨트랙트가 없기 때문에, 단순히 안전 위반 증거를 제출하고 비트코인이 이를 처리하도록 기대할 수는 없습니다. 대신, 바빌론의 프로토콜은 슬래싱으로 직접 이어질 수 있는 증거, 즉 스테이커의 개인 키를 제출할 수 있도록 합니다. 안전 위반이 발생할 때마다 스테이커의 개인 키가 노출되도록 보장하기 위해 본 연구에서는 두 가지 아이디어를 결합합니다: (a) 암호학적 책임 있는 주장 (accountable assertions) [32], (b) 블록체인 합의의 최종성 장치(finality gadgets) [18, 27, 28]입니다.

추출 가능한 일회성 서명(Extractable One-Time Signatures, EOTS)은 서명자가 동일한 개인 키를 사용해 두 개의 메시지에 서명할 경우, 해당 개인 키가 누출되도록 설계된 서명 방식입니다. EOTS는 비트코인의 이중 지불과 같은 모순(equivocation)[32]을 처벌하는 일반적인 방법으로 제안되었습니다. 그러나 합의 프로토콜의 슬래싱 조건은 특정 메시지의의 모순보다 더 복잡합니다. 예를 들어, 이더리움 PoS 프로토콜의 슬래싱 모듈인 캐스퍼 FFG(Casper FFG) [18]에서는 두 가지 슬래싱 조건이 있습니다(Figure 3). 첫 번째 슬래싱 조건은 동일한 높이에서 두 블록에 서명하는 것으로, 이는 모순에 해당합니다. 반면, 두 번째 슬래싱 조건은 더 복잡하며 모순으로 표현될 수 없습니다. 마찬가지로, 텐더민트에서도 두 가지 슬래싱 조건이 존재합니다. 첫 번째는 동일한 높이에서 동일한 라운드에 두 블록에 서명하는 것이며, 두 번째는 소위 “기억 상실 공격(amnesia attacks)” [14]에서 발생하는 조건으로, 이는 모순으로 직접적으로 표현될 수 없습니다.

본 연구에서는 기본 합의 프로토콜의 서명 체계를 변경하지 않고, 대신 기본 합의 프로토콜이 블록을 최종화한 후에 추가 서명 라운드를 도입하여 이 문제를 해결합니다. 이 추가 서명 라운드는 EOTS를 사용해 서명됩니다. 블록은 우선 기본 프로토콜에 의해 최종화(finalize)되고, 스테이크의 2/3 이상이 EOTS로 서명했을 때 진정으로 최종화된 것으로 간주됩니다. 이 추가 서명 라운드는 일종의 최종성 장치, 즉 EOTS 최종성 장치로 해석될 수 있습니다.[27] 이

수정된 프로토콜에서 안전 위반이 발생하면, 스테이크의 1/3 이상이 동일한 높이에서 두 블록에 EOTS를 사용해 서명했음이 입증됩니다.[9] 이를 통해 해당 스테이커들의 개인 키를 추출할 수 있습니다. 또한, EOTS 서명 체계는 비트코인에서 사용되는 슈노르 서명(Schnorr signatures)으로 구현될 수 있습니다. 따라서 추출된 개인 키는 슬래싱 트랜잭션을 수행하는 데 사용할 수 있습니다.

이 최종성 장치 기반 솔루션의 가장 중요한 이점 중 하나는 모듈화된 구조입니다. 이는 기본 합의 프로토콜을 변경하지 않고도 모든 BFT(Bizantine Fault Tolerance) 합의 프로토콜 위에서 사용할 수 있습니다. 이를 통해 이 기술은 PoS 체인에 구애받지 않고 활용될 수 있습니다.

7.3 비트코인 타임스탬핑(Bitcoin Timestamping)을 통한 빠른 언본딩(Unbonding)

PoS 체인에서 네이티브(native) 스테이킹을 사용하는 경우, 언본딩 기간은 매우 길게 설정됩니다(예: 코스모스 허브(Cosmos Hub)에서 3주). 이는 롱레인지 공격을 방지하기 위해 사회적 합의를 필요로 하기 때문입니다. 롱레인지 공격은 공격자가 언본딩 후 대체 포크를 생성하는 것으로, 비용이 거의 들지 않습니다. 반면, 비트코인과 같은 PoW 체인에서 롱레인지 공격은 매우 많은 에너지를 소모하며 대체 포크를 생성해야 하기 때문에 비용이 매우 큽니다. 이 비트코인 스테이킹 프로토콜에서는 언본딩 요청이 비트코인 체인에 제출되기 때문에, 이 트랜잭션을 비트코인 체인에서 제거하는 데 드는 비용은 엄청나게 큽니다. 이는 바빌론의 비트코인 스테이킹 프로토콜에서 언본딩이 사회적 합의 없이도 빠르게 이루어질 수 있음을 시사합니다.

그러나 문제는 스테이크 분배는 비트코인 체인에서 유지되지만, 블록에 대한 투표는 PoS 체인에서 이루어진다는 점입니다. 공격자는 PoS 체인을 지연시켜 PoS 블록을 검증하는 데 사용되는 스테이커 세트를 오래된 상태(out-of-date)로 만들 수 있습니다. 이는 공격자가 비트코인 체인에서 언스테이킹한 상태에서도 PoS 체인에서 포크를 생성할 수 있는 투표 권한을 여전히 가질 수 있음을 의미합니다. 스테이커의 개인 키가 노출되더라도, 비트코인 체인에서 이미 언스테이킹을 완료한 상태라면 이를 슬래싱하기에는 너무 늦습니다.

이러한 공격을 방지하고 빠른 언본딩을 가능하게 하기 위해, PoS 체인은 비트코인 체인과 긴밀히 동기화되어야 합니다. 이는 *비트코인 타임스탬핑(timestamping)*이라는 기술을 통해 가능하며, 여기서는 PoS 블록 해시와 블록에 투표한 스테이커 세트가 비트코인 체인에 기록됩니다. 흥미롭게도, 이 비트코인 타임스탬핑 기술은 PoS 체인에서 네이티브 스테이킹을 사용하는 경우에도 안전하고 빠른 언본딩을 위해 매우 유용하며, 비트코인을 외부 신뢰 요인으로 사용할 수 있도록 합니다 [35]. 이 기술은 비트코인 스테이킹 프로토콜에서 빠른 언본딩을 가능하게 하는 데 사용됩니다.

8 시스템 아키텍쳐

위에서 설명한 기본 요소를 기반으로, 비트코인 스테이킹 프로토콜의 핵심 인프라는 비트코인과 PoS 체인 간의 제어 평면(control plane)으로 구성됩니다(Figure 4). 이 제어 평면은 다음과 같은 주요 기능을 담당합니다:

- PoS 체인에 비트코인 타임스탬핑 서비스를 제공하여 PoS 체인과 비트코인 네트워크 간의 동기화를 지원.
- 시장 역할을 수행하여 비트코인 스테이킹과 PoS 체인을 연결하고, 스테이킹 및 검증 정보(예: EOTS 키 등록 및 갱신)를 추적.
- PoS 체인의 최종성 서명(finality signatures)을 기록.

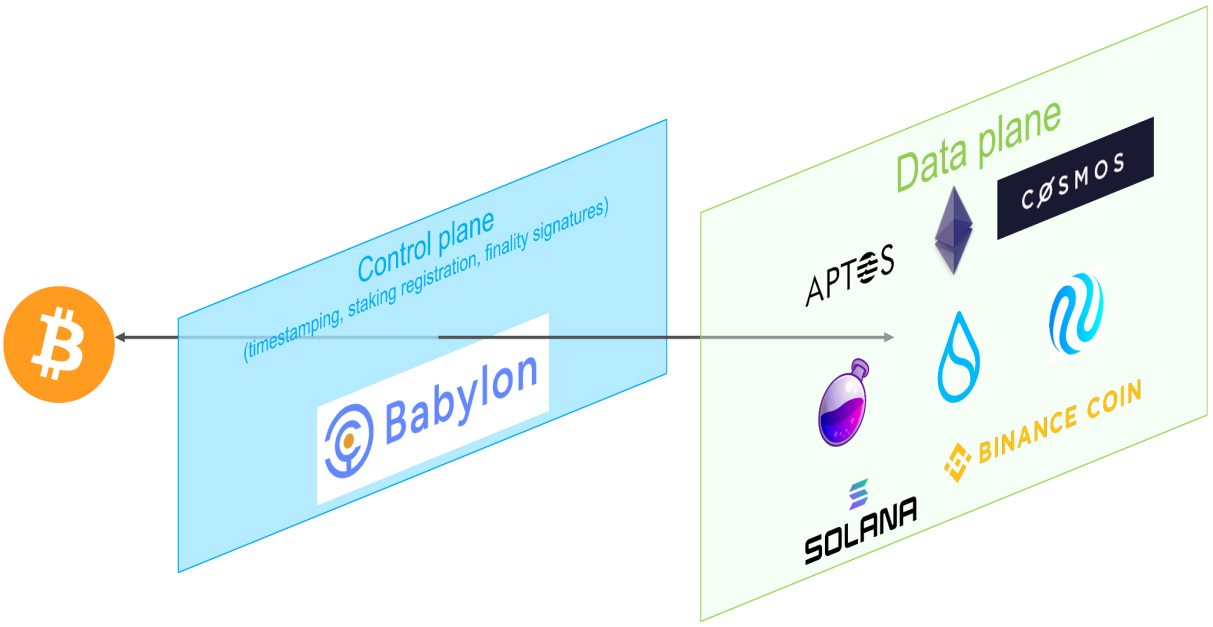

Figure 4: 제어 계층과 데이터 계층을 포함한 시스템 아키텍처

반면, 각 PoS 체인의 검증자들은 일반적인 합의 프로토콜에서와 같이 블록을 생성하고 검증하는 것 외에도, 최종성 장치에서 최종성 서명을 수행합니다. 이 검증자들은 전체 구조에서 데이터 계층 역할을 수행합니다.

제어 평면은 탈중앙화, 보안, 검열 저항성, 확장성을 보장하기 위해 별도의 체인으로 구현됩니다. 예를 들어, 비트코인 네트워크의 제한적이고 비용이 많이 드는 블록 공간은 모든 PoS 체인이 직접 비트코인에 타임스탬프를 기록하는 것을 효율성 및 확장성 없게 만들어, 비트코인 스테이킹의 도입을 저해합니다. 이 문제를 해결하기 위해, 바빌론 팀은 안전한 비트코인 타임스탬핑 프로토콜을 설계하고 이를 코스모스 SDK 기반 바빌론 체인으로 구현했습니다. 이 체인은 표준 IBC(Inter-Blockchain Communication) 프로토콜을 통해 다수의 코스모스 SDK 체인에 대해 효율적인 타임스탬프 집계를 가능하게 합니다. 바빌론 체인은 2023년 2월 첫 번째 테스트넷(testnet)을 출시했으며, 다양한 분야의 30개 이상의 코스모스 SDK 체인과 통합되었습니다(Figure 5).

결과적으로, 바빌론 체인은 제어 평면으로서 작동하며, 비트코인과 데이터 계층인 PoS 체인간의 상호작용을 가능하게 하는 3계층 아키텍처를 제공합니다. 이 아키텍처는 네트워크 효과를 창출하고 상호운용성(interoperability)의 잠재력을 열어줄 수 있습니다. 예를 들어, 두 PoS 체인의 바빌론 체인 상 최종성 상태를 기반으로 바빌론 체인에서 체인 간 거래를 정산(settle)할 수 있습니다.

9 관련 연구

9.1 크로스체인 스테이킹(Cross-chain Staking), 리스테이킹(Restaking), 그리고 메쉬 보안(Mesh Security)

기존의 모든 PoS 체인은 체인의 원장에 기록된 네이티브 자산에 의해 보안이 유지됩니다. 예를 들어, PoS 이더리움은 ETH에 의해, 코스모스 허브는 ATOM에 의해, BNB 체인은 BNB에 의해 보안이 유지됩니다. 그러나 네이티브 토큰만을 사용하는 경우, PoS 체인의 경제적 보안은 네이티브 토큰의 시가총액에 의해 상한선이 정해집니다.

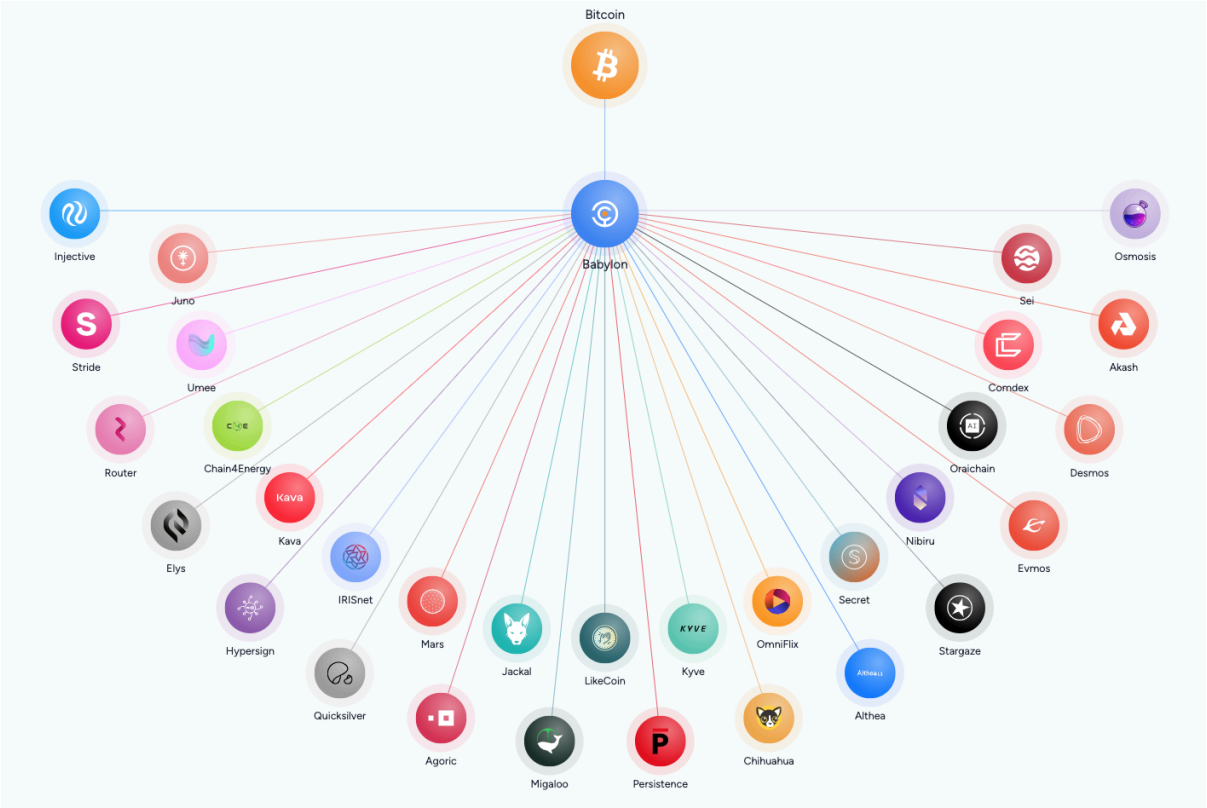

Figure 5: 31개의 IBC 지원 체인과 함께하는 비트코인 타임스탬핑 테스트넷

PoS 체인에서 네이티브 자산 대신 또는 그에 더해 원격으로 자산을 스테이킹하는 것은, 스테이킹된 총 시가총액을 증가시켜 체인의 보안을 강화할 수 있는 방법을 제공합니다. 블록체인 업계에서 떠오르고 있는 접근 방식 중 하나는 *크로스체인 스테이킹(cross-chain staking)*입니다. 여기서는 스테이킹된 외부 자산이 해당 자산의 체인에 남아 있지만, 보호하려는 체인에서 선호하는 검증자를 위해 지정된 스테이킹 컨트랙트에 잠금(lock)됩니다. 스테이킹된 자산은 검증자가 슬래싱이 가능한 잘못을 저지를 경우에만 손실됩니다. 이는 코스모스 생태계를 위해 제안된 메쉬 보안(mesh security) 개념의 기반이 되었습니다 [11, 4]. 보안 제공자 체인의 자산은 다른 보안 소비자 체인을 보호하기 위해 크로스 체인 스테이킹될 수 있습니다.

이 크로스 스테이킹 프로토콜은 아이겐레이어의 이더리움 리스테이킹(restaking) 개념에서 영감을 받았습니다 [36]. 이 개념은 PoS 이더리움에서 스테이킹된 ETH를 가져와 데이터 가용성((data availability) 계층, 브릿지, 오라클(oracle) 서비스 등과 같은 미들웨어, 소위 AVS(Actively Verified Systems)를 보호하기 위해 한번 더 스테이킹하는 것입니다. 이러한 프로젝트를 통해 암호 자산이 네이티브 체인 외의 다른 체인과 서비스를 보호하는 데 사용될 수 있는 일반화된 형태의 PoS가 등장하고 있습니다.

바빌론의 비트코인 스테이킹 프로토콜은 크로스 체인 스테이킹 프로토콜의 한 예로 볼 수 있지만, 코스모스 메쉬 보안과 이더리움 리스테이킹과는 두 가지 중요한 차이점이 있습니다. 첫째, 이더리움 리스테이킹과 코스모스 메쉬 보안에서는 자산이 이미 프로바이더 체인의 보안을 위해 스테이킹된 상태입니다. 반면, 비트코인은 비트코인 자산 자체가 아닌 PoW에 의해 보안이 유지되므로 비트코인 자산은 제약을 받지 않습니다. 이는 리스테이킹에서 발생할 수 있는 과도한 레버리지(over-leveraged) 위험을 줄여줍니다 [17, 36]. 둘째, 비트코인에는 스테이크 슬래싱을 구현하기 위한 스마트 컨트랙트가 없습니다. 대신, 비트코인 스크립트 언어를 최적화하고 고급 암호화 메커니즘을 사용하여 동일한 목표를 달성합니다.

9.2 책임성(Accountability)과 슬래시 가능성(Slashability)

많은 PoS 체인의 중요한 특성 중 하나인 책임성(accountability)은 프로토콜 위반자에게 입증 가능한 방식으로 책임을 물을 수 있는 능력입니다. [18, 20, 33] 이러한 특성은 PoW 체인에서는 존재하지 않는데, 이는 채굴자들이 온체인 신원을 가지지 않기 때문입니다. 실제로 책임 있는 안전성(accountable safety), 즉 안전 위반이 발생했을 때 1/3의 검증자에게 책임을 물을 수 있는 능력은 PoS 이더리움 설계의 핵심입니다 [18, 20].

그러나 책임성과 온체인 슬래싱, 즉 프로토콜 위반 증거를 사용해 온체인에서 위반자의 스테이크를 실제로 몰수하는 것 사이에는 격차가 존재합니다. 특히, 안전 위반의 경우 검증자 중 1/3 이상이 이미 적대적 행위자가 되어 위반 증거가 체인에 기록되고 슬래싱이 실행되는 것을 검열할 수 있습니다. 이런 상황에서는 복잡한 사회적 합의 과정이 오프체인에서 진행되어야만 위반자를 슬래싱하고 검증자 세트에서 제거할 수 있으며, 남아 있는 정직한 검증자들이 체인을 재가동할 수 있습니다 [35].

반면, 바빌론의 비트코인 스테이킹 프로토콜은 이러한 문제를 겪지 않습니다. 이는 비트코인 스테이킹이 PoS 체인이 아닌 비트코인 체인에서 이루어지며, PoS 체인에서 안전 위반이 발생하면 자동으로 슬래싱되기 때문입니다.

9.3 책임 있는 주장(Accountable Assertions)과 스테이크 체인(Stake Chain)

EOTS를 사용해 모순된 행동을 처벌하는 개념은 [32] 에서 처음 제안하였습니다. 해당 연구에서는, 분산 프로토콜의 참여자가 책임 있는 주장(accountable assertions)을 하기 위한 전제 조건으로 비트코인 체인에 예치금을 시간 잠금(timelock)해야 한다고 제안합니다. 동일한 맥락에서 서로 다른 두 주장을 할 경우, 참여자의 개인 키가 노출되고, 누구든지 그 개인 키를 사용해 예치금을 가져갈 수 있습니다.

[24]는 이 개념을 확장하여 비트코인으로 뒷받침되는 PoS 사이드체인(sidechain)을 설계했습니다. 그러나 [24]에서 제안된 PoS 프로토콜은 각 블록 높이에서 한번의 투표 단계만 포함합니다. 이는 안전 위반을 동일한 맥락에서의 모순되는 책임 있는 주장으로 간단히 모델링할 수 있게 합니다. (블록 높이를 맥락으로 간주하고, 안전 위반을 동일한 높이의 두 블록 간의 모순으로 표현) 하지만, 이 프로토콜은 공격자가 매우 적은 지분을 가지고 있어도 활성 상태(liveness)을 보장하지 못합니다.

반면, 기존 BFT 프로토콜 설계는 모두 활성 상태를 보장하기 위해 여러 단계의 투표를 포함합니다. 바빌론의 연구는 새로운 PoS 프로토콜을 처음부터 설계하려는 것이 아니라, 비트코인 스테이킹 프로토콜을 추가적인 최종성 장치로서 기존 PoS 합의 프로토콜과 결합해 사용합니다. 이는 기본 합의 프로토콜이 활성 상태를 유지하는 한 전체 프로토콜의 활성 상태를 보장하면서도, 최종성 장치에서 EOTS를 사용해 서명할 때 안전 위반이 동일한 블록 높이에서의 모순으로 표현되므로 슬래싱이 가능합니다. 또한, 바빌론의 프로토콜에서 사용되는 스테이킹 컨트랙트는 일정 지연 후 언제든 자금의 인출을 허용하는 반면, [32]에서의 컨트랙트는 고정된 기간 동안만 예치금을 유지하도록 설계되어 있습니다.

9.4 최종성 장치(nality Gadgets)

넓은 의미에서, 최종성 장치는 기존의 합의 프로토콜 위에 추가로 사용되어 보안 보장을 강화하는 오버레이 프로토콜로 볼 수 있습니다. 최초의 최종성 장치는 캐스퍼 FFG[18]로, 네트워크 분할 상황에서도 안전성을 보장하기 위해 가장 긴 체인(longest chain) 프로토콜 위에 사용됩니다(가장 긴 체인 프로토콜은 네트워크 분할 상황에서 이러한 안전성을 보장하지 못함). 또 다른 최종성 장치로는 폴카닷(Polkadot)에서 사용되는 GRANDPA[34]가 있습니다.

PoS 이더리움의 비콘 체인 합의 프로토콜인 개스퍼(Gasper) [19]는 LMD GHOST 프로토콜 위에서 캐스퍼 FFG를 최종성 장치로 사용합니다. 그러나 [27]은 개스퍼가 활성 상태 공격에 취약하다는 것을 보여줍니다. 최초로 보안성이 형식적으로 증명된 최종성 장치 설계는 스냅 앤 채팅(snap-and-chat) 프로토콜입니다 [27]. 또한, [28]에서 제안된 책임성 장치는 가장 긴 체인 프로토콜에 책임성을 추가할 수 있도록 합니다. 바빌론의 비트코인 스테이킹 프로토콜에서 사용되는 EOTS 기반 최종성 장치 설계는 이와 유사한 철학을 따릅니다. 이는 기존의 BFT 합의 프로토콜에 비트코인 스테이크의 슬래싱 가능성을 추가하는 속성을 더합니다.

9.5 비트코인 병합 채굴(Bitcoin Merge Mining)

병합 채굴(merge mining)은 2010년 사토시 나카모토(Satoshi Nakamoto)가 비트코인의 보안을 공유하기 위해 고안한 최초의 기술입니다. 이 기술은 최초의 비트코인 사이드체인인 네임코인(Namecoin)을 보호하기 위해 사용되었습니다. 현재 병합 채굴로 지원되는 가장 큰 비트코인 사이드체인은 루트스톡(Rootstock)입니다 [5]. 병합 채굴을 사용하면, 비트코인 채굴자들은 추가 에너지를 사용하지 않고도 비트코인과 다른 PoW 체인을 동시에 채굴할 수 있습니다. 그러나 보안 공유 프로토콜로서 병합 채굴은 “위험부재(nothing-at-stake)” 공격 문제에 의해 위협받습니다. 원칙적으로, 채굴자들은 비트코인 체인을 정직하게 채굴하면서도 사이드체인을 공격할 수 있습니다. 비트코인이 채굴자들에게 주요 수익원이기 때문에, 사이드체인에서 악의적인 행동을 억제할 충분한 억제력이 없을 수 있습니다. 반면, 비트코인 스테이킹에서는 모든 것이 걸려 있습니다. PoS 체인에서의 악의적인 행위는 슬래싱으로 제재받을 수 있습니다. 따라서 비트코인 스테이킹은 병합 채굴보다 훨씬 강력한 보안 공유 기술입니다.

9.6 비트코인 타임스탬핑(Bitcoin Timestamping)

비트코인의 보안을 공유하는 또 다른 기술은 타임스탬핑입니다 [35]. PoS 블록의 해시와 서명이 트랜잭션으로 제출되어 비트코인 체인에 기록됩니다. 이를 통해 PoS 체인의 포크가 발생했을 경우, PoS 블록 간의 우선 순위를 정할 수 있는 추가적인 계층을 제공합니다. 이 기술은 바빌론 비트코인 타임스탬핑 테스트넷의 기반이 됩니다. 비트코인은 트랜잭션을 확정하는 데 시간이 오래 걸리기 때문에, 이러한 타임스탬프를 비트코인 체인에 안전하게 기록하는 과정은 느립니다. 따라서 비트코인 타임스탬핑은 롱레인지 공격에 대항하는 장기적인 보안을 제공하는 데 효과적입니다. 반면, 비트코인 스테이킹은 PoS 체인의 경제적 보안을 강화하여 숏레인지 공격(short-range attack)으로부터 보호합니다. 또한, 앞서 논의된 바와 같이, 비트코인 타임스탬핑은 비트코인 스테이킹 프로토콜의 필수적인 부분으로, PoS 체인과 비트코인 간의 동기화를 담당합니다.

9.7 전송 증명(Proof-of-Transfer) 및 스택스(Stacks)

스택스(Stacks)[7]는 전송 증명(Proof-of-Transfer, PoX) 합의 메커니즘을 개발했으며, 이 메커니즘에서 채굴자들은 비트코인 체인의 특정 주소로 비트코인을 전송함으로써 다음 블록 제안자가 되기 위해 서로 경쟁합니다. 전송된 금액이 많을수록 블록 제안자로 선정될 확률이 높아집니다.
이는 PoS프로토콜과 근본적으로 다른 메커니즘이기 때문에, 슬래싱 가능성과 스테이커의 보안 속성은 스택스의 PoX에 적용되지 않습니다.
그럼에도 불구하고, 스택스의 스마트 컨트랙트가 비트코인 자산에 접근할 수 있도록 비트코인을 스택스에 연결하기 위해 스택스는 sBTC라는 합성 비트코인 토큰을 발행하고 소각하는 방법을 제안합니다. 이 토큰은 STX 토큰 스테이커, 즉 “스택커(Stackers)”[6]에 의해 보안이 유지됩니다. 스택커는 70% 임계값 서명 그룹으로 작동하며 두 가지 주요 책임을 집니다: 1) sBTC의 발행 및 상환, 2) 이미 최종화된 스택스 원장의 포크 승인.따라서 sBTC 브릿지의 보안은 스태커 중 30% 이상이 정직할 경우 안전하며, 70% 이상이 트랜잭션에 정직하게 서명할 경우 원활히 운영됩니다. 바빌론의 주요 이점 중 하나는, 브릿지 프로젝트에서 발행된 토큰의 총 잠금 자산 가치에 의해 보안이 제한되는 비트코인 브릿징 없이도 비트코인 스테이킹을 가능하게 했다는 점입니다.
스택스와 비교했을 때, 바빌론의 비트코인 스테이킹 프로토콜은 비트코인을 사용하는 것을 요구하지 않으며, 보안 위반이 발생하지 않는 한 스테이킹된 비트코인을 보존합니다. 이는 보안 애플리케이션을 위해 자산을 보다 효율적이고 확장 가능하게 활용할 수 있도록 합니다.

9.8 비트코인 브릿징(Bitcoin Bridging)

현재 비트코인 브릿지는 크게 세 가지 범주로 나뉩니다: 중앙화된 방식, 담보 기반 방식, 사이드체인 기반 방식이며, 하드웨어 솔루션을 통한 잠재적 보안 강화를 포함할 수 있습니다. 여기서는 주요 비트코인 브릿지에서 채택되지 않은 원자적 교환(atomic swap)은 논의에서 제외합니다. 이는 사용성, 지연 시간, 유동성 확보의 어려움 때문일 가능성이 있습니다.

중앙화된 브릿지는 사용자에게 신뢰받는 중앙 주체에 의해 운영됩니다. 대표적인 예로는 사용자가 비트코인과 다른 체인의 래핑된 비트코인 토큰을 입출금할 수 있는 중앙화 거래소가 있습니다. 예를 들어, 바이낸스(Binance) 사용자는 본인의 네이티브 비트코인을 바이낸스 계정에 입금한 뒤 BNB 체인에서 래핑된 비트코인 토큰으로 인출할

수 있습니다. 또 다른 예로는 wBTC가 있으며, 여기서는 비트고가 네이티브 비트코인의 수탁자 역할을 합니다 [37]. 이러한 솔루션은 중앙 주체가 악의적으로 행동하지 않거나, 공격을 받더라도 사용자 손실을 충분히 보상할 것이라는 강한 가정 하에서 작동합니다.

인터레이(Interlay)는 폴카닷 생태계로 비트코인을 가져오는 솔루션으로, 과담보된 금고(overcollateralized vault)를 통해 비트코인의 페깅(pegging) 작업(네이티브 비트코인을 받으면 래핑된 비트코인 생성, 래핑된 비트코인을 소각하면 네이티브 비트코인 반환)을 제공합니다 [23]. 이 솔루션의 주요 트레이드오프는 보안(예: 금고가 비트코인을 탈취할 경우를 대비해 높은 담보화 비율 요구)과 용량(브릿지되는 비트코인의 양은 담보와 담보화 비율에 의해 제한됨) 간의 균형입니다. 비슷하게, 스택스는 나카모토(Nakamoto) 업그레이드 [7]에서 sBTC [6]를 제안하며, 이는 스택커들이 비트코인과 스택스 체인의 sBTC 토큰 간 페깅 작업을 담당합니다.

노믹(Nomic)은 텐더민트 기반 체인으로, 비트코인을 nBTC로 브릿지할 수 있는 방법을 제공합니다. nBTC는 IBC [3]를 통해 오스모시스(Osmosis) 및 기타 코스모스 생태계 [29]에서 사용할 수 있습니다. 하지만 이러한 브릿징 솔루션의 한계는 브릿지된 토큰의 보안이 노믹 체인의 보안에 의존하며, 이는 노믹 토큰의 총 스테이킹 가치에 의해 느슨하게 제한된다는 점입니다. 비슷하게, 루트스톡(Rootstock)은 채굴자들에게 비트코인 라이트 클라이언트를 실행하도록 하고, 이를 통해 네이티브 비트코인과 루트스톡 체인의 합성 비트코인 토큰 간 페깅 작업을 수행합니다 [5, 31].

또한, 루트스톡의 비트코인 페깅 메커니즘인 파워페그(PowerPeg) [31]은 비트코인 페깅의 보안을 강화하기 위해 보안 하드웨어를 활용합니다. 유사한 하드웨어 기반 보안 강화는 아발란체(Avalanche)의 인텔 SGX[2]를 사용하는 비트코인 브릿지가 있습니다. 하드웨어 신뢰 루트(root of trust)를 활용하면 원칙적으로 코드 무결성을 실행 시점에 검증할 수 있는 경우, 이러한 브릿지의 공격 표면을 줄일 수 있습니다. 그러나 실제 소프트웨어 보안 측면에서 다음과 같은 고려사항이 적용됩니다: a) 보안 하드웨어 내부에서 실행되는 브릿징 로직이 외부 소스에서 얻은 중요한 정보에 의존하는 경우, 이러한 브릿지의 보안은 외부 구성 요소의 보안에 의해 제한됩니다. b) 보안 하드웨어 내부에서 실행되는 코드의 보안 취약점이 악용될 경우, 하드웨어가 제공하는 보안 강화는 무효화될 수 있습니다.

앞서 언급했듯이, 기존 비트코인 브릿지의 주요 위험은 래핑된 비트코인 토큰의 상환 가능성이 비트코인보다 훨씬 낮은 보안을 가진 체인에 의해 보호된다는 점에 있습니다. 다행히도, 외부 체인과 시스템을 보호하기 위해 비트코인 스테이킹을 사용할 경우, 잠금된 비트코인의 완전한 양도 가능성을 요구하지는 않습니다. 바빌론의 비트코인 스테이킹 설계는 잠금된 비트코인의 지출 작업을 안전 위반 슬래싱으로만 제한함으로써, 기존 비트코인 브릿지가 가진 보안과 용량 문제를 우회합니다. 그 결과, 본 설계는 섹션 4에서 언급된 바와 같이 강력한 안전 보장을 제공합니다.

10 결론

비트코인은 시가총액 측면에서 여전히 1위의 블록체인입니다. 그러나 가치 저장 수단 외에는 제한적인 블록 공간, 높은 지연 시간, 제한된 프로그래밍 가능성으로 인해 그 유틸리티가 제한되었습니다. 특히, 비트코인을 확장하거나 새로운 사용 사례를 추가하려는 이전의 노력은 대량의 비트코인을 다른 체인으로 브릿징하지 못한 문제로 인해 어려움을 겪었습니다. 브릿지는 보안과 용량의 한계로 인해 활용이 제한되었습니다.

본 연구는 비트코인 자산에 새로운 중요한 사용 사례를 제시합니다: PoS 세계에 보안을 제공하기 위한 스테이킹. 바빌론의 사례에는 비트코인 자산을 다른 체인에 연결할 필요 없이, PoS 체인에 완전한 경제적 보안을 제공할 수 있다는 것을 보여줍니다. 이를 달성하기 위한 가장 큰 도전은 비트코인 체인에 스마트 컨트랙트 없이 모든 안전 위반을 원격으로 처벌할 수 있는 방법을 찾는 것입니다. 바빌론은 이를 네 가지 핵심 기술을 하나의 프로토콜로 통합하여 해결했습니다:

1. 책임 있는 주장(Accountable Assertions): 이중 서명 시 개인 키를 유출하도록 설계.
2. 최종성 가젯(Finality Gadgets): 모든 안전 위반을 책임성 주장으로 변환.
3. 비트코인 커버넌트 에뮬레이션(covenant emulation): 키 유출 시 자금을 소각하도록 강제.
4. 비트코인 타임스탬핑(timestamping): 슬래싱 트랜잭션이 언본딩 이전에 실행되도록 보장.

이 프로토콜은 모듈형 설계로, 모든 PoS 합의 프로토콜 위에 적용 가능합니다.비트코인의 소프트 포크(soft fork)나 하드 포크(hard fork)는 필요하지 않습니다.

최근 오디널스(Ordinals)와 같은 새로운 사용 사례로 비트코인은 일종의 부흥기를 맞이했습니다. 바빌론의 비트코인 스테이킹은 이러한 부흥에 추가적인 동력을 제공할 것이며, 비트코인 자산의 신뢰할 수 있는 새로운 활용 사례를 찾기 위한 노력을 고무시킬 것입니다.

“비트코인에서 일어난 일은 비트코인에 머문다.”

11. 감사의 글

이 라이트페이퍼는 바빌론팀, 제로싱크(ZeroSync)의 로빈 리너스(Robin Linus), 그리고 커먼 프리픽스(Common Prefix) 및 임페리얼 콜리지(Imperial College)의 오르페아스 스테파노스 티프로니티스 리토스(Orfeas Stefanos Thyfronitis Litos)와의 협력을 통해 작성되었습니다. 바빌론 팀은 비트코인 마이애미 2023에서 로빈 리너스를 만나 그의 스테이크체인(Stakechain) 작업에 대해 들었습니다. 그 당시 바빌론 팀은 이미 비트코인 스테이킹에 대해 집중적으로 연구하고 있었고, 이를 계기로 협력하여 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/bip0119.mediawiki.

[9] Bitcoin staking. In progress., 2023.

[10] Script, 2023.

[11] Sunny Aggarwal. Mesh security talk at cosmoverse 2022. https://youtu.be/Z2ZBKo9-iRs?t=4937.

[12] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros Genesis: Composable proof-of-stake blockchains with dynamic availability. In Conference on Computer and Communications Security, CCS ’18, pages 913–930. ACM, 2018.

[13] Ethan Buchman. Tendermint: Byzantine fault tolerance in the age of blockchains. PhD thesis,University of Guelph, 2016.

[14] Ethan Buchman, Rachid Guerraoui, Jovan Komatovic, Zarko Milosevic, Dragos-Adrian Seredinschi, and Josef Widder. Revisiting tendermint: Design tradeoffs, accountability, and practical use. In DSN (Supplements), pages 11–14. IEEE, 2022.

[15] Ethan Buchman, Jae Kwon, and Zarko Milosevic. The latest gossip on BFT consensus. arXiv preprint arXiv:1807.04938, 2018.

[16] Vitalik Buterin. Proof of stake: How i learned to love weak subjectivity, 2014.

[17] Vitalik Buterin. Don’t overload Ethereum consensus. Available at: https://vitalik.ca/general/2023/05/21/dont_overload.html, May 2023.

[18] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. arXiv:1710.09437, 2019.

[19] Vitalik Buterin, Diego Hernandez, Thor Kamphefner, Khiem Pham, Zhi Qiao, Danny Ryan, Juhyeok Sin, Ying Wang, and Yan X Zhang. Combining ghost and casper. arXiv:2003.03052,2020.

[20] Vitalik Buterin, Diego Hernandez, Thor Kamphefner, Khiem Pham, Zhi Qiao, Danny Ryan,Juhyeok Sin, Ying Wang, and Yan X Zhang. Combining GHOST and Casper. arXiv preprint arXiv:2003.03052, 2020.

[21] Phil Daian, Rafael Pass, and Elaine Shi. Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. In Financial Cryptography and Data Security,FC ’19, pages 23–41. Springer, 2019.

[22] Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, and Constantinos Patsakis. A survey on long-range attacks for proof of stake protocols. IEEE Access, 7:28712–28725, 2019.

[23] Interlay Labs. Interlay v2: Bitcoin finance, unbanked, February 2023. https://gateway.pinata.cloud/ipfs/QmWp62gdLssFpAoG2JqK8sy3m3rTRUa8LyzoSY8ZFisYNB.

[24] Robin Linus. Stakechain: A bitcoin-backed proof-of-stake, December 2021. https://coins.github.io/stakechains.pdf.

[25] Gregory Maxwell. Coincovenants using scip signatures, an amusingly bad idea, 2013. https://bitcointalk.org/index.php?topic=278122.0.

[26] Malte Moser, Ittay Eyal, and Emin Gun Sirer. Bitcoin convenants. In Financial Cryptography, 2015.

[27] Joachim Neu, Ertem Nusret Tas, and David Tse. Ebb-and-flow protocols: A resolution of the availability-finality dilemma. In Symposium on Security and Privacy, S&P ’21. IEEE, 2021.

[28] Joachim Neu, Ertem Nusret Tas, and David Tse. The availability-accountability dilemma and its resolution via accountability gadgets. In Financial Cryptography, 2022.

[29] Nomic. Nomic bitcoin bridge. https://www.nomic.io/.

[30] Greg Osouri and dam Bozanich. Akt: Akash network token mining economics, January 2020. https://ipfs.io/ipfs/QmdV52bF7j4utynJ6L11RgG93FuJiUmBH1i7pRD6NjUt6B.

[31] Rootstock. Powpeg: Building the most secure, permissionless and uncensorable bitcoin peg. https://dev.rootstock.io/rsk/architecture/powpeg/.

[32] Tim Ruffing, Aniket Kate, and Dominique Schröder. Liar, liar, coins on fire! penalizing equivocation by loss of bitcoins. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS ’15, page 219–230, New York, NY, USA, 2015. Association for Computing Machinery.

[33] Peiyao Sheng, Gerui Wang, Kartik Nayak, Sreeram Kannan, and Pramod Viswanath. BFT protocol forensics. In CCS, pages 1722–1743. ACM, 2021.

[34] Alistair Stewart and Eleftherios Kokoris-Kogia. GRANDPA: A Byzantine finality gadget. arXiv:2007.01560, 2020.

[35] Ertem Nusret Tas, David Tse, Fisher Yu, Sreeram Kannan, and Mohammad Ali Maddah-Ali. Bitcoin-enhanced proof-of-stake security: Possibilities and impossibilities. In IEEE Symposium on Security and Privacy. IEEE, IEEE, 2023.

[36] EigenLayer Team. Eigenlayer: The restaking collective. https://docs.eigenlayer.xyz/overview/whitepaper.

[37] WBTC. Wrapped bitcoin (wbtc). https://wbtc.network/.