BOB: 하이브리드 L2

비전 페이퍼, 2024년 10월

알렉세이 자미야틴과 도미니크 하츠(Alexei Zamyatin) 도미니크 하츠(Dominik Harz)
research@gobob.xyz

개요

BOB는 새로운 유형의 비트코인 보안 블록체인인 하이브리드 L2이다. 하이브리드 L2는 가장 안전하고 탈중앙화된 네트워크인 비트코인의 보안을 계승한다. 비트코인 보안을 사용하여 하이브리드 L2는 비트코인, 이더리움 및 기타 L1에 대한 신뢰 최소화된 브릿지를 생성한다. 이로 인해 하이브리드 L2는 상호 운용성을 갖추기 위해 타사 브릿지에 의존하지 않으며, 파편화된 BTC 멀티체인 유동성 문제를 해결한다.

1 소개

비트코인은 처음부터 투명하고 검열에 강한 탈중앙화된 결제 시스템으로 개발되었다. 10년 후, 스마트 계약 체인을 기반으로 탈중앙화된 금융 애플리케이션과 대체 불가능한 토큰, 소셜 미디어와 게임의 토큰화, DAO와 기타 신뢰 최소화 거버넌스 구조를 포함한 다른 혁신적인 제품이 탄생했다. 비트코인은 여전히 전 세계 암호화폐 도입에 중심에 있지만, 혁신과 개발자 활동 측면에서는 뒤처져 있다.

느리고 경직된 네트워크의 특성에도 불구하고 비트코인은 시가총액, 거래량, 활성 사용자 수 측면에서 다른 모든 암호화폐를 합친 것보다 더 큰 규모를 유지하고 있다. 비트코인은 전 세계 3억 명의 사용자, 1조 달러에 달하는 시가총액, 독보적인 브랜드 인지도로 그 어느 때보다 독보적인 위상을 자랑하고 있다. 그럼에도 디파이(DeFi) 거래량의 경우, 비트코인은 가장 적은 거래량을 보이고 있다. 시가총액 대비 디파이 TVL 비율이 30%에 달하는 이더리움에 비해 비트코인의 디파이 TVL은 시장 규모의 0.1%에 불과해 300배의 격차가 존재한다.

지난 몇 년 동안 프로토콜 변경과 포크를 통해 스마트 계약과 디파이를 비트코인에 도입하려는 수많은 시도가 있었지만, 이는 번번이 실패했다. 비트코인은 스마트 계약과 같이 기능을 크게 변경하거나 복잡성을 유발하는 모든 프로토콜 업그레이드에 반대해 왔다. 비트코인이 향후 이더리움을 통해 우리가 알게 된 네이티브 프로그래밍 기능을 탑재할 일은 없어 보인다. 따라서 결국은 비트코인 L2가 BTC 디파이을 위한 솔루션으로 자리매김하게 될 것이다.

하이브리드 L2. 하이브리드 L2. 이 백서에서는 비트코인을 기반으로, 디파이를 생성하고 확장하는 데 따르는 주요 과제를 해결할 목적으로 설계된 새로운 비트코인 레이어 2 솔루션, 하이브리드 L2를 소개한다. 하이브리드 L2는 세 가지 핵심 특성을 구현한다.

- BitVM2[4]를 사용하여 비트코인에 대한 옵티미스틱 검증과 결함 증명을 구현하여 **비트코인 보안**을 강화한다.
- **신뢰 최소화 BTC 브릿지.** BitVM 기반 브릿지 설계는 비트코인이 안전하고 네트워크에 온체인 분쟁을 수행할 정직한 노드(예: 사용자 자신)가 하나 이상 있기만 하면 사용자가 BOB를 통해 BTC를 입출금할 수 있도록 한다. 이 새로운 보안 모델을 실존적 정직성(1/n)이라고 하며, 이는 정직한 다수 가정(t/n)에 의존하는 기존 BTC 다중 서명 브릿지보다 월등히 우수하다.
- **이더리움으로의 신뢰 최소화 브릿지**(비트코인 보안). BOB는 L1/L2 옵티미스틱 이더리움 롤업의 브릿지 설계를 L1 스마트 계약으로 인코딩된 비트코인 라이트 클라이언트와 결합하여 비트코인 완결성에 대한 L2 인출 정확성을 조정한다. 이 설계는 스마트 계약을 보유한 대부분의 L1 체인으로 확장있다.

최초의 하이브리드 L2인 BOB는 가장 신뢰할 수 있는 단일 네트워크인 비트코인을 통해 L2와 모든 크로스체인 브릿지 모두를 보호하여 무신뢰 상호운용성 문제에 대한 실용적인 솔루션을 제공한다. 또한 BOB는 수십 개의 체인에 걸친 BTC 유동성 파편화 문제에 대한 해결 방안을 제공한다. 사용자는 BTC를 디파이 지원 체인에 랩핑하는 대신 다양한 체인의 자산을 BOB 네트워크에 예치하여 네이티브 BTC 유동성과 비트코인 보안 인출을 활용할 수 있다. 마지막으로, BOB는 비트코인에 수수료를 제공함으로써 BTC의 보안 예산의 장기적인 지속 가능성에 기여한다.

2 오늘날의 비트코인 L2: 치료와 저주

비트코인 L2는 비트코인의 핵심 원칙을 바꾸지 않으면서도 비트코인에 혁신을 불어넣을 수 있는 잠재력을 가지고 있다. 중앙화된 거래소 없이도 수조 달러 규모의 비트코인 시장에서 거래, 대출, 스테이킹과 같은 디파이 사용 사례를 실현할 수 있는 비트코인 L2의 가능성은 수천 명의 개발자를 끌어모았고, 이미 수십 개의 체인이 "비트코인 L2"라는 이름을 내세우고 있다.

그러나 비트코인 L2를 구축하는 것은 어려운 일이며, 이전의 시도들은 이더리움 수준의 관심을 끌어내는 데 어려움을 겪었다. 당사는 성공적인 비트코인 L2를 출시하기 위해 다음 세 가지 과제를 고려했다.

- **비트코인 보안과 신뢰 최소화 BTC 브릿징.** 이것이 바로 비트코인 L2를 다른 모든 체인으로부터 차별화시키는 요소이다. 이는 가장 강력하고 탈중앙화된 네트워크의

보안과 제3자를 신뢰하지 않고도 BTC를 입출금할 수 있는 방법의 결합을 의미한다. 지금까지는 거의 모든 BTC 브릿지가 신뢰성 다중 서명을 사용했기 때문에 이것이 불가능했다. 하지만 BitVM2로 인해 이제 비트코인 역사상 처음으로 이를 실현할 수 있는 청사진이 마련되었다.

- **경쟁 우위의 생태계 구축.** L2의 성공은 디앱 생태계의 성공에 기반한다. 성공적인 제품을 만들기 위해서는 지갑, 기관 수탁, 오라클과 같은 업계 최고의 개발자 도구와 디파이 인프라가 필수적이다. 이는 또한 1초 미만의 거래 속도와 가스 토큰의 추상화 등 새로운 개발에 발맞춰야 한다는 의미이기도 하다. 경쟁력 있는 구축 환경 없이 비트코인 애플리케이션이 이더리움 및 다른 네트워크의 경쟁자들과 경쟁하는 것은 거의 불가능하다. 이 글이 작성된 시점에서, 비EVM 스마트 계약 환경의 장점은 특정 사용 사례에 최적화되어 있는 경우에도 일반적으로 인프라 부족과 그로 인한 애플리케이션의 시장 출시 일정이라는 부정적인 단점에 가려져 있다.
- **블루칩 유동성 온보딩(콜드 스타트 문제).** 스테이블코인, 온/오프 램프, 중앙화된 거래소 액세스, 다른 네트워크와의 연결, 파워 유저의 유동성은 디파이 생태계의 성공에 매우 중요하다. 네트워크 효과는 신제품의 성공에 결정적인 영향을 미치는 것으로 나타났기 때문에, 고립적으로 운영되는 체인을 기반으로 구축하는 것은 애플리케이션 개발자에게 큰 위험을 초래할 수 있다.

3 배경: 브릿지, 라이트 클라이언트, BitVM

하이브리드 L2는 라이트 클라이언트, 브릿지, BitVM을 통해 비트코인에 옵티미스틱 검증이라는 이 세 가지 주요 개념을 적용한다.

라이트 클라이언트 블록체인의 라이트 클라이언트 프로토콜(비트코인의 경우 "간편 결제 검증"(SPV)이라고도 함)은 제한된 리소스를 가진 노드가 기본 블록체인의 전체 데이터를 다운로드하지 않고도 결제 실행을 효율적으로 검증할 수 있도록 한다. 대신 합의 완결성을 검증하기에 충분한 데이터가 포함된 블록 헤더와 선택된 트랜잭션만을 요청한다. 라이트 클라이언트 프로토콜의 복잡성과 보안은 각 체인의 합의 메커니즘에 따라 결정된다. 비트코인의 라이트 클라이언트는 안전성이 입증되었으며 스마트 계약 기능을 갖춘 다른 체인에서 쉽게 검증할 수 있다(예: Threshold는 수년 동안 이더리움에서 라이트 클라이언트를 운영해 왔다) [1] . 반면, 이더리움은 100만 명이 넘는 검증자의 공개 키를 저장하고 추적해야 하는 복잡성으로 인해 아직 안전한 라이트 클라이언트를 제공하지 않는다[2].

브릿지 두 개의 서로 다른 블록체인에 자산을 안전하게 연결하거나 “랩핑”하는 것은 (i) 두 체인이 모두 올바르게 작동해야 하며 (ii) 신뢰할 수 있는 제3자 없이는 불가능하다[5]. 그러나 실제로는 모든 네트워크 참여자가 이 역할을 맡을 수 있도록 함으로써 이 제3자에 필요한 신뢰를 감소한다. 이는 소위 “라이트 클라이언트 브릿지”라고 불리는 것을 통해 구현할 수 있으며, 이때 두 개의 체인(*A* 와 *B*)은 온체인 스마트 계약의 일부로 서로의 합의 프로토콜을 검증한다. 자산 a를 체인 *A*의 브릿지에 예치하면, 체인 *B* 의 스마트 계약은 이 트랜잭션이 체인 *A*의 합의에 따라 완료되었는지 확인한 후 랩핑된 표현 *b (a)*를 민팅한다. 반대로, 체인 *B* 에서 *b (a)* 를 파괴하여 체인 *A*에서 기초 자산 a를 받을 때는 체인 *A*의 컨센서스의 일부로 체인 *B* 에서 이 거래가 실제로 확정되었는지 확인한다. 따라서 두 체인의 안전한 운영 외에 필요한 유일한 신뢰는 두 네트워크 간에 검증을 수행하는 데 필요한 데이터를 중계할 노드가 하나 이상 있다는 것이다. 안타깝게도 이 설계는 라이트 클라이언트의 복잡성으로 인해 실제로 성공적으로 구현된 적은 거의 없다. 비트코인의 경우, 스크립트 언어의 제한된 표현력과 블록 및 스택 크기 제한으로 인해 지금까지 어떤 형태의 온체인 라이트 클라이언트도 구현할 수 없었다.

BitVM BitVM은 비트코인에서 임의 프로그램을 옵티미스틱 방식으로 실행하는 메커니즘으로, 오프체인에서 실행되지만 실패할 경우 분쟁이 해결된 후 온체인에서 시행된다[3]. 이 메커니즘의 두 주요 사용 사례는 비트코인 옵티미스틱 롤업(Arbitrum[2]과 유사)과 신뢰 최소화 브리지이다. 두 경우 모두, BitVM는 사용자가 L2에서 BTC를 입출금할 수 있도록 하여 네트워크에 라이트 클라이언트 검증을 사용하는 정직한 온라인 노드가 하나만 있는 한 예치금의 탈취를 방지한다.

BitVM2 프로토콜의 전체 프로토콜 사양과 연결된 체인에서의 라이트 클라이언트 구현을 위한 BitVM2 신뢰 최소화 BTC 브릿지[4]는 최신 백서에서 확인할 수 있다.
간략한 설계는 다음과 같다:

(1) 비트코인 스크립트로 구현된 SNARK 검증기(예: Groth16[1])로 프로그램을 압축한다.
(2) 검증기를 각각 최대 4MB의 하위 프로그램 단위로 분할하여 각각 비트코인 트랜잭션에서 실행할 수 있도록 한다.
(3) BitVM2 작업자가 탭루트 트리[3]와 트랜잭션 사전 서명을 사용해 설정하는 동안 프로그램에 커밋한다.
(4) 사용자가 BitVM2에 일부 자금을 예치한다(예: 브릿지 예치금).
(5) BitVM2에서 자금 인출을 시도할 때, 누구든 작업자에 이의를 제기할 수 있다(예: 작업자가 브릿지에서 탈취를 시도하는 경우).
(6) 이의가 제기된 경우, 작업자는 모든 중개 하위 프로그램 결과를 공개하여 최종 계산 결과에 도달한 방법을 밝혀야 한다.
(7) 작업자가 부정행위를 하고 있다면, 공개된 하위 프로그램 결과 중 하나가 틀린 것으로 나타난다. 누구나 비트코인 트랜잭션에서 특정 하위 프로그램을 실행하여 올바른 결과를 생성함으로써 작업자를 반증할 수 있으며, 이를 결함 증명으로 삼을 수 있다.
(8) 결함이 있는 작업자는 쫓겨나 더 이상 BitVM2에 예치된

[1] https://github.com/keep-network/tbtc-v2/blob/main/solidity/contracts/relay/LightRelay.sol
[2] https://github.com/ethereum/annotated-spec/blob/master/altair/sync-protocol.md
[3] https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

자금에 접근할 수 없게 된다.

4 BOB 하이브리드 L2

하이브리드 L2 설계는 비트코인 보안의 신뢰라는 개념과 합의 검증의 단순성을 기반으로 한다.

4.1 비트코인 보안

BOB 하이브리드 L2는 정산 및 보안에 비트코인을 사용한다. 비트코인 L2의 이상적인 설계에서는 오프체인에서 상태 변경을 계산한 다음 영지식 증명을 사용해 온체인에서 유효성을 증명하는 영지식 롤업(zk-롤업)이 널리 받아들여지고 있다. 비트코인 스크립트에서 영지식 검증자를 효율적으로 구현하려면 합의 포크를 통해 추가 연산 코드를 도입해야 하기 때문에 현재로서는 비트코인에서 아직 zk 롤업을 구현하는 것이 어렵다.

따라서 실질적으로 현재 비트코인 보안을 구현하기 위해서는 BitVM2로 구동되는 옵티미스틱 검증을 사용해야만 한다. 이는 각 상태 전환에 대해 유효성 증명을 생성하는 zkVM을 구현하고, 이러한 증명을 상태 차이와 함께 비트코인 메인체인에 정기적으로 게시하는 것을 의미한다. 옵티미스틱 검증과 BitVM2을 결합하면 모든 네트워크 참여자가 결함 증명을 통해 결함을 검증하고 반증할 수 있다. ETH L2와 마찬가지로, 챌린지 기간(예: 7일) 동안 결함 증명이 없으면 상태가 확정된 것으로 간주한다. 네트워크에 결함 증명을 트리거할 온라인 노드가 하나만 있다면 보안은 *사실상* 비트코인을 의미하는 것과 같다.

BitVM 설계 공간 내 다양한 옵티미스틱 롤업 접근 방식 사이에는 여러 가지 기술적 절충점이 존재하기 때문에 데이터 가용성 및 비허가 챌린지, 라이트 클라이언트 모델 등을 고려하여, 보안, 효율성, 실용성 간의 균형을 맞추어야 한다. BOB의 하이브리드 L2 구현에 대한 자세한 내용은 곧 발표될 기술 사양에서 확인할 수 있다.

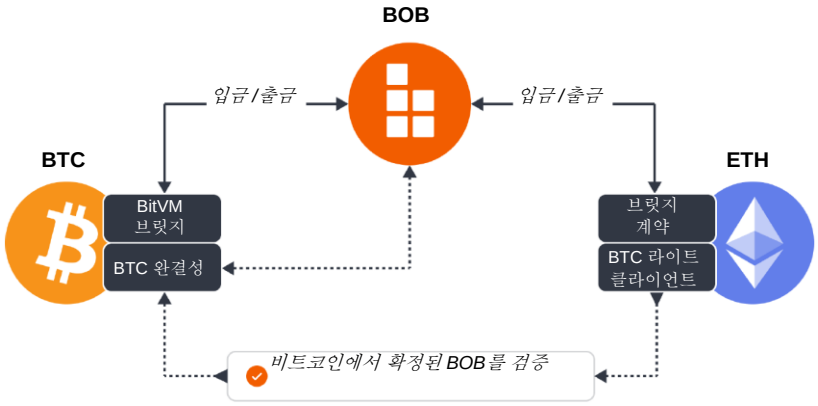

그림 1: BOB 하이브리드 L2는 비트코인과 이더리움 모두에서 신뢰 최소화된 브릿지를 제공한다(BitVM을 통해). 이더리움 브릿지 스마트 계약은 내장된 비트코인 라이트 클라이언트를 사용하여 BOB가 비트코인에서 확정되었는지 확인한다.

4.2 신뢰 최소화 비트코인 브릿지

또한 BitVM2 결함 증명을 통한 옵티미스틱 검증은 BOB가 신뢰 최소화된 비트코인 브릿지를 생성할 수 있게 한다. 특히 비트코인이 BitVM2에서 BOB용 라이트 클라이언트를 실행하는 라이트 클라이언트 브릿지 생성이 가능하여 올바른 브릿지 출금을 시행할 수 있다. 비트코인이 안전하고 네트워크에 결함 증명을 트리거할 온라인 노드가 하나만 있으면 BOB에 BTC를 입금하는 모든 사용자가 비트코인으로 다시 출금할 수 있다.

브릿지의 보안 모델은 *실존적 정직성*이라고 불리며, 올바른 작동을 위해 1/*n*의 정직성 가정만 요구한다. 비교: 오늘날 대다수의 BTC 브릿지는 다중 서명 체계에 의존하며 *정직한 다수 가정*, 즉 $t > 50\%$에 달성하는 t/n 서명자를 요구한다. 서명자의 대다수가 부정직한 경우, 서명자는 브릿지의 모든 자금을 탈취할 수 있다. 반면, BitVM2에서는 *모든 브릿지 작업자가 정직하지 않더라도 브릿지 설계 자금을 훔칠 수 없다.* 온라인 참여자(이 참여자는 브릿지 사용자 본인일 수도 있음)가 있는 한, 부정직한 작업자에 대한 이의가 제기되어 하나씩 운영에서 배제될 수 있다. 최악의 경우 모든 작업자가 브릿지에서 제거되어 자금이 동결될 수도 있다. 이는 운영 실패로 간주되지만, 이 모델과 기존 브릿지 모델과의 미세하지만 중요한 차이점은 작업자가 실제로 BTC를 훔칠 수 없기 때문에 공격을 시도할 경제적 인센티브가 전혀 없다는 점이다. 이는 비트코인 역사상 가장 안전한 BTC 브릿지 설계라고 할 수 있다.

4.3 신뢰 최소화 이더리움 브릿지

BOB의 하이브리드 설계는 ETH와 ERC20의 안전한 입출금을 지원한다. 이는 네이티브 옵티미즘 브릿지와 유사하게 작동한다. 사용자가 이더리움으로 자산을 인출하고자 할 때, ETH 메인넷의 브릿지 스마트 계약은 L2가 확정될 때까지 대기한다. ETH L2의 경우, 이더리움 메인넷에 결함 증명이 게시되지 않는지 확인하기 위해 7일을 기다린다. BOB의 하이브리드 L2 설계에서는 ETH 브릿지 스마트 계약이 BOB가 *비트코인에서 확정*될 때까지, 즉 비트코인에 결함이 증명이 게시되지 않을 때까지 기다린다. 이는 비트코인 블록체인을 검증할 수 있는 비트코인 라이트 클라이언트(브릿지 스마트 계약의 일부)를 통해 이루어진다. 따라서 비트코인이 안전하고 *비트코인*에서 네트워크에 결함 증명을 트리거할 온라인 노드가 하나만 있으면 BOB에 ETH와 ERC20을 입금하는 모든 사용자가 이더리움으로 다시 출금할 수 있다.

5 전망: BOB, BTC 디파이의 중심

하이브리드 L2는 비트코인과 이더리움의 네트워크 효과를 활용하여 최대 규모의 디파이 생태계로 자리매김하고 있으며 향후 다른 체인으로 확장할 수 있는 독보적인 위치에 있다.

이더리움을 통한 부트스트랩 BOB의 디앱은 이더리움 네트워크를 통해 부트스트랩하고 동급 최고의 인프라와 툴을 활용할 수 있으며, 디파이 파워 유저를 온보딩하고 모든 거래소 및 기관 플레이어와의 관계를 활용할 수 있다. 특히, 거의 모든 이더리움 사용자가 BTC를 보유하고 있으며, 대부분의 비트코인 파워 유저 또한 ETH 디파이를 사용하고 있다.

비트코인을 통한 성장. 시간이 지남에 따라 비트코인의 강화된 보안과 신뢰 최소화(BitVM2) 브릿지를 통한 BTC 액세스는 그동안 개발되지 않은 대규모 비트코인 유동성 풀을 점점 더 많이 개방하여 BOB의 디앱이 이더리움 경쟁자들을 따라잡을 뿐만 아니라, 그들을 능가하는 성장을 이룰 수 있도록 할 것이다. 이러한 효과는 비트코인의 전 세계적인 채택과 다양한 커뮤니티를 통해 더욱 높아질 것이다. ETH L2가 동일한 사용자 기반을 놓고 계속 경쟁하는 동안, BOB 디앱은 비트코인의 3억 글로벌 사용자와 수천 개의 실제 비즈니스에 활용될 것이다.

멀티체인 디파이(DeFi) 허브로서의 비트코인 비트코인, 이더리움, 스테이블코인은 시장의 90%를 차지한다. 그러나 세상에 수백 개의 은행이 존재하는 것처럼, 다양한 사용 사례와 지리적 위치에 특화된 수백 개의 체인이 생겨날 것이다. 이러한 체인의 사용자들에게는 BTC에 안전하게 액세스하고 자산을 교환할 수 있는 방법이 필요하다.

오늘날 중앙화된 거래소는 모든 체인에 연결하여 사용자가 자산을 입금하고 거래하고, 각자의 L1으로 다시 인출할 수 있도록 한다. 하지만 중앙화된 거래소는 머지 않아 사라질 것이다. 중앙화된 거래소는 과거에 중대한 문제를 일으켰으며, 디파이로 완전히 전환할 때까지 이러한 문제는 계속 발생할 것이다.

BOB의 임무는 이러한 중앙화된 거래소 대신 비트코인을 안전하고 투명한 디파이 생태계의 중추로 만드는 것이다.

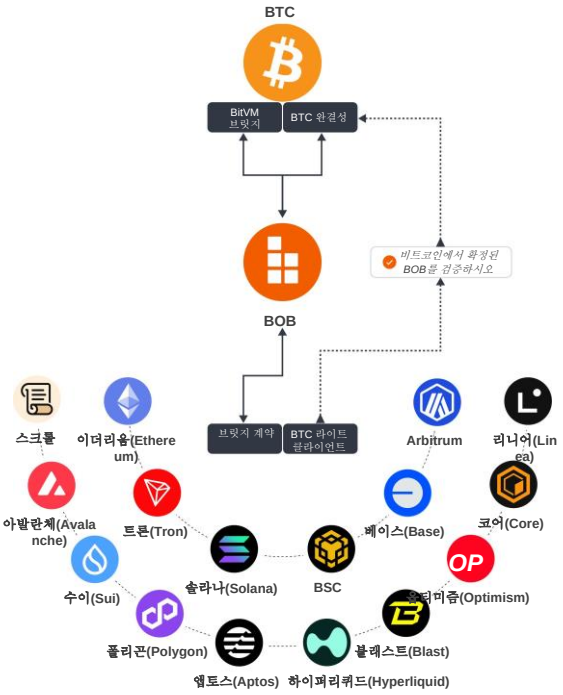

그림 2: 비트코인 라이트 클라이언트를 운영할 수 있는 모든 L1 체인(예로 스마트 계약)은 BOB에 신뢰 최소화 브릿지를 생성한다.

BOB는 하이브리드 L2로서 비트코인 블록체인을 검증할 수 있는 모든 스마트 계약 체인에 비트코인으로 보호되는 신뢰 최소화 브릿지를 운영한다. 여기에는 솔라나(Solana), 트론(Tron), 수이(Sui), 앱토스(Aptos), 모나드(Monad), 아발란체(Avalanche), 코스모스(Cosmos), 폴카닷(Polkadot) 등 최신 L1과 L2의 90%가 포함된다. 이러한 체인의 사용자는 비트코인이 안전하기만 하다면 ETH, SOL, TRX, DOT와 같은 기본 자산을 BOB에 입금하고, 비트코인 또는 다른 디지털 자산과 거래하고, 해당 L1 체인으로 다시 출금할 수 있다. 이 경우, 사용자는 바이낸스(Binance)나 코인베이스(Coinbase) 대신 비트코인을 신뢰하게 된다. 사용자는 제3자 브릿지에 의존하는 대신 비트코인을 사용해 멀티체인 입출금을 보호할 수 있다.

하이브리드 L2 설계의 강점은 비트코인을 신뢰 기반으로 삼아 상호 운용 가능한 디파이 생태계를 구축한다는 점이다. BOB는 BTC 유동성을 수십 개의 체인에 분산시키는 대신, 중앙화된 거래소에 대한 신뢰를 최소화하는 대안으로 비트코인에 유동성을 집중시켜 BTC를 디파이의 중심으로 만든다.

6 로드맵

1단계: ETH L2로서의 부트스트랩핑 BOB는 OP 스택으로 구축된 이더리움 L2로 처음 출시되어[4] 네이티브 이더리움 브릿지를 운영하며 여러 타사 비트코인 브릿지를 지원했다.

2단계: 비트코인 "소프트" 완결성 BOB는 이더리움 L2 설정에 비트코인 완결성을 추가한다. 시퀀서는 에포크당 한 번(하나 이상의 BOB 블록), 비트코인 완결성 프로토콜[5] 참여자의 사인오프를 요청하고, 이들은 BOB 체인을 완전히 검증한다. BitVM을 사용하면 이 비트코인 "소프트" 완결성 프로토콜로 보호되는 신뢰 최소화 비트코인 브릿지를 구축할 수 있다. 즉, 비트코인 브릿지를 공격하려면 대부분의 비트코인 완결성 프로토콜 참여자(해시 비율 또는 BTC 지분)를 손상시켜야 한다. 이더리움 브릿지는 이더리움에 의해 보안이 유지된다. 따라서 비트코인 "소프트" 완결성은 이더리움 브릿지의 출금을 가속화하여 지연 시간을 7일에서 몇 분/시간으로 단축하는 데 사용될 수 있다.

3단계: 전체 비트코인 보안 마지막 단계는 섹션 4.1에서 설명한 바와 같이 비트코인의 보안을 계승하는 것이다.온체인 zk 검증자를 활성화하는 비트코인 포크가 없는 경우, BOB는 BitVM을 통해 옵티미스틱 검증을 사용해야 한다. 추가적인 신뢰 가정 없이 비트코인에서 옵티미스틱 롤업을 구현하려면 비트코인 메인체인을 데이터 가용성 계층으로 사용해야 한다. 이는 부담스러운 비용을 수반하여 경제적인 측면에서 문제가 될 수 있다. 따라서 3단계로의 전환을 완료하려면 BOB는 충분한 활성 사용자 규모를 확보하여 추가 데이터 가용성 수수료가 발생하더라도 경쟁 이더리움 L2보다 거래 수수료가 증가하지 않도록 해야 한다. 대체 데이터 가용성 계층은 비트코인 이상의 추가적인 신뢰 가정을 도입하므로 비용과 보안 간의 절충안으로 고려될 수 있다.

7 결론

BOB 하이브리드 L2는 비트코인의 제한된 표현력과 그에 따른 디파이 지원 역량 부족을 해결하기 위한 새로운 접근 방식이다. 비트코인의 보안을 계승하고 이를 사용해 이더리움 및 기타 L1 스마트 계약 체인에 대한 신뢰 최소화된 브릿지를 생성함으로써 BOB는 디파이에서 다른 방식으로 BTC를 활용한다. 중앙화된 브릿지를 통해 BTC를 다른 네트워크에 랩핑하는 대신, 사용자는 BTC와 기타 자산을 비트코인 보안이 적용된 디파이 환경에 예치한다.

[4] https://docs.optimism.io/

[5] 현재 시험 중인 두 가지 비트코인 완결성 프로토콜은 병합 채굴과 비트코인 스테이킹이다. 이 결정의 핵심 요소는 BitVM의 검증이 얼마나 용이한가이다.

8 면책 조항

본 백서는 일반적인 정보 제공만을 목적으로 한다. 투자 자문이나 투자 매매를 위한 추천 또는 권유가 아니며, 투자 결정의 장점을 평가하는 데 사용해서는 안 된다. 회계, 법률 또는 세무 자문이나 투자 권고에 사용해서도 안 된다. 본 백서는 저자의 현재 의견을 반영하며 BOB 재단 또는 그 계열사를 대신하여 작성된 것이 아니다. 이러한 의견은 본 문서에 업데이트되지 않고 변경될 수 있다.

참고 문헌

[1] Jens Groth. 2016. On the size of pairing-based non-interactive arguments. In *Advances in Cryptology–EUROCRYPT*. Springer, 305–326.

[2] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S Matthew Weinberg, and Edward W Felten. 2018. Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*. 1353–1370.

[3] Robin Linus. 2023. BitVM: Compute Anything on Bitcoin. *URL: https:// bitvm.org/ bitvm.pdf* (2023).

[4] Robin Linus, Lukas Aumayr, Alexei Zamyatin, Andrea Pelosi, Zeta Avarikioti, and Matteo Maffei. 2024. BitVM2: Bridging Bitcoin to Second Layers. *URL: https:// bitvm.org/ bitvm_bridge.pdf* (2024).

[5] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios KokorisKogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J Knottenbelt. 2021. Sok: Communication across distributed ledgers. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II 25*. Springer, 3–36.