2024 AUGUST 3

BITCOIN CAMBRIAN EXPLOSION

MIRRORING INNOVATION, REDEFINING BOUNDARIES

YONGWON JEON, WONJAE CHOI, BOHYEON PARK
DECIPHER

Disclaimer: 본 레포트는 2022 년 이후 확장되고 있는 비트코인 생태계에 대한 분류와 정의가 명확하지 않다는 문제의식에서 시작해 비트코인에 기반을 두거나 비트코인을 활용한 솔루션 분석을 통해 생태계를 재정의하는 것을 목표로 합니다. 해당 레포트에서 분석 대상으로 선정된 프로젝트는 단지 설명하기 위한 예시일 뿐, 프로젝트로부터 금전적으로 이득을 취하지 않았으며 해당 프로젝트가 좋은 프로젝트임을 확언 할 수 없다는 점을 명백히 합니다. 또한, 모든 내용은 투자 조언으로 해석될 수 없으며 이에 따른 책임은 모두 본인에게 있습니다. 마지막으로, 해당 레포트는 저자의 주관이 포함된 글임을 밝힙니다.

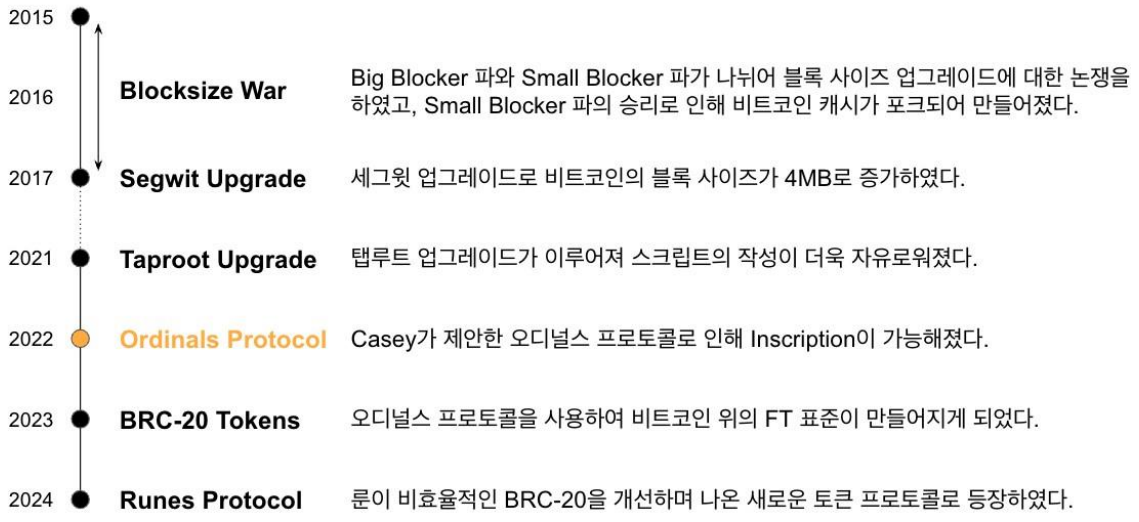
목차

1. INTRODUCTION

MASSIVE EXPANSION OF THE BITCOIN ECOSYSTEM

지구가 탄생하고 약 35 억년 동안 지구 상의 생명체는 원시적인 단세포 생물의 수준에 불과하였습니다. 근데 약 5 억 5 천만년 전, 어떠한 (아직 과학적으로 밝혀지지 않은)미지의 사건은 35 가지의 생물문을 갑작스럽게 출현시키며 오늘날 우리가 알고 있는 생태계를 만들어냈고, 이 사건을 캄브리아기 대폭발(Cambrian Explosion)이라 부릅니다.

2024 년, 가장 원시적인 블록체인인 비트코인에서도 이와 같은 대폭발이 일어나고 있습니다. 몇 년 전만해도 비트코인을 업그레이드하고 다양한 방향으로 활용하고자 하는 시도는 1 년에 1~3 개에 불과하였습니다. 하지만 2024 년에 들어서서 거의 매달 새로운 비트코인 레이어 2 들이 등장하고 있고, 그 외에도 비트코인을 활용하고자 하는 다양한 솔루션들이 우후죽순 생기고 있습니다.

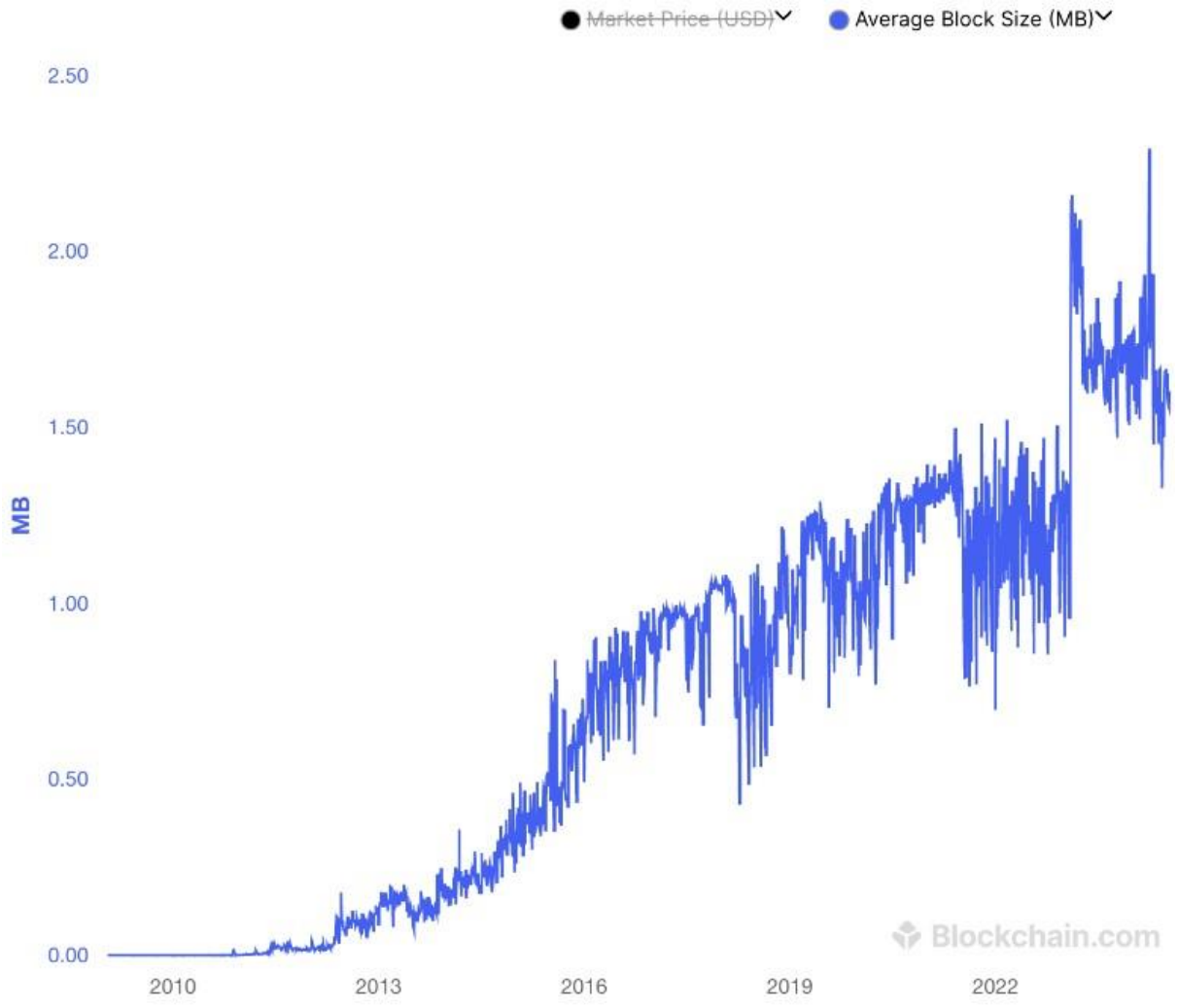


Source: Yongwon Jeon

비트코인 커뮤니티에서 확장성이나 프로그래머빌리티(Programmability) 등을 높이기 위한 논의는 오래 전부터 이루어졌습니다. 사토시 나카모토가 비트코인의 블록 사이즈를 1MB 로 제한한 2009 년부터 이러한 논의는 반복해서 이루어졌고, 특히 레딧에서 이루어진 2015 년 비트코인 블록사이즈에 대한 토론은 전쟁에 가까웠습니다. 블록사이즈 전쟁은 Small Blockers 의 승리로 끝나며 2017 년 Bitcoin Cash 의 하드 포크와 Segwit 업그레이드 소프트 포크라는 결과를 낳았습니다. 세그윗 업그레이드는 가상바이트의 개념을 도입하고 Witness Data 를 분리시켜 더 많은 데이터가 블록에 담길 수 있도록 하여 블록 사이즈는 4MB 로 증가하였습니다. 2021 년에는 탭루트(Taproot) 업그레이드가 이루어지며 더욱 다양한 스크립트의 활용이 더 적은 비용으로 가능해지게 되었습니다.

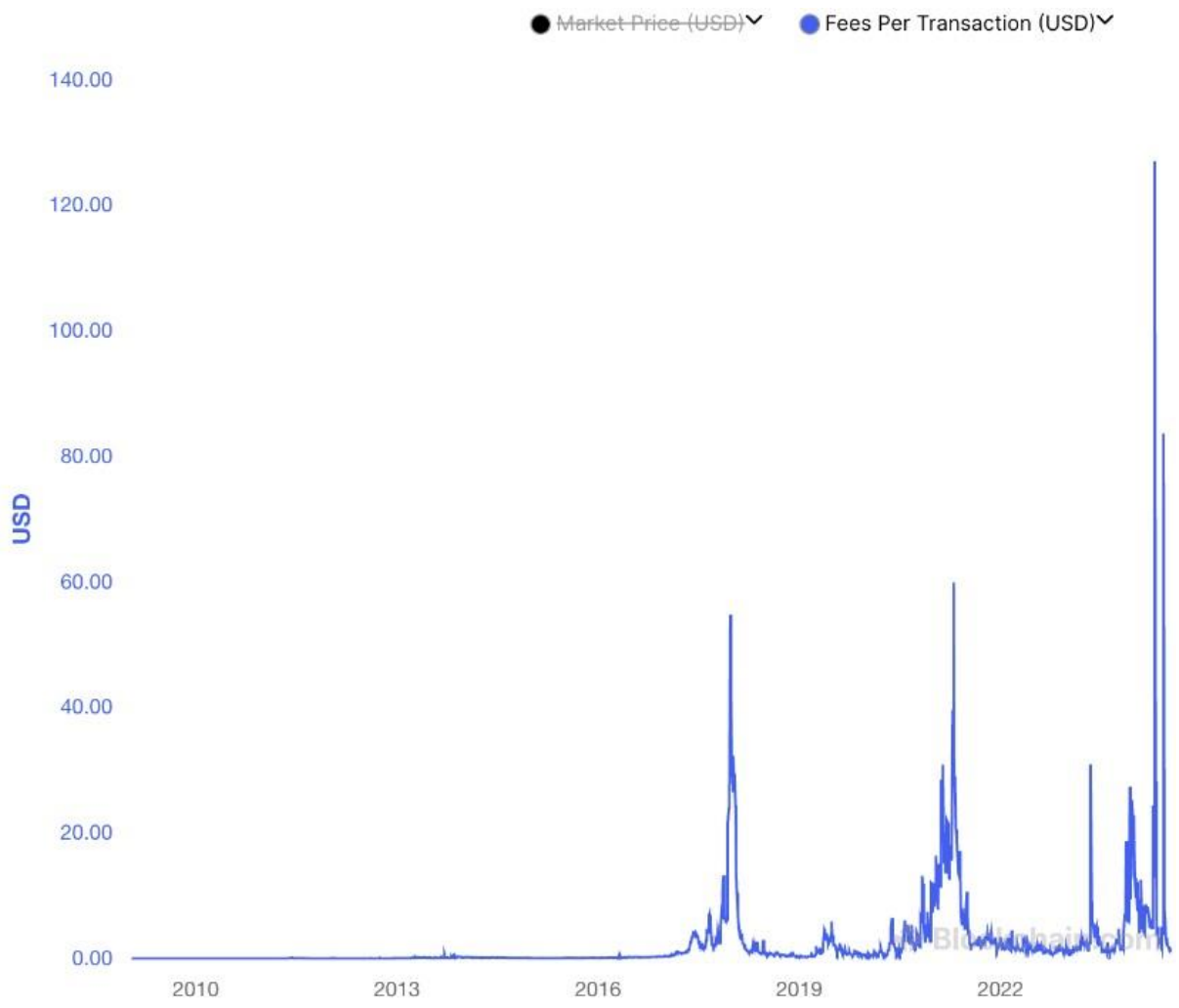
본격적인 비트코인 생태계의 붐은 2022 년 12 월, Casey Rodarmor 가 Ordinals 프로토콜을 출시하며 시작되었습니다. Ordinals 프로토콜은 비트코인의 사토시 위에 Inscription 을 가능하게 하면서 NFT 와 같은 개념의 표준을 만들었으며, 비트코인 위의 NFT 가 가능하다는 사실은 많은 커뮤니티를 주목하게 만들었습니다. 2023 년 Ordinals 프로토콜을 이용한 FT 표준인 BRC-20 이 탄생하였고, 수많은 BRC-20 이 만들어졌습니다. 최초의 BRC-20 토큰인 ORDI 토큰은 중앙화 거래소에 상장되기도 하였으며 2024 년 7 월 22 일 현재 기준 전체 토큰의 시가총액 중 84 위를 기록하고 있습니다. 2024 년에는 BRC-20 의 비효율성을 지적한 Casey 가 새로운 토큰 표준인

Runes 프로토콜을 발표하였습니다. 새로운 프로토콜들의 성공으로 Ordinals 와 BRC-20, Runes 를 거래하고 활용하기 위한 다양한 디앱(DApp)들도 개발되기 시작하였습니다.



Source: Blockchain.com

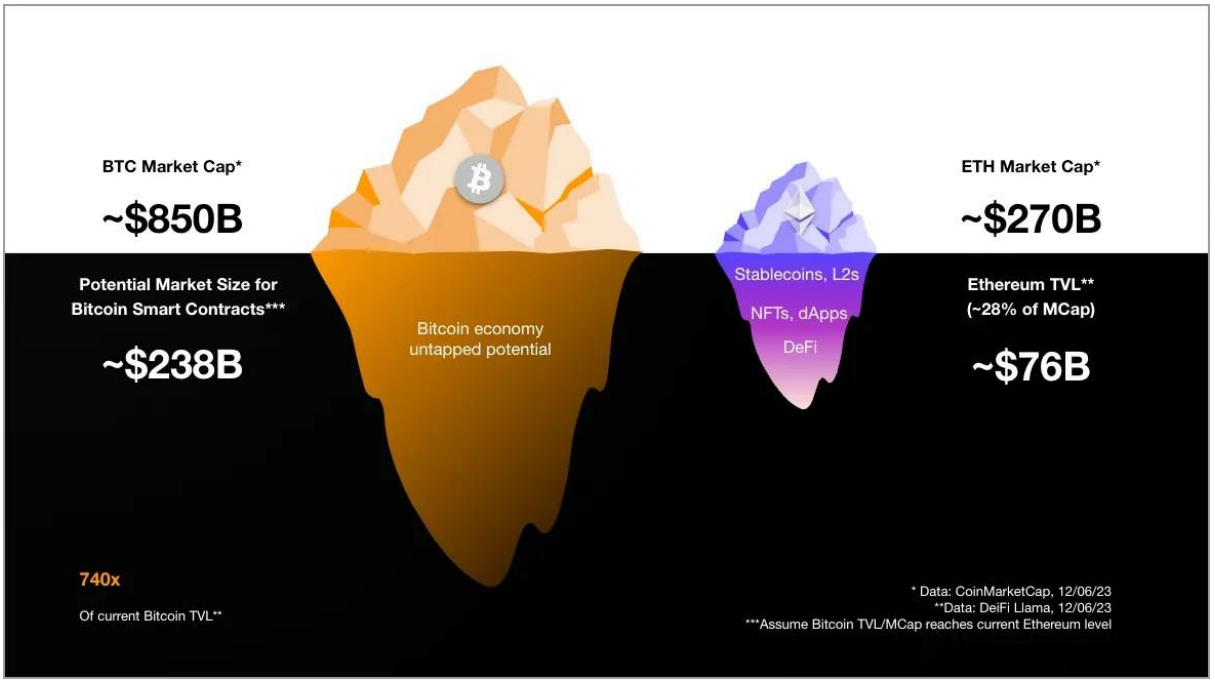
이러한 혁신의 결과는 여러 수치적인 지표로도 확인할 수 있는데, 비트코인의 평균 블록 사 이즈는 Ordinals 프로토콜의 출시 이후로 약 1MB 에서 1.5MB 로 150% 이상 크게 증가하였 습니다.



Source : Blockchain.com

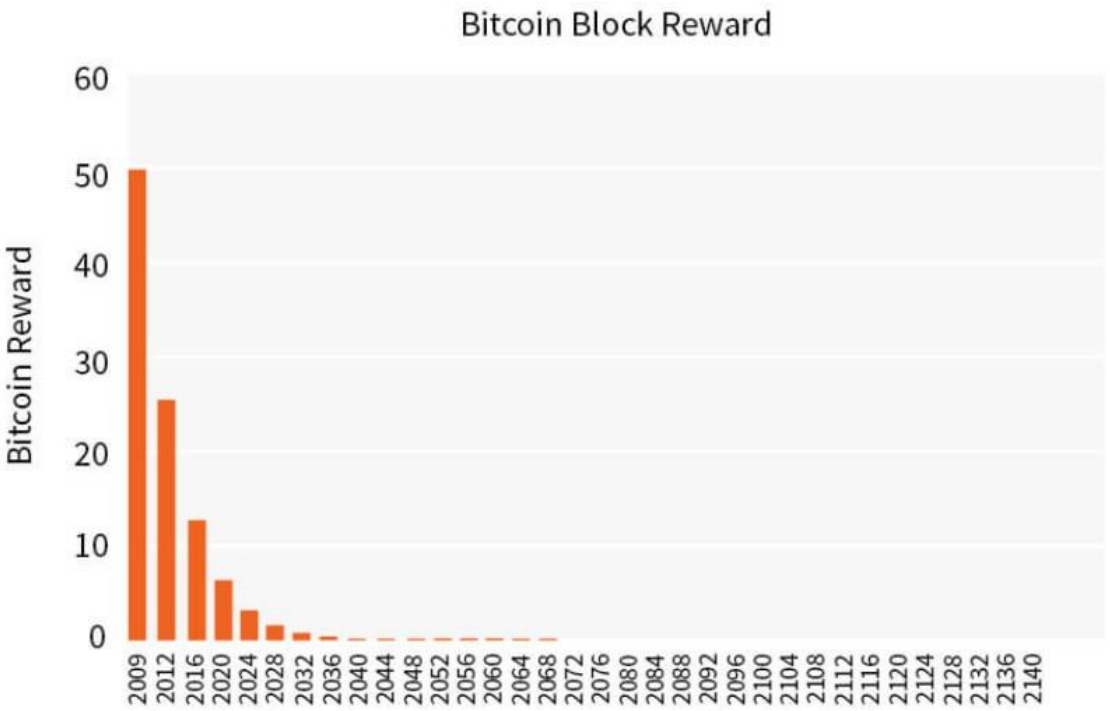
비트코인 수수료와 멤풀(Mempool)의 혼잡도도 상당히 증가하였는데, 비트코인의 평균 트랜잭션 수수료는 2022 년 평균 1.5 달러에서 2024 년 현재 평균 9.5 달러로 약 6 배 이상 증가하였습니다.

IMPORTANCE OF THE BITCOIN ECOSYSTEM



Source : The Spartan Group

Ordinals 프로토콜의 성공으로 많은 관심이 주목되면서 비트코인의 새로운 가능성이 다시 조명되기 시작하였는데, 바로 비트코인에 잠자고 있는 엄청난 규모의 휴면 자본입니다. 비트코인에는 약 1 조 3 천억 달러, 1800 조원에 가까운 자본이 특별히 활용되지 않은 상태로 누군가의 지갑에 방치되어 있습니다. 이더리움의 시가총액인 4100 억 달러 중 약 30%가 다양한 디앱들에서 활용되고 있다는 것을 보았을 때 비트코인의 잠재적 유동성은 4 천억 달러에 가깝다고 할 수 있습니다. 즉, 약 600 조원 규모의 블루오션 시장이 존재한다는 뜻이며, 이는 많은 빌더들과 투자자들에게 매력적인 시장임이 분명합니다.



Source : FXTM

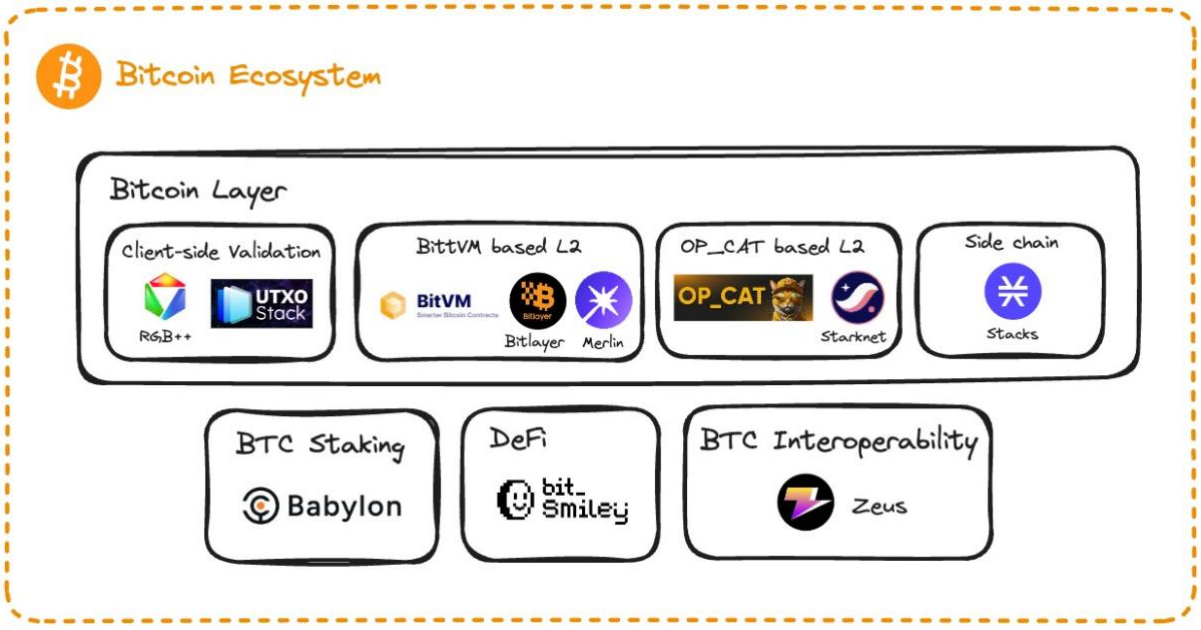
이러한 흐름이 잠깐의 하입(hype)이 아닌가 생각될 수도 있지만, 꼭 Ordinals 열풍이 아니었더라도 비트코인의 생태계 확장은 어쩌면 당연히 필요할 일이었을지도 모릅니다. 비트코인은 4 년마다 반감기를 거치며 블록 보상이 반으로 줄어드는 매커니즘을 갖고 있습니다. 2024 년 현재 블록 보상은 제네시스 블록을 채굴 했을 때의 50 BTC 에서 16 배 줄어든 3.125 BTC 에 불과하며 12 년 뒤 2036 년에는 0.39 BTC 까지 줄어들 예정입니다. 블록 채굴 보상은 채굴자들에게 매우 중요한 인센티브로 이것이 줄어들면 채굴자들의 동기부여 또한 줄어들어 전체 채굴자 수가 적어질 수 있고, 이는 비트코인 전체의 보안에 큰 악영향을 끼칠 수 있습니다. 계속해서 채굴자들에게 충분한 인센티브를 주기 위해선 블록 보상 이외에도 수수료 수익이 필요하고 비트코인 위의 생태계 확장은 비트코인의 지속가능성에 큰 도움이 될 것입니다.

OBJECTIVES OF THE REPORT

비트코인 생태계가 빠르게 확장을 하고 있는 반면에, 혹은 어쩌면 그 때문에 아직 전반적인 비트코인 생태계에 대한 분석이나 분류, 용어의 정립 등은 제대로 이루어지지 못하고 있습니다. 또한 비트코인은 스마트 컨트랙트(Smart contract)가 존재하지 않는 튜링 불완전한 체인이라는 독특한 특성을 가지고 있기 때문에 기존의 이더리움 등의 생태계를 바라보는 시점으로는 온전히 정의할 수 없습니다.

본 아티클에서는 비트코인 생태계를 크게 7 가지로 분류하고, 분류 별 대표 프로젝트를 분석함으로써 비트코인에 어떠한 다양한 접근들이 이루어지고 있는지를 톺아보고자 합니다. 또한, 각 생태계 분류 별로 기대되는 점과 한계점을 조명하며 향후 전망에 대한 저자의 주관적 의견을 제기하고자 합니다.

2. BITCOIN ECOSYSTEM



Source : Bohyeon Park

앞서 언급한 것처럼 비트코인의 잠재적 가치는 매우 크지만, 그에 비해 생태계에 많은 서비스가 등장한 지 얼마 되지 않았고, 아직 많은 프로젝트들이 초기 단계라서 서비스 분류가 명확하지 않다고 느꼈습니다. 실제로 프로젝트 분류에 대해 명시하고 있어도 모호한 경우가 많았기에 본 레포트에서 약 10 개의 프로젝트를 분석하면서 새롭게 분류를 진행했고, 보이는 다이어그램과 같이 생태계를 구성했습니다. 앞서 설명한 것처럼 크게 4 가지, 작게 7 가지의 분류를 통해 생태계를 표현해봤으며, 해당 분류의 기준과 함께 각 프로젝트에 대한 Overview, Technical Features, Market Analysis, Limitations 을 설명하도록 하겠습니다.

각 항목은 다음과 같은 내용을 포함합니다:

- **Overview**: 프로젝트에 대한 전반적인 정보로 출시일, 펀딩 정보, 비전, 중요한 점 등이 포함됩니다.
- **Technical Features**: 프로젝트의 주요 기술에 대한 설명으로, 컨 센서스 및 코어 기술에 대한 설명이 포함됩니다.
- **Market Analysis**: 시장 분석으로 통해 프로젝트가 해당 생태계 에서 얼만큼의 파이를 차지하고 있는지와 더불어 TVL(Total Value Locked), 타프로젝트와의 비교 분석 등이 포함됩니다.
- **Limitations**: 프로젝트를 분석하면서 발견된 한계점 혹은 상위 분 류에 대한 한계점을 제시합니다.

CLIENT-SIDE VALIDATION

Client-side Validation(CSV)는 비트코인 거래가 비트코인의 합의 규칙 하에서의 유효성과는 별도로 유효성이 결정되는 일부 데이터에 커밋할 수 있도록 합니다. 이 프로토콜 하에서 생성된 자산은 소유권 보장과 이중 지불 방지를 위해서만 비트코인을 사용하며, 자산의 유효성은 오프체인(Off-chain)에서 개별 클라이언트에 의해 검증됩니다.

다양한 프로토콜은 여러 가지 방식으로 데이터를 비트코인에 제출합니다. 예를 들어, RGB 프로토콜은 온체인(On-chain)에서 약속에만 커밋하고, 탭루트 자산은 상태 트리의 루트에 커밋하며, Ordinals 프로토콜은 비트코인을 데이터 가용성(Data Availability, DA) 레이어로 사용하여 데이터를 직접 제출합니다.

이 프로토콜에서 사용되는 트랜잭션들에는 해당 프로토콜에서 사용되는 규칙에 따른 데이터 가 포함되며, 이 데이터는 비트코인에서는 의미없는 데이터로 보입니다. 이 데이터는 오프체인에서 이 프로토콜을 사용하는 사람들에게만 이해되면 되며, 이 작업은 오프체인 인덱서 (Indexer)라는 주체에 의해 해석되고 다른 사람들에게 결과만 공유되기도 합니다.

PROS AND CONS

이 방식의 장점으로는 우선 뛰어난 확장성을 들 수 있습니다. 기존 비트코인에서는 불가능했던 새로운 자산 발행이나 스마트 컨트랙트를 정의하여 비트코인에서 스마트 컨트랙트를 사용할 수 있는 다양한 확장 사례가 가능합니다. 또한, 데이터가 비트코인에 직접 저장되고 사용되는 비트코인 네이티브(Native) 프로토콜이기 때문에, 비트코인 내에서의 상호운용성과 데이터 보안이 매우 높습니다.

단점으로는 첫째로 중앙화 문제가 있습니다. Ordinals 와 같은 프로토콜에서는 모든 사용자가 모든 데이터를 직접 다운로드하고 처리하기 어렵기 때문에, 주로 오프체인 인덱서가 비트코인에서 데이터를 다운로드하여 계산한 결과만을 사용자에게 제공하며, 사용자들은 이를 신뢰하고 사용합니다. 이 방식은 중앙화 문제를 야기하며, 오프체인 인덱서가 악의적인 행동을 할 경우 큰 문제가 발생할 수 있습니다. 또한, 비트코인에 의해 검증되지 않는 프로토콜만의 규칙이 존재하는데, 이는 비트코인의 보안에 의해 보호되지 않습니다. 따라서 시빌어택 (Sybil Attack) 등의 공격에 의해 합의 규칙이 비교적 쉽게 무너질 수 있어 보안적으로 안전 하지 않다는 단점이 있습니다.

SOLUTION

위의 문제점을 해결하기 위해 최근에는 프로토콜에 맞게 동작하는 미러링(Mirroring) 블록 체인을 사용합니다. 이는 별도의 합의 알고리즘과 프로토콜에 따라 동작하는 블록체인으로, 비트코인에 포함된 CSV 트랜잭션을 자동으로 실행하고 상태를 업데이트합니다.

이 방식은 사용자가 직접 데이터를 검증하거나 오프체인 인덱서를 신뢰해야 할 필요성을 없 애고, 해당 블록체인의 보안을 신뢰하며 프로토콜을 사용할 수 있게 합니다. 이 경우 실행 결 과의 보안은 해당 블록체인의 합의 알고리즘에 의해 보장되지만, 트랜잭션 데이터는 비트코인에 존재하므로 검열 저항성과 누구나 부정행위를 알아차릴 수 있다는 중요한 보안적 이점 을 제공합니다. 이 글에서는 이러한 방식을 사용하는 블록체인을 앞으로 CSV 체인이라 부르겠습니다.

UTXO STACK

UTXO Stack

OVERVIEW

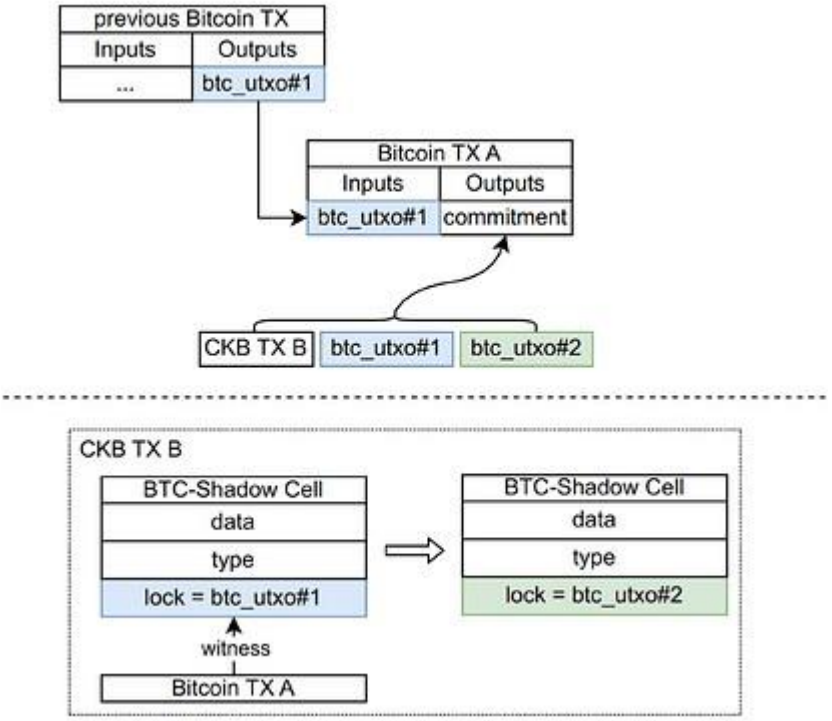
UTXO Stack 은 CSV 프로토콜인 RGB++를 활용하는 모듈형 블록체인 출시 플랫폼입니다. UTXO Stack 을 사용하면 튜링 완전한 컨트랙트를 생성할 수 있는 비트코인 CSV 체인을 쉽게 출시할 수 있으며, 출시된 체인의 보안은 BTC, CKB 및 기타 비트코인 자산의 스테이킹으로 보장됩니다. UTXO Stack 은 현재 비트코인의 스마트 컨트랙트 기능 및 성능에 대한 한계를 극복하는 것을 목표로 하며, 개발자들에게 비트코인 생태계의 잠재력을 최대한 활용할 수 있는 도구를 제공합니다.

UTXO Stack 은 Nervos Network 의 창업자인 Cipher Wang 이 설립했습니다. 2024 년 4 월에 ABCDE Capital 과 SNZ Holding 이 리드한 시드라운드 투자를 완료했으며, 구체적인 투자금액과 가치평가는 공개되지 않았습니다.

또한 2024 년 7 월, UTXO Stack 은 Babylon 과 협력해 비트코인 UTXO 모델 기반의 확장 솔루션을 발표했습니다. 이 솔루션은 PoS(Proof of Stake) DA 체인을 도입해 보안을 강화하고, 저수수료로 고성능 튜링 완전 스마트 컨트랙트를 지원합니다. 테스트넷은 3 분기에, 메인넷은 연말에 출시될 예정입니다.

또한, 비트코인 생태계에서 금융 운영을 지원하는 첫 BTC 앱체인도 3 분기에 테스트넷을 오픈합니다. 이 앱체인은 UTXO 모델과 PoS 메커니즘을 사용해 초고속 거래 처리와 낮은 수수료를 제공합니다. 사용자는 비트코인 지갑을 통해 앱체인과 상호작용하고, CKB 스마트컨트랙트로 자산을 스테이킹할 수 있습니다. UTXO Stack 은 더 많은 커뮤니티 앱체인이 플랫폼에 구축될 것으로 기대합니다.

TECHNICAL FEATURES RGB++ PROTOCOL



Source : RGB++ Light Paper

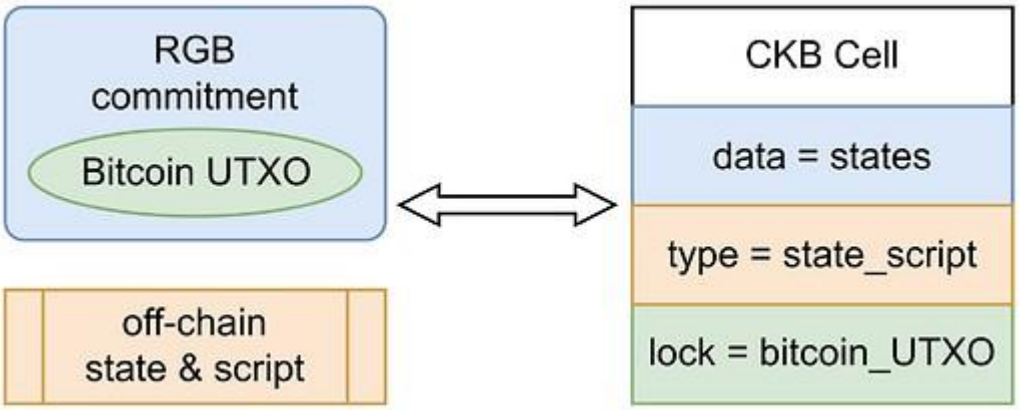
RGB++는 RGB 를 기반으로 하는 확장 프로토콜로, 일회용 씰과 클라이언트 측 검증 기 술을 활용하여 상태 변경 및 거래 검증을 관리합니다. 이 프로토콜은 비트코인 UTXO 를 동형 바인딩(Isomorphic Binding)을 통해 Nervos CKB 셀에 매핑하고, CKB 및 비트 코인 체인에서 스크립트 제약을 사용하여 상태 계산의 정확성과 소유권 변경의 유효성을 검증합니다. 이때 CKB 는 다른 UTXO 기반의 블록체인이 될 수 있습니다.

RGB++에서 트랜잭션은 다음과 같이 동작합니다:

1. 오프체인 계산: 오프체인 계산 단계에서, 먼저 다음에 사용할 일회용 씰(Single-use Seal)을 선택합니다(예: btc_utxo#2). 이때 일회용 씰은 이중지불을 방지하기 위한 방법으로, 여기에서는 비트코인의 UTXO 를 사용합니다. 그런 다음 오프체인 계산을 통해 CKB 로 전송할 RGB++ 거래(CKB_TX_B)를 생성합니다. 이 과정에서 커밋먼트(Commitment)를 생성하는데, 이는 hash(CKB_TX_B | btc_utxo#1 | btc_utxo#2)로 계산됩니다.
2. 비트코인 거래 제출: 비트코인 거래 제출 단계에서는 비트코인 거래(BTC_TX_A)를 생성하고 전송합니다. 이 거래는 btc_utxo#1 을 입력으로 사용하며, OP_RETURN 을 통해 앞서 생성한 커밋먼트를 추가합니다.
3. CKB 거래 제출: 마지막으로 CKB 거래 제출 단계에서는 앞서 생성한 CKB 거래(CKB_TX_B)를 전송합니다. 이 거래의 출력 데이터(CKB_TX_B.output.data)가 사용자의 최신 상태를 유지하게 합니다. 이후 상태 변경이 필요할 때는 btc_utxo#2 와 CKB_TX_B 의 출력을 사용합니다.
4. 온체인 검증: 온체인 검증 단계에서는 비트코인이 관련 UTXO 가 지정된 사용자에 의해서만 사용될 수 있음을 검증합니다. 또한, CKB 에 있는 비트코인 라이트 클라이언트가 비트코인 거래를 검증합니다. 비트코인 거래는 CKB 거래의 증인으로 제출되어 검증에 도움을 주며, CKB 는 비트코인 거래가 올바른 UTXO 를 사용했는지, 그리고 올바른 커밋먼트를 커밋했는지를 검증합니다. 마지막으로, CKB 는 상태 전이가 규정 된 컨트랙트 규칙을 준수하는지 확인합니다.

또한 RGB++는 스마트 컨트랙트의 실행환경으로, 새로운 가상머신(Virtual Machine) 인 AluVM 을 사용합니다. AluVM 은 UTXO 기반의 스마트 컨트랙트에 최적화된 결정론적(Deterministic)인 RISC 기반의 함수형(Functional) 가상머신입니다. 하지만 미성숙한 개발과, 사용사례가 거의 없다는 큰 단점이 있습니다.

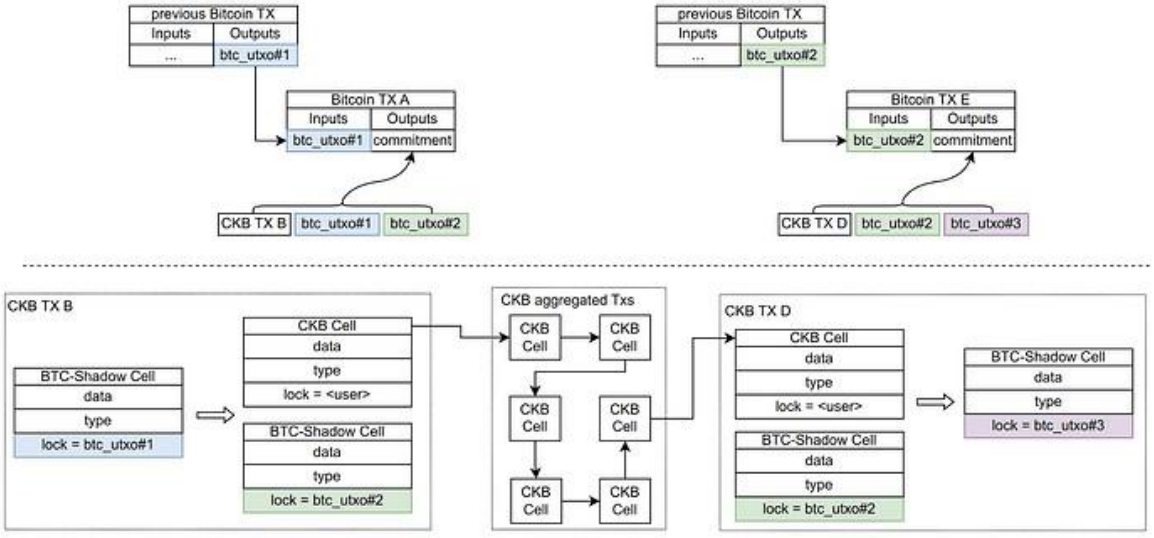
ISOMORPHIC BINDING



Source : RGB++ Light Paper

RGB++의 동형 바인딩 기술은 비트코인 UTXO 를 CKB 셀에 일대일로 매핑하고, 비트코인 UTXO 잠금을 통해 소유권을 동기화하며, 셀 데이터와 타입을 사용하여 상태를 유지 합니다. 따라서 UTXO 가 사용될 때마다 해당 eUTXO 도 함께 전송되어 비트코인 레이어와 RGB++ 레이어 간의 동기화를 지속적으로 유지합니다. 이로써 RGB++는 비트코인과 CKB 간의 원활한 연동을 통해 스마트 컨트랙트 기능을 확장하고, 상태 관리의 정확성과 보안을 강화합니다.

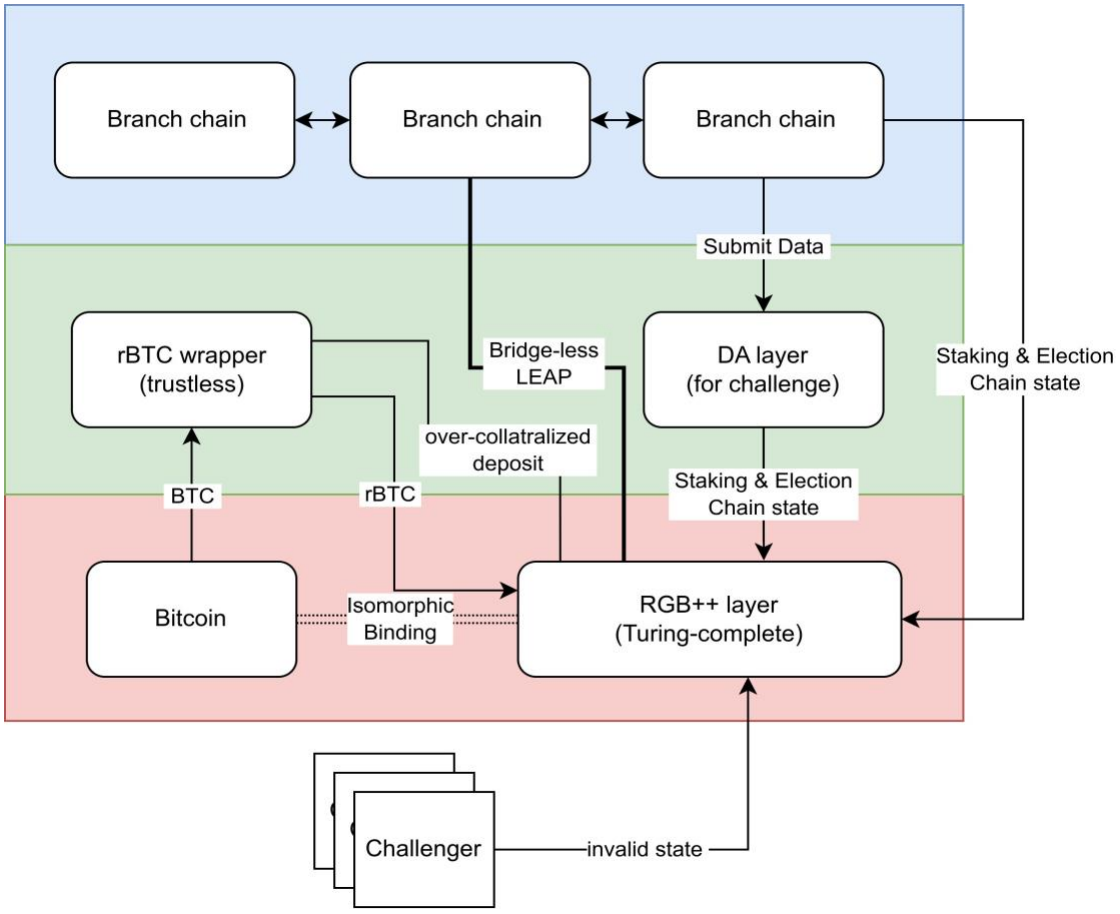
TRANSACTION FOLDING



Source : RGB++ Light Paper

여러 RGB++ 거래를 하나의 비트코인 거래로 집계할 수 있습니다. 이러한 트랜잭션 폴딩(Transaction Folding)은 수수료를 줄이고 처리량을 증가시켜 롤업과 유사한 효과를 제공합니다.

BRANCH CHAIN



Source : UTXO Stack Docs

개발자는 클릭 한 번으로 UTXO 기반의 PoS CSV 체인을 구축할 수 있습니다. 이러한 체인은 높은 TPS, 낮은 거래 수수료 및 RGB++ 자산 발행을 지원하며, 자산이 브리지를 사용하지 않고 UTXO 기반 체인 간에 자유롭게 이동할 수 있습니다.

브랜치 체인의 보안은 Babylon 프로토콜을 사용하는 스테이킹 메커니즘을 통해 강화됩니다. Babylon 프로토콜은 PoS DA 체인을 도입하여 Layer 2 의 보안을 유지합니다. 이 체인은 비트코인과 동일한 UTXO 모델을 사용하며, 사용자 스테이킹 RGB++ 토큰과 Babylon 의 원격 BTC 스테이킹을 통해 이중 보안 메커니즘을 구현합니다.

구체적으로, UTXO Stack 은 BTC, CKB, 그리고 BTC L1 자산을 재스테이킹하여 Layer 2 의 보안을 보장합니다. 이는 비트코인 생태계의 'OP Stack + EigenLayer'와 유사한 방식으로, 고성능, 저수수료 환경을 조성하면서도 튜링 완전한 스마트 컨트랙트를 지원합니다.

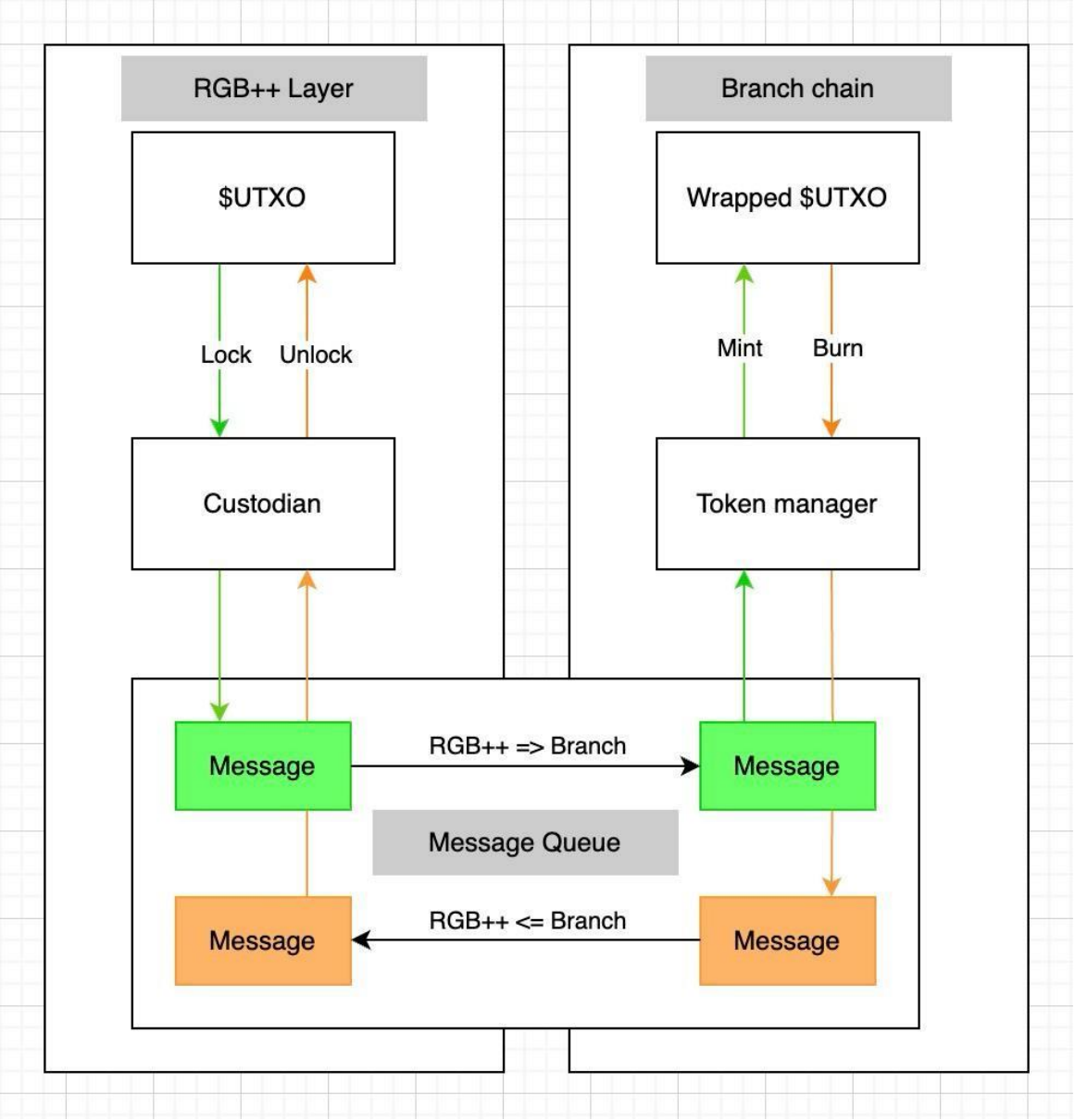
Babylon 프로토콜의 PoS DA 레이어는 데이터 가용성을 보장하며, 체인 간의 원활한 상호 운용성을 지원합니다. 이를 통해 UTXO Stack 기반의 Layer 2 솔루션은 더욱 효율적이고 안전하게 운영될 수 있습니다.

FORCED EXIT

사용하는 DA 레이어가 해킹 등의 이유로 사용할 수 없는 경우, 사용자들은 보안을 위협 받으므로 자금을 인출해야 합니다. 이 경우에는 CSV 데이터를 로컬에 저장하고 있다면 브랜치 체인에서 자산을 여전히 인출할 수 있습니다. 이는 UTXO 가 사용된 경로를 통해 스스로를 증명할 수 있는 특성 덕분에 가능합니다.

이 CSV 데이터를 사용하여 머클 증명(Merkle Proof)을 생성하여 RGB++ 레이어로 강 제 탈출을 수행할 수 있습니다. 사용자가 정직하다면 이 증명은 일정 기간의 도전 기간이 지난 후, 최종적으로 자산을 레이어 1 으로 복구할 수 있도록 합니다.

BRIDGELESS CROSS-CHAIN LEAP



Source : UTXO Stack Docs

RGB++ 자산은 브리지를 사용하지 않고 체인을 넘나들 수 있습니다. 이는 자산 소유권이 비트코인 UTXO 에 묶여 있기 때문입니다. UTXO 의 잠금 해제 조건을 목표 체인의 UTXO 로 설정하여 자산이 다른 UTXO 기반 체인(예: 라이트코인)으로 이동할 수 있습니다.

MARKET ANALYSIS

UTXO Stack 은 아직 매우 초기 단계에 있으며, 테스트넷도 출시되지 않은 신생 프로젝트입니다. 개발과 홍보 모든 측면에서 아직 시작 단계에 있으며, 트위터 팔로워 수는 현재 1100 명에 불과합니다. 그럼에도 불구하고, CSV 를 활용한 확장성 솔루션 중에서는 가장 큰 주목과 기대를 받고 있는 프로젝트입니다.

LIMITATIONS

UTXO Stack 과 RGB++ 프로토콜은 아직 개발 단계에 있어, 완전한 구현 전에 추가적인 개선과 철저한 테스트가 필요합니다. 이러한 기술들은 매우 유망하지만, 안정적이고 신뢰할 수 있는 시스템으로 자리 잡기 위해서는 다른 프로젝트와 프로토콜들이 그렇듯, 시간이 필요할 것입니다

브랜치 체인의 보안은 PoS 의 컨센서스와 DA 레이어의 보안에 크게 의존합니다. 이는 스마트 컨트랙트의 실행이 비트코인의 해시파워가 아닌 스테이킹된 자산에 의해 보호됨을 의미합니다. DA 레이어 또한 시스템 전체의 보안에 큰 영향을 미칩니다. 따라서, 이 구성 요소들 의 안정성과 보안을 강화하는 것이 중요합니다.

마지막으로, UTXO 기반의 스마트 컨트랙트는 기존의 EVM 기반 계정 모델과 다른 사용성과 개발 환경을 제공합니다. 이는 사용자와 개발자들에게 새로운 도전 과제를 제시하며, 특히 개발자들에게는 새로운 아키텍처와 프로그래밍 언어의 학습이 큰 진입 장벽이 될 수 있습니다. 사용자들도 새로운 인터페이스와 사용 방식에 어려움을 겪을 수 있습니다.

SIDE CHAIN

현재 비트코인의 확장성 솔루션들을 생각해보면 단연 가장 많은 형태를 띠고 있다고 할 수 있는 것은 사이드 체인입니다. 비트코인은 애초에 프로그래머빌리티를 위해 출시된 블록체 인이 아니기 때문에 복잡한 스마트 컨트랙트와 같은 코드 구현이 불가능합니다. 이러한 특성 으로 인해 사이드 체인이 많은 현재의 모습은 충분히 예상할 수 있는 생태계의 모습입니다. 일례로 현재 이더리움의 확장성 솔루션이 주목받으며 롤업 형태의 레이어 2 가 주류를 차지 하고 있지만 롤업이 등장하기 전 초기에는 확장성에 대한 솔루션 중 하나로 사이드 체인을 사용했습니다.

SIDE CHAIN INTRODUCTION

사이드 체인(Side chain)에 대한 일반적인 정의를 먼저 보면 “메인넷과 투웨이 페그(TwoWay Peg)로 연결된 독립적 블록체인”입니다. 가장 일반적으로 쓰이는 정의지만 생태계에 많은 종류의 솔루션이 있기 때문에 사이드 체인임을 명확하게 구분하는 데에 있어 정의에 따른 속성을 파악하는 것이 중요합니다. 따라서 본 리포트에서는 구체적인 몇 가지 속성을 통해 사이드 체인을 분류하고자 하며, 해당 분류는 후술할 사이드 체인 프로젝트를 분석하고 설명하는 데 사용될 속성임을 명시합니다. 사이드 체인의 속성은 다음과 같습니다:

- 독립적인 체인이다. 독립적이라는 것은 자체 컨센서스 (consensus)를 가질 수 있어야하고, 그에 따라 네이티브 토큰 (native token)을 가질 수 있어야 한다는 것을 의미합니다.
- 메인 체인의 네이티브 토큰을 가스비로 활용할 수 있다. 본 리포트 에서는 비트코인 생태계를 다루고 있기 때문에 BTC 가 메인 체인의 네이티브 토큰이 됩니다.
- 메인 체인의 보안을 100 퍼센트 완전하게 상속받지 못한다. 사이드 체인에서의 트랜잭션 유효성이 메인체인에 의해 검증되지 않고 사이드 체인의 보안에 의존합니다.

즉, 속성을 통해 사이드 체인을 한 문장으로 정의하면 사이드 체인은 메인 체인에 종속적이 지만 독립적인 합의 알고리즘을 가진 체인이라고 재정의됩니다. 여기서 말하는 “종속적”이란, 해당 체인의 작동 가능성이 메인 체인의 존재 유무에 의존한다는 것을 의미하며, 메인 체인이 없으면 체인이 작동하지 않을 경우에 ”종속적”이라 칭합니다.

후술할 사이드 체인 프로젝트는 Stacks 입니다. 프로젝트의 공식적인 분류를 살펴보면 사이드 체인이라고 언급하고 있지 않지만, 앞서 재정의한 사이드 체인의 속성에 부합했기에 사이드 체인으로 분류하였습니다.

Stacks

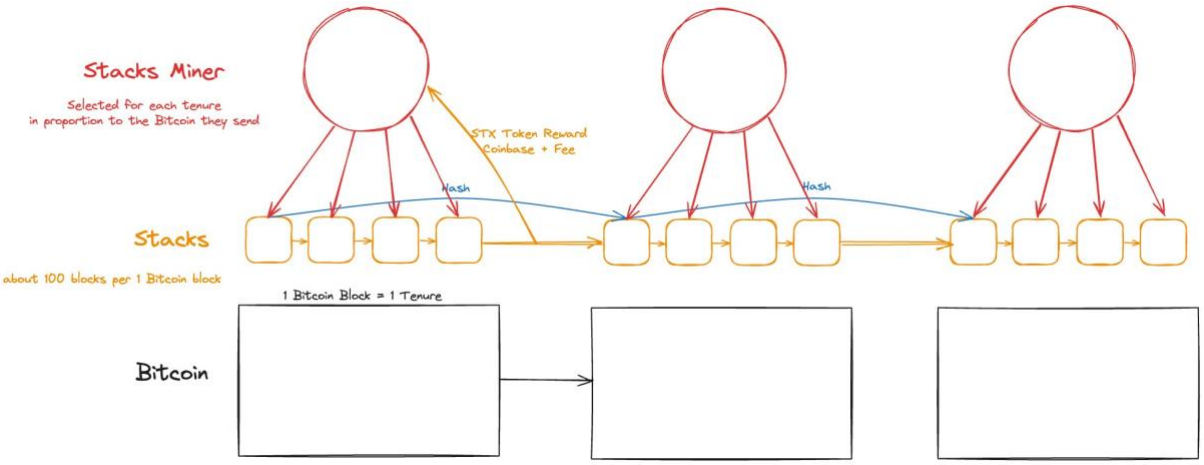
OVERVIEW

Stacks 는 2013 년 Muneeb Ali 의 박사 논문 과정을 시작으로 연구 개발이 시작되어 2021 년 01 월에 메인넷을 런칭한 사이드 체인으로, Muneeb Ali 와 Ryan Shea 가 설립한 Blockstack PBC 팀이 비트코인의 유틸리티를 높이고자 하는 비전을 가지고 출시했습니다. 비트코인의 유틸리티성을 높인다는 비전을 가지고 나온 만큼, 오직 자금 전송 만을 위한 비트코인 네트워크 위에 스마트 컨트랙트를 이용해 다양한 어플리케이션을 사용할 수 있도록 합니다.

Blackstack PBC 팀은 2017 년과 2018 년 총 2 년에 걸쳐 약 $52.2M 의 펀드를 투자받았습니다. 또한 Y Combinator, Digital Currency Group, Union Square Ventures 등의 유명한 VC 를 비롯한 40 여개의 VC 에서 9 번의 라운드를 걸쳐 $93.8M 의 펀드레이징을 하기 도 했습니다. 이러한 Stacks 는 미국 증권 거래 위원회(SEC)의 인가를 받은 첫 번째 암호화 폐이기도 한 만큼 비트코인 생태계에서 많은 관심을 끌었습니다. 실제로 여러 통계를 종합했 을 때, 2022 년 비트코인 생태계 내에서 가장 많은 사용성을 보여준 것을 확인할 수 있습니다.

2024 년 04 월에 나카모토 릴리즈(Nakamoto Release)를 거쳤는데, Stacks 측에서는 나카모토 릴리즈 이전은 확실하게 사이드 체인이라고 명시하였지만, 이후에는 사이드 체인이 아닌 비트코인 레이어 2 라고 명시하고 있습니다. 나카모토 릴리즈를 간단하게 살펴보면, 릴리즈 이전과 이후 달라진 점은 크게 3 가지입니다. 먼저, 트랜잭션의 처리속도가 증가했습니다. 기존에는 비트코인의 블록 타임에 맞춰 10 여분 정도의 블록타임을 가지던 Stacks 는 나카모토 릴리즈 이후 약 6 초의 블록타임을 가지게 됐습니다. 다음으로, 비트코인의 Finality 를 100 퍼센트 상속받습니다. Stacks 는 후술하겠지만 Tenure 의 가장 첫 번째 블록 해시를 블록 커밋 트랜잭션에 포함하게 하여 Finality 를 보장하고자 합니다. 마지막으로 sBTC 를 출시할 수 있게 됐습니다. sBTC 는 비트코인과 투웨이페그 방식을 이용해 1 대 1 로 페깅된 토큰입니다.

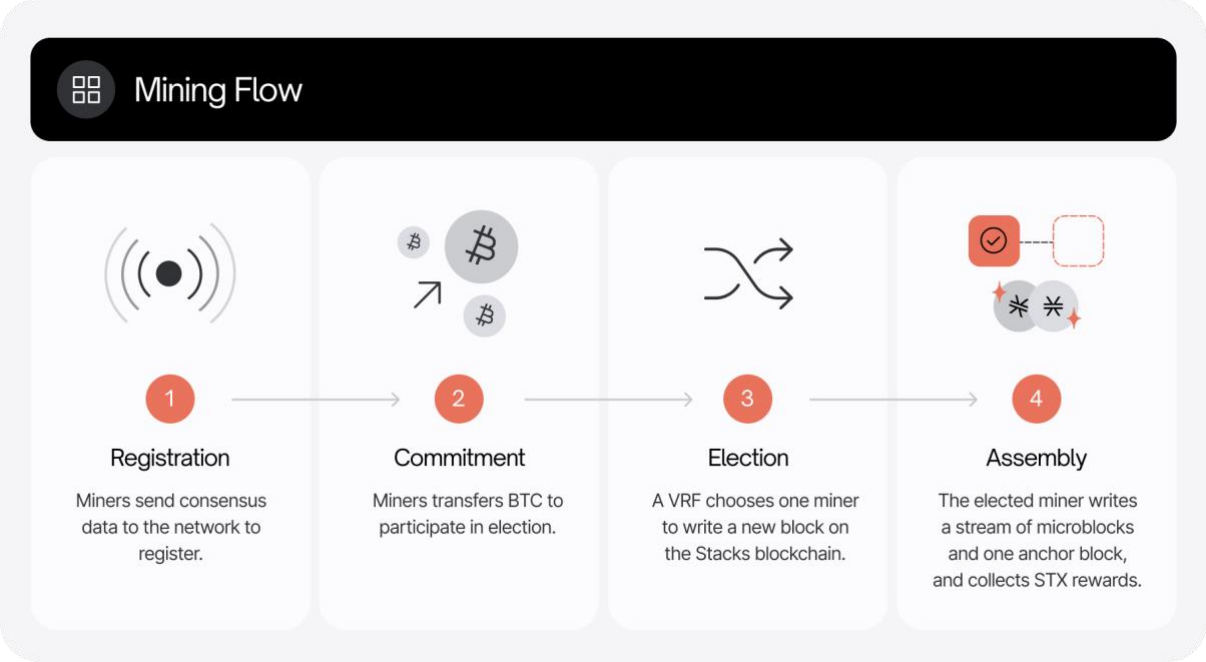
TECHNICAL FEATURES PROOF OF TRANSFER (POX)



Source : Bohyeon Park

Stacks 는 Proof of Transfer(이하 PoX)라는 자체적인 합의 알고리즘을 통해 작동합니다. 기존에 사용하던 Proof of Burn(이하 PoB) 매커니즘은 네트워크에 있는 토큰을 소각했다면, PoX 매커니즘은 소각 대신 네트워크의 다른 참여자들에게 분배하는 방식으로 매커니즘을 설정했습니다. 본 네트워크 내에서 Tenure 라는 시간 단위를 사용하는데 1 Tenure 는 하나의 비트코인 블록이 생성되는 시간(약 10-15 분)을 의미합니다. 비트코인의 한 블록은 Stacks 의 약 100 개의 블록과 상응하게 되므로, 1 Tenure 에는 약 100 개의 Stacks 블록이 포함된다고 할 수 있습니다. 즉, Stacks 의 블록들은 비트코인 블록과 1 대 다로 연결되어 있 게 됩니다. Stacks 는 각 블록마다 채굴자를 선정하는 것이 아닌 각 Tenure 마다 채굴자를 선정하고, 해당 Tenure 에 생성되는 모든 블록을 선정된 한 명의 채굴자가 채굴하도록 합니다.

Stacks 가 어떻게 채굴자를 선정하고 채굴을 진행하는지를 확인해보면 크게 4 가지 과정으로 나타낼 수 있습니다.



Source : Stacks docs

1. Registration

   채굴자는 추후에 있을 Tenure 의 채굴자로 선정되기 위해 미리 Consensus Data 를 네트워크에 전송하여 등록합니다.

2. Commitment

   앞의 등록 과정을 마친 채굴자들은 네트워크에 지정된 Set address 주소 중 2 개의 주소로 BTC 를 전송하며, 이때 전송된 BTC 를 “Committed BTC”라고 합니다. Committed BTC 는 후술할 Stacking 의 보상(incentive)으로 사용됩니다. 기본적으로 Stacks 프로토콜에 의해 강제되는 BTC Commiment 의 양은 없지만 Bitcoin Dust 라 는 개념에 의해 유효한 Commiment 를 제출하기 위해서 최소 11,000 satoshis 를 Commit 할 것을 권고합니다.

3. Election

   BTC 를 커밋한 채굴자들 중 한 명의 채굴자를 선정합니다. 이때, 해당 Tenure 의 채굴자로 채택될 확률은 (본인이 전송한 BTC 의 양)/(전송된 모든 BTC 의 양)으로 계산되며, 많은 금액을 보낼수록 채굴자로 채택될 가능성이 높아집니다.

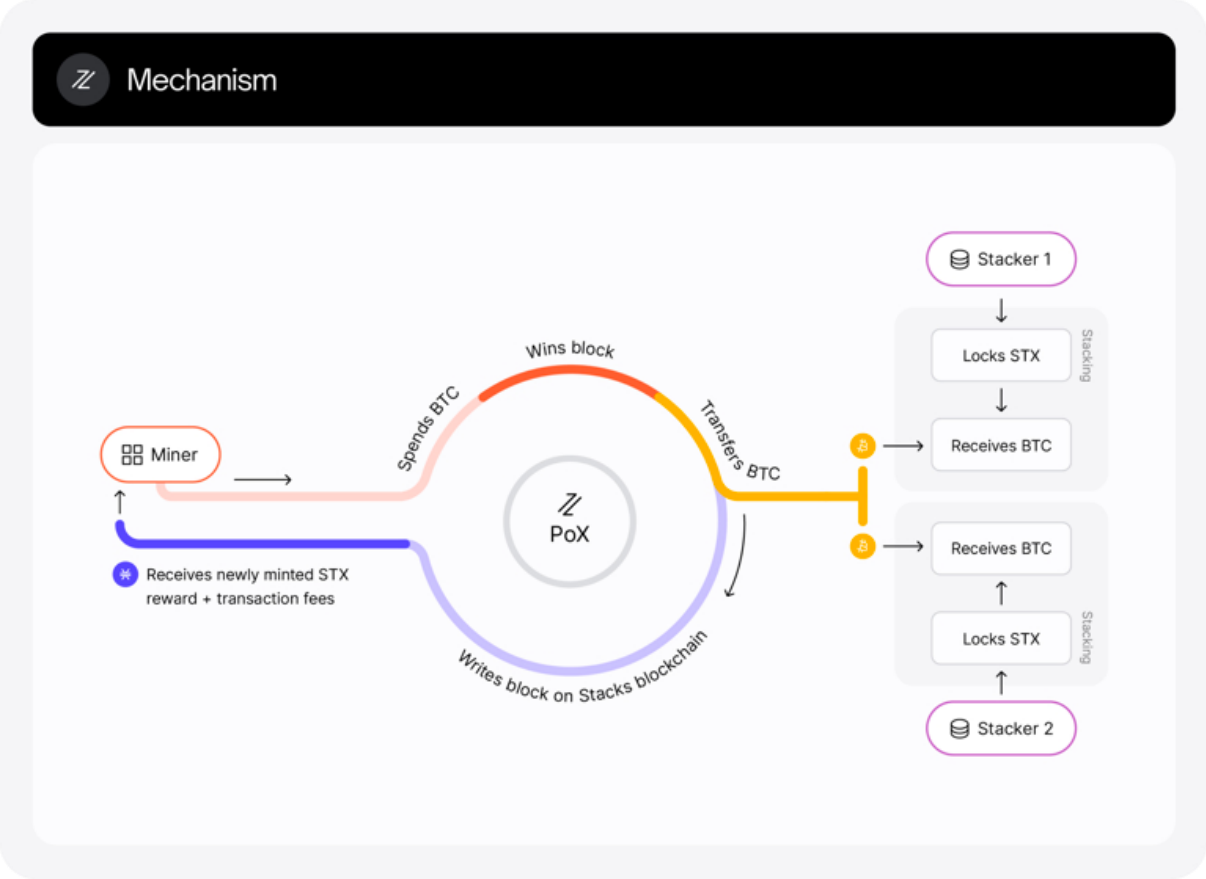
4. Assembly

   새로운 블록에 대한 채굴을 진행하고, 채굴 보상으로 새롭게 민팅되는 STX 을 수령합니다. 해당 보상은 바로 수령이 아닌, 비트코인에서 최종적으로 확정되야 수령할 수 있기 때문에 1 Tenure 가 지난 뒤에 수령할 수 있습니다.

PoX 컨센서스가 가지는 의의를 생각해봤을 때, 소각 방식이 아닌 BTC 커밋을 통해 네트워크의 다른 참여자 보상에 기여할 수 있다는 점과 다른 무엇도 아닌 BTC 의 제출을 강제함으로써 메인넷인 Bitcoin 과의 종속성을 강화한다는 점에서 의의를 가집니다.

STACKING

Stacking 은 Stacks 에서 만든 용어로, STX 토큰을 스테이킹(Staking)하는 것을 의미합니다. Stacks 는 STX 토큰을 일정기간 동안 네트워크에 락업(Lock up)하고, BTC 를 보상으로 받을 수 있게 합니다. 일반적인 PoS 컨센서스를 지닌 체인의 스테이킹과 비교하여 생각 했을 때, 크게 2 가지의 차이점을 가집니다. 먼저, 스테이킹에 대한 보상이 네이티브 토큰으로 이뤄지는 스테이킹과 달리 메인넷의 토큰으로 이뤄진다는 점입니다. STX 를 스테이킹한 Stacker 가 받는 BTC 보상은 앞서 서술한 채굴자들의 BTC 커밋먼트를 통해 이뤄집니다. 즉, 일반적인 스테이킹의 보상은 대부분 새로 발행하는 네이티브 토큰인 반면, Stacks 에서는 새로 발행하는 것이 아닌 이미 마련된 유한 자산을 통해 보상을 제공합니다. 다음으로, Stacking 한 자산에 대한 슬래싱(Slashing) 매커니즘이 존재하지 않는다는 점입니다. 스테이킹을 통해 밸리데이터(Validator) 업무를 수행하는 일반적인 PoS 체인에서는 밸리데이터가 업무를 제대로 수행하지 않았을 경우, 슬래싱 매커니즘을 통해 패널티를 부과할 수 있습니다. 하지만 Stacking 을 하고 Signer 업무를 해야 하는데(위임을 다른 주체에게 넘기면 해당 업무를 수행하지 않아도 됩니다) 제대로 수행하지 않은 경우, 일반적인 슬래싱과는 조금 다르게 STX 토큰을 언락(unlock)할수 없으며 BTC 보상도 받을 수 없습니다. 일반적으로 스테이킹 지분의 일부분을 차감하는 슬래싱과는 조금 다른 방법이라고 볼 수 있습니다.



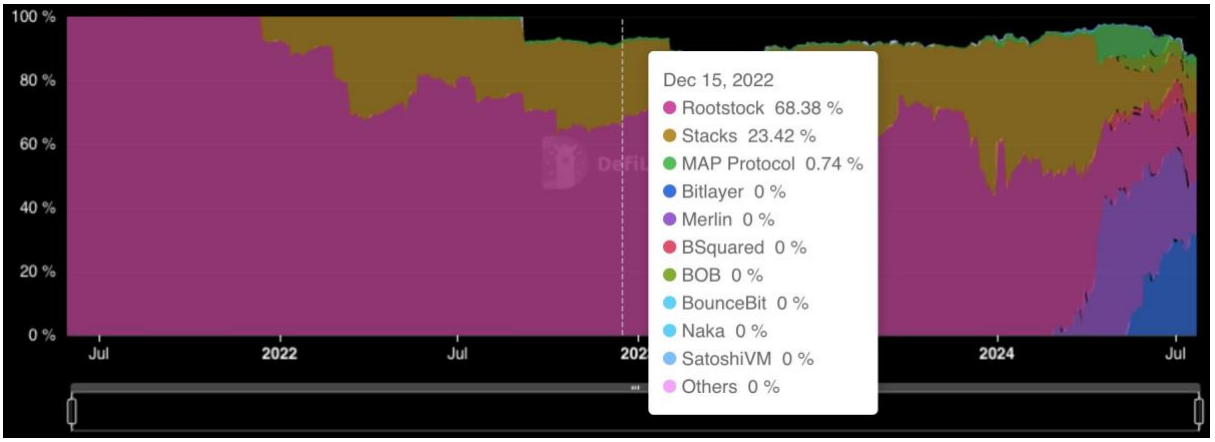
Source : Stacks docs

현재 PoX 와 Stacking 은 상호보완적이기 때문에 독립적으로 존재할 수 없는 구조로 이루어져 있습니다. 위 다이어그램을 통해 정리해보면, PoX 를 통해 채굴자는 BTC 커밋먼트를 하게 되며, 해당 토큰은 STX 를 락업한 2 명의 Stacker 지급되는 것을 확인할 수 있습니다. Tenure 에 선발된 채굴자는 블록을 채굴하고 해당 Stacks 블록이 Bitcoin 에 제출되면 보상으로 STX 와 트랜잭션 비용을 수령하게 됩니다. 이를 통해 알 수 있는 점은 BTC Commitment 를 소각하지 않고 또 다른 보상으로 사용하는 PoX 컨선세스는 결론적으로 Stacker 의 Stacking 을 독려함으로써 Stacks 의 보안을 높이는 데 긍정적인 작용을 하고, 비트코인 메인넷과 Stacks 의 종속성을 강화합니다.

Stacks 는 자체적인 컨센서스를 통해 블록을 생성하여 비트코인 네트워크에 제출하게 되는데, 제출한 블록의 유효성에 대해 비트코인에서 자체적으로 검증을 할 수 없고, 자체 토큰을 사용하기 때문에 비트코인의 보안을 완벽하게 상속받는다고 말하기 어렵습니다. 일반적으로 메인넷 위의 다른 체인이 메인넷의 보안을 상속받는다고 말하는 경우, 메인넷에 해당 체인의 블록이 유효하다는 증명을 같이 제출하거나 메인넷 자체적으로 블록의 유효성을 검증할 수 있어야 합니다. 하지만 Stacks 의 경우, 위 두 가지 모두 충족하지 않기 때문에 비트코인의 Finality 는 상속받지만 보안을 완벽하게 상속한다고 할 수 없습니다. 결론적으로 Stacks 는 1) PoX 라는 자체적인 컨센서스를 가진 독립적인 체인이며, 2) 네이티브 토큰인 STX 를 가스비로 활용하고, 3) 메인넷인 비트코인의 보안을 100 퍼센트 온전하게 상속받지 못합니다.

Stacks 는 자체적으로 사이드 체인이 아닌 레이어 2 라고 주장하지만, 위에서 제시한 사이드 체인 세 가지 정의에 모두 부합하기 때문에 사이드 체인으로 분류했습니다.

MARKET ANALYSIS



Source : DeFiLlama

2024 년 07 월 22 일을 기준으로 Market cap 은 약 $2.7B 이며, TVL 은 $142M 입니다. 해당 통계 수치는 비트코인 사이드 체인 생태계 내에서 Rootstock(RSK) 다음으로 높은 수치로, 모든 확장성 솔루션 중 10% 비율을 차지하고 있습니다. Stacks 가 출시되기 이전에 출시된 RSK 가 모든 파이를 가지고 있다가, 2021 년 01 월 이후 Stacks 쪽으로 파이가 조금씩 넘어오면서 지금은 $50M 의 차이로 RSK 가 조금 더 많은 TVL 을 가지고 있습니다.

하지만 2024 년 03 월 이후로 사이드 체인 자체의 TVL 이 많은 줄었고, 많은 파이가 다른 L2 솔루션, 특히 후술할 BitVM 을 기반으로 하는 L2 솔루션으로 전환된 것을 확인할 수 있습니다. 하지만 아직 BitVM 을 프로덕션 단계까지 개발하여 어플리케이션을 구축하는 것이 불가능한 상황이고, 구현 완료 일정 또한 미지수이기 때문에 이를 기반으로 한 롤업 솔루션도 현재는 사이드 체인 단계에 머물러 있습니다. 따라서 프로젝트 TVL 의 비율 변화에 사이드 체인보다 다른 솔루션이 더 선호된다고 확언할 순 없지만, 메인넷의 보안을 상속받지 못하는 사이드 체인에 반해 메인넷의 보안을 상속받을 수 있는 다른 L2 솔루션 등장에 대한 약간의 기대감이 표출된 것으로 보입니다.

LIMITATIONS

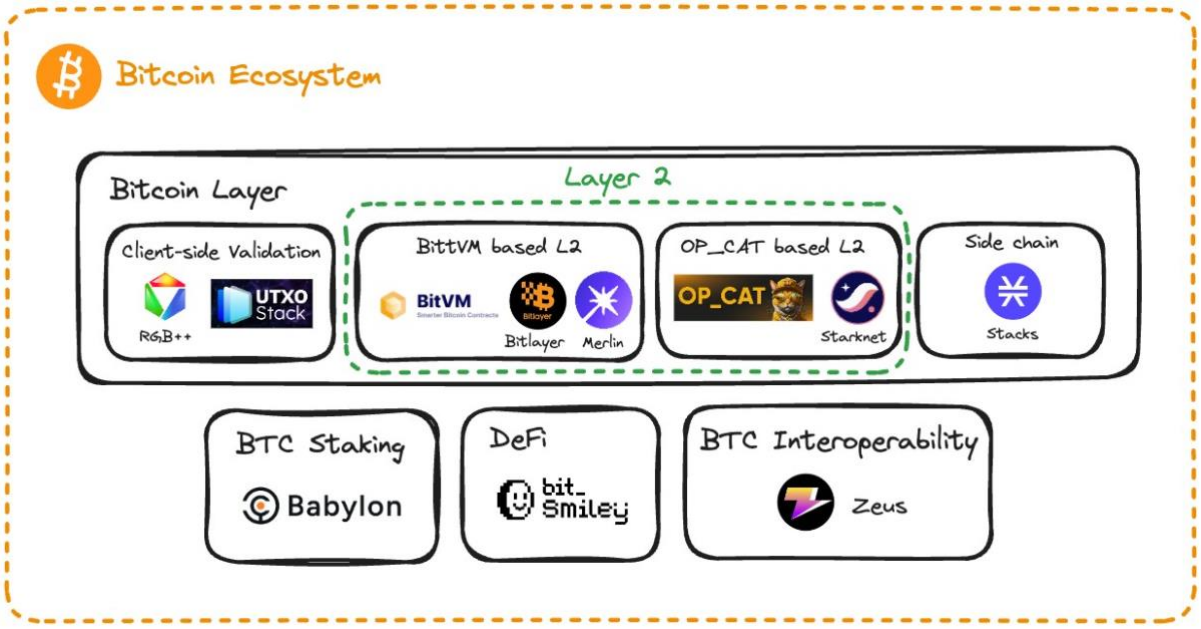
Stacks 의 주된 목적이 비트코인의 유틸리티성을 높이는 것이라는 점에서 이에 일조를 한 것은 분명히 맞으며, 이로 인해 비트코인 생태계에 다양한 사용자가 유입된 것도 사실입니다. 특히 기존 비트코인의 한계인 어플리케이션 가동성과 느린 트랜잭션 처리 속도를 해결하기 위해 스마트 컨트랙트를 Stacks 에 올릴 수 있게 하고, 트랜잭션 처리 속도를 높였다는 점은 비트코인이 할 수 없는 부분을 Stacks 만의 방식으로 잘 풀어냈다고 생각이 듭니다.

하지만 어쩔 수 없는 비트코인 메인넷의 한계로 인해 Stacks 에도 한계가 존재합니다. 결국 Stacks 가 사이드 체인이기 때문에 사이드 체인의 한계가 곧 Stacks 의 한계로 이어집니다. 자체적인 컨센서스를 가지고 빠르게 합의를 진행해 트랜잭션을 처리한다는 장점은 곧 비트코인의 보안을 상속받을 수 없다는 단점을 의미하는 데, 비트코인의 탈중앙성과 보안성을 중시하는 관점에서 보면 이는 치명적인 한계입니다. 실제로 이더리움을 보면, 많은 사이드 체 인들이 이더리움의 보안을 상속받는 롤업이 개발된 뒤 사용도가 감소한 것을 확인할 수 있습 니다.

또한 Stacks 의 자체 컨센서스인 PoX 가 비트코인의 Finality 를 100 퍼센트 상속받지만, 1 Tenure 가 하나의 비트코인 블록과 대응하기 때문에 해당 시간 동안은 Re-org Resistance 가 보장되지 않습니다. 1 번부터 Stacks 블록이 자체 네트워크에 제출되었다고 가정했을 때, 100 개의 Stacks 블록이 제출되면 101 번째 블록부터 비트코인의 Finality 를 상속받아 Reorg Resistance 를 지닐 수 있습니다. 물론 앞서 언급한 것처럼 해당 Tenure 의 첫 번째 블록 인덱스

해시를 블록 커밋 트랜잭션에 포함해야 하지만, 여전히 완벽하게 Re-org 가능성 을 해결했다고 보긴 힘듭니다. 이는 일반적인 롤업 구조에서도 비슷하기 때문에 분명한 한계 지만 큰 틀에서 봤을 때 심각한 한계로 받아들여지지 않습니다.

LAYER 2



Source : Wonjae Choi

비트코인은 가장 안전하고 탈중앙화된, 검열 저항성이 있는 블록체인입니다. 이러한 이유로, 많은 사람들은 더 저렴하고 스마트 컨트랙트 기능을 갖춘 다른 블록체인이 존재함에도 불구 하고 더 높은 비용을 지불하며 비트코인의 블록 공간을 사용하고자 합니다. 따라서 비트코인을 개선하는 모든 노력들은 이런 가치를 보존하면서 진행되어야 전제되어야 할 것입니다.

하지만 비트코인 확장성 문제는 오랫동안 거래를 비트코인 외부(오프체인)으로 이동시키는 방식의 해결책에 의존해왔습니다. 이러한 해결책들은 비트코인의 가장 중요한 가치인 보안, 탈중앙성, 검열저항성을 상속받지 못합니다. 이들은 단지 대체 블록 공간을 제공할뿐이며, 비트코인을 확장하지 않습니다.

현재에 비트코인 확장성 솔루션으로 가장 많이 사용되는 방식은 사이드체인입니다. 이 방식은 비트코인의 블록 공간을 확장하는 것이 아니라 대체 블록 공간을 제공할 뿐이므로, 비트코인 블록체인을 확장하지 못합니다. 즉, 사이드체인으로 이동된 비트코인은 더 이상 원래 비트코인의 속성을 가지지 않습니다. 또한 대체 블록 공간으로 사이드체인을 구축하는 것은 장기적으로 비트코인과 경쟁하며, 불안전한 브리지와 네트워크 구조를 통해 사용자의 자금을 위험에 빠뜨립니다. 따라서 사이드체인에 의해 지배되는 비트코인은 낮아진 보안, 탈중앙성, 검열 저항성을 가지게 될 것입니다.

비트코인을 진정으로 확장하려면 비트코인과 확장 솔루션 사이의 공생 관계를 구축해야 합 니다. 그러기 위해서 확장 솔루션은 프로토콜을 변경하지 않고 비트코인의 보안을 사용하는 방식으로 표현력과 처리량을 증가시켜야 합니다. 이를 달성하는 유일한 방법은 비트코인 록 공간을 확장하는 것입니다. 다른 대안은 비트코인 보안을 완전히 상속받지 못합니다.

비트코인 블록 공간을 확장하기 위해서는 롤업을 통한 레이어 2 솔루션을 사용할 수 있습니다. 레이어 2 는 비트코인의 보안을 온전히 상속받습니다. 그러기 위해서는 레이어 2 블록체인에서 일어난 트랜잭션들의 유효성이 비트코인 컨센서스에 의해 검증받아야 합니다. 이더리움에서는 이 과정은 스마트 컨트랙트로 구현되기 때문에 그동안 비트코인에서는 롤업 레이어 2 솔루션의 구현이 불가능 했습니다. 하지만, BitVM 이라는 새로운 방법론과 OP_CAT 이라는 비트코인

소프트 포크 제안을 통해 구현이 가능하며, 뒤에서 두 방법에 대해 자세하게 알아보도록 하겠습니다.

BITVM-BASED L2

What is BitVM?

BitVM 은 비트코인 상에서 튜링 완전한 컨트랙트를 표현하기 위한 계산 패러다임입니다. 이 방식은 비트코인의 프로토콜을 변경하지 않고 구현되어 비트코인의 보안에 어떠한 영향도 미치지 않습니다. BitVM 은 비트코인에서 직접 계산을 실행하는 대신, 오프체인에서 계산하고 이를 온체인 상에서 사기 증명(Fraud Proof)을 통해 검증하는 방식으로 동작합니다. 이는 옵티미스틱 롤업(Optimistic Rollup) 방식과 유사합니다.

이 시스템은 증명자(Prover)와 검증자(Verifier)라는 두 주체로 구성된 설정을 가정합니다. 증명자는 특정 계산이 올바르다는 것을 비트코인 상에서 증명하고자 하며, 이는 함수, 입력, 입력에 대한 출력, 이 세 가지 요소가 올바른 계산을 이루는 것을 증명하는 것이 목표입니다. 검증자는 그 주장이 거짓임을 밝혀내면 사기 증명을 수행하고 증명자를 처벌할 수 있습니다. 이 메커니즘을 통해 어떠한 계산 가능한 함수도 비트코인 상에서 검증할 수 있습니다.

BitVM 은 튜링 완전성과 오프체인 계산 및 사기 증명을 구현하기 위해 비트코인의 해시락(Hashlock), 타임락(Timelock), 그리고 탭루트를 사용합니다.

BitVM 의 과정을 단계별로 간략하게 보면 다음과 같습니다:

1. 증명자가 비트코인에서 증명하고 싶은 프로그램을 정의합니다. 이 프로그램은 입력과 출력이 존재하는 어떤 계산 가능한 함수도 될 수 있으며, 이를 검증하고자 하는 검증자가 있어야 합니다.

   예시: 덧셈 프로그램 f(a, b) = a + b

2. 증명자는 이 프로그램(계산 가능한 함수)을 논리 회로 단위로 컴파일하여 이를 비트코인 스크립트로 탭루트에 커밋합니다. 이 커밋된 스크립트들은 이 프로그램을 검증할 수 있도록 합니다. 예시: f → 논리 회로 → 비트코인 스크립트들 → 탭루트
3. 증명자와 검증자는 나중에 분쟁을 해결할 수 있도록 미리 일련의 챌린지-리스폰스(Challenge-Response) 트랜잭션들을 공동으로 사전 서명(Pre-sign)합니다. 이 트랜잭션들은 HTLC(Hashed Timelock Contract) 방식의 스크립트를 사용하고, 각자의 개인 키로 서명하여 상대방에게 줍니다.
4. 증명자는 예치금(Deposit) 비트코인을 특정 탭루트 주소에 입금합니다. 이 예치금은 계산이 올바르지 않거나 증명자가 부정 행위를 했을 경우, 검증자가 이 예치금을 가져가 증명자를 처벌하기 위함입니다. 이는 옵티미스틱 롤업의 슬래싱을 위한 보증금과 같은 역할을 합니다.

여기까지 설정(Setup) 과정이 끝나면 BitVM 컨트랙트가 활성화됩니다. 이제 증명자는 예치 금을 걸고 프로그램이 올바르다고 주장하며, 검증자는 증명자의 틀린 주장과 부정 행위에 대해 온체인 상에서 처벌할 수 있는 모든 권리를 가집니다. 이는 3 번의 사전 서명 트랜잭션을 통해 가능합니다.

5. 프로그램을 검증하기 위해 오프체인에서 데이터를 교환하는 방식으로, 증명자는 프로그램에 대한 입력과 출력 값을 검증자에게 제공합니다. 예시: 입력 = 2, 5 / 출력 = 7
6. 검증자는 프로그램, 입력, 출력 값을 이용해 오프체인에서 직접 실행하며 이를 검증합니다. 예시: 2 + 5 = 7 → O

7-a. 계산이 올바르게 검증된 경우, 검증자는 챌린지를 걸지 않습니다. 챌린지 기간이 지나면 증명자는 예치금을 가져갈 수 있으며, 해당 계산은 비트코인에 의해 검증이 완료됩니다.

7-b. 계산이 올바르지 않은 경우, 검증자는 사전 서명 트랜잭션을 이용해 챌린지를 걸고 챌린지-리스폰스 프로토콜을 시작합니다. 이 과정을 통해 검증자는 증명자를 처벌하여 증명자의 예치금을 가져갈 수 있게 됩니다.

이러한 과정을 통해 BitVM 은 어떤 계산도 비트코인 상에서 검증할 수 있도록 합니다.

ZK ROLLUP WITH BITVM

이더리움에서롤업은 스마트 컨트랙트를 통해 이더리움에 의해 검증됩니다. 이를 통해 롤업 체인들은 레이어 1 인 이더리움과 같은 보안을 누리고, 레이어 2 라고 부를 수 있게 됩니다. BitVM 은 롤업에서 이더리움의 스마트 컨트랙트가 하는 동일한 역할을 수행할 수 있습니다. 롤업에서 가장 중요한 두가지 컨트랙트는 롤업 트랜잭션들의 유효성을 검증하는 컨트랙트와 자산을 이동시켜주는 브릿지(Bridge) 컨트랙트입니다.

트랜잭션들의 유효성을 검증하는 방식에는 두가지 방식이 있는데, 유효성 증명(Validity Proof)와 사기 증명(Fraud Proof)입니다. BitVM 자체가 사기 증명의 방식을 사용하기 때문에, 사기 증명을 사용하는 경우 여러가지 문제가 발생하고, 구현의 복잡성과 비효율성 등이 존재하기 때문에 BitVM 을 사용하는 경우에는 유효성 증명을 사용합니다.

유효성 증명은 ZK 증명을 사용하여 암호학적으로 계산의 무결성을 보장하는 방법입니다. ZK 증명을 생성하는 것은 많은 계산을 요구하지만, 증명을 검증하는 것은 매우 적은 계산을 필요로 한다는 점을 활용합니다. 즉, 증명의 생성은 오프체인에서 하고, 검증만 레이어 1 의 온체인 상에서 하면 매우 낮은 온체인 비용으로 많은 트랜잭션들의 유효성을 보장할 수 있습니다. 여기서 증명을 검증하는 검증기 컨트랙트가 레이어 1 에 필요하고, 이를 BitVM 으로 구현할 수 있습니다. 이를 통해 BitVM 을 활용한 ZK 롤업 솔루션은 트랜잭션들이 레이어 1 에 의해 검증되고 보안을 상속받을 수 있습니다.

DATA AVAILABILITY

데이터 가용성(Data Availability)은 새롭게 생성된 블록을 검증할 수 있는 데이터에 완전히 접근할 수 있음을 보장하는 속성입니다. 롤업에서는 이를 위해 두 가지 방식을 사용합니다. 첫째, 데이터 가용성을 레이어 1 체인의 온체인 상에서 제공하는 방법으로, 보안이 뛰어나지만 비용이 높고 확장성이 낮습니다. 둘째, Celestia 나 Avail 과 같은 오프체인 DA 레이어를 활용하는 방법으로, 보안은 상대적으로 낮지만 비용 효율성과 확장성이 뛰어납니다. 유효성 증명을 사용하는 경우 Validium, 사기 증명을 사용하는 경우 Optimium 으로 구분합니다.

	Validity Proof	Fraud Proof
DA on-chain	ZK Rollup	Optimistic Rollup
DA off-chain	Validium	Optimium(Plasma)

BitVM 을 사용하는 ZK 롤업의 경우, 오프체인 데이터 가용성을 사용하는 방식은 Validium 과 유사합니다. 즉, 데이터 가용성이 보장되지 않더라도 Optimium 과 같은 방식에서 발생할 수 있는 모든 자금 탈취 위험을 제거할 수 있습니다. 데이터 가용성이 없는 상황을 가정해 봅시다. 레이어 2 시퀀서가 블록을 비트코인에 제출했지만, DA 레이어가 동작하지 않는다면 사용자들은 이 새로운 블록을 검증할 수 없습니다. 이 경우, 사용자는 무조건 챌린지를 걸면 됩니다. 그러면 증명자는 반드시 ZK 증명을 비트코인에 제출해야 하며, 제출하지 않으면 처 벌을 받습니다. 이 ZK 증명 자체로 트랜잭션의 모든 유효성을 증명할 수 있기 때문에, 데이터 가용성이 제공되지 않더라도 새로 생성된 블록의 유효성을 검증할 수 있게 됩니다. 일반적으로 Validium 은 보안적으로 안전하다고 여겨지기 때문에, BitVM 을 사용하는 Validium 의 방식도 충분히 안전하다고 할 수 있습니다.

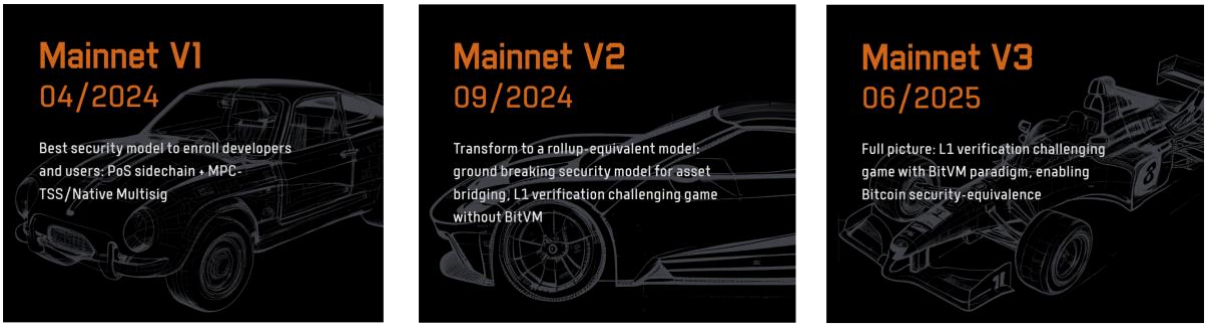
BITLAYER

Bitlayer

OVERVIEW

Bitlayer 는 BitVM 을 기반으로 한 비트코인 ZK 롤업 레이어 2 솔루션입니다. Bitlayer 는 비트코인의 보안을 계승하면서도 사용자에게 높은 처리량과 저비용 거래 경험을 제공하는 비트코인의 컴퓨팅 레이어(Computation Layer)가 되는 것을 목표로 하고 있습니다. 그러나 현재에는 BitVM 의 구현 문제로 인하여 PoS 의 합의 알고리즘을 사용하는 사이드체인으로 동작하고 있습니다.

Bitlayer 는 다음과 같은 로드맵을 가지고 있습니다. 첫번째 페이즈인 V1 은 2024 년 4 월에 런칭한 현재의 메인넷으로, PoS 사이드체인과 멀티시그 지갑(Multi-sig Wallet)을 이용한 브릿지를 사용하고 있습니다. 메인넷 V2 는 2024 년 9 월에 업그레이드가 예정되어 있으며, PoS 에서 롤업의 구조로 바꾸지만, BitVM 을 사용하지 않기 때문에 이 단계까지는 사이드체인으로 머무릅니다. 마지막으로 메인넷 V3 는 Bitlayer 가 기존에 말한 방향성을 모두 구현한 단계로, BitVM 을 통해 비트코인에서 검증을 하는 완전한 롤업 레이어 2 의 체인의 모습을 가집니다.



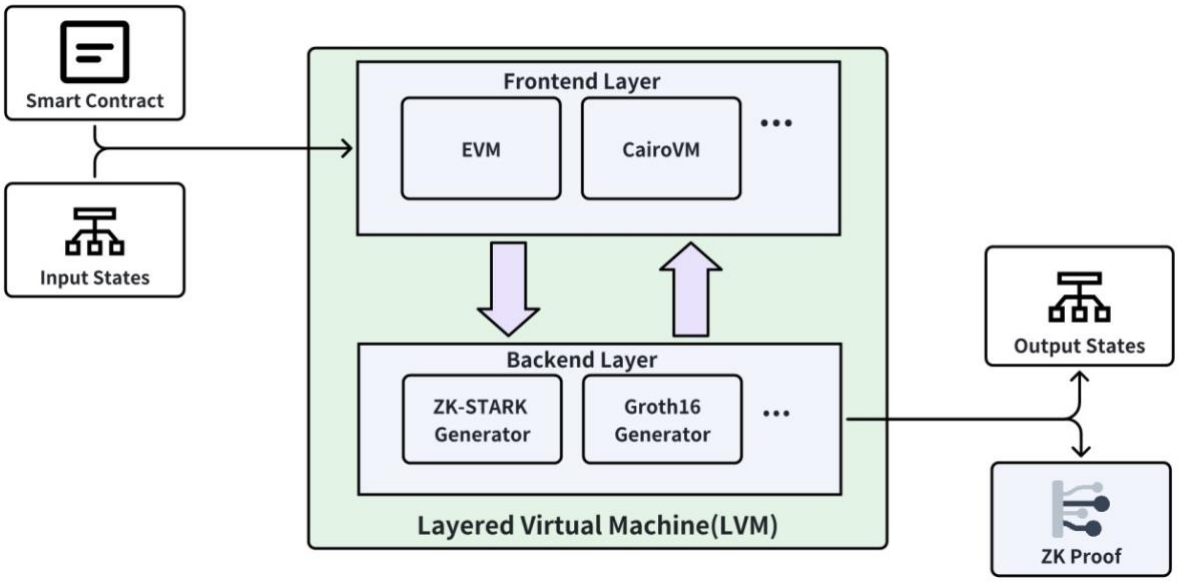
Source : Bitlayer

Bitlayer 의 팀인 Bitlayer Labs 는 싱가포르에 위치하며, 두 중국인 Kevin He 와 Charlie Yechuan Hu 에 의해 설립되었습니다. Bitlayer 는 2024 년 3 월 Framework Ventures 와 ABCDE capital 이 리드한 시드라운드 투자에서 $5M 을 유치하고, 2024 년 6 월 Franklin Templeton 과 ABCDE Capital 이 리드한 시리즈 A 라운드 투자에서 $11M 을 유치하여 총 합 $16M 의 투자를 성공적으로 유치했습니다.

Source : Bitlayer on X

TECHNICAL FEATURES

LAYERED VIRTUAL MACHINE



Source : Bitlayer Whitepaper

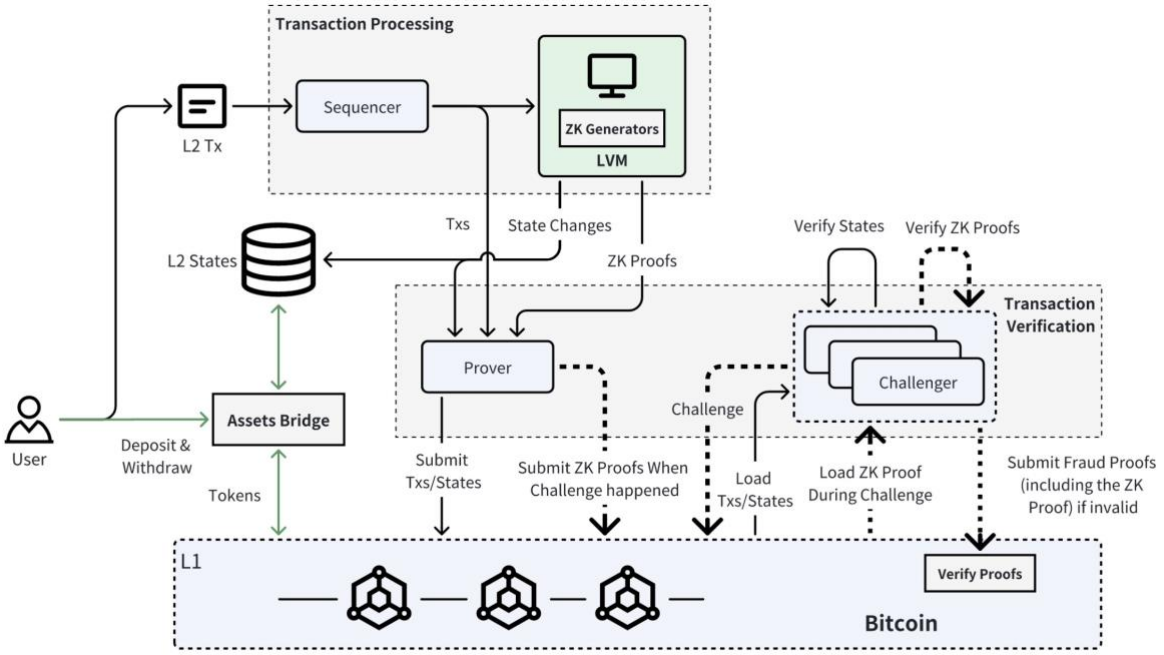
Layered Virtual Machine(이하 LVM)은 Bitlayer 에서 스마트 컨트랙트의 실행과 이에 대한 영지식 증명의 생성을 담당합니다. 이는 일반적으로 ZK 롤업에서 사용하는 zkVM 과 같은 역할을 합니다. 하지만 LVM 의 차이점은 스마트 컨트랙트의 실행과 영지식 증명의 생성을 분리하여 독립적인 개선과 확장을 가능하게 합니다.

LVM 은 프론트엔드와 백엔드로 나누어 프론트엔드는 스마트 컨트랙트의 실행을 담당하는 EVM, CairoVM 과 같은 가상머신을 의미하고, 백엔드는 STARK, Groth16 증명 생성기와 같이 영지식 증명을 생성하는 생성기로 나눕니다. 이렇게 분리함으로써 프론트엔드에서는 여러 가상머신을 지원하여 다양한 생태계와 통합하고 개발자를 생태계로 끌어들일 수 있으며, 백엔드에서는 더

뛰어난 영지식 증명 기술이 나왔을 때 쉽게 이를 적용하거나 독립적으로 최적화를 할 수 있다는 장점이 있습니다.

BITVM

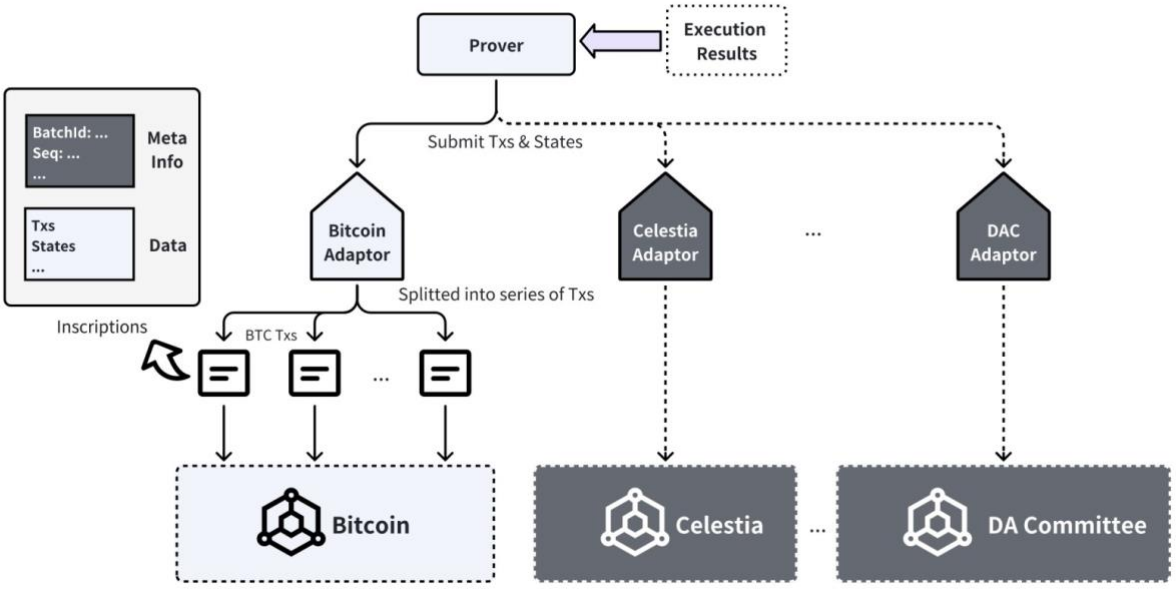
LVM 에서 생성된 영지식 증명은 레이어 1 체인인 비트코인에서 검증을 받음으로써 Bitlayer 의 거래들이 비트코인의 보안에 의해 보호됩니다. 이를 위해 Bitlayer 에서 사용하는 방식은 BitVM 입니다.



Source : Bitlayer Whitepaper

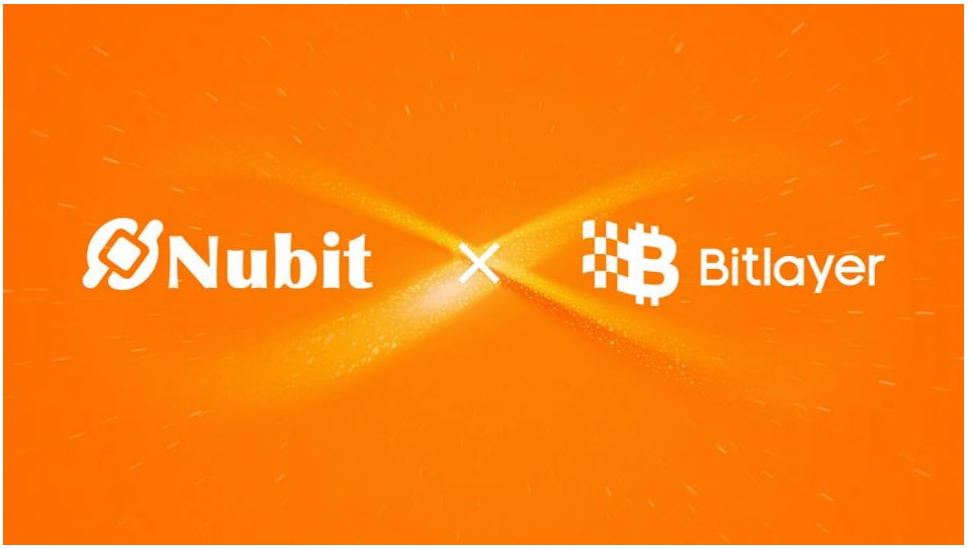
그림과 같이, 비트코인에는 BitVM 을 이용하여 LVM 에서 생성된 영지식 증명에 맞는 검증기(Verifier)가 BitVM 으로 구현됩니다. 증명자는 트랜잭션들과 상태 값을 비트코인에 제출합니다. 누구든지 검증자로 참여할 수 있으며, 검증자는 오프체인에서 계산을 해보고, 올바르지 않은 경우에는 챌린지를 겁니다. 그렇게 되면 증명자는 영지식 증명을 제출해야 하며, 영지식 증명이 올바르게 검증되지 않는 경우나 제출하지 않는 경우에 증명자는 제출했던 예치 금을 검증자에게 몰수 당하는 방식으로 처벌됩니다. 오프체인 계산이 올바른 경우에는 검증 자는 챌린지를 걸지 않으며, 일정 챌린지 기간이 지난 후에 해당 트랜잭션들은 비트코인에 의해 검증이 완료된 상태가 됩니다 정리해보자면, BitVM 을 통해 기존의 옵티미스틱 롤업과 유사하게 사기 증명의 방식으로 레 이어 1 인 비트코인으로의 Settlement 가 이루어지며, 챌린지의 상황에서는 영지식 증명을 통해 검증하게 됩니다.

DATA AVAILABILITY



Source : Bitlayer Whitepaper

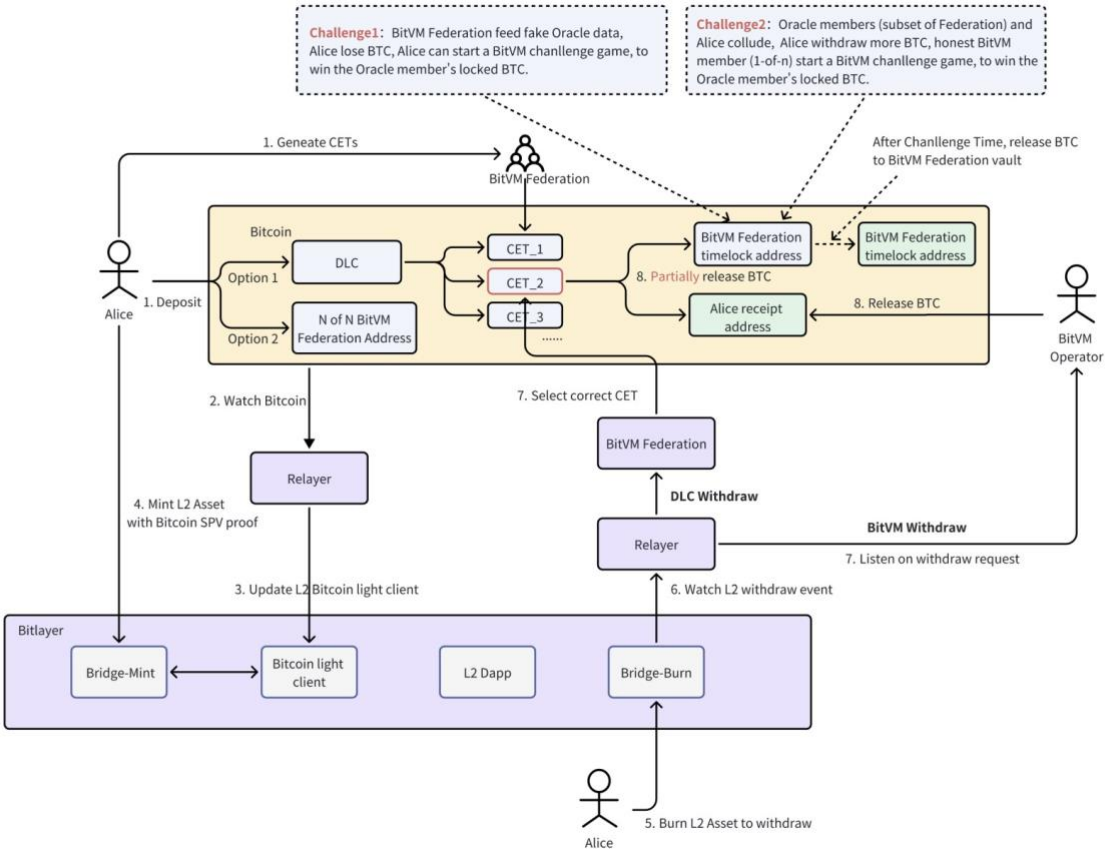
2024 년 4 월 기준의 Bitlayer 백서에 따르면, Bitlayer 는 가장 높은 보안을 위해 비트코인의 온체인 데이터 가용성을 보장한다고 나와있습니다. 이 경우에는 ZK 또한 오프체인 데이터 가용성을 사용하는 방법 또한 고려하고 있다고 적혀있습니다. 하지만 이는 로드맵 상의 이야기이고, 현재는 PoS 사이드체인으로 데이터 가용성 솔루션을 따로 제공하지 않고 있기 때문에, 추후에 적용될 때는 바뀔 가능성도 존재합니다.



Source : Nubit on X

또한 2024 년 3 월에는 Nubit 이라는 DA 레이어와 파트너쉽을 맺으면서, Bitlayer 가 Nubit 을 DA 레이어로 활용할 가능성도 있습니다. Nubit 은 비트코인의 자산을 스테이킹 받아 작동하는 비트코인 사이드체인 DA 레이어 프로젝트입니다.

ASSET BRIDGE

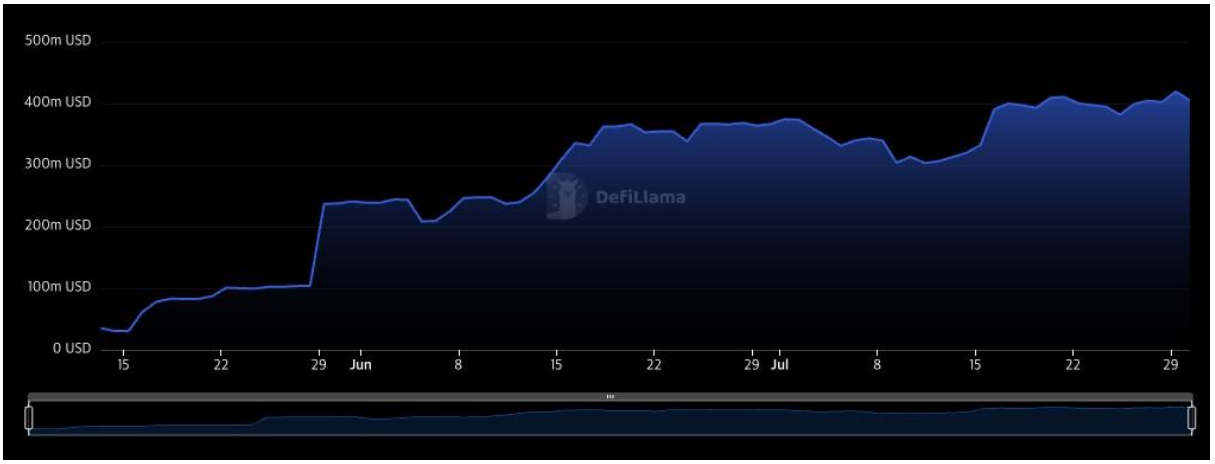


Source : Bitlayer Whitepaper

Bitlayer 는 OP-DLC 브리지와 BitVM 브리지로 구성된 이중 채널 양방향 페그 자산 브리지를 도입하여 동시에 운영됩니다. 첫번째는 OP-DLC 브릿지입니다. OP-DLC 브릿지는 사용자가 무신뢰(Trustless)한 방식으로 BTC 를 잠글 수 있는 채널입니다. 새로운 챌린지 프로토콜을 통합하여 OP-DLC 는 기존 DLC 프로토콜에서 오라클과 관련된 공모(Collusion) 문제를 효과적으로 해결합니다.

두번째는 BitVM 브릿지입니다. BitVM 채널은 옵티미스틱 롤업과 같은 보안 수준인 N 명 중 1 명의 보안 수준만 요구합니다. 견고한 보안과 Self-custody 을 원하는 사용자에게는 OP- DLC 채널이 제공되며, 더 큰 유연성과 속도가 필요한 사용자에게는 BitVM 채널이 적합합니다. 또한, 이중 채널 설계는 확장성을 향상시켜 높은 수요에서도 효율적인 성능을 보장합니다.

MARKET ANALYSIS



Source : Defillama

Bitlayer 의 7 월 30 일 기준 TVL 은 $579M 으로, 비트코인 사이드체인들 중 Merlin 에 이어 두번째로 높은 TVL 을 가지고 있으며, DeFi TVL 은 $403M 으로 가장 높은 TVL 을 차지하고 있습니다. Bitlayer 의 메인넷 출시는 2024 년 4 월에 이루어졌으며, 메인넷 출시와 함께 'Mining Gala' 이벤트를 진행하며 빠르게 사용자들과 그들의 자금을 끌어모았습니다. 이벤트 종료 이후에도 시즌 2 이벤트를 재개하는 한 편, 에어드랍 계획을 구체적으로 밝히며 마케팅의 모멘텀을 이어나가려 노력 중인 것으로 보입니다.

트위터 또한 굉장히 빠르게 성장하여 최근 50 만 팔로워를 달성하였고, 디스코드 회원 수는 13 만명을 돌파하였습니다. Huobi 출신 창업자가 있는 만큼 중국, 한국을 포함한 동아시아 계를 대상으로 마케팅을 활발하게 진행하는 것으로 보이며 꽤 성공적인 결과를 만들어내고 있습니다.

다만, 이러한 결과는 현재 진행 중인 여러 이벤트로 인한 일시적인 현상일 가능성도 있습니다. 이벤트와 에어드랍이 종료된 후 얼마나 많은 유저와 자금이 유지되는지, 그리고 자체적인 생태계가 얼마나 잘 기능하는지를 확인해야 진정한 성과를 평가할 수 있을 것입니다.

LIMITATIONS

Bitlayer 는 프로젝트의 소개와 강점으로 비트코인과 동일한 보안을 가지는 비트코인의 첫번째 ZK 롤업 레이어 2 라는 것을 내세웁니다. 하지만 이것은 현재 PoS 사이드체인의 방식으로 동작하고 있으므로 틀렸습니다. Bitlayer 가 광고하는 것처럼 진정한 레이어 2 가 되기 위해서는 BitVM 의 방식으로 구현된 ZK 검증기가 필수적입니다. 이는 Bitlayer 의 로드맵 상 V3 에 예정되어 있으며, 2025 년 6 월에 예정되어 있습니다.

BitVM 은 분명 혁명적인 패러다임이지만, 아직 개발 초기 단계로, 실제로 운영 중인 프로젝트가 없다는 점이 가장 큰 한계점입니다. 완전한 상용화를 위해서 얼마나 걸릴지, 또 다른 문제점이 발생할 지는 아무도 모릅니다. 이를 위해 Bitlayer 는 BitVM 과 관련한 리서치를 진행 하고 있으며, 이는 Bitlayer 의 1 순위 과제가 되어야만 할 것입니다.

Merlin chain

OVERVIEW

Merlin 은 2024 년 04 월에 메인넷을 런칭한 네트워크로, zkEVM 을 사용하는 ZK Rollup 비트코인 레이어 2 를 목표로 하는 프로젝트입니다. 현재 메인넷은 PoS 합의 알고리즘의 사이드체인으로 동작하고 있습니다. Merlin 은 Bitmap.Game (Bitmap 메타버스), BRC-420, 그리고 Recursiverse 를 개발한 Bitmap Tech 의 Founder 이자 CEO 인 Jeff 가 설립했으며, Bitmap Tech 팀에 의해 개발되었습니다. “Make Bitcoin Fun Again”이라는 문장을 내세워 사용자들이 BTC 를 비트코인 상에서 편하게 사용할 수 있도록 비트코인의 확장성을 제고하는 것을 목표로 합니다.

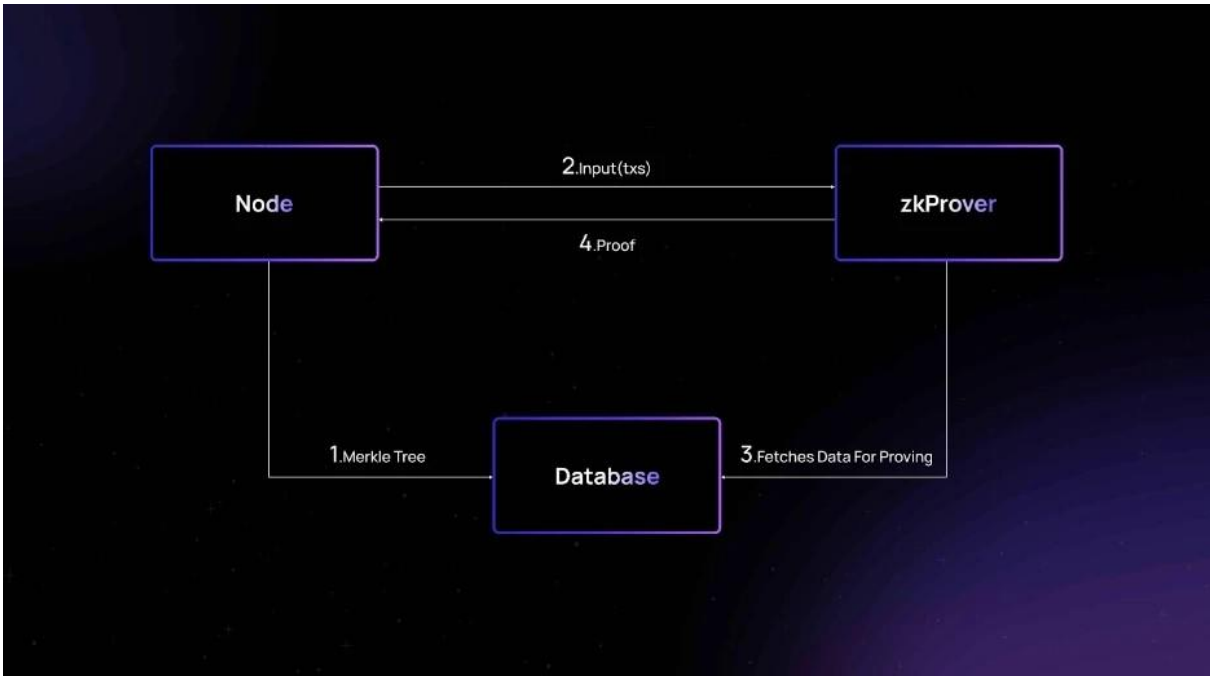
OKX Ventures, ABCDE Capital 와 같은 비트코인 생태계의 주요 VC 를 포함해 총 20 개의 VC 로부터 투자를 받았습니다. 특히 ABCDE Capital 는 비트코인 생태계에만 투자를 하는 VC 이며, 현재까지 출시된 프로젝트 중 비트코인 생태계 내에서 많은 관심을 받고 있는 대부분의 프로젝트에 투자하기도 했습니다. 해당 VC 가 투자를 했다는 점에서 Merlin 을 긍정적으로 바라보고 있다고 생각되며, 이뿐만 아니라 20 개의 VC 로부터 투자를 받았다는 점에서 현재 비트코인 생태계 내에 꽤 유망한 체인으로 보입니다.

Merlin 은 스스로를 ZK Rollup 으로 분류하지만, 앞서 언급한 것처럼 비트코인에서 ZK Rollup 을 구현하기 위해서는 BitVM 의 구현이 선행되어야 합니다. 하지만 현재 BitVM 은 구현이 완료되지 않았으며, 그 시기도 미지수이기 때문에 Merlin 역시 BitVM 이 구현된다는 가정 하에 분류를 진행하고자 합니다. 자세한 내용은 Technical Reseasrch 에서 후술하겠지만 BitVM 로직을 제시하며 ZK Rollup 의 구조를 띄고 있으나, DA layer 로 Celestia 를 사용하고 있기 때문에 ZK Rollup 이 아닌 BitVM 을 기반으로 하는 Validium 으로 분류했습니다.

현재는 BitVM 이 아닌 자체적인 Decentralized Oracle Network(이하 DON)을 이용하여 ZK Proof 에 대한 증명 검증을 진행하고 있으며, 검증 기능은 BitVM 의 구현이 되면 전환될 예정입니다. DON 은 증명 검증 외에도 외부 데이터에 대한 검증 및 데이터 분산 등 몇 가지 다른 기능을 하기도 하며, Merlin 의 주요 컴포넌트 중 하나로, Merlin 의 주요 컴포넌트는 ZK-Rollup Network, DON, Data Availability 를 꼽을 수 있습니다.

TECHNICAL FEATURES

ZK-ROLLUP NETWORK

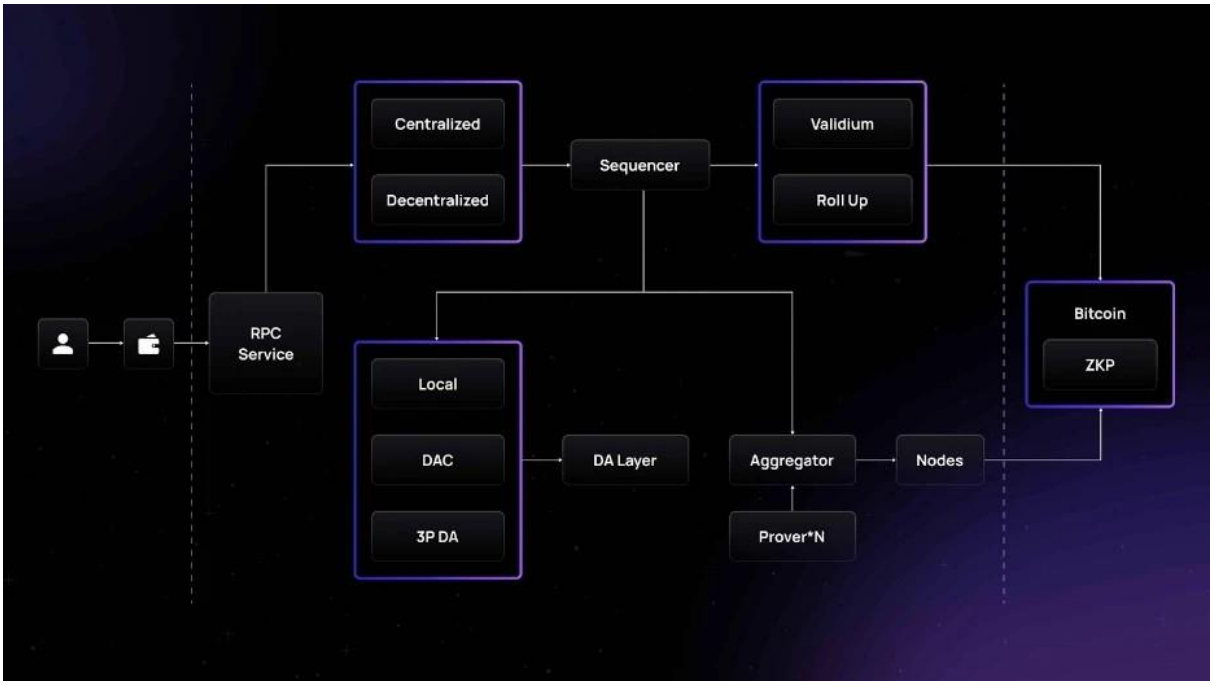


Source : Merlin docs

Merlin 의 ZK-Rollup 네트워크는 비트코인에 영지식 증명(ZKP)과 롤업 데이터를 기록하여 확장성을 높이는 솔루션을 제시하고 있습니다. 해당 네트워크는 트랜잭션 데이터를 배치로 압축하여 zkProver 를 통해 유효성을 검증하고, Merkle Tree 내용을 데이터베이스에 저장합니다. 주요 구성 요소는 노드, zkProver, 데이터베이스로 이루어져 있으며, 높은 보안성과 EVM 호환성을 제공하며, 낮은 거래 비용과 높은 성능을 목표로 하고 있습니다. 노드는 트랜잭션 데이터를 수집하고 배치 처리를 하며, 해당 데이터를 Merkle Tree 의 형태로 데이터베이스에 저장하여 트랜잭션 데이터를 안전하게 저장합니다. 이후, zkProver 를 통해 ZK 증명을 생성하여 데이터의 유효성을 검증하게 됩니다.

일반적인 ZK-Rollup 은 모든 트랜잭션 데이터를 배치 압축하여 메인넷 블록체인에 기록하여, 높은 보안성을 유지하지만, Merlin 의 경우, Celestia 라는 DA layer 를 따로 지정해 Celesti 에 기록하는 방식을 택했습니다. 앞서 언급한 것처럼 구조는 Rollup 의 형태를 띄고 있으나 DA 를 메인넷에 의존하지 않고, 제 3 의 솔루션에 의존하는 Validium 방식에 속합니다.

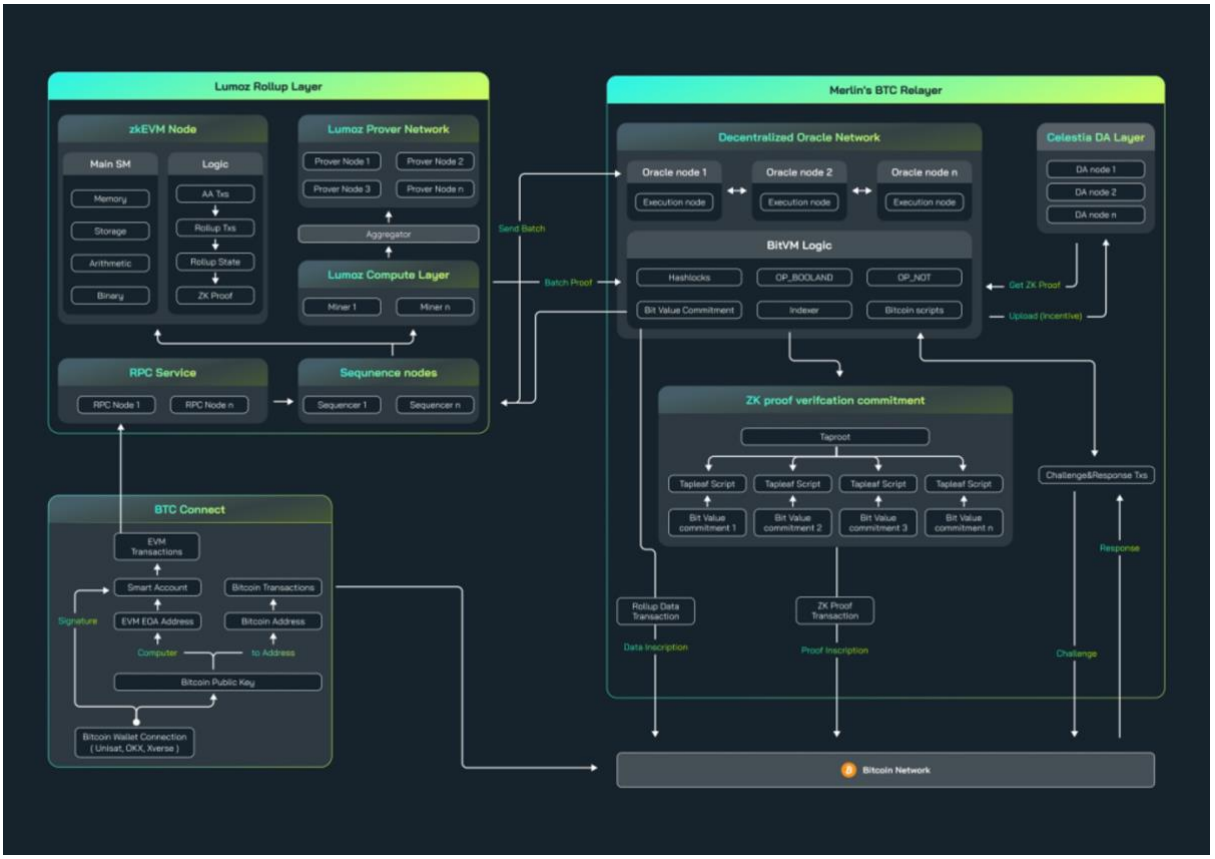
DECENTRALIZED ORACLE NETWORK (DON)



Source : Merlin docs

Merlin 은 자체적으로 탈중앙 오라클 네트워크(Decentralized Oracle Network)를 이용해서 시퀀서(Sequencer)로부터 받은 배치 데이터(Batch data)와 ZK 증명으로 해당 배치가 옳은 지 검증합니다. DON 은 트랜잭션 데이터를 수집하고 배치 처리하는 시퀀서 노드로 구성되어 있습니다. 해당 데이터는 압축된 트랜잭션 데이터, ZK 상태 루트 등을 생성하여 오라클 네트워크를 통해 비트코인의 탭루트에 업로드됩니다. 일반적인 ZK Rollup 의 구조는 Prover 라는 주체가 ZK 증명을 생성하면, ZK 증명을 받은 메인넷(L1)의 검증자(Verifier)가 증명에 대한 유효성을 검증하지만, Merlin 의 경우는 앞서 말씀드린 Lumoz 레이어에서 zk 증명을 생성하고, 자체적으로 운영하고 있는 DON 에서 ZK 증명을 받습니다. 받은 ZK 증명 은 DON 에서 분산되어 검증되며, 오라클을 이용해 off-chain 을 통해서 받은 ZK 증명이 맞는 지에 대한 검증도 진행합니다. Merlin 은 현재 BitVM 이 구현되지 않아 현재는 임의로 Verifier 를 세팅해서 검증하고 있습니다.

MERLIN'S OVERALL ARCHITECTURE



Source : The Block

Merlin 의 전반적인 아키텍쳐는 위와 같습니다. 먼저 사용자는 EVM 지갑 혹은 BTC Connect 를 이용해 비트코인 지갑을 사용하여 Merlin 체인에 트랜잭션을 제출합니다. 제출 된 트랜잭션들은 롤업 체인의 시퀀서 노드들에 의해 정렬되고 배치로 구성됩니다. 이 배치는 zkProver 에게 전달되어 zkEVM 의 결과로 나온 ZK 증명이 생성됩니다. 또한 트랜잭션들의 데이터는 DA 레이어인 Celestia 에 업로드 됩니다. 이 배치와 ZK 증명은 ZK-Rollup 네트워 크를 벗어나 Merlin 의 DON 에 전달되며, DON 은 BitVM 의 방식으로 ZK 증명이 검증받을 수 있도록 데이터를 컴파일하여 비트코인 탭루트에 커밋합니다. 비트코인에서는 사기 증명 의 방식으로 해당 ZK 증명에 대한 검증이 완료되면, Merlin 의 트랜잭션이 비트코인에 의해 검증이 완료됩니다.

MARKET ANALYSIS

2024 년 07 월 29 일을 기준으로 Merlin 의 TVL 은 $2.7B 입니다. 현재 Optimism, Arbitrum, Base 를 제외한 대부분의 이더리움 레이어 2 보다 높은 TVL 이며, 비트코인 내에 서는 가장 높은 TVL 을 가지고 있습니다. Merlin 은 런칭한지 반년도 되지 않았지만, 총 8 분 야—AI, DeFi, NFT, Social, Game, Infra, LaunchPad, Other—에서 꽤 많은 디앱이 이미 생태계에 올라와 있으며 트위터와 같은 기본적인 커뮤니티도 굉장히 활성화되어 있습니다.

현재 비트코인 레이어 2 중 가장 기대받고 있는 프로젝트 중 하나며, BitVM 기술을 활용하여 ZK 롤업을 구현하지만, BitVM 이라는 단어의 사용을 지양하고 있는 것으로 보아 이를 차용해 자체적으로 개발하여 내러티브(Narrative)를 가져오려는 것이 목표로 보입니다.

LIMITATIONS

Merlin 은 BitVM based L2 라는 점에서 해당 분류의 프로젝트들이 가지는 한계와 유사한 한계점을 지닙니다. 앞서 서술한 Bitlayer 와 마찬가지로 진정한 레이어 2 가 되기 위해서는 BitVM 의 방식으로 구현된 ZK 검증기가 필수적입니다. 즉, BitVM 의 구현 여부에 따라 Merlin 이 Rollup 의 로드맵을 완성할 수 있을지에 대한 여부가 결정됩니다. 이는 Merlin 이 가지는 분명한 한계점으로, 구현 기간과 여부를 확정할 수 없으며, 현재 제시된 아키텍처 또한 수정될 수 있다는 것을 의미합니다.

OP_CAT BASED L2

OP_CAT

비트코인은 단순한 가치 전송을 넘어 다양한 애플리케이션과 서비스를 지원하기 위해 지속 적으로 발전하고 있습니다. 그 과정에서 스크립트 언어인 비트코인 스크립트는 중요한 역할을 해왔습니다. 그러나 초기 비트코인 스크립트에는 몇 가지 제한이 있었고, 그 중 하나는 OP_CAT 명령어의 비활성화였습니다. 이 섹션에서는 OP_CAT 명령어의 개요와 역사를 살펴보고, 현재 비트코인 커뮤니티에서 논의되고 있는 재활성화 제안에 대해 알아보겠습니다.

OP_CAT 은 원래 비트코인의 명령어(Opcode) 중 하나로, 스택(Stack)에 있는 두 요소를 하나의 요소로 결합하는 기능을 제공합니다. 그러나 2010 년에 비활성화되었으며, 그 이후로 다양한 형태로 다시 도입하려는 제안이 계속되어 왔습니다. OP_CAT 의 주요 목적은 스크립트 작성자가 제공하는 데이터와 스크립트를 사용하는 사람이 제공하는 데이터를 결합하는 것입니다. 이를 통해 더욱 복잡하고 유연한 스크립트를 작성할 수 있게 됩니다.

비트코인 스크립트는 루프나 조건문을 지원하지 않아 복잡한 논리를 구현하는 데 제한이 있었지만, OP_CAT 과 같은 명령어를 통해 이러한 한계를 극복할 수 있는 가능성이 열립니다. 특히, OP_CAT 은 다양한 스마트 컨트랙트와 디앱을 구현하는 데 중요한 역할을 할 수 있습니다.

OP_CAT 은 비트코인 스크립트의 명령어 중 하나로, 스택에 있는 두 요소를 하나의 요소로 결합하는 기능을 제공합니다. 예를 들어, 스택에 ‹0xB10C›와 〈0xCAFE〉 두 요소가 있을 때, OP_CAT 을 사용하면 이 두 요소가 결합되어 〈0xB10CCAFE〉가 됩니다.

이 명령어는 스크립트 작성자가 제공한 데이터와 스크립트를 사용하는 사람이 제공한 데이 터를 결합하는 데 사용됩니다. 예를 들어, Alice 가 경쟁 지출을 방지하기 위해 자신의 자금을 위험에 노출시키지 않도록 하는 스크립트를 작성하려고 할 때, OP_CAT 을 사용할 수 있습니다. Alice 는 일반적인 방식으로 개인 키를 생성하고, 이를 통해 공개 키를 도출합니다. 그런 다음, 무작위로 선택한 개인 논스(Nonce)를 생성하고, 이를 통해 공개 논스를 도출합니다. 그런 다음, 다음과 같은 스크립트에 지불합니다:

```
< public nonce> OP_CAT <pubkey> OP_CHECKSIG
```

나중에 Alice 가 서명할 때, 전체 슈노르 서명(Schnorr signature)을 제공하는 대신, 스크립트에서 제공한 공개 논스를 사용해야 합니다. 이때, Alice 는 증명 필드에 스칼라만 제공하면 됩니다. 스칼라와 공개 논스가 결합되어 슈노르 서명을 생성하고, 이는 OP_CHECKSIG 명 령어를 통해 Alice 의 공개 키로 정상적으로 검증됩니다.

만약 Alice 가 나중에 다른 버전의 거래에 서명하려고 시도하면, 동일한 공개 논스를 다시 사 용해야 하지만, 슈노르 서명의 방정식 때문에 다른 스칼라를 생성해야 합니다. 동일한 논스를 다른 서명에서 재사용하는 경우, 누구나 Alice 의 개인 키를 도출할 수 있으며, 아직 자금이 소비되지 않았다면 자신의 서명을 생성하여 Alice 의 자금을 소비할 수 있습니다. 이러한 방식으로 기존의 비트코인 스크립트로는 구현할 수 없는 다양하고 복잡한 로직들을 구현할 수 있습니다. 이외에도 OP_CAT 은 비트스트림(Bitstream), 머클 트리 서명(Merkle Tree Signature), 램포트 서명(Lamport Signature), Non-equivocation 컨트랙트, 볼트 (Vaults), CheckSigFromStack 과 같은 다양한 사례를 가능하게 하고, 특히 ZK 검증기 또 한 구현할 수 있게 하는 매우 강력하고 간단한 명령어입니다.

STARK VERIFIER

STARK(Scalable Transparent Argument of Knowledge)는 ZK 증명 시스템 중 하나로, 복잡한 연산을 오프체인에서 수행하고 결과를 온체인에서 검증하는 암호학적 프로토콜입니다. 이를 통해 연산의 정확성을 증명할 수 있습니다. STARK 의 주요 특징으로는 양자 컴퓨터에 대해 안전한 Post-quantum Security, Trusted Setup 의 과정이 없음, 추가적인 보안 가정 없이 비트코인의 보안으로 검증, 그리고 대규모 연산을 빠르게 처리할 수 있는 빠른 확장성이 있습니다.

OP_CAT 을 사용하면 비트코인 스크립트에서 ZK 검증기를 구현할 수 있습니다. 특히 STARK 는 비트코인 친화적인 검증기 중 하나입니다. 그 이유는 STARK 가 주로 해시 함수를 사용하므로 비트코인 스크립트에서 효율적으로 구현할 수 있으며, 이는 비트코인 스크립트가 해시 연산을 기본적으로 지원하기 때문에 추가적인 대수적 연산이 필요 없기 때문입니다. 또한, STARK 의 Circle-STARK 변형은 31 비트 필드 크기를 사용하므로 비트코인 스크립트의 4 바이트 제한에 잘 맞아 더 효율적이고 쉽게 구현할 수 있습니다. STARK 는 복잡한 연산을 필요로 하지 않기 때문에, OP_CAT 과 같은 간단한 명령어만으로도 충분히 구현할 수 있어 비트코인 스크립트의 제한 내에서 강력한 검증 기능을 제공할 수 있습니다.

STARK 증명 시스템은 오프체인에서 복잡한 연산을 수행하고, 온체인에서는 이를 검증하는 데 필요한 최소한의 연산만 수행하므로, 비트코인 블록체인의 확장성을 크게 향상시킬 수 있습니다. 또한, 비트코인 스크립트는 단지 연산의 정확성을 검증하는 데 사용되므로, 연산 과정에서 발생할 수 있는 오류나 공격으로부터 안전합니다. STARK 를 통해 더 복잡한 연산을 지원할 수 있으므로 스마트 컨트랙트의 표현력을 크게 강화할 수 있으며, 다양한 프로그래밍 언어로 작성된 연산을 비트코인 스크립트에서 검증할 수 있어 스마트 컨트랙트 개발의 편의성과 안전성을 높입니다.

Starknet

OVERVIEW

Starknet 은 현재 이더리움에서 작동하는 ZK 롤업 기반의 레이어 2 솔루션으로, STARK 기 술을 사용하여 높은 확장성을 제공합니다. Starknet 은 StarkWare 에 의해 개발되었으며, 이더리움의 확장 문제를 해결하기 위해 설계되었습니다. Starknet 은 높은 처리량과 낮은 수수료를 제공하면서도 이더리움의 보안을 유지합니다.

StarkWare 은 2024 년 6 월에 비트코인을 확장하겠다고 발표하고 그 비전을 공유했습니다. Starknet 의 목표는 OP_CAT 업그레이드가 이루어진 후 6 개월 이내에 비트코인과 이더리움 모두에 정착하는 최초의 네트워크가 되는 것입니다. 이를 통해 Starknet 은 두 네트워크 간의 안전하고 자율적인 자산 이동을 가능하게 하여, 단일 레이어 2 솔루션으로서 두 블록체인을 동시에 확장할 수 있습니다.

2008 년 글로벌 금융 위기 이후, Satoshi Nakamoto 는 혁신적인 비트코인 백서를 발표하여 더 높은 수준의 투명성과 무결성을 요구했습니다. 비트코인은 전통적인 은행 시스템 대신, 광범위한 기여자들에게 공정하고 투명하게 가치를 분배하는 프로토콜을 도입했습니다.

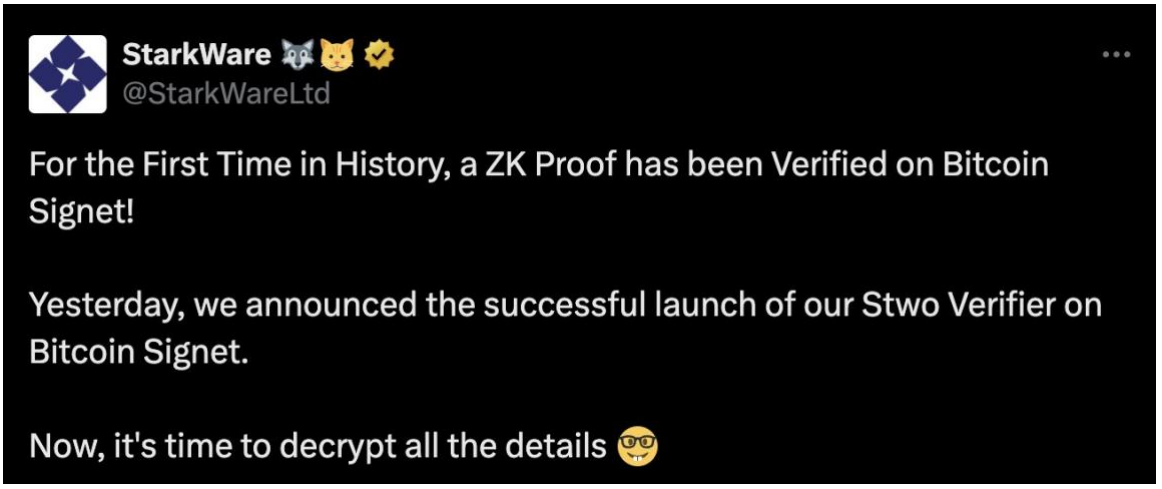
Starknet 은 이러한 비전을 이어받아, 비트코인과 이더리움을 동시에 확장하여 대규모 거래 처리를 가능하게 하고 금융 접근성을 향상시키는 것을 목표로 합니다.

StarkWare 는 ZeroSync Foundation 과의 전략적 파트너십을 통해 OP_CAT 기반 컨트랙트와 STARK 검증기를 개발하고 있습니다. 또한, $1M 연구 기금을 출시하여 OP_CAT 의 영 향을 연구하는 비트코인 연구자와 개발자를 지원하고 있습니다.

TECHNICAL FEATURES

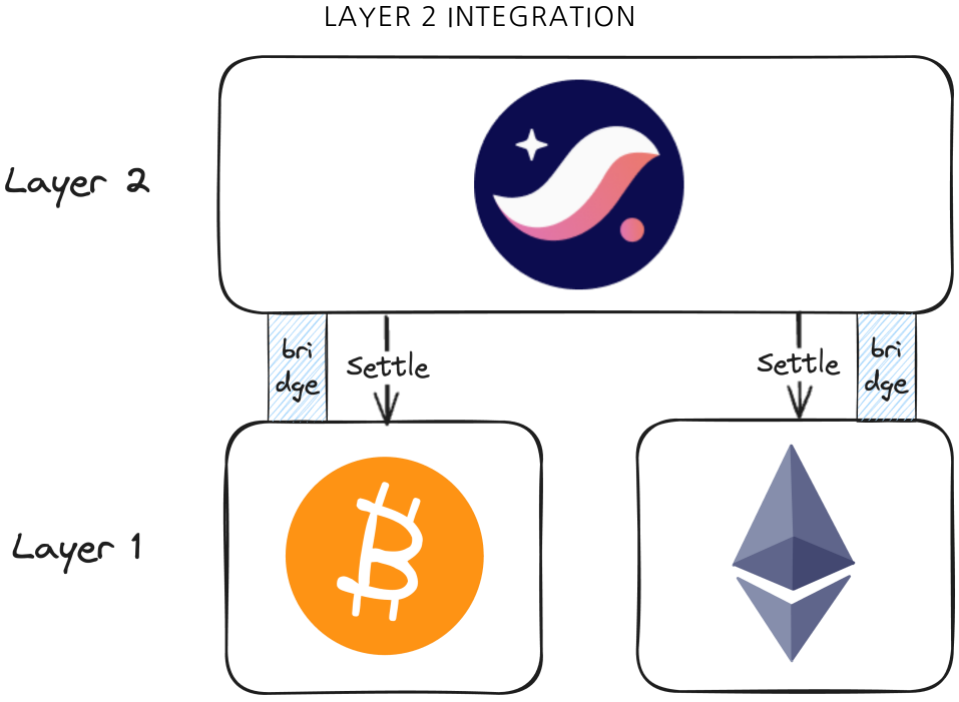
STARK PROOF SYSTEM

앞서 언급했듯이, STARK 증명 시스템은 가장 진보된 증명 시스템 중 하나로, ZK 롤업을 만드는 데에 잘 사용되고 있습니다. 특히, STARK 는 다른 시스템에 비해 비트코인에 매우 친화 적입니다.



Source : StarkWare on X

2024 년 7 월 17 일, StarkWare 는 OP_CAT 이 활성화된 비트코인 테스트넷인 시그넷 (Signet)에서 처음으로 비트코인에서 STARK 증명 시스템을 이용하여 ZK 증명에 대한 검증을 완료했습니다. 이는 앞서 언급한 비전들이 현실화될 수 있음을 보여주며, 비트코인의 발전 가능성을 나타내는 중요한 사건이라 할 수 있습니다.



Source : Wonjae Choi

Starknet 은 비트코인과 이더리움 모두에 정착하는 레이어 2 통합을 통해 자산의 자율적 상태 관리 및 업데이트를 가능하게 합니다. 이는 OP_CAT 을 사용하여 머클 트리를 생성하고 검증하는 데 중요한 역할을 합니다. OP_CAT 은 STARK 검증에 필요한 해시 결합을 가능하게 하며, 이는 재귀적 컨트랙트를 통해 자산의 상태를 자율적으로 관리할 수 있게 합니다. 이를 통해 Starknet 은 두 네트워크 간의 안전하고 자율적인 자산 이동을 가능하게 하여, 단일 레이어 2 솔루션으로서 두 블록체인을 동시에 확장할 수 있습니다.

CAIRO PROGRAMMING LANGUAGE

Cairo Programming Language

Starknet 의 고유한 프로그래밍 언어인 Cairo 는 Rust 와 유사하여 개발자들이 쉽게 접근할 수 있습니다. Cairo 는 Starknet 에서 더 복잡한 스마트 컨트랙트와 탈중앙화 애플리케이션을 구현할 수 있게 합니다. Cairo 를 통해 다양한 프로그래밍 언어로 작성된 연산을 비트코인 스크립트에서 검증할 수 있어, 스마트 컨트랙트 개발의 편의성과 안전성을 높입니다.

ENHANCED USER EXPERIENCE

Starknet 은 사용자 친화적인 자가 관리 인터페이스를 제공하여, 비트코인 레이어 1 보안을 활용한 장기적인 가치 저장소 기능을 제공합니다. 이를 통해 사용자는 일상적인 필요를 위해 안전하고 간편한 자가 관리 상호작용을 할 수 있으며, 비트코인의 견고하지만 복잡한 레이어

1 보안을 장기적인 가치 저장소로 사용할 수 있습니다. 이와 같은 사용자 경험 향상은 Starknet 이 비트코인 생태계에서 더욱 널리 채택되도록 하는 데 기여할 것입니다.

MARKET ANALYSIS

Starknet 은 2021 년 11 월부터 메인넷이 동작하는 오래된 이더리움 레이어 2 중 하나이며, 긴 기간동안 쌓아올린 탄탄한 사용자와 개발자 커뮤니티를 보유하고 있습니다. 또한 Starknet 위의 다양한 디앱들과 DeFi 또한 존재합니다. 이는 새롭게 시작하는 비트코인 레 이어 2 에 비해 매우 큰 장점이며, 현재 있는 인프라와 커뮤니티를 활용하여 OP_CAT 도입 초기에 많은 유저와 자금을 모을 수 있는 가능성이 있습니다.

Starknet 은 비트코인과 이더리움을 통합하는 첫번째 레이어 2 솔루션이 되는 것이 목표이므로, 이를 달성하면 가장 큰 두 블록체인을 잇는 매우 안전하고 탈중앙화된 다리로써 사용될 수 있습니다. 별 다른 기능을 제공하지 못하고 중앙화된 비트코인-이더리움 브릿지인

WBTC(Wrapped BTC)가 현재 $10B 이 넘는 TVL 을 보유한 점으로 미루어 보아, 비트코인-이더리움 브릿지에 대한 요구를 채워주면서 성장할 수 있는 가능성이 있습니다.

LIMITATIONS

StarkWare 의 노력에도 불구하고, OP_CAT 이 비트코인에 도입되지 않으면 모든 계획이 실현되지 못할 것입니다. 또한, OP_CAT 을 이용한 시도가 처음이기 때문에 예상치 못한 변수로 인해 문제가 발생하거나 개발이 지연될 가능성도 있습니다. 따라서 StarkWare 는 OP_CAT 을 공식적으로 지지하고 자금을 투입하여 연구를 진행하고 있습니다. 스타크넷의 계획을 위해서 이러한 노력이 지속적으로 뒷받침되어야 할 것입니다.

BABYLON

BabylonChain

OVERVIEW

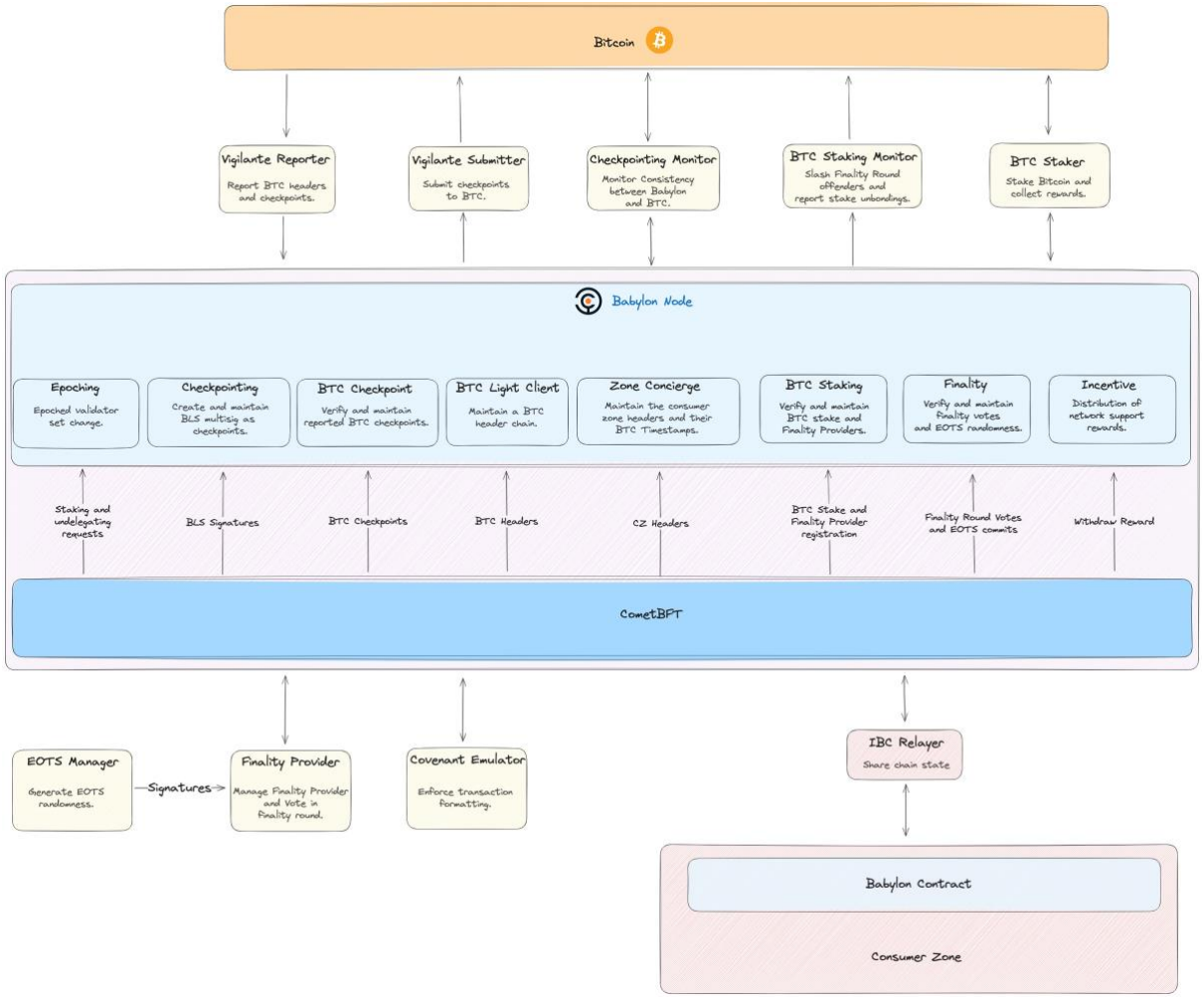
Babylon 은 2022 년 스탠포드의 David Tse 교수와 Fisher Yu 교수가 설립한 블록체인 프로젝트로, '비트코인으로 보호되는 분산형 세계를 구축하자'라는 사명 아래에 설립되었습니다. 이러한 사명을 달성하기 위하여 Babylon 은 세 가지 핵심 프로토콜인 Bitcoin Staking, Bitcoin Timestamping, Bitcoin Data Availability 을 개발하고 있습니다.

Babylon 을 쉽게 비유한다면 비트코인의 EigenLayer 라고 부를 수 있습니다. 비트코인을 가 지고 있는 홀더들은 Babylon Staking contract 를 통해 비트코인을 스테이킹하고, 스테이킹된 자본은 PoS 체인, 레이어 2, DA 레이어, 오라클 등의 PoS 이 필요한 곳들의 보안을 위해 사용됩니다. PoS 의 경우 PoW 에 비해 더 나은 접근성과 환경친화적인 장점을 갖고 있지만, 결국 스테이킹된 자산의 시가총액에 대비한 보안성을 가지기 때문에, 작은 규모의 PoS 시스템은 낮은 보안성이라는 문제를 극복하기 어렵습니다. 또한, 위에서 말씀드린대로 비트코인은 공급은 방대하지만 현재 수익률이 없다시피 한 오로지 가치 저장소의 역할만을 해왔기 때문에, 네이티브한 스테이킹 프로토콜은 비트코인 보유자에게 크게 매력적으로 다가갈 수 있습니다.

Babylon 의 총 투자 유치 금액은 $103M 으로, 비트코인 생태계 역사상 가장 큰 규모의 투자 를 받은 프로젝트 중 하나이기도 합니다. 2022 년 1 월 Babylon 은 IDG Capital, Frontiers Capital 등으로부터 엔젤 투자를 받았고 다음해 2023 년 3 월 Breyer Capital 과 IDG Capital 이 주도한 시드 라운드를 통해 $8.8M 을 추가 모금하였습니다. 2023 년 12 월 Polychain Capital 과 Hack VC 가 주도하여 Series A 를 $18M 의 규모로 성공적으로 마쳤 습니다. 그리고 2024 년 2 월 Binance Labs 는 미공개 금액으로 투자에 참여하였고, 2024 년 5 월 Paradigm 의 주도로 $70M 의 추가 투자를 유치하였습니다. 또한, Babylon 은 Paradigm 이 처음으로 투자한 비트코인 생태계 관련 프로젝트가 되었습니다.

TECHNICAL FEATURES

BABYLON ARCHITECTURE



Source : Babylon Docs

Babylon 시스템은 Cosmos SDK 를 기반으로 구축된 네트워크로, 바빌론 노드와 BTC 스테이킹, Finality 라운드 참여, 비트코인 및 Consumer Zone 과의 통신을 지원하는 다양한 프로그램들로 구성되어 있습니다. 이 시스템은 주로 바빌론 노드 모듈, Vigilante 프로그램, BTC 스테이킹 프로그램, 그리고 Consumer Zone 으로 나뉩니다.

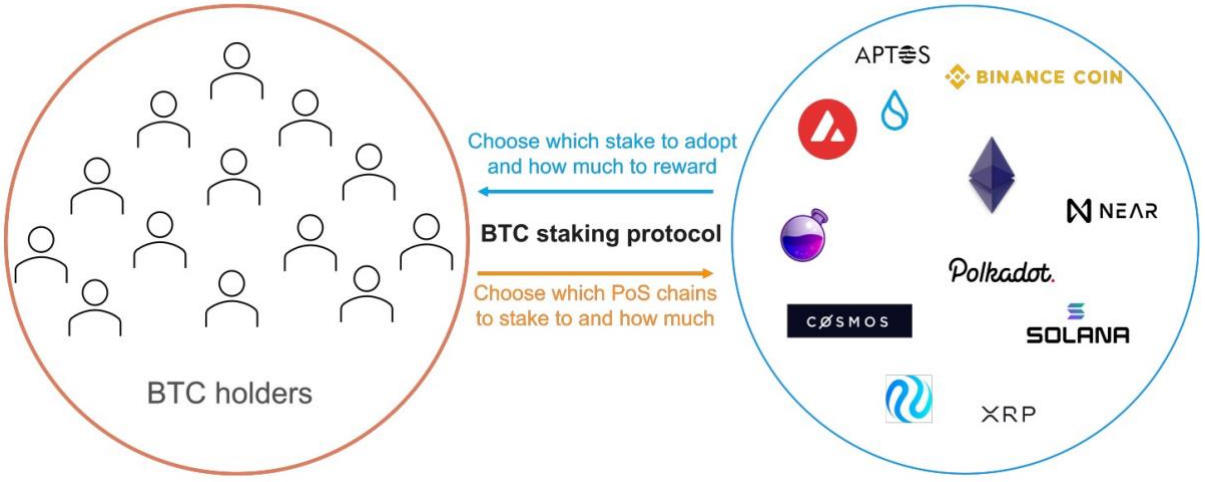
바빌론 노드 모듈은 블록체인을 에포크(Epoch) 단위로 나누어 검증자 세트의 변경을 지연시킴으로써 체크포인트(Checkpoint) 비용을 절감하고, 비트코인 헤더(Header)를 수신하여 유지하는 기능을 합니다. 이를 통해 BTC 체크포인트를 검증하고 블록의 BLS 서명을 수집하여 비트코인 체크포인트에 포함시키며, IBC 라이트 클라이언트를 통해 Consumer Zone 헤더를 추출하여 비트코인 확인 상태를 유지하고 전달합니다. 또한, BTC 스테이킹 요 청을 검증하고 활성화하며 Finality Provider 의 투표를 통해 블록을 Finalize 합니다. 이 과 정에서 발생하는 보상은 비트코인 스테이커와 Vigilante 에게 분배됩니다.

Vigilante 프로그램은 바빌론과 비트코인 간의 데이터를 중계하는 역할을 합니다. 바빌론 체크포인트를 비트코인에 제출하고, 비트코인 원장을 스캔하여 체크포인트를 보고하며, BTC 라이트 클라이언트와 비트코인 체인의 일관성을 모니터링합니다. 또한, 스테이킹 언본딩(Unbonding) 및 슬래싱 거래를 모니터링하여 시스템의 안정성을 유지합니다.

BTC 스테이킹 프로그램은 비트코인 스테이커와 Finality Provider 의 기능을 지원합니다. 비트코인 소유자는 스테이킹 거래를 생성하여 바빌론에 알리고, Finality Provider 는 EOTS(Extractable One-time Signature) 서명 커밋과 블록에 대한 Finality 투표를 수행 합니다. 이를 통해 블록의 Finality 을 확보하고 네트워크의 안전성을 강화합니다.

Consumer Zone 은 바빌론 사용자가 상호작용하는 주요 인터페이스입니다. IBC Relayer 는 바빌론과 Consumer Zone 간의 IBC 프로토콜 연결을 유지하며, Babylon Contract 는 CosmWasm 컨트랙트가 Consumer Zone 에 배포되어 비트코인 체크포인팅 기능을 제공 합니다.

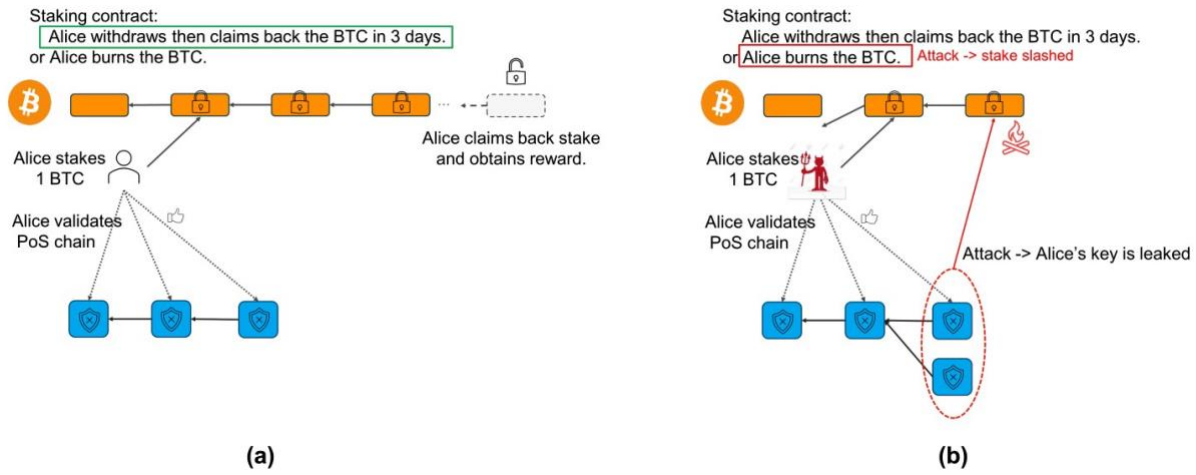
BITCOIN STAKING



Source : Babylon Bitcoin Staking Whitepaper

바빌론 비트코인 스테이킹 프로토콜은 비트코인 소유자가 제 3 자 커스터디(Custody), 브릿지(Bridge), 래핑(Wrapping) 없이 PoS 블록체인에 비트코인을 스테이킹할 수 있도록 설계되었습니다. 이 프로토콜은 PoS 체인에 슬래시 가능한 경제적 보안 보증을 제공하며, 비트코인 소유자의 유동성을 높이기 위해 효율적인 스테이크 언본딩을 보장합니다. 또한, 모듈 형 플러그인으로 다양한 PoS 합의 프로토콜과 호환되며, 리스테이킹(Restaking) 프로토콜을 구축하기 위한 기초 구성 요소로 작동합니다.

바빌론 비트코인 스테이킹 프로토콜은 보안을 위해 다음과 같은 특징을 가집니다. 첫째, 완전 슬래시 가능한 PoS 보안을 제공하여 안전 위반 발생 시 비트코인 스테이크의 1/3 이 슬래시됩니다. 둘째, 스테이커 보안을 통해 스테이커가 프로토콜을 정직하게 따르는 한 스테이킹된 비트코인은 안전하게 인출 가능합니다. 마지막으로, 스테이커 유동성을 보장하여 사회적 합의 없이도 스테이킹된 비트코인의 언본딩이 신속하고 안전하게 이루어집니다. 비트코인 스테이커의 관점에서 비트코인 스테이킹 프로토콜은 다음과 같이 작동합니다.



Source : Babylon Bitcoin Staking Whitepaper

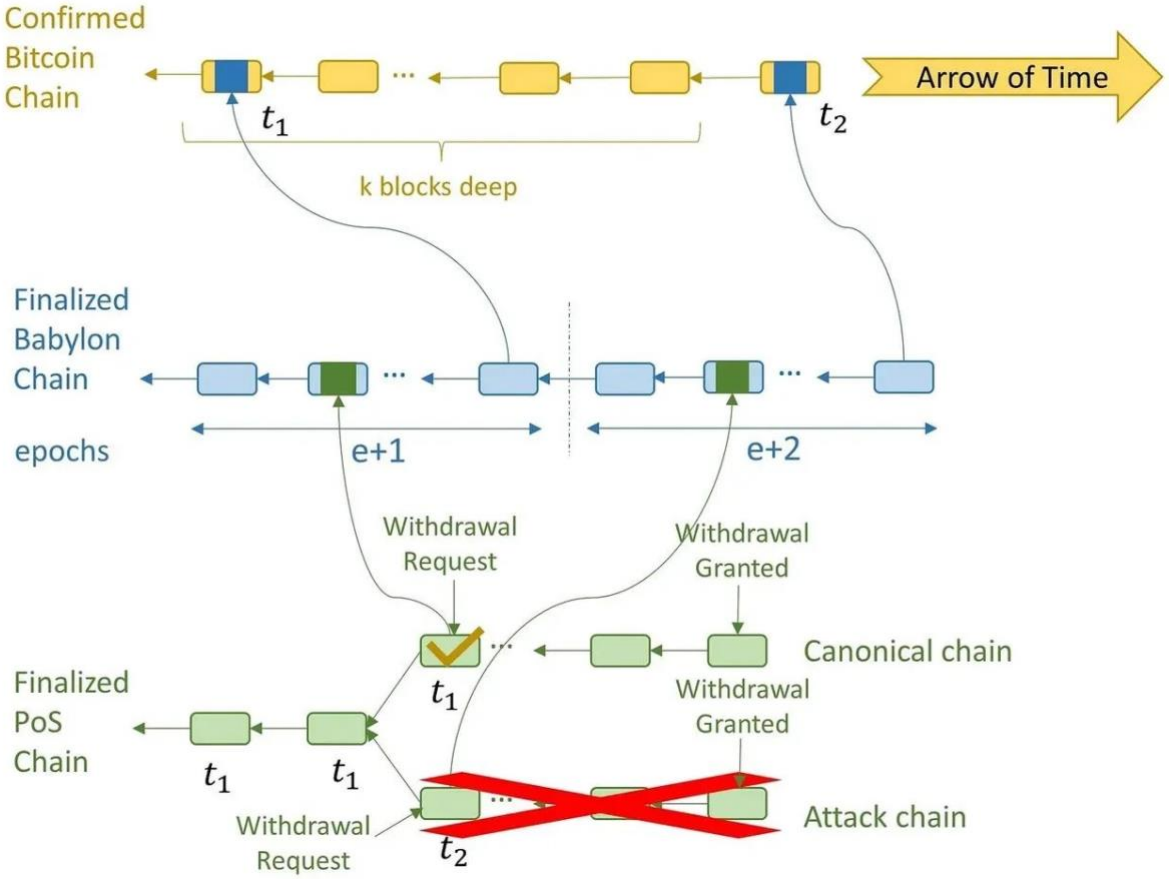
먼저 스테이커는 비트코인 체인에 스테이킹 거래를 보내 비트코인을 셀프 커스터디 볼트에 잠급니다. 이 과정에서 스테이커는 개인 키를 사용하여 인출할 수 있는 타임락과 EOTS 를 통해 UTXO 를 생성합니다. 만약 스테이커가 위임을 선택한 경우, EOTS 는 위임된 검증자의 것입니다. 비트코인 체인에서 스테이킹 거래가 확인되면, 스테이커 또는 위임된 검증자는 PoS 체인을 검증하고 EOTS 개인 키를 사용하여 유효한 블록에 서명할 수 있습니다.

정상 경로에서는 스테이커가 프로토콜을 정직하게 따르고 수익을 얻습니다. 그런 다음 타임락이 만료되기를 기다리거나 비트코인에 언본딩 거래를 제출하여 비트코인을 언본딩할 수 있습니다. 스테이커가 악의적인 행동을 하는 비정상 경로(b)에서는 스테이커의 EOTS 개인 키가 공개됩니다. 그 결과 누구나 스테이커를 대신하여 비트코인 체인에 슬래싱 거래를 제출 하고 비트코인을 소각할 수 있습니다.

비트코인 스테이킹 프로토콜은 안전 위반에 대응하기 위한 슬래싱 메커니즘을 도입합니다. 이 메커니즘은 안전 위반이 발생할 때 스테이커의 개인 키가 노출되도록 하는 것을 중심으로 합니다. 이를 위해 암호학에서의 책임 있는 주장(Accountable assertions from cryptography)과 블록체인 합의에서의 Finality Gadget 라는 두 가지 개념을 결합합니다. 동일한 개인 키를 사용하여 동일한 높이에서 다른 블록에 서명하면 개인 키가 노출되며, 블 록이 2/3 이상의 비트코인 스테이크의 EOTS 서명을 받으면 Finalize 된 것으로 간주됩니다.

이 모듈식 접근 방식은 기본 프로토콜을 변경하지 않고 다양한 BFT 합의 프로토콜에 적용할 수 있어, 다양한 PoS 블록체인과 호환됩니다. 바빌론 비트코인 스테이킹 프로토콜은 비트코인을 스테이킹하여 PoS 체인의 보안을 강화하고, 비트코인 소유자가 수익을 창출할 수 있는 새로운 기회를 제공합니다. 이 프로토콜은 비트코인 체인과 PoS 체인 간의 원활한 통합을 가능하게 하며, 전체 시스템의 신뢰성과 유동성을 높입니다.

BITCOIN TIMESTAMP



Source : Why babylon chain is the next big thing in Shared security narrative

Babylon 은 주기적으로 PoS 체인들이 비트코인에 체크포인트를 기록할 수 있게 하여 Long-range Attack 과 같은 Safety Attack 에 대해 보호할 수 있도록 합니다. 비트코인 타임스탬핑의 프로세스는 요약하자면 다음과 같이 이루어집니다.

1. Babylon 의 밸리데이터들은 PoS 체인의 해시값과 서명을 Babylon 체인의 블록에 담습니다.
2. Babylon 체인의 한 에포크마다 마지막 블록의 해시에 서명하고 이 해시를 OP_RETURN 의 형태로 비트코인에 기록합니다.

따라서 PoS 체인에 대한 악의적인 공격으로 인하여 포크가 발생하였을 때 PoS 체인은 체크포인트를 바탕으로 손쉽게 Canonical 체인을 찾을 수 있습니다. Canonical 체인의 판단 기준은 포크 시점 이후로부터 더 빠른 블록에 체크포인트가 찍힌 체인인지에 따라서 결정됩니다. 즉, 가장 빠른 체크포인트가 찍힌 체인이 Canonical 체인이 됩니다. 이는 언본딩 기간을 크게 줄여주어 PoS 체인 유저들의 사용자 경험을 향상시켜줍니다.

MARKET ANALYSIS

Babylon 은 아직 메인넷 런칭 전이며, Testnet-4 를 진행 중이기 때문에 실질적으로 얼마나 많은 BTC 가 스테이킹 될 지 알 수는 없습니다. 다만, 여러가지 지표들을 통해 커뮤니티에 대한 관심을 확인 할 수 있습니다. Testnet-4 에는 현재까지 34 만명이 참여하였고, 총 700 Signet BTC 가 예치되었습니다.

Babylon 의 트위터 구독자 수는 50 만명으로 어떤 비트코인 생태계 프로젝트보다 압도적으로 높은 수치입니다. 비트코인의 사이드 체인으로 상당히 오랜기간 개발되어온 Stacks 의 경우에도 팔로워 수는 20 만명에 불과합니다.

또한 Solv Network, pSTAKE 등 Babylon 을 기반으로 한 LST(Liquid Staking Token) 플랫폼도 빠르게 개발되어 함께 주목을 받고 있습니다. 현재 Babylon 네트워크를 사용하겠다고 파트너십을 맺은 PoS 체인은 88 개이며 빠르게 늘어나고 있습니다.

LIMITATIONS

위에서 설명했다시피 Babylon 은 EigenLayer 와 유사한 구조를 가지고 있습니다. EigenLayer 의 경우 해당 솔루션에 대한 개발 난이도가 매우 높은 것으로 알려져 있고, 실제 로 현재 슬래싱 매커니즘을 구현하지 않고 메인넷 출시가 이루어져 보안에 대한 논란이 있는 상황입니다. Babylon 의 경우에도 아직 구체적인 스테이킹 컨트랙트, 슬래싱 컨트랙트 등에 대한 코드를 밝히지 않은 상황이기 때문에 개발이 순조롭게 진행되고 있는 지 알 수 없습니다. 만약 EigenLayer 와 같이 슬래싱 컨트랙트 등을 구현하지 않고 메인넷이 출시 될 경우 보안적으로 위협을 받을 수 있는 가능성이 존재합니다.

BITSMILEY

bitSmiley

OVERVIEW

bitSmiley 는 비트코인 네트워크에서 발행되는 첫 탈중앙 비트코인 네이티브 스테이블 코인 (Bitcoin Native Stable coin) 프로젝트로, 2023 년 12 월에 처음 백서를 발표하고 2024 년 5 월에 런칭한 DeFi 서비스입니다. 앞서 언급했듯이 현재 비트코인에 디파이 생태계가 거의 구축되어 있지 않고, 그 이유로는 비트코인의 프로그래머빌리티를 꼽을 수 있습니다. 하지만 2023 년 Inscription 으로 인해 비트코인 상에서도 간단한 기능 구현이 가능해졌고, 이로 인 해 네트워크로 많은 트래픽과 자본이 유입되었습니다. bitSmiley 는 비트코인에서의 Inscription(인스크립션) 기능을 활용하는 DeFi 서비스로, 비트코인에 묶여있는 자본의 새로운 사용사례가 된다는 점에서 의의를 가집니다. 어느 정도까지의 DeFi 기능 구현이 가능하냐에 대한 문제를 차치하고도 bitSmiley 는 출시 하루만에 $25M 의 TVL 을 기록하며 많은 사람들의 관심을 받았습니다. 실제로 비트코인 생태계에 주요 프로젝트에 집중적으로 투자를 하고 있는 VC 인 ABCDE Capital 과 OKX Ventures 외 6 곳이 토큰 투자를 진행했습니 다.

bitSmiley 는 비트코인 생태계의 디앱이기 때문에 인프라에 의존합니다. 따라서 현재 여러 비트코인 레이어 2 프로젝트와 파트너십을 체결하여 스테이블 코인 및 DeFi 생태계 상품을 공급하기 위해 노력하고 있습니다. 반대로 비트코인 생태계의 레이어 2 인프라 프로젝트도 BTC 의 사용성을 제고할 수 있는 보다 포괄적인 디파이 인프라가 필요하기 때문에 bitSmiley 와 스폰서십은 긍정적인 영향을 줍니다. 일례로, bitSmiley 는 Lolenzo 나 ENZOFinance 와 파트너십을 체결하였으며, Merlin 과 Bitlayer 에서 어플리케이션을 사용 할 수 있도록 합니다.

이 외에 bitSmiley 는 커뮤니티의 활성도를 높이기 위해 NFT 발행하기도 했는데, bitDisc 와 bitDisc-Black NFT series 를 발행해 많은 사람들을 bitSmiley 커뮤니티로 편입하려는 노력을 했습니다. bitDisc 는 비트코인 OG 와 업계 리더에게만 에어드랍 하는 NFT 로 100 개 한정으로 발행되었으며, bitDisc-Black NFT series 는 일반 사용자, 초기 지지자, 기여자 등에게 에어드랍 하는 NFT 로 10,000 개 한정으로 발행되었습니다. 해당 NFT 를 소유한 사람들은 bitSmiley 의 모든 제품에 우선권 부여하며, Private Bitcoin OG Club 에 초대됩니다.

TECHNICAL FEATURES

bitSmiley 는 MakerDAO 와 Compound 의 비트코인 버전이라는 생각이 들 만큼 유사한 부분이 많은데, 크게는 bitLending, bitUSD(stable coin), bitInsurance(Derivatives)으로 분류되는 3 가지의 서비스를 제공합니다. 런칭한 지 얼마 되지 않은 프로젝트이며, Stable coin 이 주요

서비스이기 때문에 bitLending 과 bitInsurance 에 대한 자세한 정보는 많지 않아, 관련 정보는 현재(2024.07.28)까지 나온 자료들을 바탕으로 했음을 언급합니다.

BITUSD

bitUSD 는 비트코인에서 발행되는 최초의 탈중앙 스테이블 코인으로, USD 와 1 대 1 페깅이 되어있습니다. bitUSD 가 발행되는 과정은 이더리움의 DeFi 서비스인 MakerDAO 와 비슷한 구조를 지니고 있는데 BTC 를 담보로 입금하면 그에 상응하는 bitUSD 를 발행받습니다.
실물자산이 아닌 변동성이 높은 토큰을 담보로 하기 때문에 과담보 메커니즘을 이용하여 안정성을 높이고 있으며, 주목할 점은 기존에 비트코인 네트워크에서 사용하던 BRC-20 규격 의 토큰이 아닌 bitRC-20 이라는 새로운 토큰 규격을 만들어서 사용한다는 점입니다.

```
{
    "p": "bitRC-20",
    "tick": "bitUSD",
    "op": "deploy",
    "init": "21000000",  // the initial token amount
    "dec": 18,
    "v": 1,              // the version number
    "scripts": {
        "mint": "hash256 or empty",
        "burn": "hash256 or empty",
        "transfer": "hash256 or empty"
    }
}
```

Source - bitSmiley white paper

위에 보이는 것이 bitRC-20 이라는 새로운 토큰의 규격으로, 기존의 BRC-20 은 발행과 소각 등 일부 행위가 자유롭지 않아 BRC-20 과 호환되는 새로운 토큰 규격을 통해 스테이블 코인의 발행 및 소각 요구를 충족하기 위한 Mint 와 Burn 작업을 추가했습니다. 즉, bitRC- 20 은 Deploy, Upgrade, Mint, Burn, Transfer 의 작업을 허용하는 BRC-20 의 업그레이 드 버전이라고 볼 수 있습니다.

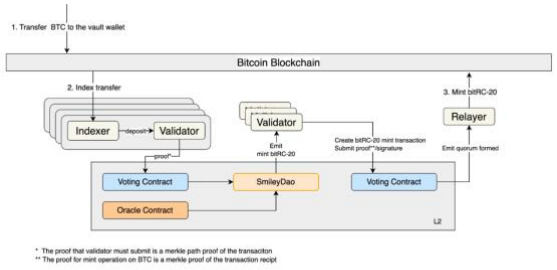


Figure1:Mint bitUSD flow

Source - bitSmiley white paper

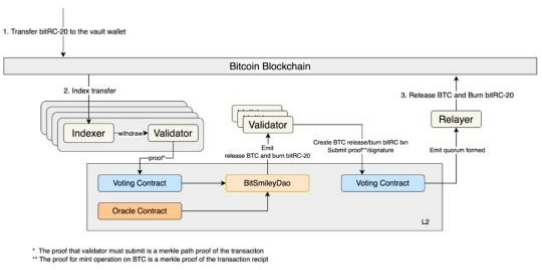


Figure2:Withdraw bitUSD flow

Source - bitSmiley white paper

bitUSD 가 민팅되고 출금되는 내역은 보이는 다이어그램과 같습니다. 일반적인 스테이블 코인 프로젝트와 비슷한 구조를 가지고 있습니다. 오라클을 이용해 입금 및 출금 사실을 전달받고 bitSmileyDAO 에 의해 Mint 나 Burn 메시지가 각 체인에 전송되는 구조입니다. Mint 와 Withdraw 의 각 과정을 조금 더 상세하게 보면 다음과 같습니다.

먼저 Mint 는 아래와 같은 순서로 실행됩니다:

1. 메인넷에 있는 'bitSmiley Treasury' 스마트 컨트랙트에 사용자 가 담보인 BTC 를 입금합니다.
2. BTC 가 입금된 사실을 인덱서에 기록되면, 오라클이 해당 사실을 SmileyDao 로 전달합니다.
3. SmileyDao 와 밸리데이터에 의해 bitRC-20 mint 트랜잭션이 생성됩니다.
4. 릴레이어(Relayer)를 통해 해당 트랜잭션이 비트코인(메인넷)에 제출되면 비트코인에서 담보에 상응하는 bitUSD 를 민팅합니다.

Burn 은 아래와 같은 순서로 실행됩니다:

1. 비트코인에 사용자가 bitUSD 를 입금합니다.
2. bitUSD 가 입금된 사실을 인덱서에 기록되면, 오라클이 해당 사실을 SmileyDao 로 전달합니다.
3. SmileyDao 와 밸리데이터에 의해 bitRC-20 Burn/Release 트랜잭션이 생성됩니다.
4. 릴레이어를 통해 해당 트랜잭션이 비트코인(메인넷)에 제출되면 제출된 bitUSD 를 소각하고, 상응하는 BTC 를 인출합니다.

bitSmiley 에서는 담보로 제출한 BTC 의 가격이 하락하면, Dutch Auction 방식을 이용해 청산 메커니즘이 실행되게 구현되어 있습니다. 먼저, CDR(Collateral to Debt Ratio)이 특정 임계점(Threshold) 밑으로 떨어지면 Liquidation Process 가 호출됩니다. 청산과정에서 MakerDAO 와 비슷하게 Dutch Auction 방식을 차용하지만, 특이한 점이 있다면 Liquidator 라는 주체가 개입한다는 점입니다. 청산당한 BTC 는 bitSmiley 와 Liquidator 가 특정 비율로 분배받게 되는데, 해당 비율은 청산 과정의 길이에 따라 정해집니다. 청산 과정이 길어질수록 Liquidator 가 더 많은 BTC 를 분배받게 됩니다. 청산 과정에서 발생하는 Dutch Auction 에서 초기 가격은 시스템의 Price Buffer Coefficient 파라미터에 의해 자동으로 설정됩니다.이후, Price Function 에 의해 시간이 지날 수록 자동적으로 가격이 하락하며, 큰 하락폭을 방지하기 위해 Maximum Auction Price Drawdown 에 의해 하락폭에 대한 제한을 둡니다. 또한, 경매가 일정 시간에 끝날 수 있도록 Maximum Auction Period 에 의해 경매 진행 시간에 제한을 둡니다.

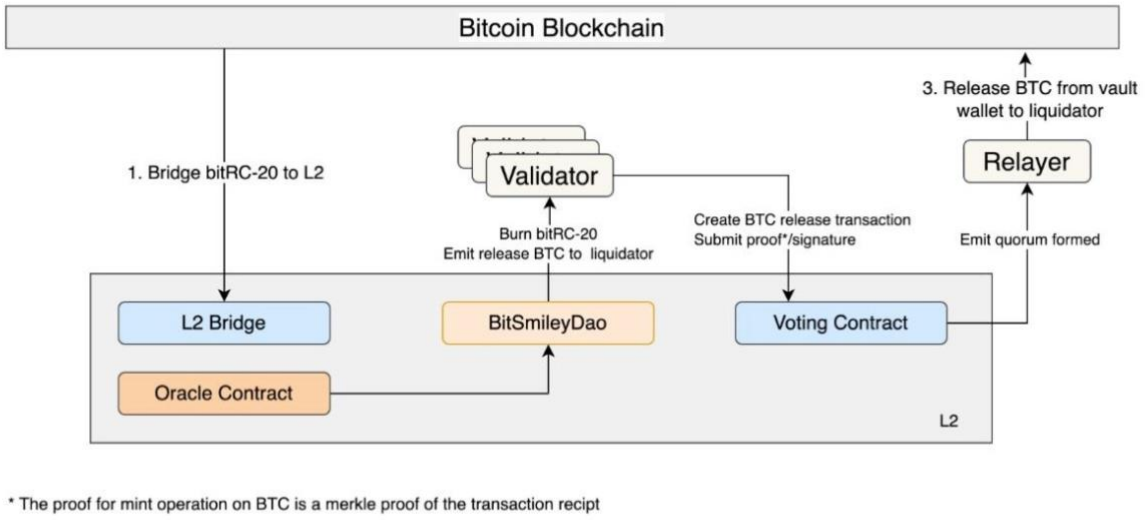


Figure3:Liquidate bitUSD flow

Source - bitSmiley white paper

청산은 아래와 같은 순서로 실행됩니다:

1. CDR 이 특정 임계점 이하로 떨어진 컨트랙트를 식별하여 L2 Bridge 에서 읽어옵니다.
2. 오라클이 해당 사실을 BitSmileyDao 에 전달합니다.
3. SmileyDao 와 밸리데이터에 의해 bitRC-20 Burn/Release BTC 트랜잭션이 생성됩니다.
4. 릴레이어를 통해 해당 트랜잭션이 비트코인(메인넷)에 제출하여 청산 절차를 진행하고, 분배 비율에 따라 청산된 BTC 중 일부를 Liquidator 에게 전달합니다.

DERIVATIVES - BITINSURANCE

타체인에 비해 상대적으로 긴 블록 시간(10-15 분)을 가지고 있는 비트코인은 타대출 프로젝트처럼 오라클을 기반으로 빠른 정산을 할 수 없습니다. 하지만, 변동성이 매우 빠른 토큰의 특성과 빠르게 대처하는 속도가 생명인 금융 시장에서 이는 사용자가 해당 상품을 사용할 수 없게 하는 큰 요인이 됩니다. 따라서 bitSmiley 는 관련된 파생상품 서비스를 출시했으며, 현 재 첫 번째 서비스는 대출 보험인 bitInsurance 입니다. Borrower 의 담보 자산 가격이 크게 하락하면 Borrower 가 대출 상환 거부할 가능성이 높아집니다. 이때, Borrower 에게 자산을 빌려준 Lender 는 손실이 발생하게 됩니다. 이러한 문제를 해결하기 위해 대출 보험인 bitInsurance 이 도입됐습니다.

Borrower 와 Lender 의 보험료는 2 가지 이론—Extreme Value Theory, T-Copula—에 의해 다르게 형성되며, 멀티시그 지갑을 사용하여 대출이 상환되는 시점 혹은 보험금을 지불할 때까지 lock 되게 됩니다. 피해보상을 해주는 보증인은 멀티시그 주소(multisig address)로 보험료를 수령하고 대출자의 손실에 대한 보증을 해줍니다. 즉, Borrower 가 채무 불이행을 하면 멀티시그 주소에 있는 자금은 Lender 에게 보상금으로 주어지며 Lender 의 이익을 보호합니다.

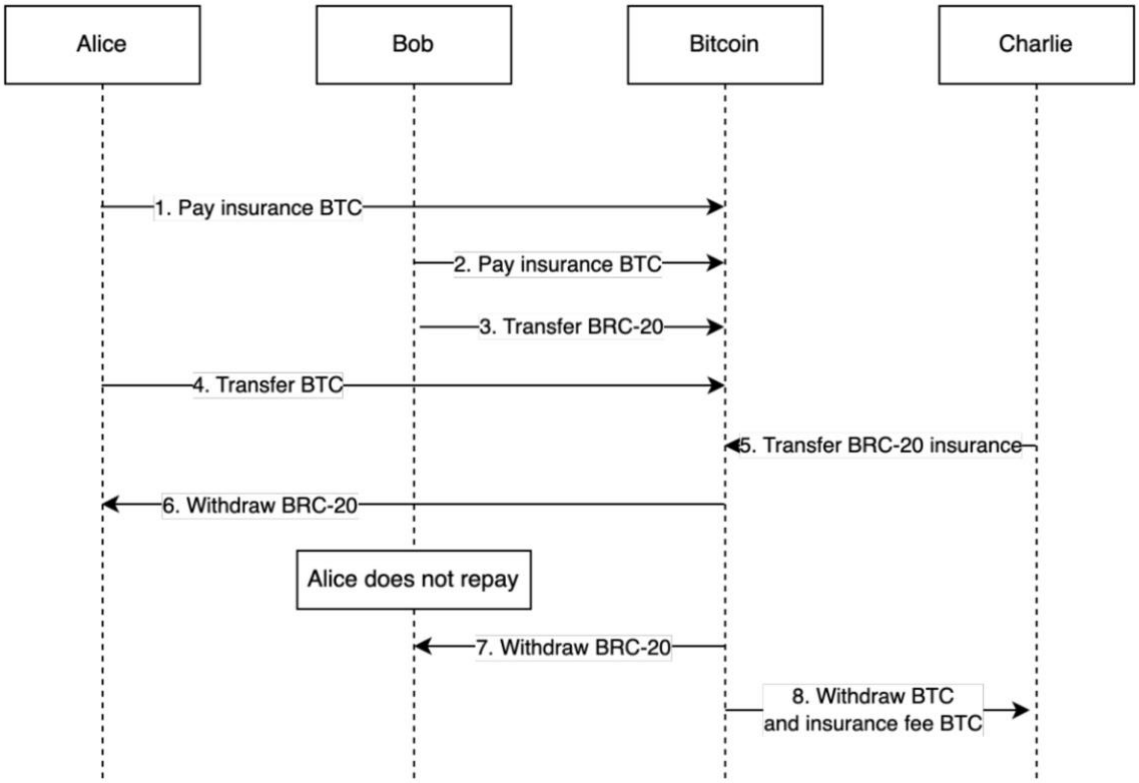


Figure5:bitInsurance flow

Source - bitSmiley white paper

보험이 이뤄지는 과정은 다음과 같습니다:

1. Borrower 인 Alice 는 담보를 송금하기 전에 멀티시그 주소로 보험료를 BTC 로 송금합니다.
2. Lender 인 Bob 은 대출금을 송금하기 전에 멀티시그 주소로 보험료를 BTC 로 송금합니다.
3. Bob 이 Alice 에게 빌려줄 BRC-20 토큰을 멀티시그 주소로 전송합니다.
4. Alice 가 Bob 에게 담보로 맡길 BTC 를 멀티시그 주소로 전송합니다.
5. 보증자 Charlie 가 Bob 이 빌려준 BRC-20 토큰에 대해 보험료로 줄 양을 멀티시그 주소로 전송합니다.
6. Alice 는 BRC-20 토큰을 출금합니다. (BTC 가격이 급격하게 하락해 Alice 가 상환을 안하는 상황을 가정합니다.)
7. Bob 은 보험을 클레임(Claim)하고 멀티시그 지갑으로부터 Charlie 에게 BRC-20 토큰을 상환받습니다.
8. 보증인 Charlie 는 Alice 가 전송한 BTC 와 Alice 와 Bob 이 지불한 보험금 BTC 를 출금합니다.

LENDING

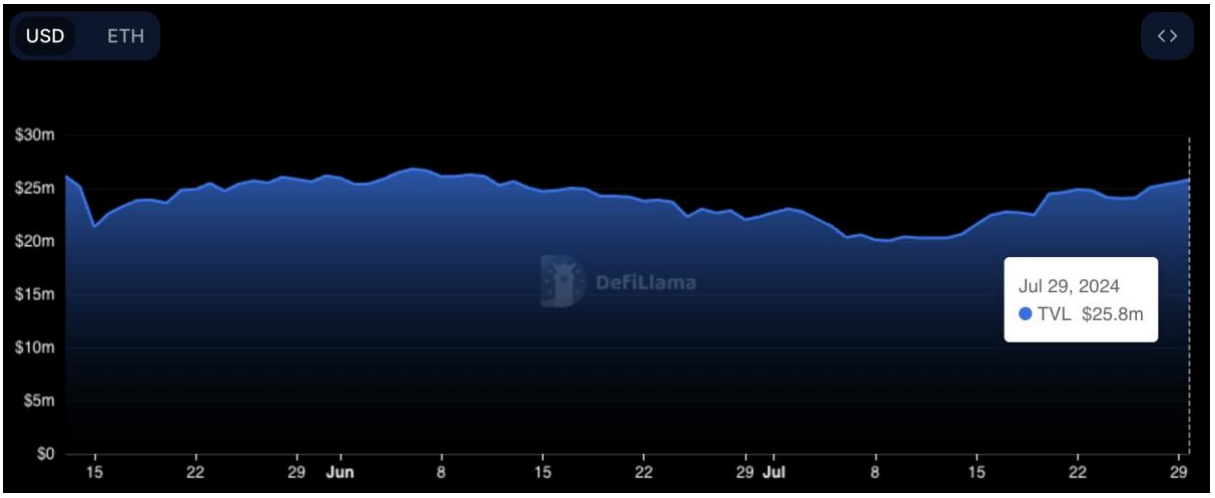
저희가 흔히 생각하는 랜딩과 유사합니다. BTC 를 담보로 bitUSD 를 빌리는 서비스로 Compound 와 비슷하지만 비트코인의 체인 특성상 매칭과정은 P2P 오프라인으로 진행이 된다는 점에서 차이를 가집니다. 즉, P2P lending 서비스로 BTC 를 담보로 bitRC-20 토큰 (bitUSD)을 빌려주고, 빌릴 수 있습니다. 비트코인 자체에서 구현할 수 있는 기술의 한계로 매칭 과정은 P2P

loan matching 매커니즘을 사용하지만, 멀티시그 지갑과 비트코인의 기존 Opcode 를 이용해 자금 이동 과정 자체는 탈중앙화하여 온체인에서 이뤄지게 합니다.

대출 과정은 아래와 같습니다:

1. 제공자는 대출 제안을 게시하여 제공하는 bitRC-20 토큰의 종류와 금액, 대출 조건, 이자율을 명시합니다.
2. 대출자는 원하는 대출 제안을 수락합니다.
3. 매칭이 되면, 자금 전송을 위한 멀티시그 주소가 생성됩니다.
4. 해당 주소로 두 명 모두 자금 전송 후 온체인에서의 Confirmation 기다립니다.
5. Confirmation 이 되면, 대출자와 제공자는 각각 자금을 출금할 수 있으며, 해당 과정은 Atomic Swap 으로 이루어집니다. 이때, 제공자는 빌려준 금액에 대한 이자를 받게 됩니다.
6. 제공자가 제공한 bitRC-20 토큰이 반환되면 대출받은 사람도 담보로 걸어둔 BTC 를 반환할 수 있습니다.

MARKET ANALYSIS



Source : DeFiLlama

bitSmiley 는 비트코인을 기반으로 하는 첫 네이티브 스테이블 코인이라는 점에서 굉장히 많은 관심을 받았습니다. 특히, 현재 비트코인 레이어 2 가 주목받고 있고 많은 돈이 몰리고 있기 때문에 시기상으로도 적합할 때 런칭되었습니다. 이러한 상황에서 bitSmiley 는 비트코인을 활용한 DeFi 를 더 유용하게 해줄 수 있는 가능성이 높습니다.

bitSmiley 의 TVL 을 확인해보면 런칭한지 24 시간 만에 $25M 의 TVL 을 달성했고, 현재는 $25.8M 의 TVL 을 가지고 있습니다. 또한, Market Cap 은 $8.91M 입니다. 수치를 보면 에어드랍을 향한 기대감으로 인해 TVL 이 유지된 것으로 볼 수도 있으나 첫 런칭 이후 급격한 하락이나 상승없이 꾸준히 TVL 이 유지되는 것으로 보아 비트코인 DeFi 시장에 대해 사용자들이 많은 관심을 보이며 사용성에 대해 지켜보고 있는 것으로 보입니다.

다수의 비트코인 레이어 2 와 지속적으로 파트너십을 진행하고 있기 때문에, 얼마나 많은 시장성을 보여줄지에 대한 부분은 추후 진행되는 파트너십을 통해 검토해볼 필요가 있습니다.

LIMITATIONS

bitSmiley 로 인해 비트코인의 활용성이 증가해 생태계가 확장될 수 있습니다. 특히 스테이블 코인으로 인해 다양한 DeFi 서비스를 이용할 수 있습니다. 하지만, DeFi 의 특성상 인프라 없이는 존재할 수 없기에 비트코인 레이어 2 들과의 협업이 필수적입니다. 이에 따라, bitSmiley 의 사용성은 레이어 2 에 일부분 의존할 수 밖에 없게 되기 때문에 이 부분에서 한계를 가집니다. 현재 많은 비트코인 레이어 2 이 출시되고 있지만, 완벽하게 구현된 프로젝트가 없기 때문에 DeFi 에 대해서도 확언할 수 없습니다.

이와 별개로, 비트코인 자체적으로 가지는 한계에 영향을 받기도 합니다. 비트코인은 디앱을 위해 나온 체인이 아니기 때문에 자체적으로 다양한 기능을 실현할 수 없고, 이는 bitSmiley 와 같은 DeFi 어플리케이션의 한계로 이어집니다. 특히, 현재는 스테이블 코인 발행과 같은 간단한 기능을 가능한 서비스를 제공하고 있지만 DEX(Decentralized Exchange)와 같은 DeFi 서비스는 초 단위로 트랜잭션 처리가 필요하며, 복잡한 코드 로직을 요구하기 때문에 이러한 부분에 있어 bitSmiley 가 얼마나 더 발전할 수 있을 지에 대해서는 회의적입니다. 이 부분도 앞서 말씀드린 레이어 2 구현 여부가 상당히 큰 영향을 미칠 것으로 보입니다.

BTC INTEROPERABILITY

ZEUS NETWORK

Zeus Network

OVERVIEW

Zeus Network 는 2023 년 설립된 비트코인과 솔라나 사이의 상호 운용 가능한 커뮤니케이션 레이어를 표방하는 프로젝트입니다. Zeus Network 는 SVM(Solana Virtual Machine)을 기반으로 개발되었으며, Zeus 레이어라는 자체 레이어를 사용하여 서로 다른 체인을 연결하는 것을 목표로 합니다. 쉽게 이해하자면 Zeus Network 의 첫번째 목표는 솔라나를 마치 비트코인의 사이드체인처럼 사용하는 것이라고 볼 수 있습니다.

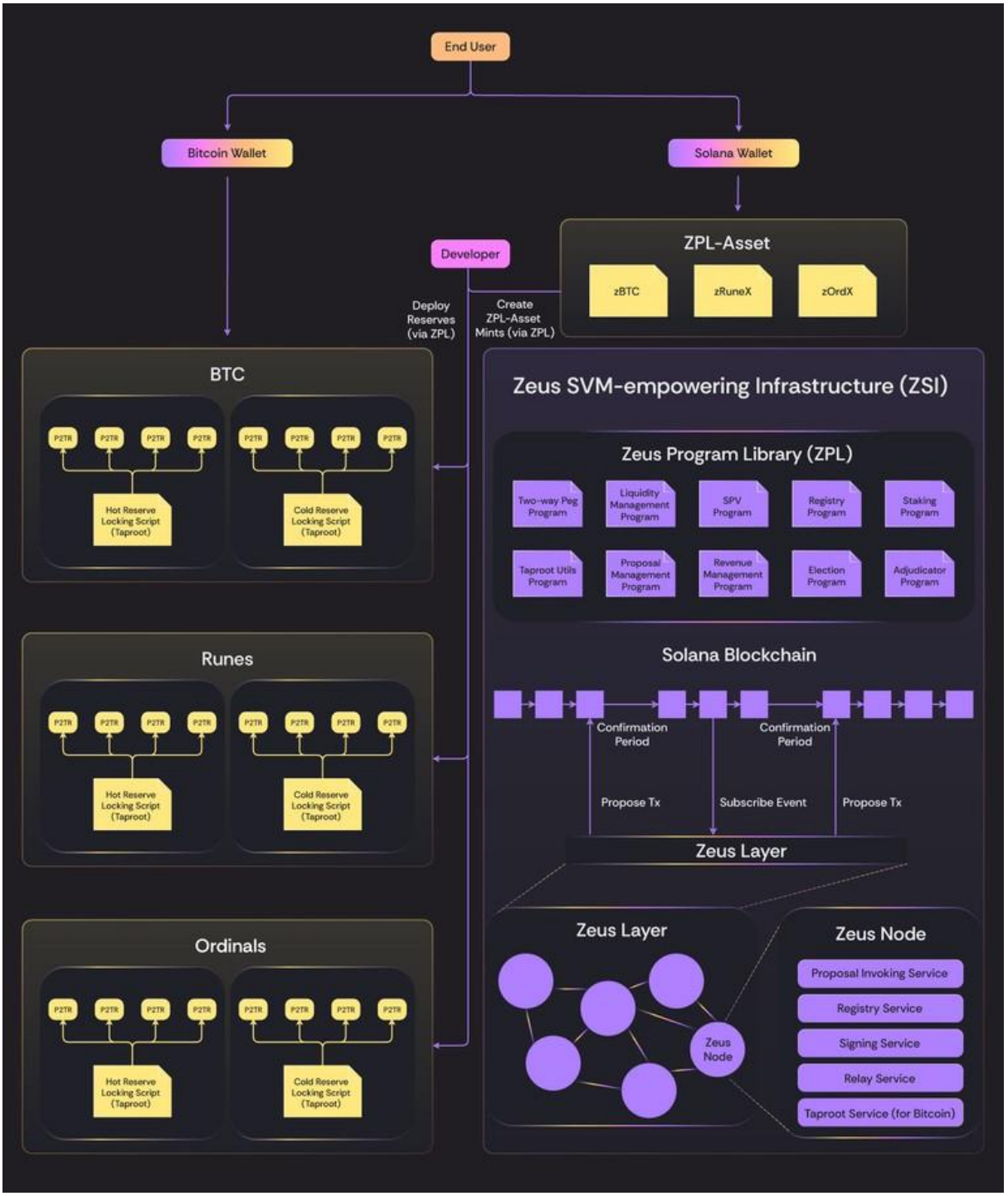
Zeus Network 는 2024 년 Solana 의 Co-founder 인 Anatoly Yakovenko, Mechanism Capital 의 Founder 인 Andrew Kang, Stacks 의 Co-founder 인 Muneeb Ali 에게 엔젤 투자를 유치하였으며, 이후 진행된 시드 라운드에서 Mechanism Capital 과 OKX Ventures 의 주도로 $8M 의 투자를 추가 유치하였습니다.

처음 등장했을 때부터 Zeus Network 는 많은 솔라나 커뮤니티의 지지를 갖고 있었는데, 그 이유는 Zeus Network 가 Jupiter 에서 진행하는 Jupiter LFG 런치패드의 첫번째 프로젝트로 뽑혀 LFG 런치패드를 통해 IDO(Initial DEX Offering)를 진행했기 때문입니다.

Zeus 의 첫번째 디앱인 Apollo 는 최근 Muses 업데이트를 통해 테스트넷에 출시되었으며, 2024 년 4 분기 이내로 메인넷 출시를 목표로 하고 있습니다.

TECHNICAL FEATURES

ZEUS PROGRAM LIBRARY

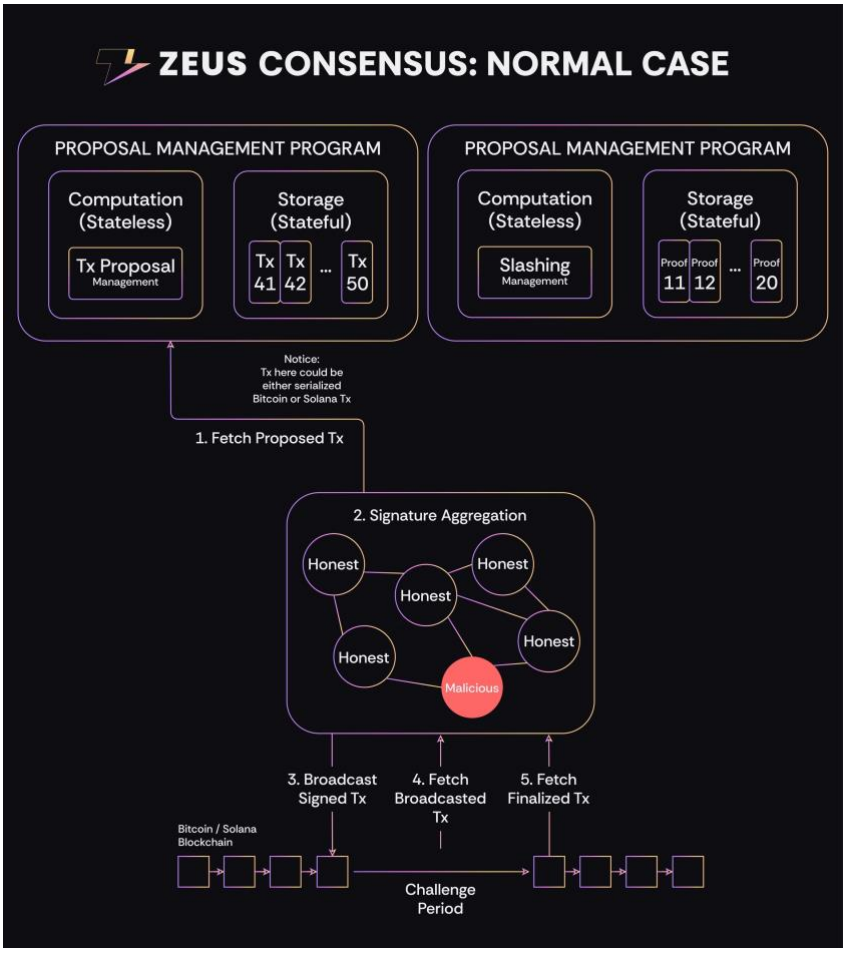


Source : Zeus Docs

Zeus Program Library 는 SVM 위에 구축된 프레임워크로, 블록체인 애플리케이션의 상호운용성과 프로그래머빌리티를 향상시키기 위해 설계되었습니다. Plug-and-play 특성을 지닌 ZPL 은 다양한 블록체인 간의 상호운용성을 제공하고, 개발자들에게 검증 가능한 인터페이스를 제공합니다. 또한 ZPL 은 SVM 의 트랜잭션 병렬처리를 이용한 빠른 트랜잭션을 제공합니다. ZPL 의 주요 목표는 ZPL-Asset 을 통해 다양한 네트워크 간의 통신 및 가치 전송 을 촉진하는 것입니다.

ZPL-Asset 은 Zeus 네트워크에 의해 인증된 맞춤형 및 검증 가능한 자산으로, 솔라나 생태계의 유연성과 상호운용성을 강화합니다. 비트코인 자산을 ZPL-Asset 으로 변환하여 사용자들이 비트코인과 솔라나 네트워크의 이점을 동시에 활용할 수 있도록 합니다. 주요 ZPL- Asset 으로는 zBTC, zRuneX, zOrdX 가 있습니다.

ZEUS NETWORK



Source : Zeus Network Docs

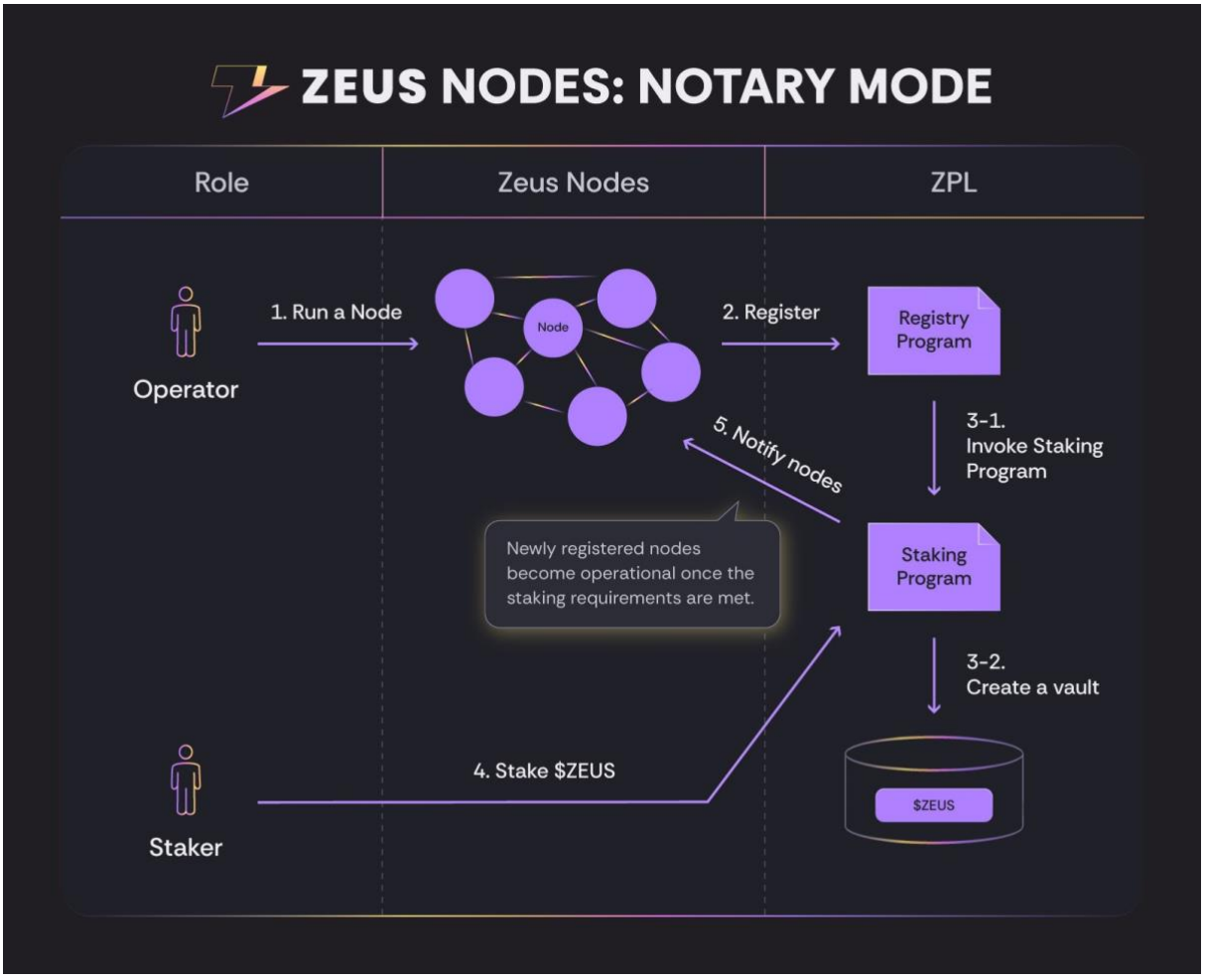
Zeus Network 는 다음과 같은 순서로 작동합니다:

1. 체인에 구애받지 않는(Chain Agnostic) 트랜잭션은 솔라나에 제안되고 저장됩니다. 비트코인과 솔라나 트랜잭션은 먼저 Zeus 노드에 의해 제안된 후 Zeus 프로그램 상태에 제출됩니다.
2. 서명은 Zeus 레이어에서 서명되고 집계됩니다. Zeus 레이어는 Zeus 프로그램 라이브러리(ZPL)를 통해 프로그래머블 서명을 제공합니다.
3. 서명된 트랜잭션을 목표 블록체인에 브로드캐스트합니다. Zeus 노드는 서명된 제안된 트랜잭션을 목표 블록체인으로 중계합니다.
4. 사기 증명을 통해 크로스체인 통신을 보안 유지합니다. 특정 Zeus 노드들이 공모할 때, 정직한 노드는 사기 증명을 제출하여 악의적인 노드들을 처벌함으로써 네트워크를 안전하게 유지할 수 있습니다.

직렬화된 비트코인과 솔라나 트랜잭션은 체계적으로 저장되며, 검증자는 솔라나 블록체인에서 이러한 제안된 트랜잭션을 가져옵니다. 이러한 제안된 트랜잭션에 대한 합의 메커니즘은 독특한 과정을 통해 이루어지며, 검증자는 온체인 트랜잭션 제안과 별개로 검증에만 집중합니다. 검증자는

비트코인 탭루트에 슈노르 서명을 사용하는 임계 서명 메커니즘을 구현하며, 이 개념은 솔라나의 Ed25519 서명 알고리즘으로 확장됩니다. 또한 사기 증명을 통한 추가적인 보호 계층이 합의 과정을 강화합니다.

이 네트워크 인프라는 다양한 애플리케이션을 수용하도록 설계되어 있으며, 특히 브릿지와 유사한 맥락에서 그 잠재적 적용 가능성을 잘 보여줍니다. 정상적인 경우, Zeus 합의는 트랜잭션 제안, 서명 집계, 트랜잭션 브로드캐스트, 사기 증거 및 도전 기간(Challenge Period)으로 운영됩니다. Zeus 노드는 Chain-agnostic 트랜잭션을 제안하고 솔라나 블록체인에 저장하며, Zeus 레이어는 ZPL 을 사용하여 서명을 집계하고, 서명된 트랜잭션을 Zeus 노드가 대상 블록체인에 브로드캐스트합니다. Zeus 노드 간의 공모가 발생할 경우, 정직한 노드는 사기 증거를 제출하여 악의적인 노드를 퇴출함으로써 네트워크의 보안과 무결성을 보장 합니다.



Source : Zeus Network Docs

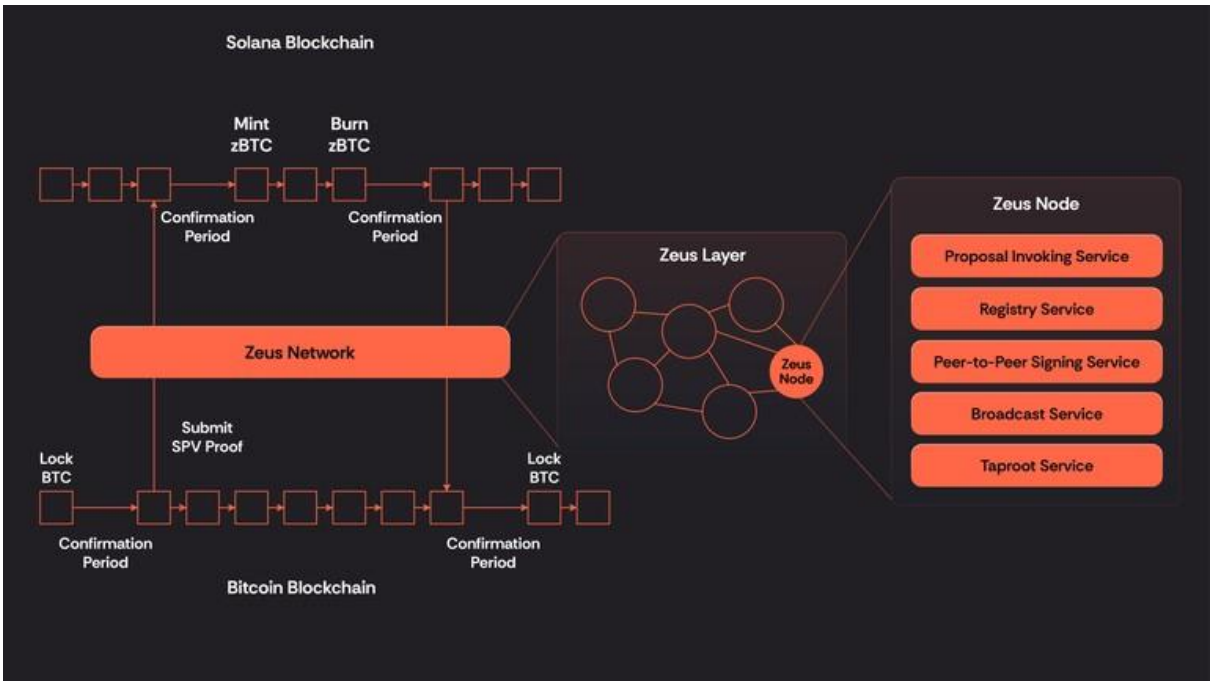
Zeus 네트워크는 분산되고 허가가 필요 없는(Permissionless) 그룹 모델을 기반으로 운영 되는 검증 프로세스를 가지고 있으며, 연합 공증 시스템(Federated Notary System)과는 구별됩니다. 검증자가 되기 위해서는 노드를 운영해야 하며, 이는 개인 키 유지와 서명 기능을 담당합니다. 또한 검증 과정에는 $ZEUS 를 스테이킹하여 PoS 합의와 투웨이 페그 메커니즘에 기여할 수 있도록 해야 합니다. 스테이커들은 Verifier Registry Program 에 등록해야 하며, 보안 프레임워크는 과담보(Over-collateralized) 설계를 기반으로 하고, 잠재적 취약점은 재정적 슬래싱 조치를 통해 해결되어 검증 시스템의 견고성과 탄력성을 강화합니다.

Zeus 노드 시스템은 Peer-to-peer(P2P), 브로드캐스트, 서명(서명 집계 포함) 및 온체인과 오프체인 모두에서 작동하는 레지스트리(Registry) 서비스와 같은 여러 필수 구성 요소로 구성됩니다. 시스템의 확장성을 높이기 위해 잠재적인 수정 사항에는 대체 서명 알고리즘 구현, 비트코인 레이어 2, EVM, MoveVM 등 다양한 체인을 지원하기 위한 브로드캐스트 서비스 어댑터 통합, 그리고 Solidity, Move 등 다양한 프로그래밍 언어를 사용한 온체인 레지스트리 프로그램이나 스마트 컨트랙트 개발이 포함됩니다. 이러한 다각적인 접근 방식 덕분에 적응성과 상호 운용성이 보장되어 시스템이 진화하고 다양한 블록체인 생태계와 통합될 수 있습니다.

Zeus 레이어는 노드들로 구성된 오프체인 P2P 네트워크로, Zeus 노드는 네트워크의 효율적인 운영을 가능하게 하고 탈중앙화 특성에 기여합니다. 이 노드들은 P2P 통신 및 서명과 브로드캐스트와 같은 검증자 임무를 담당합니다. Zeus 네트워크는 개인 키를 유지하고 트랜잭션에

서명하는 노드를 운영하는 검증자들에 의해 보안이 유지됩니다. 검증자가 되기 위해 서는 SOL 토큰이나 SOL 의 Liquid Staking 파생상품(LSD-SOL)을 스테이킹하여 네트워크의 PoS 합의 메커니즘에 참여할 수 있습니다.

APOLLO



Source : Apollo Docs

APOLLO 는 Zeus Network 에서 ZPL 을 활용해 만들어진 첫번째 디앱으로 비트코인과 솔라나 간의 가치 전송을 검열 없이 가능하게 하는 크로스체인 Liquid Staking 솔루션입니다. APOLLO 는 비트코인 보유자들을 위한 게이트웨이 역할을 하며, 솔라나 생태계 내에서 비트코인 자산을 원활하게 활용할 수 있도록 합니다. APOLLO 를 통해 비트코인 위의 BTC 를 예치하고 1:1 비율 고정 페깅된 솔라나 체인의 zBTC 를 빌릴 수 있습니다. zBTC 는 ZPL 자산이며, ZPL 은 SPL 을 기반으로 호환될 수 있도록 만들어진 표준이기 때문에 zBTC 는 솔라나 생태계에서 활용될 수 있습니다. 즉, 마치 이더리움의 WBTC 와 같이 비트코인의 유휴 BTC 를 솔라나로 가져와 새로운 유동성을 만들어낼 수 있습니다.

APOLLO 가 기존 브릿지와 다른 점은 자산이 Zeus 레이어를 거쳐 허가 없는 참여와 검열 없는 환경을 제공하며, 중앙 기관이 BTC 를 보관하지 않는다는 점이 있습니다.

MARKET ANALYSIS

Solana 에서 Zeus Network 에 대한 인지도는 처음부터 높았습니다. 그 이유는 앞서 언급한 LFG 런치패드 때문입니다. LFG 런치패드에서 Zeus Network 는 총 201,857,511 votes 중 117,318,490 votes (58%)를 획득하여 2 등 Sharky(20%)와도 압도적인 격차로 우승하여 IDO 를 진행하였습니다. LFG 런치패드는 현재 솔라나 DeFi 생태계에서 가장 영향력이 있 는 Jupiter 에서 만든 런치패드이기 때문에 많은 주목을 받는 상태였으며, 첫번째 우승자라는 타이틀은 초기 마케팅에 큰 도움이 되었습니다.

현재 Zeus Network 의 트위터 팔로워는 20 만명으로 4 월 기준 12 만명에서 3 개월만에 크게 늘었으며, 디스코드 또한 8 만명에서 16 만명으로 증가하였습니다.

아직 Apollo 의 메인넷 출시가 이루어지지 않아서, 얼마나 많은 규모의 BTC 가 zBTC 로 넘어 올지를 정확하게 알 수는 없지만, 7 월 15 일 테스트넷 출시 이후 현재까지 467.84 zBTC 가 민팅되었으며 2,867 개의 Unique Wallets 이 참여하였습니다.

LIMITATIONS

Zeus Network 의 문제는 현재 보유한 커뮤니티와 타겟 유저가 다르다는 점입니다. Zeus 가 성공적으로 운영된다면 솔라나 생태계에 새로운 유동성이 들어오기 때문에 많은 솔라나 커뮤니티는 환호하며 Zeus 에 대한 좋은 반응을 보여주고 있지만, 그들은 Zeus 가 필요로 하는 공급자가 아닙니다. Zeus 의 타겟 유저는 BTC 를 솔라나를 통해 유동화시키고 싶은 BTC 홀더들인데, 비트코인 커뮤니티에서 Zeus 의 존재감은 아직 미약합니다. 특히나, 브릿지 방식 이 아니라고는 하지만, 브릿지와 유사한 UX 를 가지고 있는 Apollo 는 많은 BTC 홀더들에게 거부감을 느끼게 할 가능성이 높습니다.

Zeus Layer 가 충분히 탈중앙화되어있느냐도 중요한 문제입니다. 만약 충분히 탈중앙화되어있지 않고, 보안에 대한 대비가 되어있지 않다면 Zeus 의 수탁 계정에 대한 공격 및 해킹이 발생할 수 있고, 이는 프로젝트에 대한 신뢰 추락으로 이어질 것입니다.

3. CONCLUSION

FUTURE OF THE BITCOIN ECOSYSTEM

본 레포트를 통해 비트코인 생태계에 대해 7 가지로 분류를 하고, 각 분류에 대한 정의를 프로젝트 분석과 함께 알아보았습니다. 특히, 본 레포트에서는 비트코인 생태계의 확장성에 초점을 맞춰, 기능적인 확장성 또는 금융적인 확장성에 따른 분류 사항들을 중점적으로 다뤘습니다. 각 분류별로 지니는 주요한 점과 한계점을 제시하며 마무리하고자 합니다. 제시하는 내용은 앞서 서술한 조사를 기반으로 판단하였으며 주관이 포함되어 있음을 밝힙니다.

CLIENT-SIDE VALIDATION

- **Highlights**: CSV 프로토콜은 뛰어난 확장성을 제공하여 다양한 자산 발행 및 스마트컨트랙트 구현이 가능합니다. 이를 통해 비트코인 네트워크에서 정교한 금융 상품과 디앱을 구현할 수 있습니다. 또한, 온체인에 데이터가 저장되어 데이터에 대한 보안이 높습니다.
- **Limitations**: 중앙화 문제가 여전히 존재하며, CSV 프로토콜만의 규칙은 비트코인의 보안에 의해 보호되지 않기 때문에 보안적인 취약성이 있습니다.

SIDE CHAIN

- **Highlights**: 현재는 타체인과 달리 비트코인 구조 상 레이어 2 에서 제출되는 내용들에 대한 유효성 검증이 힘들기 때문에 사이드 체인은 실질적으로 활용 가능한 유일한 형태입니다. 또한, BitVM 과 OP_CAT 의 구현 시기가 미지수이기 때문에 그 전까지 생태계를 견고하게 쌓아둔다면 해자를 만들 수 있다고 판단됩니다.
- **Limitations**: 이더리움과 같은 다른 경우를 살펴보았을 때, BitVM 혹은 OP_CAT 기반 레이어 2 가 등장할 시 빠르게 전환하지 않으면 Mainstream 을 유지하지 못할 것으로 생각됩니다. 사이드 체인은 엄밀히 따지면 비트코인을 온전히 확장하는 솔루션이라기보 단 비트코인을 활용하는 솔루션이기 때문에 비트코인의 보안을 완벽하게 상속받을 수 없고, 불안전한 브릿지와 네트워크 구조는 탈중앙성과 보안을 보장할 수 없기 때문입니다.

BITVM-BASED L2

- **Highlights**: BitVM 기반 L2 솔루션은 비트코인의 보안을 온전히 상속받아 높은 보안성을 제공합니다. 이를 통해 튜링 완전한 스마트 컨트랙트를 비트코인에서 실행할 수 있어, 다양한 디앱을 구현할 수 있습니다.
- **Limitations**: BitVM 은 아직 초기 단계에 있어 실제 상용화까지는 시간이 걸릴 수 있습니다. 개발 과정에서는 예상치 못한 기술적 문제들이 발생할 가능성이 있으며, 초기 도입 단계에서는 기술적인 복잡성과 사용성 문제로 인해 사용자 경험이 저하될 수도 있습니다. 또한 이와 비슷한 역할을 할 수 있는 OP_CAT 은 더 효율적이고 간단한 솔루션이 될 수 있기 때문에, OP_CAT 이 도입되면 BitVM 은 경쟁에서 밀릴 가능성이 있습니다.

OP_CAT-BASED L2

- **Highlights**: OP_CAT 기반 L2 솔루션은 비트코인 스크립트를 통해 STARK 검증을 가능하게 하여 높은 확장성과 보안성을 제공합니다. Starknet 의 기존 인프라와 기술력을 활용하여 안정적이고 빠르게 개발할 수 있으며, 비트코인과 이더리움을 연결해 두 네트워크의 상호 운용성을 강화하고 더 큰 확장을 가능하게 합니다.
- **Limitations**: OP_CAT 의 도입 여부가 불확실하며, 이를 활성화하는 데 필요한 합의가 이루어져야 합니다. 또한, OP_CAT 기반 L2 솔루션을 구현하는 과정에서 비트코인 스크립트의 복잡한 연산 처리 제한 등 기술적 난관이 있을 수 있습니다.

BTC STAKING

- **Highlights**: Babylon 은 비트코인 버전 EigenLayer 로 이미 성공적인 유사 사례를 갖고 있으며, 최대 규모 투자를 유치하고 커뮤니티의 큰 지지를 받고 있습니다. 이러한 점과 비트코인에서 네이티브한 스테이킹 컨트랙트를 제공하여 접근성을 높인다는 큰 장점을 고려하면, 조만간 메인넷 런칭이 이루어졌을 때 꽤 큰 자금들이 예치될 것으로 기대됩 니다.
- **Limitations**: 유사 사례인 EigenLayer 의 경우 매우 높은 개발 난이도로 인해 결국 슬래싱 시스템을 제외하고 메인넷에 출시하여 보안에 대한 많은 논란이 있었습니다. Babylon 또한 비슷한 일이 발생한다면 보안적으로 안전하다고 보기 어려울 것입니다.

DEFI

- **Highlights**: bitSmiley 를 보면 DeFi 생태계가 거의 없는 비트코인에서 나쁘지 않은 결과를 보이고 있고, 좋은 시도라고 판단됩니다. 특히, bitSmiley 의 지표를 보면 비트코인 생태계에서 적지 않은 사람들이 DeFi 에 관심이 있다는 것의 반증으로 보입니다.
- **Limitations**: 여전히 스테이블 코인을 발행하는 것 외의 다른 네이티브 DeFi 서비스는 출시되지 못하고 있으며, DeFi 디앱은 레이어 2 에서의 활용성에 의존할 수 밖에 없는 한계가 있기 때문에 자체적인 사용성에 대해서는 검토해볼 필요가 있습니다. 또한, DeFi 의 꽃이라고 할 수 있는 DEX 와 같은 서비스는 특정 기준 이상의 기술적 스펙을 요구하는데 이런 측면에서 과연 비트코인 생태계에서 진정으로 실행될 수 있을 지는 의문입니다.

BTC INTEROPERABILITY

- **Highlights**: Zeus 는 솔라나에 이미 구축된 DeFi 생태계를 바탕으로 BTC 의 활용도를 만들어낼 수 있고, 단순 브릿지가 아닌 커뮤니케이션 레이어를 통한 크로스체인 어플리케이션의 활용을 가능하게 합니다. 솔라나 커뮤니티의 열렬한 지지를 바탕으로 Zeus 커뮤니티 또한 빠르게 성장하고 있습니다.
- **Limitations**: 실제로 BTC 를 예치하고 솔라나에서 활용해야 할 비트코인 커뮤니티를 아직 충분히 끌어들이지 못한 것으로 보이며, 결국 브릿지와 비슷한 사용자 경험을 가지고 있기 때문에 생기는 거부감을 극복하기 어려울 수 있습니다. 또한, 아직 Zeus 레이어는 충분히 탈중앙화되지 않은 것으로 보이며, 이를 극복하는 것이 앞으로의 과제가 될 것입 니다.

FINAL SENTENCE : MIRRORING INNOVATION, REDEFINING BOUNDARIES

비트코인은 탈중앙 금융의 필요성을 역설하며 나온 최초의 블록체인입니다. 여느 생태계처럼 블록체인 산업도 사회의 발전 방향을 따라서 발전해왔습니다. 다양한 기능의 서비스를 필요로 하는 사회에서 비트코인의 제한된 기능은 명백한 한계점으로 받아들여졌고, 이를 한계로 인식한 타

블록체인이 출시되며 지속적으로 더 나은 서비스를 개발하기 위해 블록체인 산업군은 변화했습니다. 불과 2022 년까지도 비트코인은 여전히 금융 레이어로 머물러 있었지만, 혁신의 움직임을 받아들이고자 하는 움직임이 비트코인 생태계 내에도 존재했기에 2022 년도를 기점으로 비트코인도 Inscription, 레이어 2 와 같은 프로젝트가 등장했습니다. 이를 통해 우리는 비트코인이 다른 블록체인처럼 유틸리티성을 제고하고자 혁신을 받아들이 며 생태계의 역할을 재정의하고 있다고 믿습니다. 본 레포트를 통해 이러한 비트코인의 혁신에 대해 분석 및 비트코인의 생태계에 대해 정의해봤습니다. 마지막으로 **"Bitcoin: Mirroring Innovation, Redefining Boundaries"**라는 문장과 함께 이 글을 마칩니다.