

Multi-chain future is here!

멀티체인 시대의 도래 – 생태계 소개

DSRV Jin Hyung Park (Sigrid Jin) | '22. 5. 11.

발표자 소개

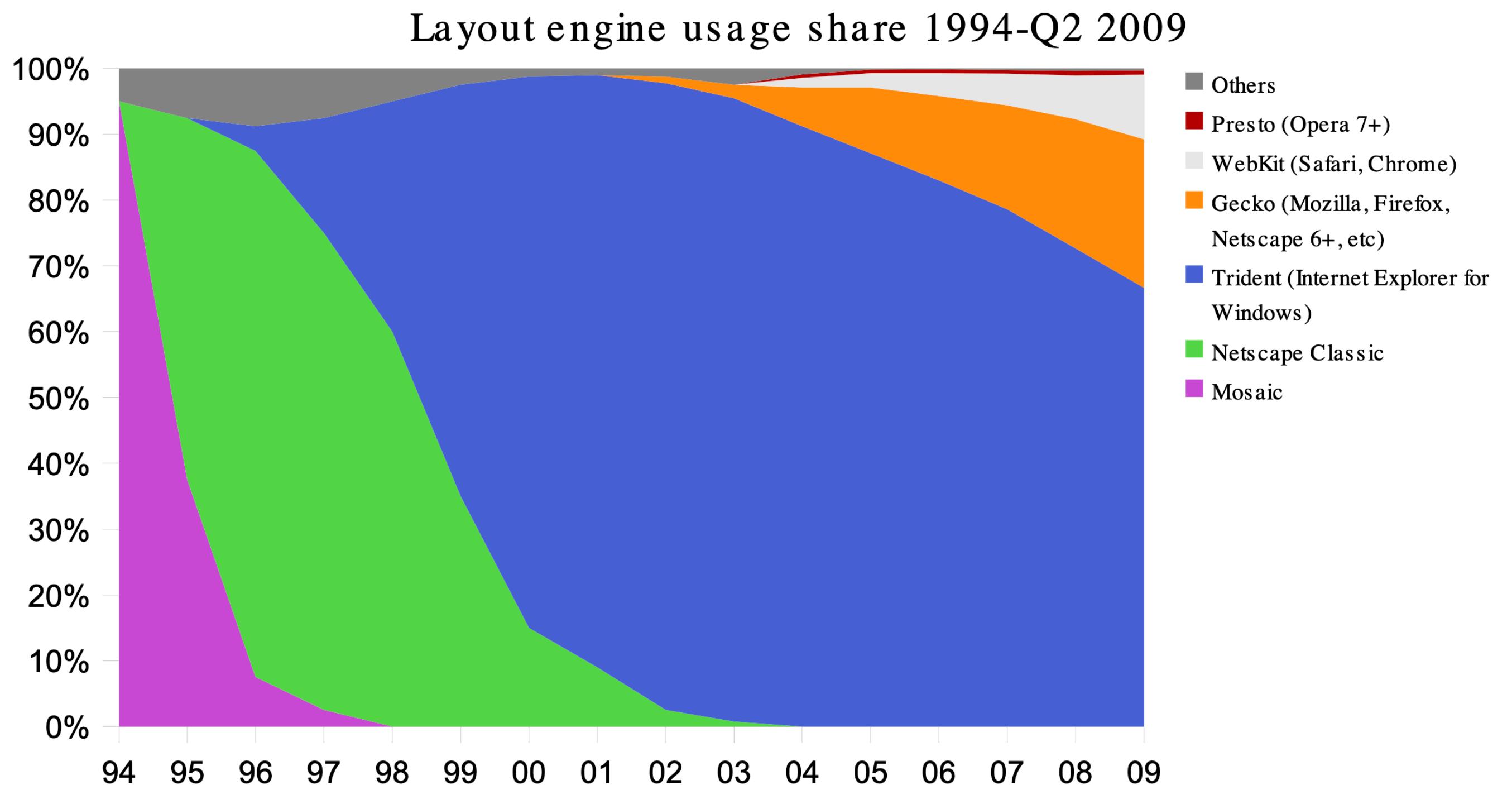
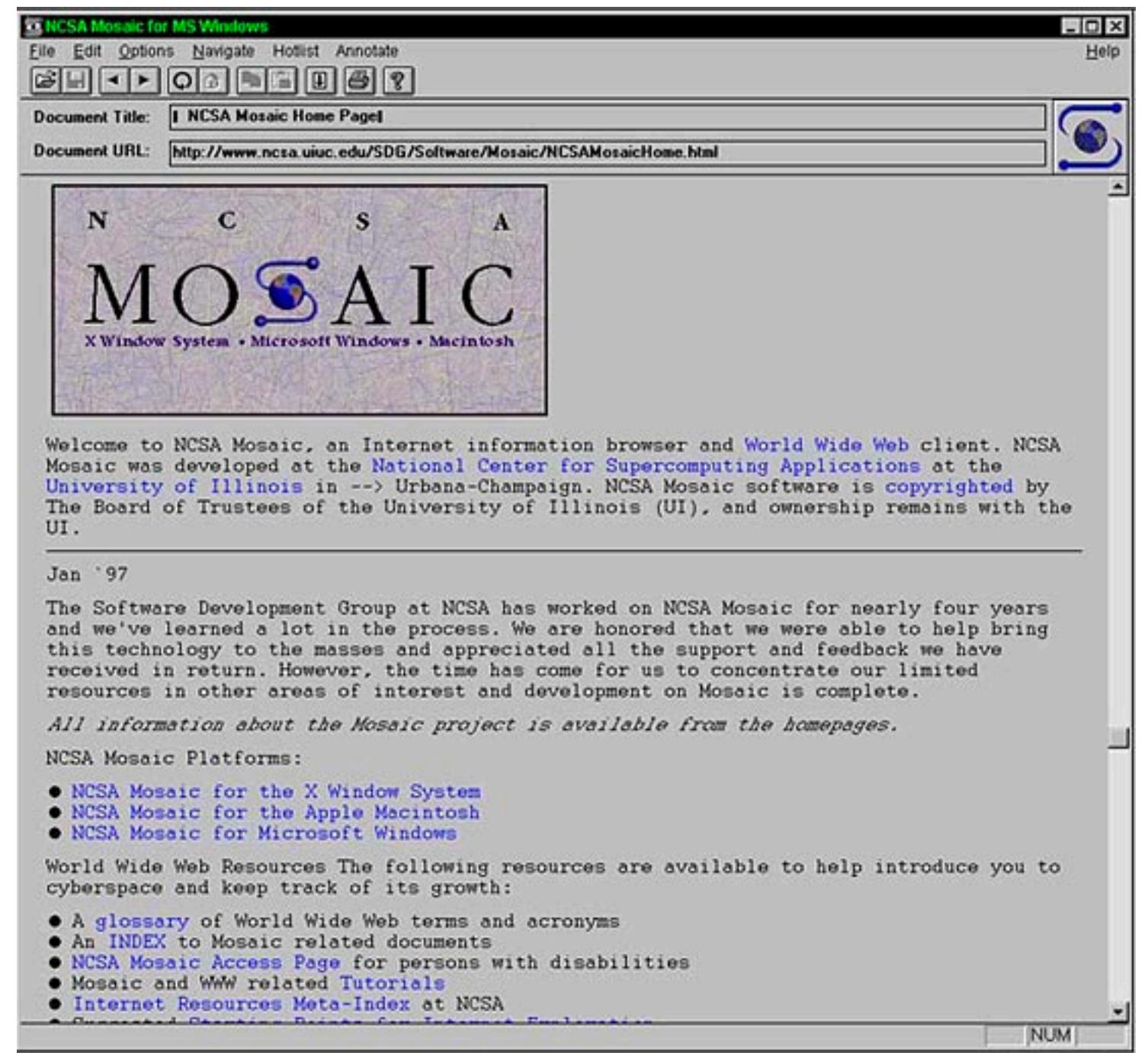
박진형 (Jin Hyung Park)

- (현) 블록체인 인프라 스타트업 **DSRV** Technical Writer & Developer Advocate
- (현) 고품질 소프트웨어 교육 **코드스쿼드** 마스터즈 과정 Java 백엔드 코드리뷰어
- (전) 네이버 커넥트재단 Research Assistant (부스트캠프 팀, 엔트리 AI 교육팀)
- (전) 블록체인 및 핀테크 인큐베이터 팀위 (**teamw.e**) Research Assistant Intern
- (전) 블록체인 인큐베이터 체인파트너스 Research Assistant Intern
- (전) 한국 이더리움 연구회 연구원 (4기 기술 리서치 분과, 5기 토큰 이코노미 분과)
- (전) The Economist Corporate Network, 중앙일보 폴인 등 다수 리서치 프리랜서

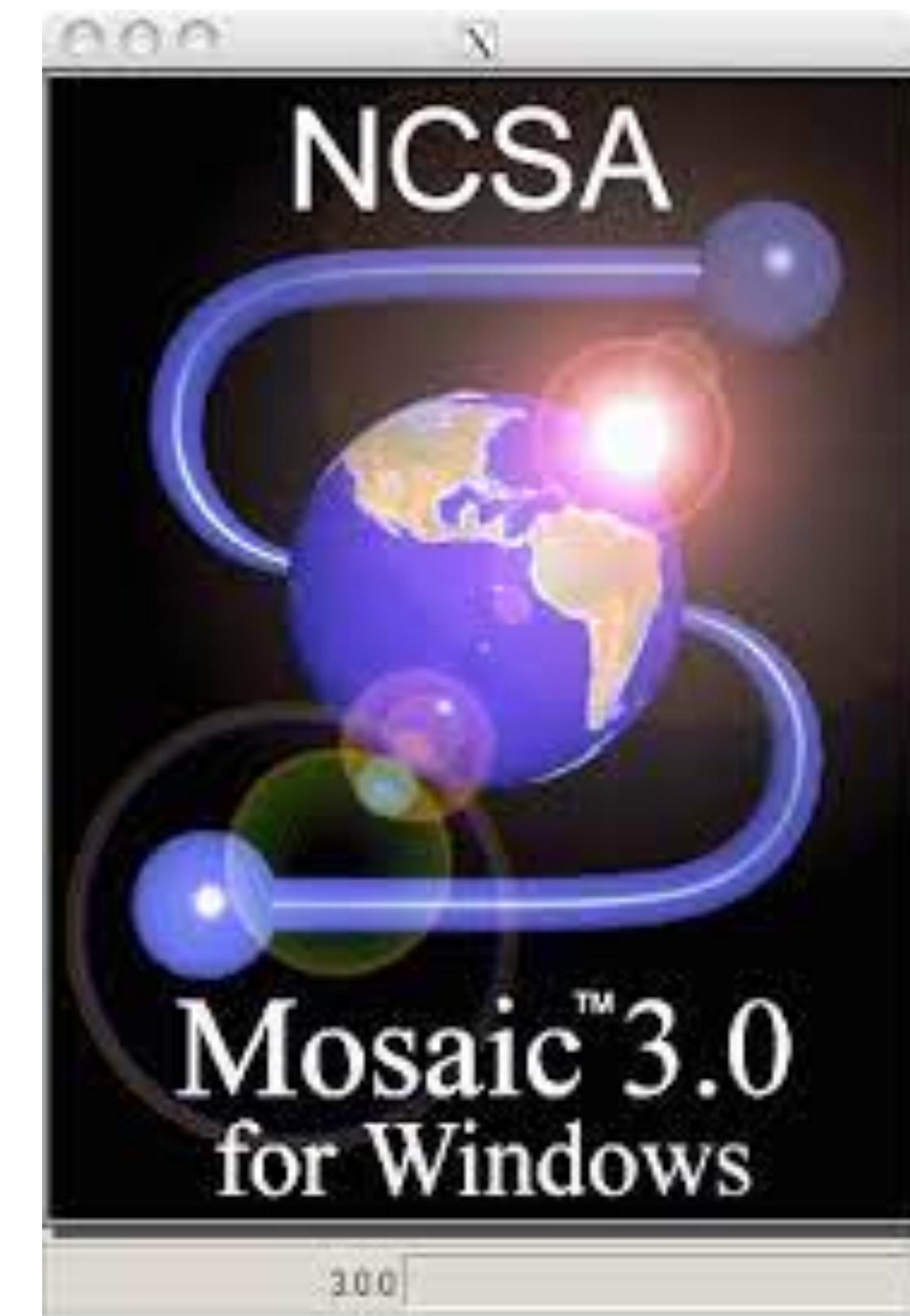
오늘의 내용

- 멀티체인 시대는 무엇이고, 왜 등장했는가
 - 브라우저 전쟁을 통해 바라보는 웹 1.0 및 2.0 시대의 흐름
 - 블록체인 트릴레마란 무엇인가
 - 이더리움 진영에 대한 간략한 소개: Layer 2와 Rollups
 - 코스모스 진영에 대한 간략한 소개
 - 솔라나 진영에 대한 간략한 소개
- Interoperability is a King
 - 상호운용성이 중요한 이유
 - 멀티체인과 크로스체인의 공통점, 차이점
 - ERC20 토큰과 메인넷 코인의 차이점
 - 브릿지란 무엇인가
- 실습 1: DeFi 체험해보기, PoS 스테이킹 이해해보기
- 실습 2: ERC20 토큰 컨트랙트 멀티체인으로 배포해보기

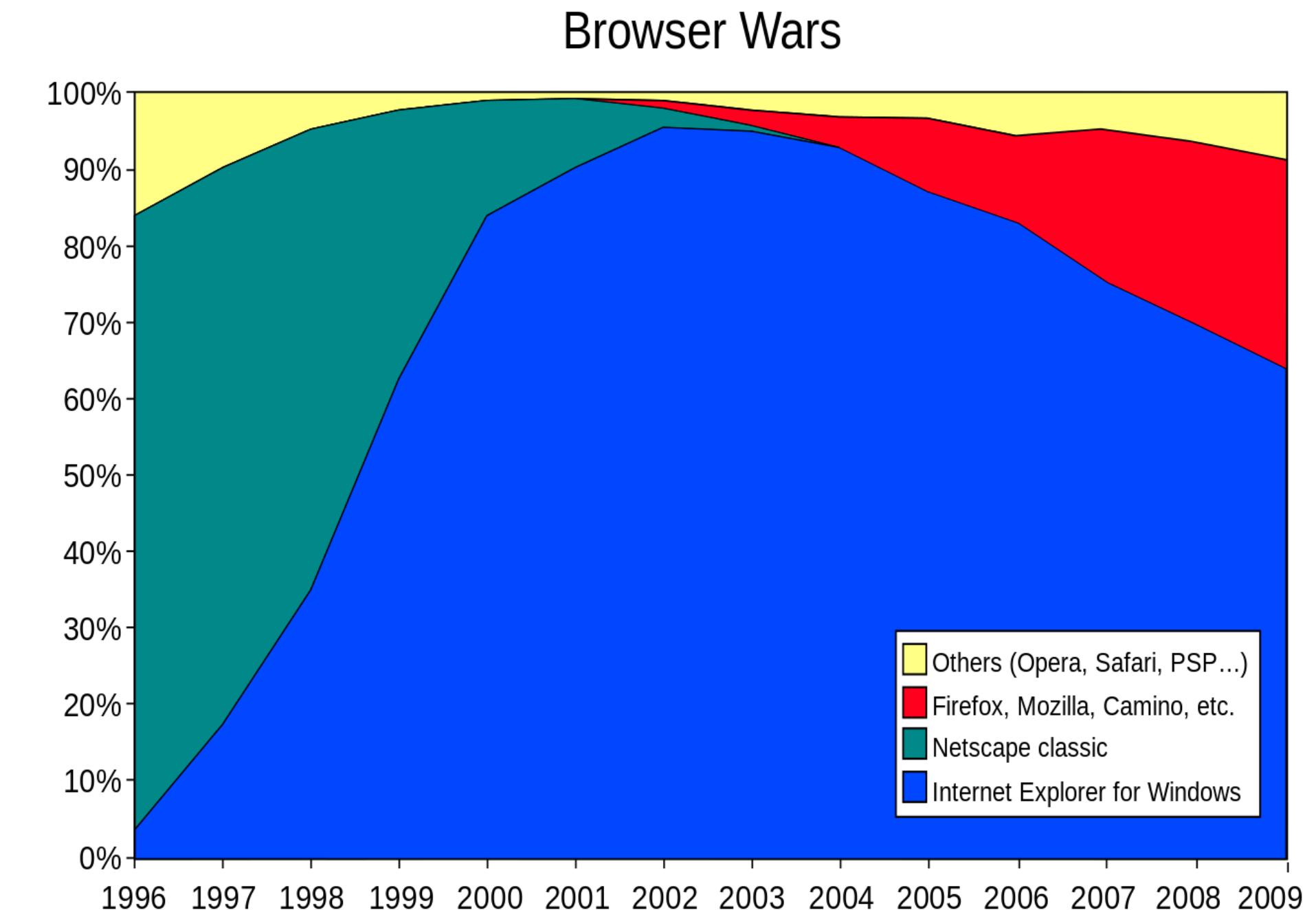
태초에 모자이크 브라우저가 있었으니...



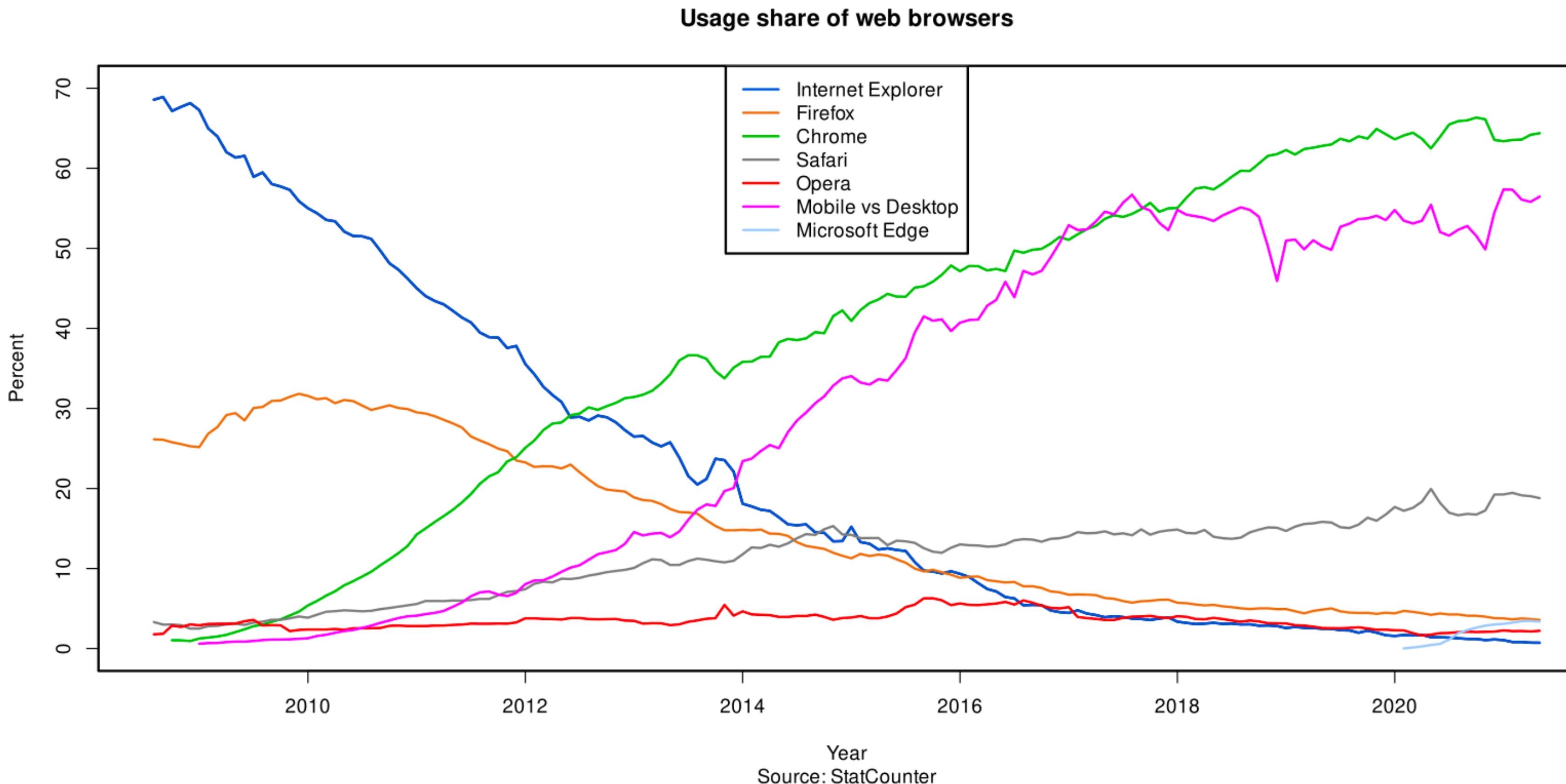
INTERNET EXPLORER 1.0 VS 자바스크립트를 구현한 모자이크 3.0



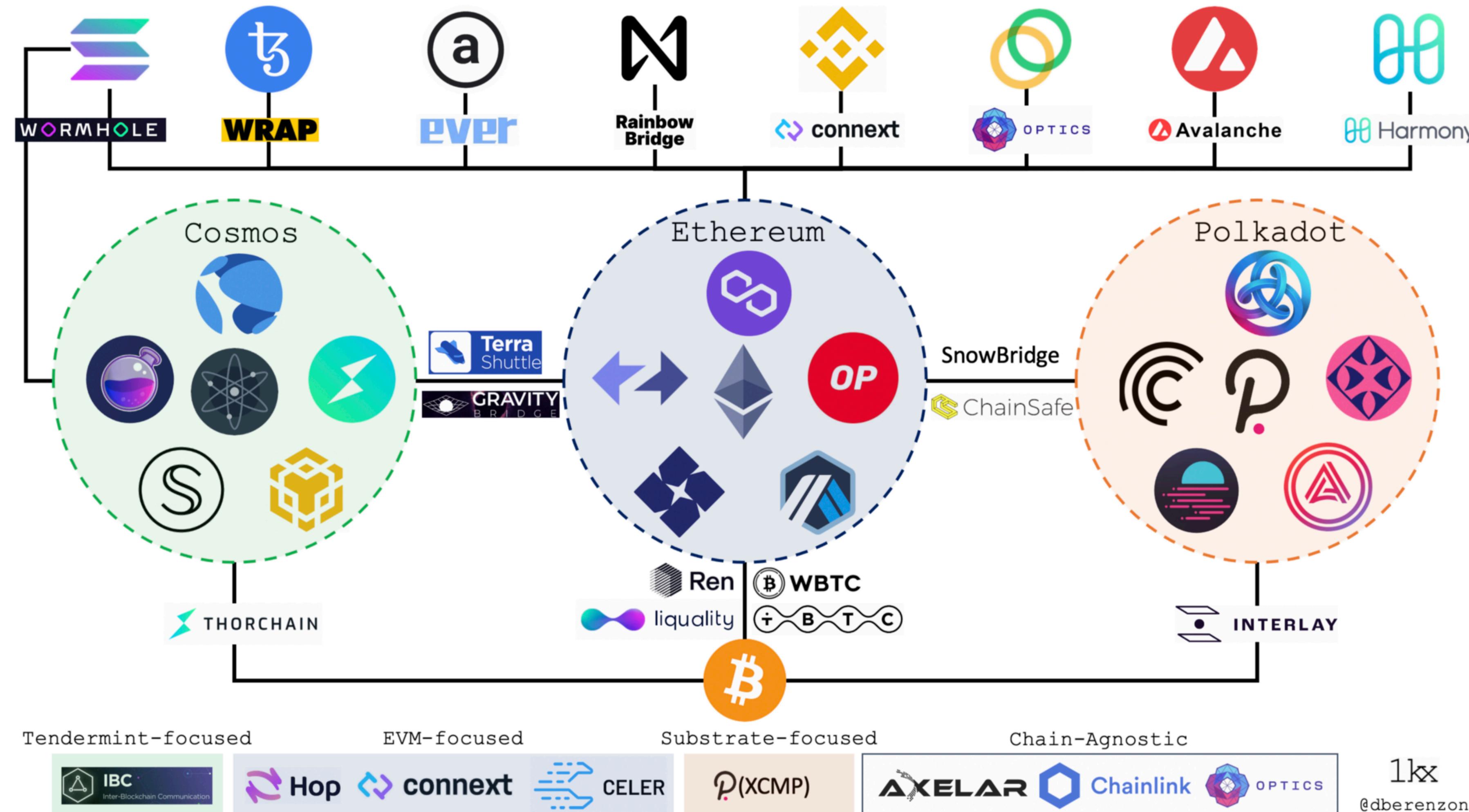
INTERNET EXPLORER 4.0 출시, 윈도우 끼어팔기, 독자 규격



CHROME의 등장, FIREFOX의 부활, IE의 멸망

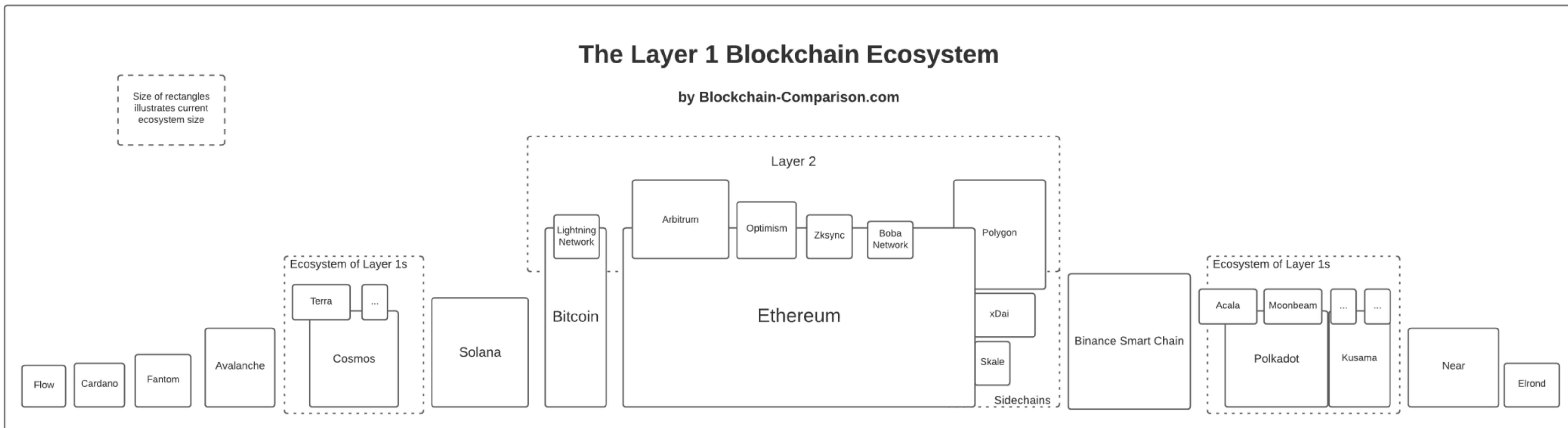


멀티체인 시대의 등장

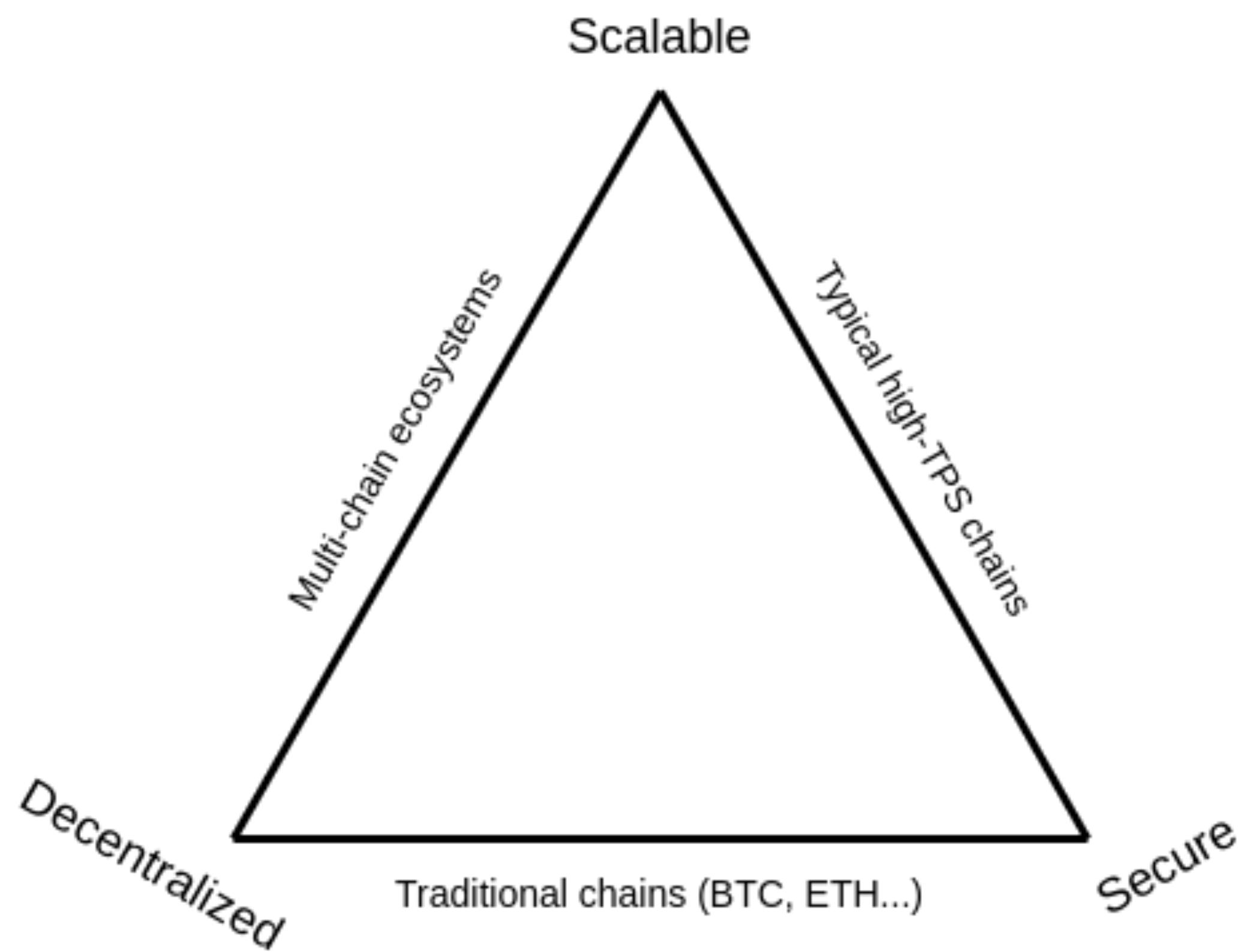


Why Multi-chain universe is blooming?

- 2022년 5월 현재, 약 100여개의 퍼블릭 블록체인이 존재
- 각 블록체인은 블록체인의 대중화를 위해 필요한 문제 해결 (속도, 수수료)를 위한 각자만의 해결 방식 (합의 알고리즘 등)을 도입

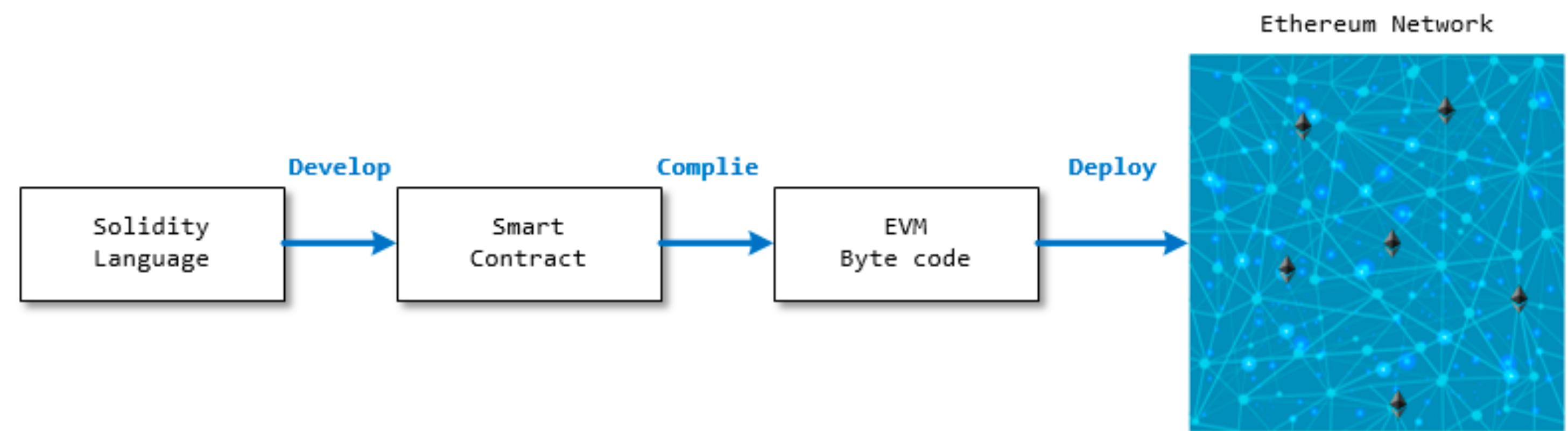
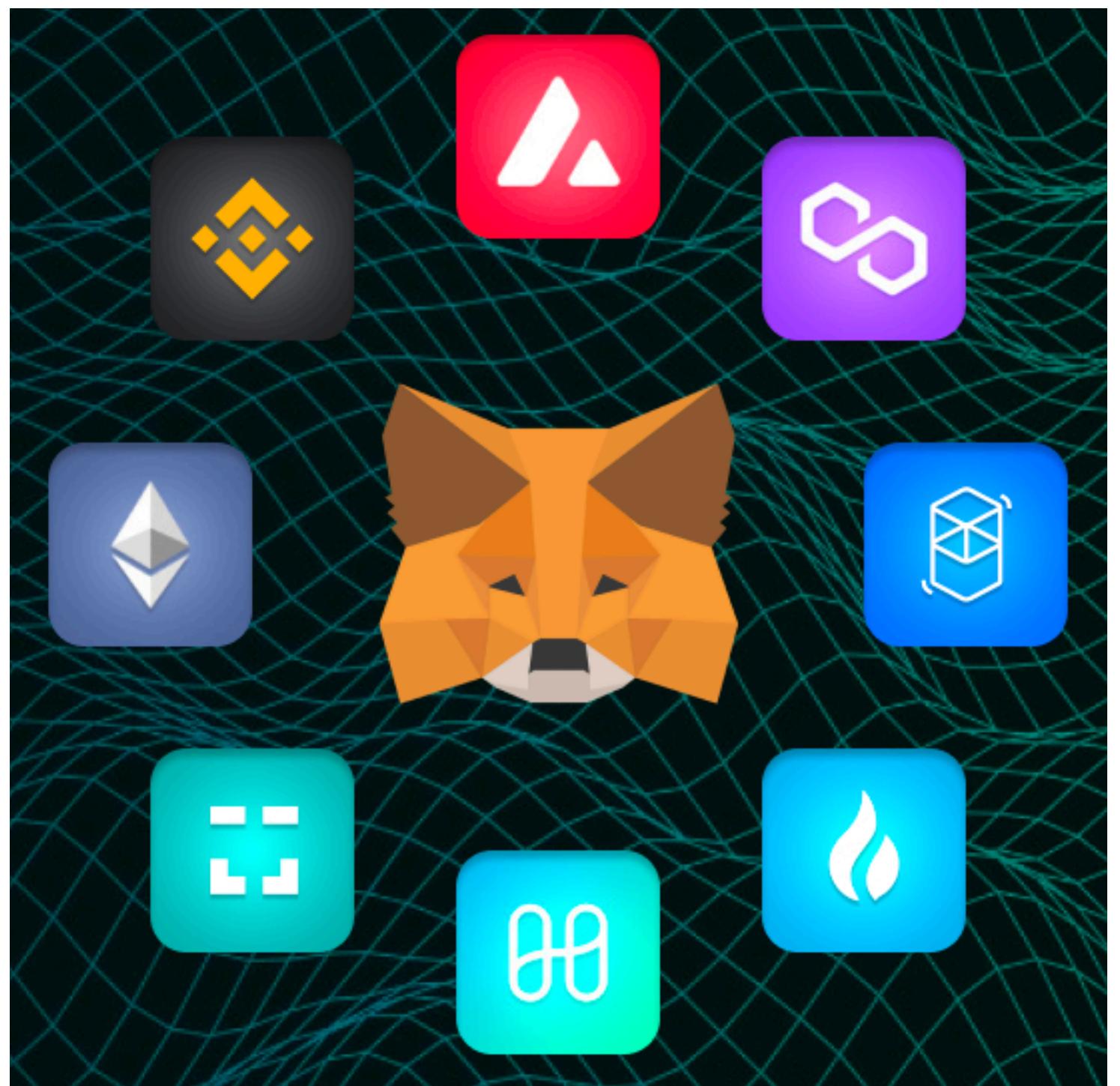


The Great Blockchain Trilemma



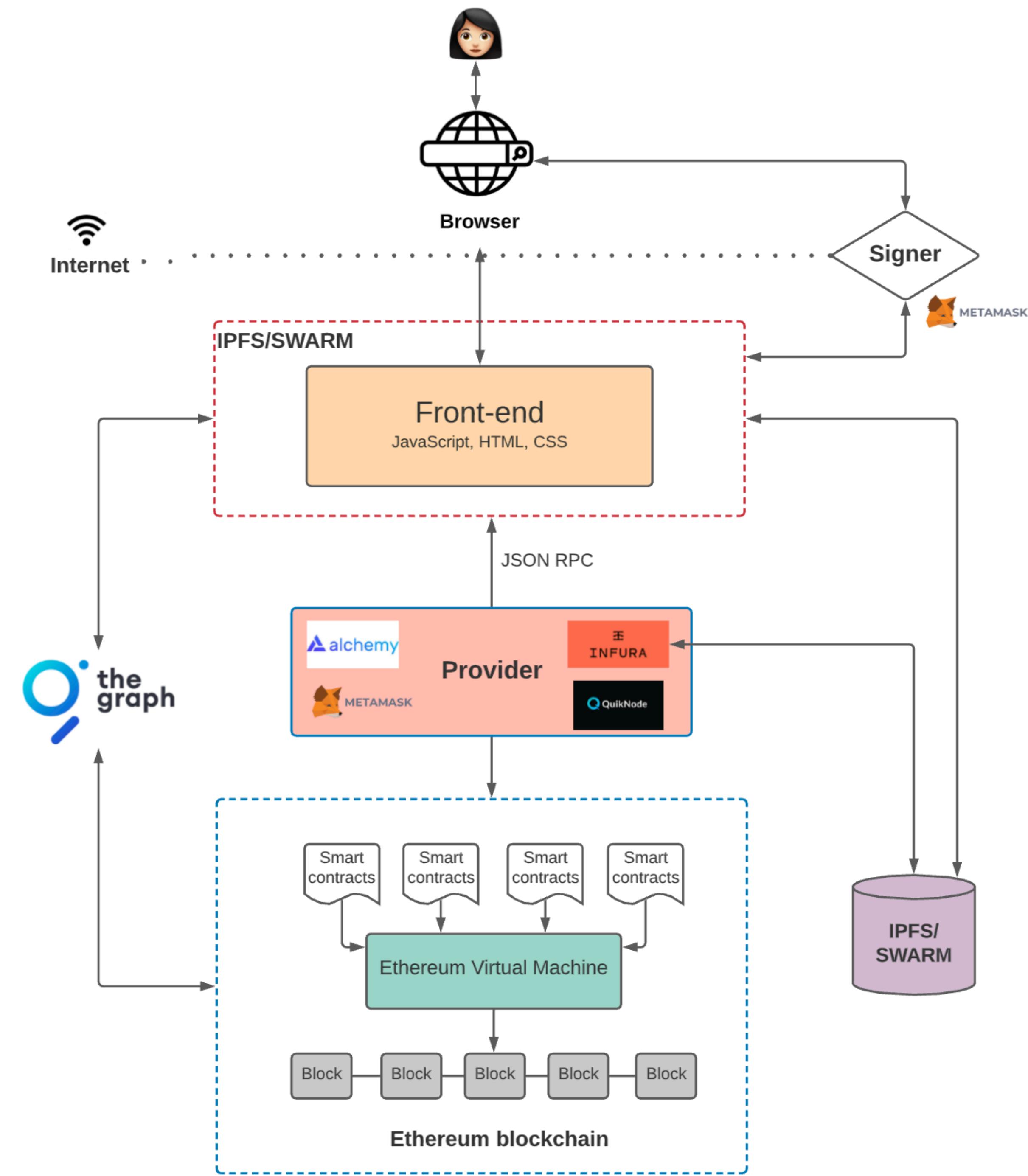
- 비탈릭이 처음 제시한 트릴레마란 블록체인이 탈중앙성, 보안성, 확장성 세가지를 동시에 만족하기 힘들다는 개념
- 탈중앙성: 네트워크가 중앙화된 주체에 의해 좌지우지 되지 않는가
- 보안성: 악의적으로 행동하는 참여자의 존재에도 네트워크가 유효한 합의를 이루어 낼 수 있는가
- 확장성: 블록체인이 트랜잭션들을 얼마나 많이, 그리고 빠르게 처리할 수 있는가?
- 트릴레마는 이를 평가하는 절대적인 기준이 존재하는 것이 아니라 모두 상대적인 개념으로 이해해야 하며 탈중앙성, 보안성, 확장성중 무엇을 높이는 선택을 하든 장점과 단점이 존재

이더리움 진영: EVM 호환되는 블록체인 프로토콜

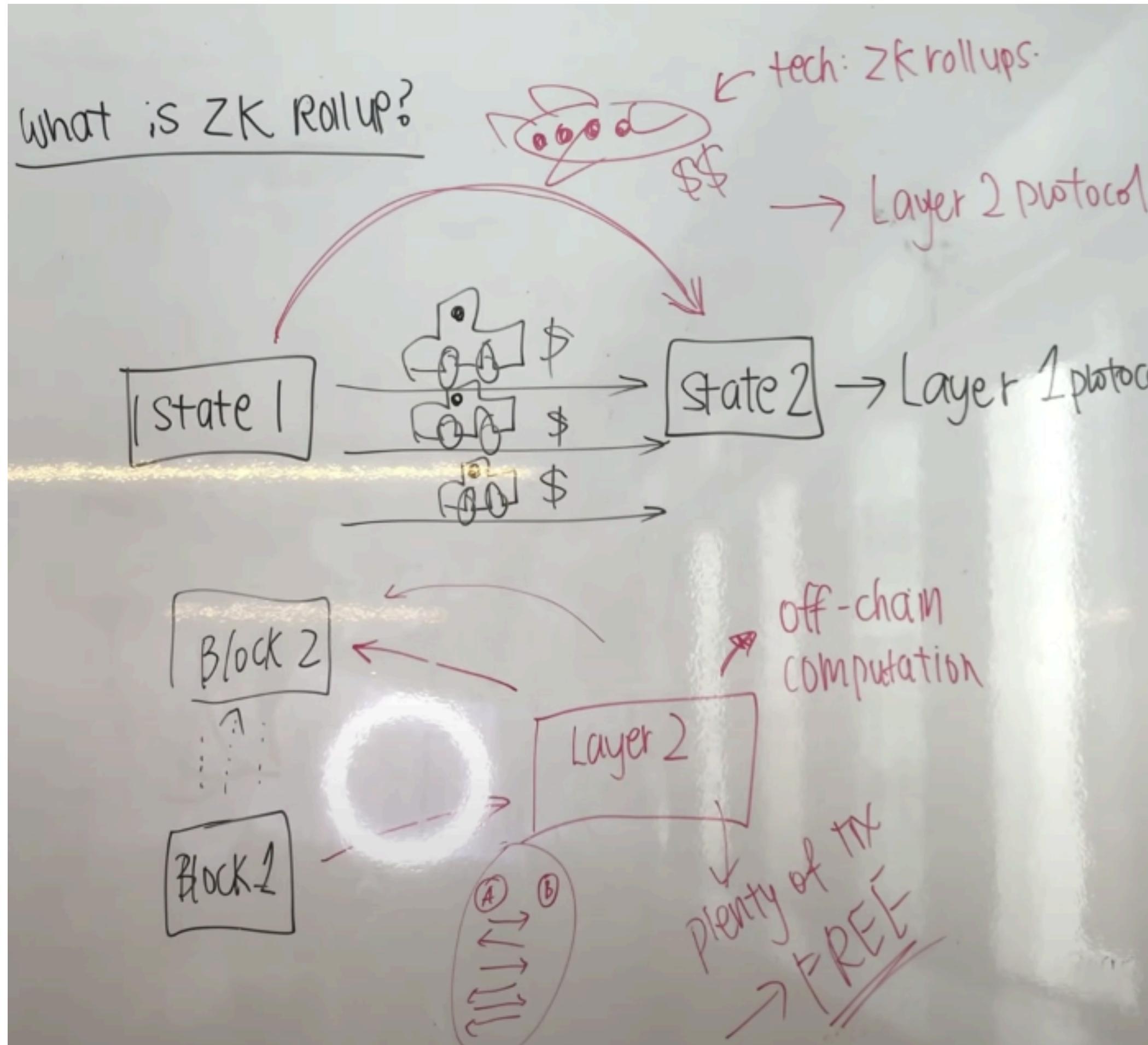


DAPP 생태계가 제일 활발하고, 가장 개발 자료가 많으며, 제일 오래되었음

<https://chainlist.org/>



LAYER 2: 이더리움의 속도와 수수료 문제를 해결하자!

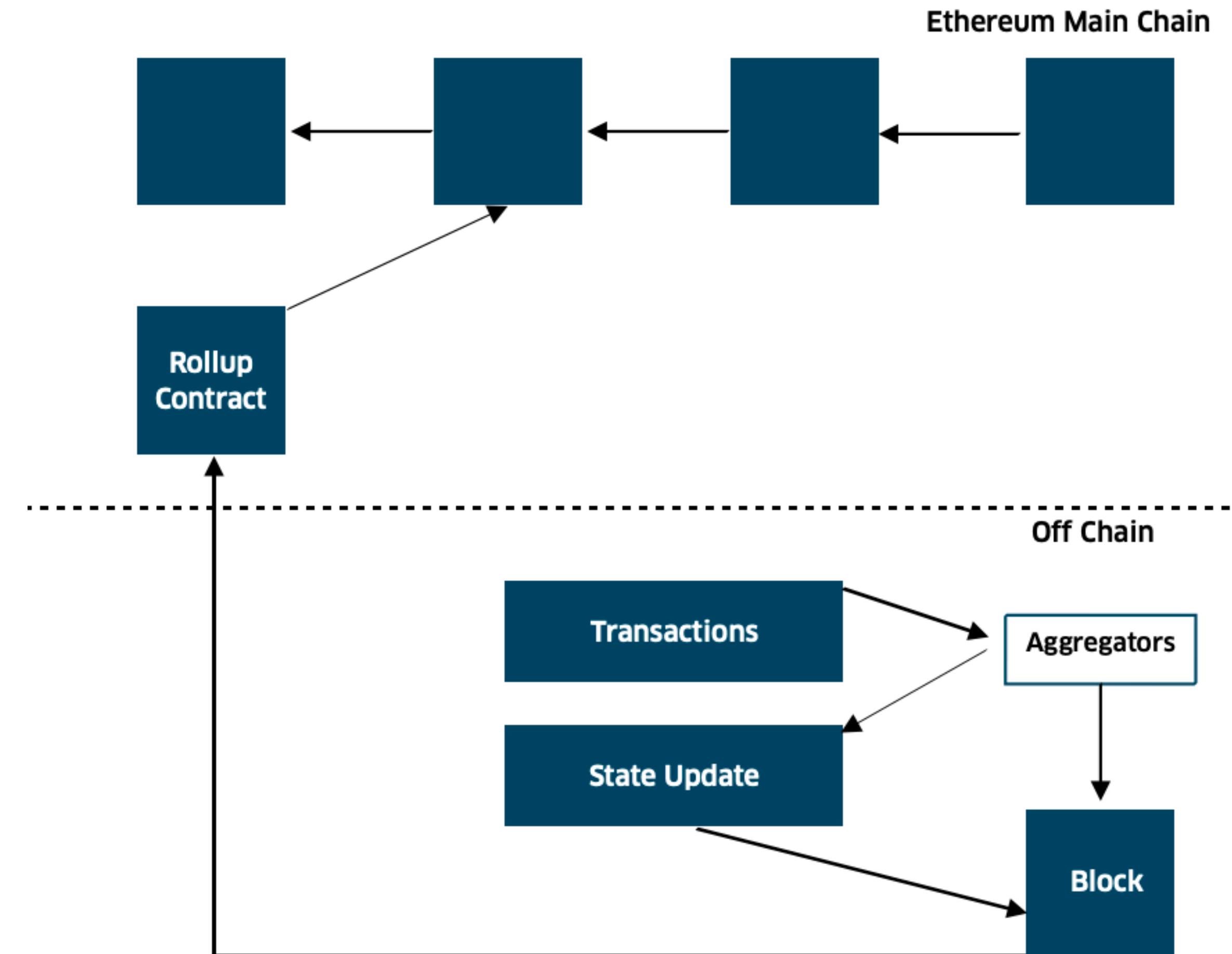
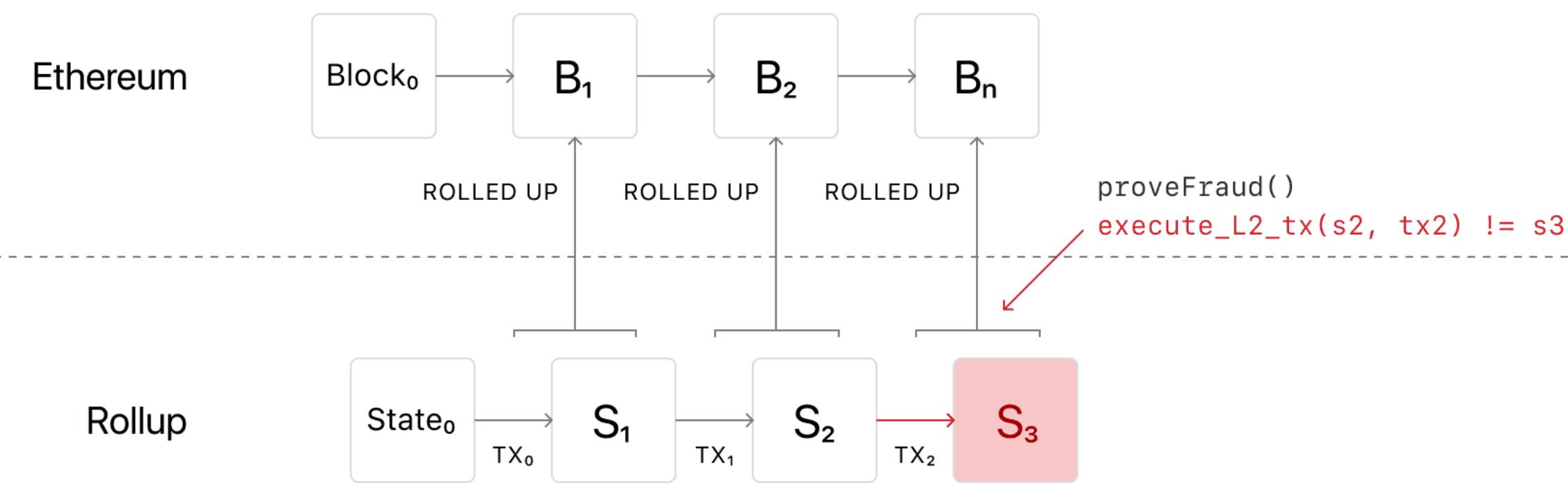


은행에서 제가 친구 A에게 백만원을 송금한다면, 대략 이러한 과정을 거치게 될것입니다.

1. '나'로부터 'A'에게 백만원 송금 (기록)
2. '나'의 계좌에서 백만원 차감 / 'A'의 계좌에서 백만원 추가 (처리)

이 새로운 방식의 특징은 바로 1번 과정만 이상한 상자에 기록하고 실질적인 거래 처리 과정인 2번은 모두 보조 상자에서 처리한다는 것입니다. 만약 단순한 송금이 아니라 더 복잡한 경제활동을 다룬다면 2번 과정이 매우 복잡해질 것이고, 이를 보조 공장에서 처리하게 된다면 매우 효율적이겠죠.

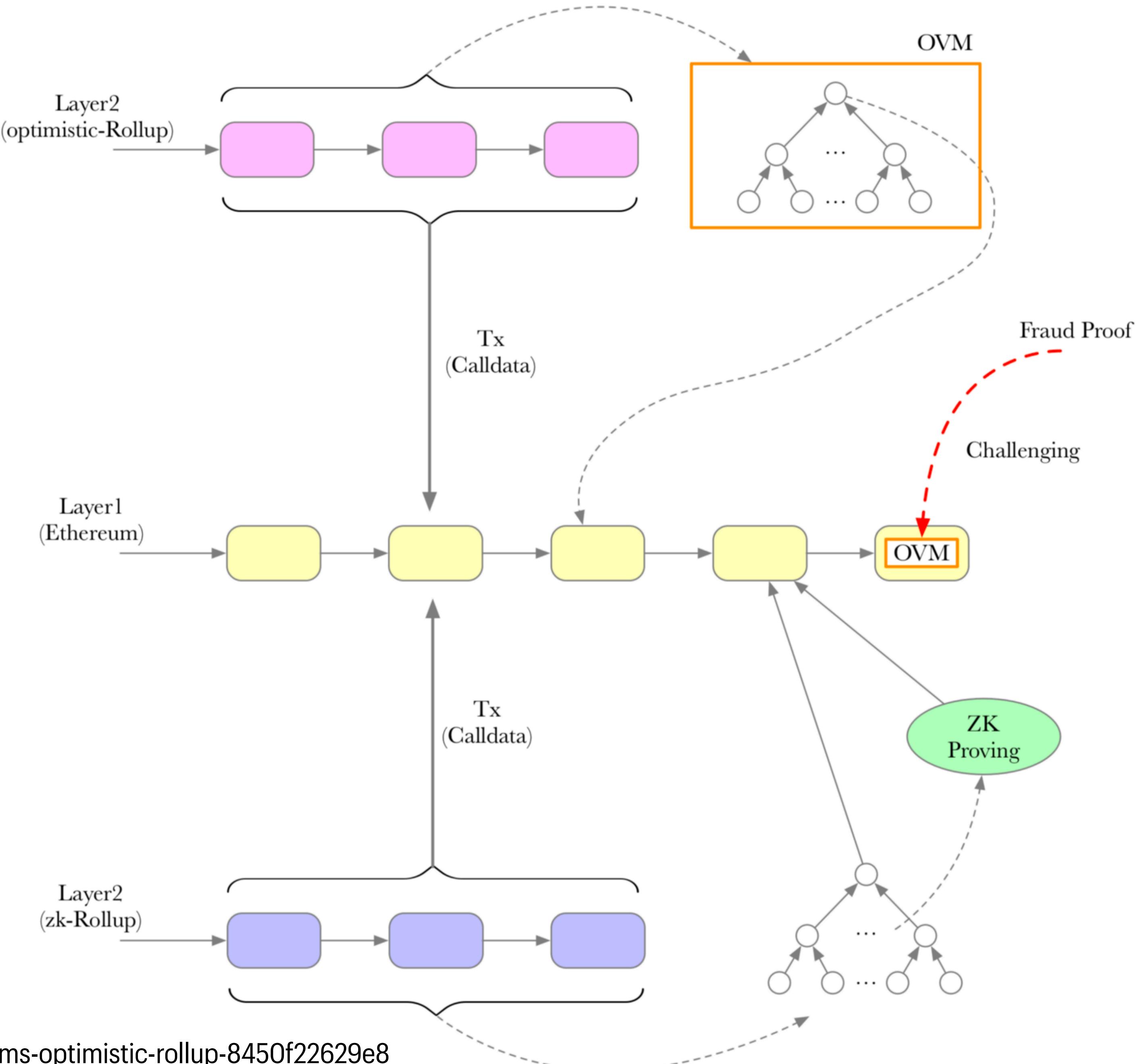
WHAT IS ROLLUP?



OPTIMISTIC ROLLUP

하지만 이 방식 또한 완벽하지는 않았습니다. 거래내역만 따로 이상한 상자에 기록한다고 했지만 그 양이 만만치가 않기 때문입니다. 더 효율적으로 상자를 생산하겠다고 보조 공장까지 따로 세웠는데, 막상 보조 공장에서는 거래를 처리하는 역할만 맡기 때문에 이상한 공장의 모든 문제를 해결하기에는 그 한계가 명확했습니다.

2. Once processed, the sequencer will submit both the transaction data and the new L2 state root to L1.
3. Then, all other L2 nodes mentioned above will process the transaction on their copy of the L2 chain.
4. In order to ensure that the new state root submitted to L1 is correct, verifier nodes will compare their new state root to the one submitted by the sequencer.
5. If there is a difference, they will begin what's called a fraud proof. The fraud proof will execute the L2 transaction but on L1 so that the resultant state root cannot be faked.
6. If the fraud proof's resultant state root is different from the one submitted by the sequencer, the sequencer's initial deposit (known as a bond) will be slashed. The state roots from that transaction onward will be erased and the sequencer will have to recompute those lost state roots correctly this time.



OPTIMISTIC ROLLUP

<https://bridge.arbitrum.io/>



ARBITRUM

You can withdraw assets back to Ethereum Layer 1 through the [Arbitrum Bridge](#). The standard withdrawal process takes **at least 7 days** in order to allow sufficient time for verifiers to detect fraud on the Arbitrum network. Some third-party services offer faster withdrawal for a fee.

<https://app.optimism.io/bridge>



Optimism

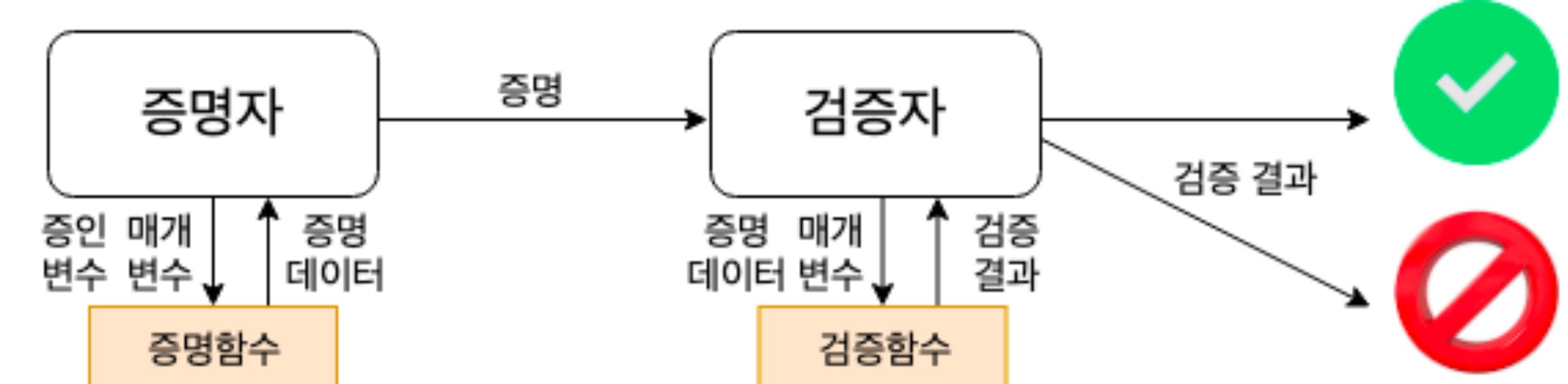
ZK-ROLLUP

이러한 아이디어를 바탕으로 이상한 나라의 마법사들은 상자 제작과 동시에 상자가 올바르게 제작되었음을 증명하는 기발한 마법[영지식증명]을 개발했습니다. 이 마법을 이용하면 보조 공장주가 상자를 위조하는 것 자체가 불가능했습니다. 잘못된 보조 상자는 마법이 걸리지 않았고, 이는 단번에 이상한 공장에서 알아챌 수 있었기 때문이었죠.

이를 가능하게 하는 것이 영지식증명(Zero-Knowledge Proof)을 활용한 zkRollup입니다. 영지식증명은 마치 마법과도 같아서 블록이 올바르게 제작되었음을 누구든지 확인할 수 있게 됩니다. 거래내역을 하나하나 일일히 확인하지 않고서도 말이죠!

하지만 마법은 언제나 막대한 에너지를 필요로 하죠. 앤리스의 나라에서도 마찬가지였습니다. 마법은 너무나 많은 에너지를 필요로 했기 때문에, 보조 상자에 포함된 거래가 조금이라도 복잡하거나 양이 많다면 마법을 거는데 막대한 시간이 걸렸습니다. 물론 비교적 단순한 거래활동들은 쉽게 마법으로 처리할 수 있었기 때문에 주로 단순한 송금들을 처리하는데는 뛰어난 성능을 발휘했습니다.

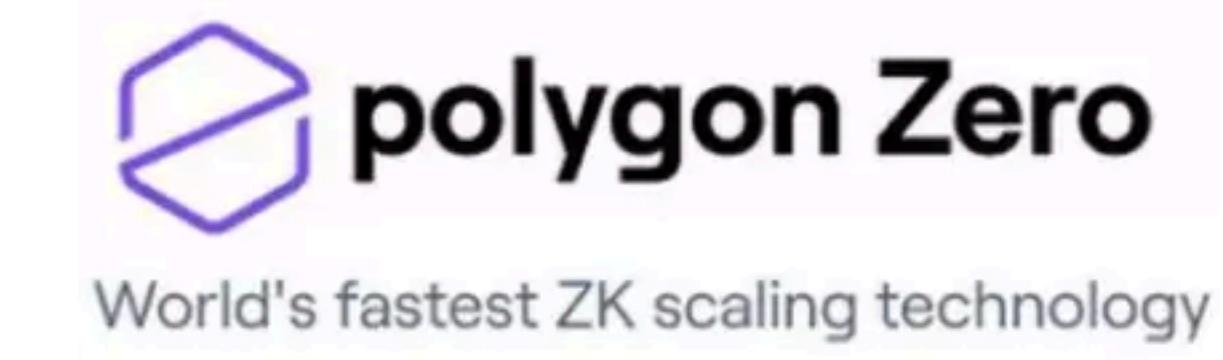
영지식증명은 복잡한 거래과정을 증명하는데에는 너무나 많은 시간을 필요로 하지만, 비교적 단순한 거래들은 손쉽게 증명이 가능합니다. 따라서 단순한 송금을 안전하게 처리하는데에는 안성맞춤이지만, 반대로 통상적인 이더리움의 트랜잭션들은 복잡도가 높기 때문에 현재 시점에서 zkRollup을 사용하는 것은 불가능합니다.



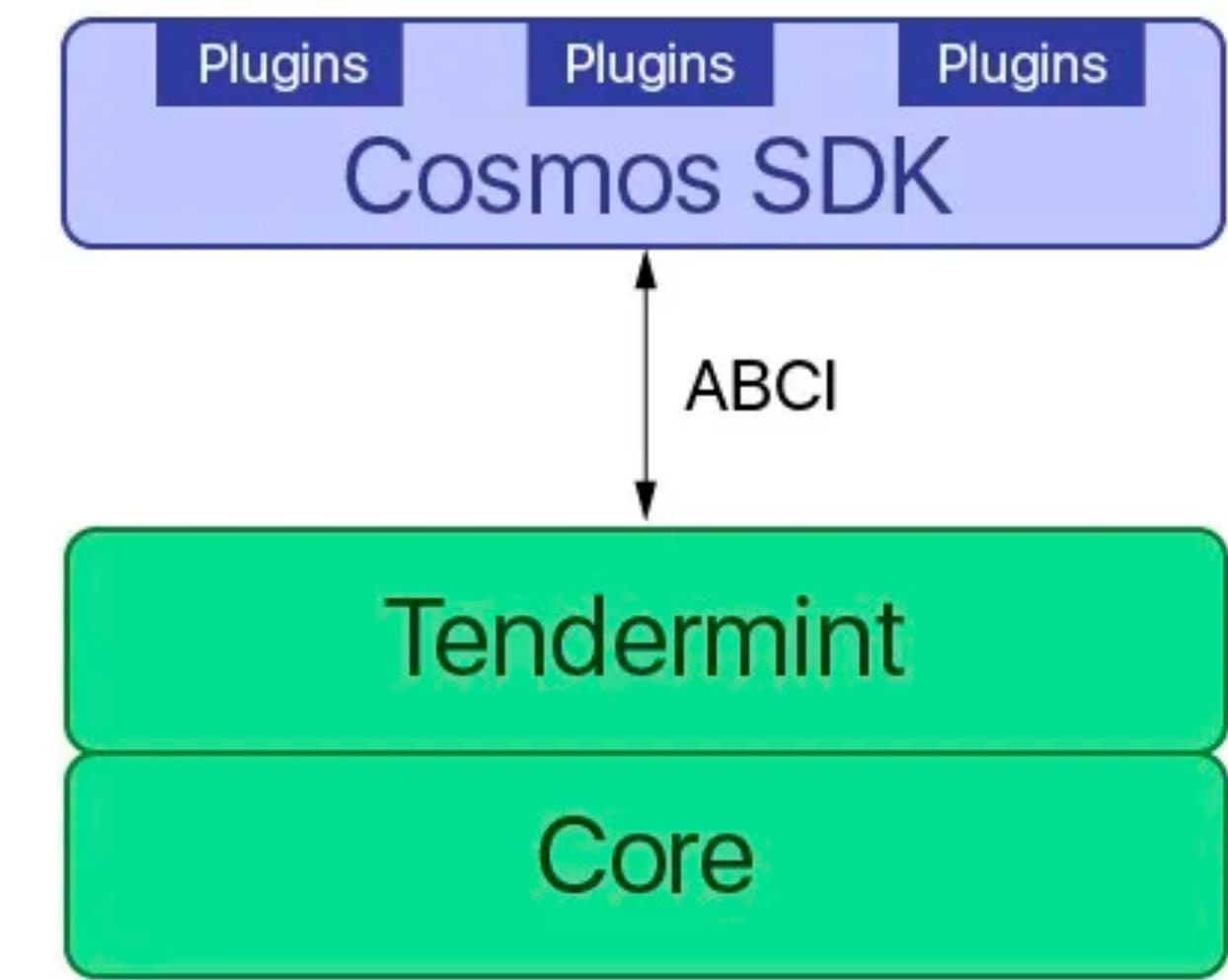
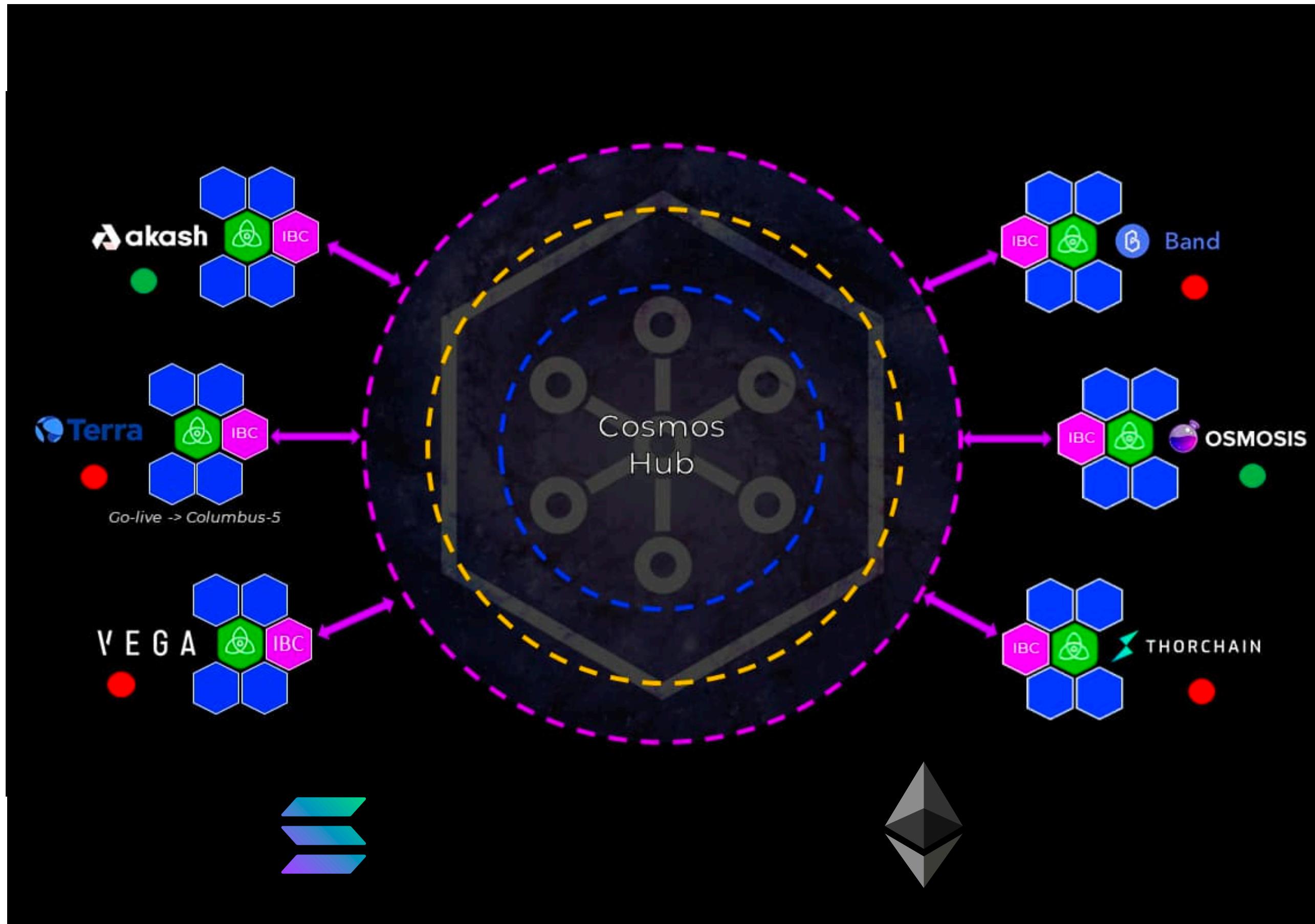
<https://wallet.zksync.io/>



<https://polygon.technology/solutions/polygon-zero/>

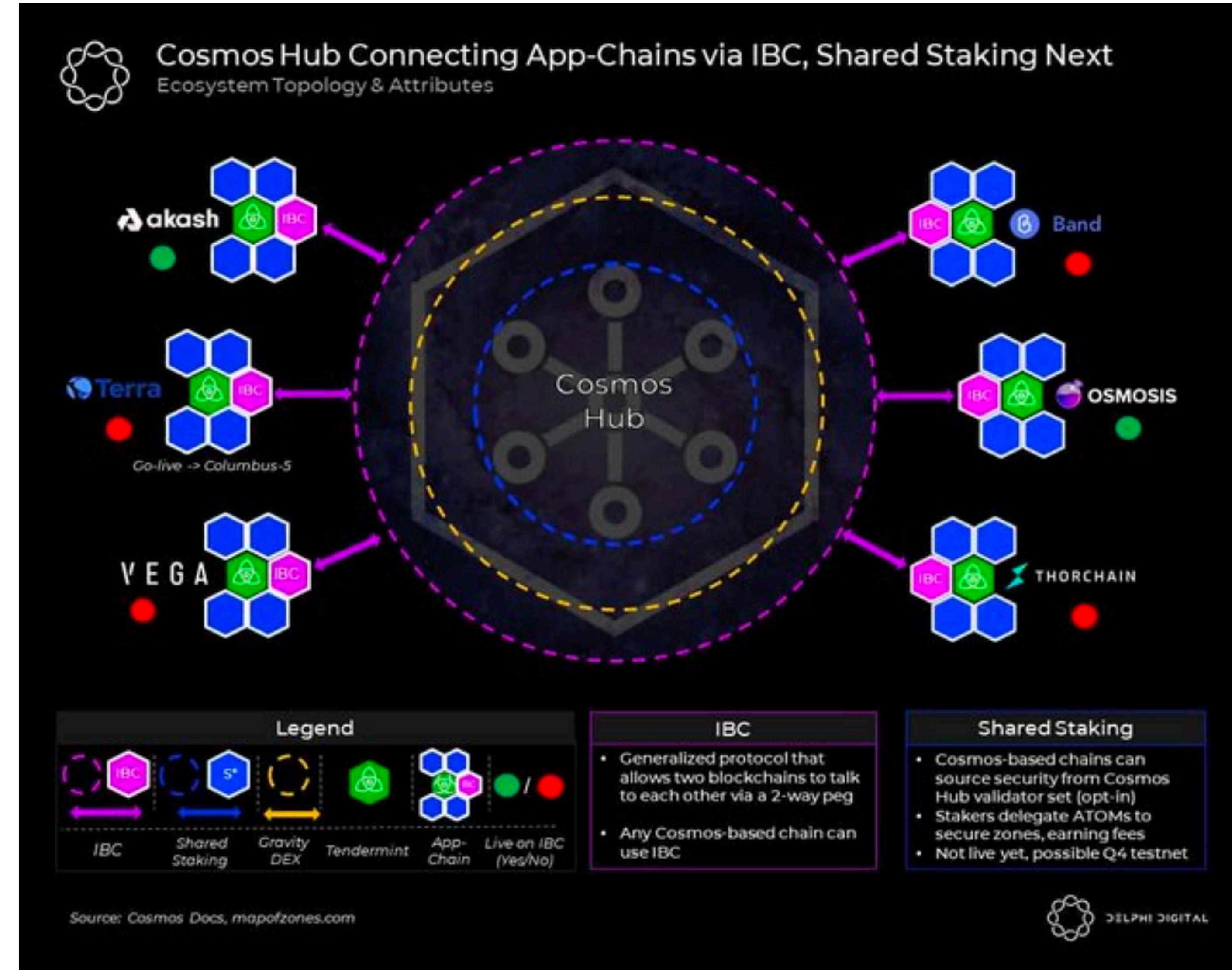


코스모스 진영: 여러 블록체인을 연결하자



Hub는 Tendermint로 만들어진 블록체인 “Zone” 간의 통신을 지원하고, “Zone” 별로 dApp (Smart Contract)를 따로 배포할 수 있다.

<https://mapofzones.com/>



<https://medium.com/a41-ventures/ecosystem-%EC%9D%B8%ED%84%B0%EC%B2%B4%EC%9D%B8%EC%9D%98-%EC%8B%9C%EB%8C%80%EB%8A%94-%EB%8F%84%EB%9E%98%ED%95%98%EB%8A%94%EA%B0%80-%EC%BD%94%EC%8A%A4%EB%AA%A8%EC%8A%A4-%EC%83%9D%ED%83%9C%EA%B3%84-%EC%86%8C%EA%B0%9C-b401e89ea799>

코스모스 기반 블록체인-이더리움 간 첫 NFT 전송

Posted: 2021-11-26

좋아요 0개



코스모스-SDK 기반 WenChang Chain과 이더리움 간 NFT 브릿지가 구축됐다고 유투데이가 보도 했다. 코스모스 트위터에 따르면 코스모스 소프트웨어 개발 키트는 4개 블록체인 네트워크 간 최초의 NFT 전송(travel)에 활용됐다. NFT 전송의 기반이 되는 기술은 TIBC(Terse Inter-Blockchain Communication protocol)로, IRIS Hub는 TIBC를 이더리움에 매끄럽게 연결한다. 이번 실험에 사용된 NFT는 이더리움 최대 NFT 마켓플레이스인 오픈씨(OpenSea)에서 판매된다. 미디어는 “이번 실험은 이더리움과 BSN(중국 국가 주도 블록체인 서비스 네트워크) 같은 무허가형, 허가형 블록체인을 연결하는 코스모스의 역할을 보여준다”고 설명했다.

– By CoinNess.com

<https://dstreet.io/blockchain/flash-news/2021/11/38491/>

- Zone(또는 App-chain): 우선 코스모스 생태계엔 Zone이라는 개념이 있는데. 쉽게 말해서 코스모스 생태계를 이루는 개별 블록체인들이다. 앱체인(App-chain)을 표현하는 또 다른 말이라고 볼 수도 있다. 이들은 모두 코스모스 SDK를 사용하여 각각의 블록체인을 구성하는데, 대표적인 예시로 테라(Terra)가 있다. 테라 말고도 현재 DEX 거래량 순위 2등을 기록하고 있는 오스모시스(Osmosis)도 코스모스SDK를 활용한 앱체인이며 Zone이다. 이들은 별도의 체인이기 때문에 별도의 벨리데이터들을 갖춰야 한다 (물론 추후 설명할 Shared Staking이 활성화 되면 좀 다른 양상을 띠긴 할 것이다).
- Hub: 허브도 Zone의 일종이지만, 다른 Zone들과 소통할 수 있는 여러 채널이 연결된 것이라고 볼 수 있다. 그런데 보통 허브라고 하면 우리는 코스모스 허브를 이야기 한다. 결국 Zone(앱체인)들이 코스모스 허브를 중심으로 연결돼서 서로 소통하는 구조를 형성하기 때문이고, 현재 Zone들과 소통할 수 있는 채널의 수도 코스모스가 제일 많다.
- IBC: IBC 역시 하나의 프로토콜로 이것을 통해 데이터들이 IBC에 연결된 각 체인으로 전달될 수 있다. 이론상으론 어떤 블록체인이든 IBC 프로토콜을 통해서 연결이 가능하다.

<https://evmos.org/>

Evmos



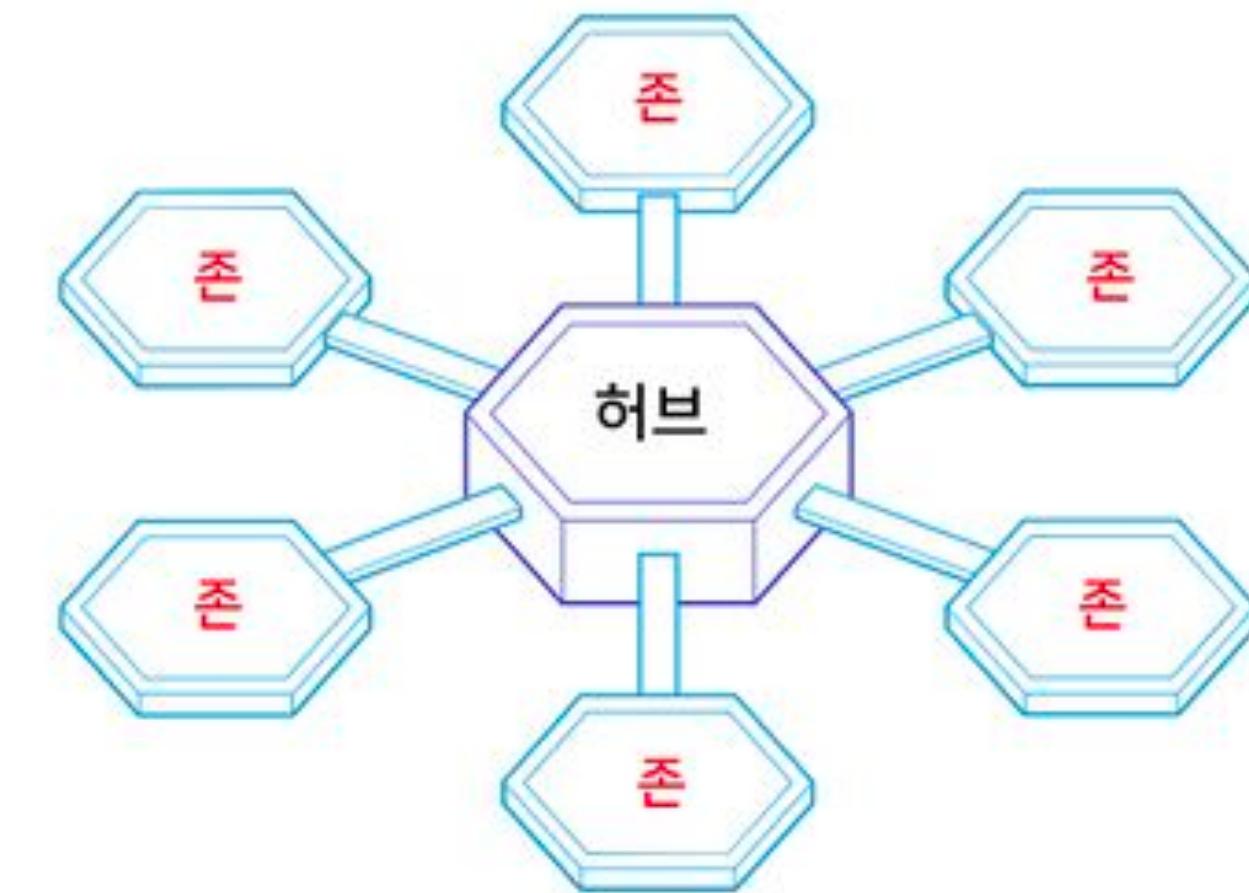
<https://scrt.network/>

<https://www.terra.money/>



<https://www.stargaze.zone/>

STARGAZE



<https://Obase.vc>

<https://wallet.keplr.app/#/dashboard>



사실 여느 레이어1 체인의 거버넌스 토큰과 비슷하게 ATOM은 두 가지 주요 기능을 가지고 있다.

1. 코스모스 허브의 보안: 기존 PoS 성향의 레이어1들과 같이 ATOM 토큰은 네트워크에 예치돼서 네트워크 자체에 보안성을 제공한다. 결국 네트워크를 지배하기 위해선 네트워크에 예치되어있는 ATOM을 지배해야하는 구조이기 때문에 ATOM의 가격이 비싸질수록, 또는 네트워크에 예치된 ATOM이 많아질수록 악의적 참여자가 네트워크를 지배할 수 있는 확률이 줄어들게 된다.
2. 코스모스 네트워크에 대한 거버넌스: 이 역시 기존 PoS 성향의 레이어1들과 같이 코스모스 네트워크가 발전하는데에 있어서 중요한 사안들을 결정할 수 있는 결정권이 ATOM을 스테이킹한 유저들에 한해서 부여가 되는 구조다.

이 외에도 ATOM을 매력적인 투자처로 느낄 수 있는 부분은, ATOM을 스테이킹해서 얻어가는 스테이킹 수익(스테이킹 수익은 자체적인 인플레이션 수익과, 트랜잭션에 대한 비용에서 발생하는 수익이 있다)과 더불어, 코스모스 SDK를 사용해서 만들어지는 새로운 체인들이 자신들의 토큰을 ATOM 스테이커에게 에어드롭을 해주기 때문에 스테이킹 자체만으로도 새로운 토큰에 대한 간접적인 투자가 가능하다는 부분들에 있다.

현재 코스모스 허브에 자체적으로 만들어진 DEX(탈중앙 거래소)인 Gravity DEX에서 발생하는 트랜잭션 비용도 ATOM 스테이커에게 돌아가고 있다. (물론 현재 코스모스 생태계 전체에서 거래량이 제일 높은 DEX는 오스모시스라는 별도의 Zone이다).

<https://emeris.com/>



<https://osmosis.zone/>



솔라나 진영: 속도도 빠르고, 수수료도 낮지만 중앙화된 블록체인

by  SOL mates	 Solana	 Ethereum	 Binance Smart Chain	 Polkadot	 Cardano	 Tron
Transaction per second	65,000	15	100	1000	270	1,000
Avg. Fee Per Transaction	\$0.0015	\$15	\$0.01	\$1	\$0.25	free
Transaction latency	0.4 sec	~5 min	75 sec	2 min	10 min	3 sec
Number of Validators	702	11,000+	21	297	2,376	27
Total Transactions to date	15 Billion	1.07 Billion	227 Million	1.7 Million	5.9 Million	1.7 Billion

블록체인	솔라나	이더리움2.0
HW 최소 요구사항	<ul style="list-style-type: none"> CPU with 16 cores / 32 threads RAM 256GB 4TB disk space 최첨단 GPU 권장 	<ul style="list-style-type: none"> CPU with 2 cores SSD: 4GB RAM (HDD: 8GB RAM) 8 Mbit/s bandwidth
최소 스테이킹 수량	<ul style="list-style-type: none"> 0.027 SOL 다만, 트랜잭션 투표 비용으로 매일 최대 1.1SOL이 소모될 수 있음 (1년 기준 71,000 달러, 2021.12.05 기준) 	<ul style="list-style-type: none"> 32 ETH (2021. 12.05 기준 134,000 달러)



<https://www.fractal.is/>

<https://magiceden.io/>



비트코인이나 이더리움을 보면 알 수 있듯이 높은 트랜잭션 수수료는 그것을 감당하지 못하는 유저들을 반강제적으로 이탈시킨다는 단점이 있지만, 반대로 너무 낮아도 똑같이 문제는 있다. **트랜잭션 수수료가 너무 낮으면 DDoS 공격에 취약하고, 이는 곧 네트워크 셧다운으로 이어질 수 있기 때문이다.** 가스비가 매우 높은 이더리움에서는 상상도 못하겠지만, 트랜잭션 당 수수료가 \$0.0001~\$0.01 수준인 L1 블록체인(솔라나)에서는 충분히 가능한 일이다. 솔라나 입장에서 이러한 문제를 해결할 수 있는 현실적인 방법은 두 가지다.





AVALANCHE

APTOOS



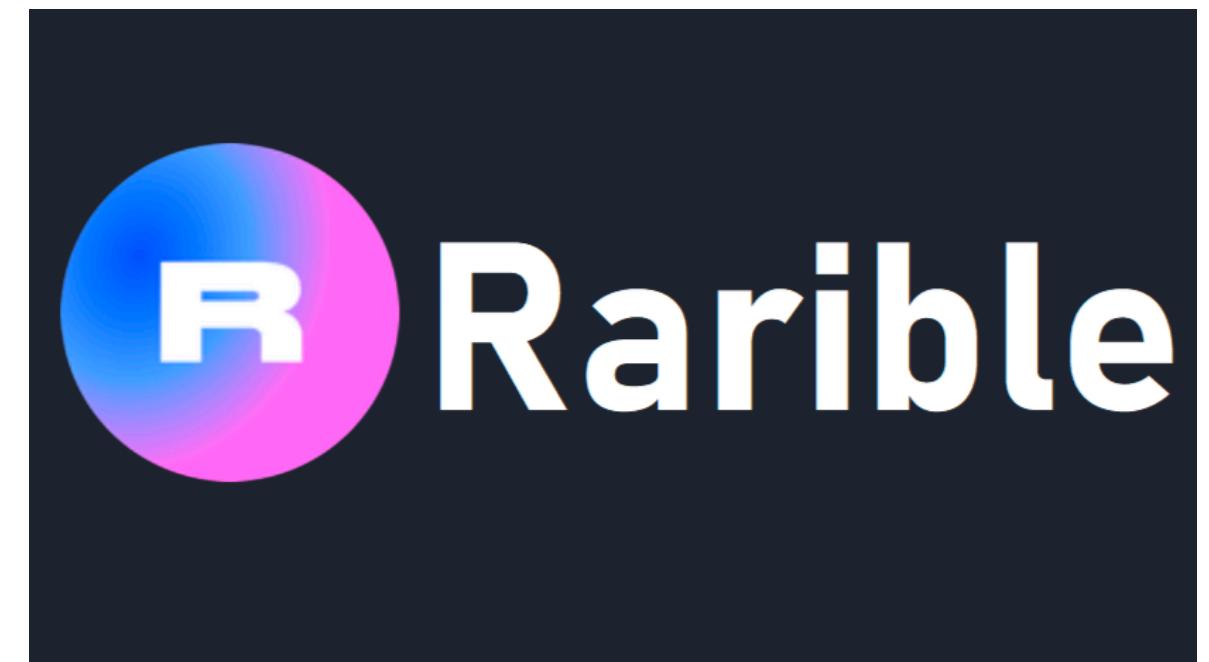
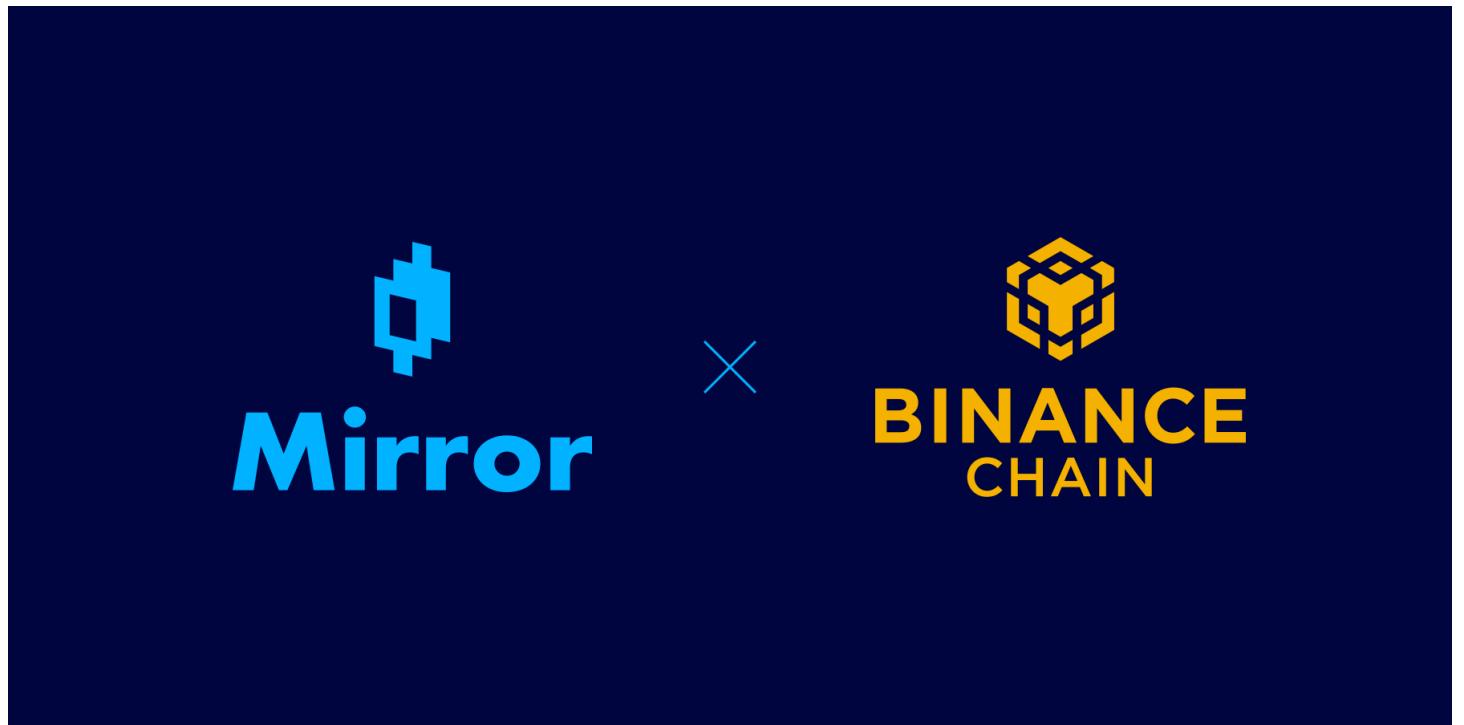
N NEAR



and many more...

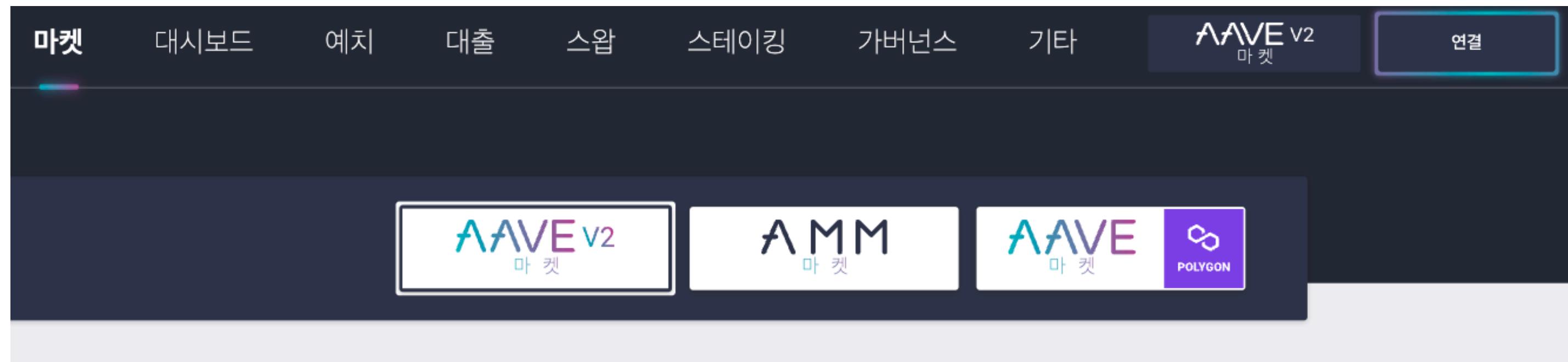
Interoperability unlocks innovation

- 블록체인 별로 강점이 있는 지역이 있고, 디앱 서비스가 존재
- 예: Klaytn – 한국, Astar – 일본 / Terra – DeFi, Flow – Sports NFT
- 상호운용성을 확보하여 이종 간의 블록체인 내부에 존재하는 토큰 간의 상호 작용 촉진 필요성
- ex) Sending DAI to Terra to buy a synthetic asset on Mirror, or earn yield on Anchor
- ex) Sending a TopShot from Flow to Ethereum to use as collateral on NFTfi
- ex) Using DOT and ATOM as collateral to take out a DAI loan on Maker
- ex) Cross-chain shared order books for NFTs on Ethereum and Flow for Rarible Protocol
- ex) Pay for storage on Arweave using Bitcoin or UST



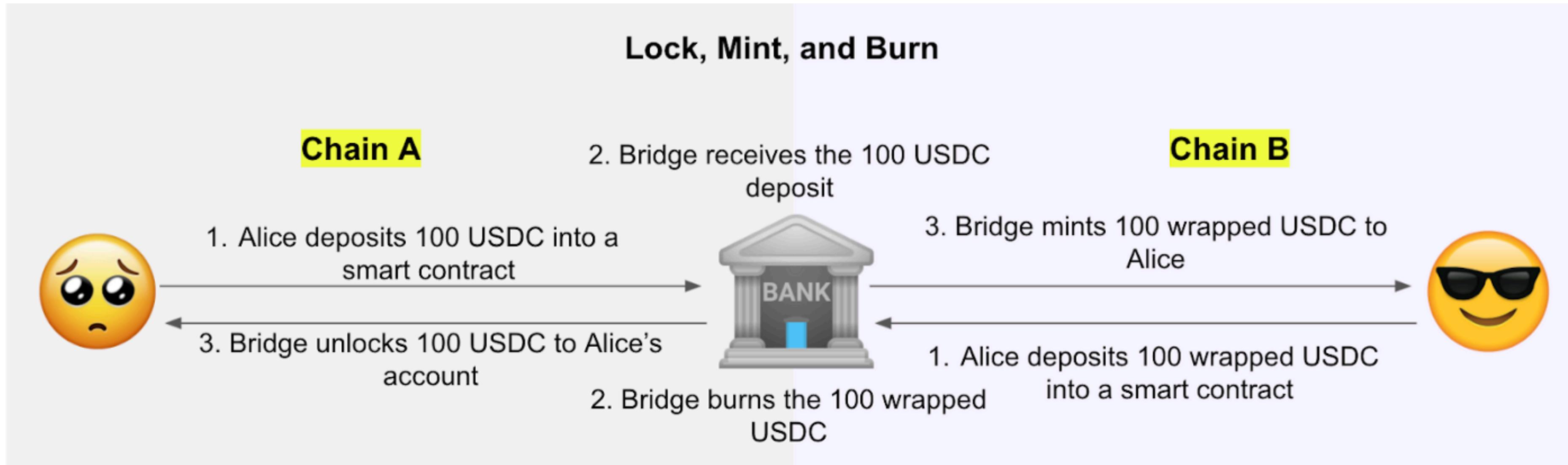
멀티체인 vs 크로스체인

- 멀티체인이란, 용어 그대로 여러개의 블록체인을 의미
- 멀티체인 디앱이라고 함은 최소 둘 이상의 체인 상에서 구동되고 있는 디앱
- 예: Ethereum 메인체인과 Polygon Layer 2 체인에서 모두 서비스되고 있는 대출 서비스 아베
- 예: 이더리움, 폴리곤 뿐 아니라 BSC, 문빔 네트워크, 팬텀 등에도 서비스하는 스시스왑

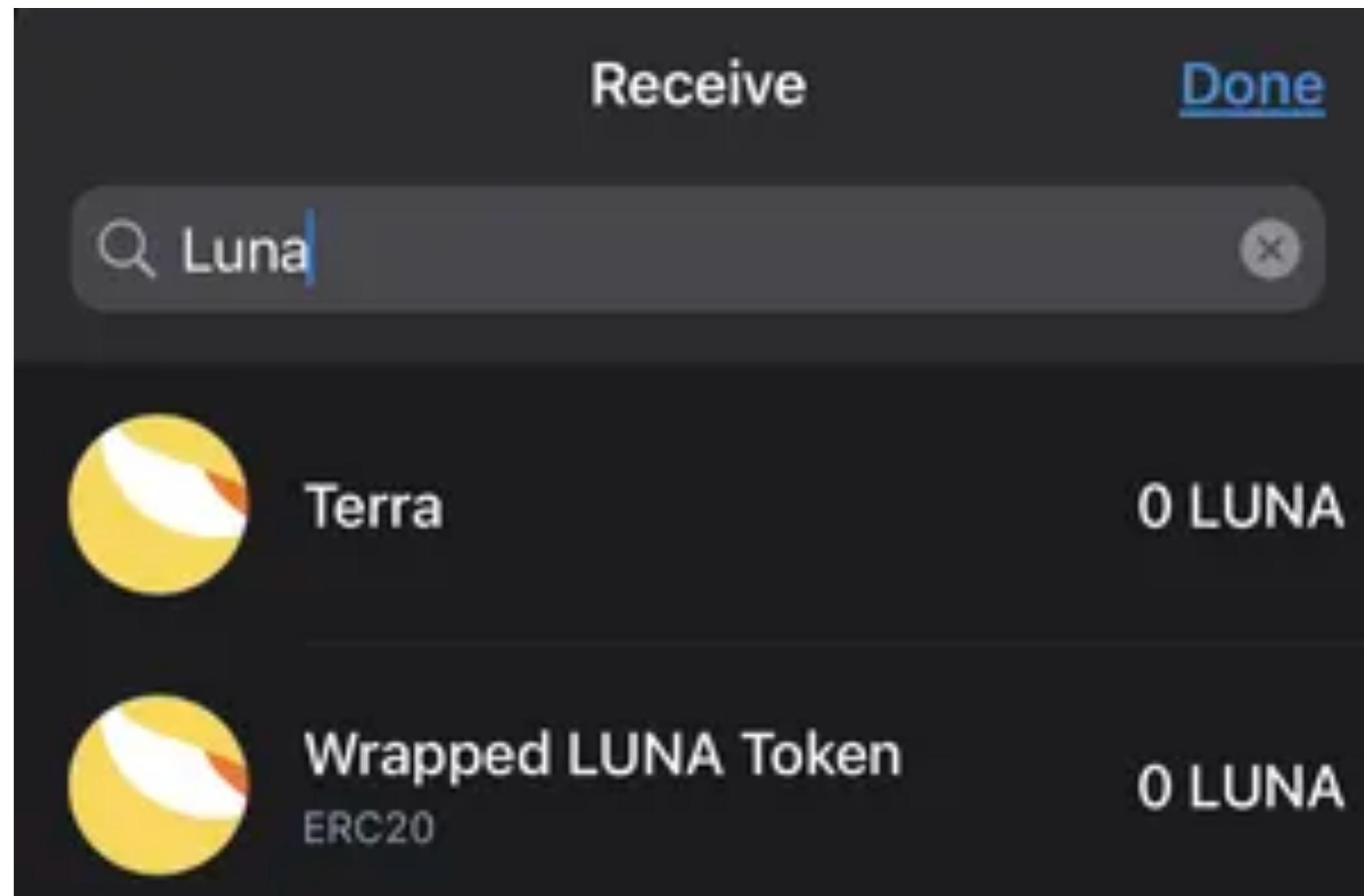


멀티체인 vs 크로스체인

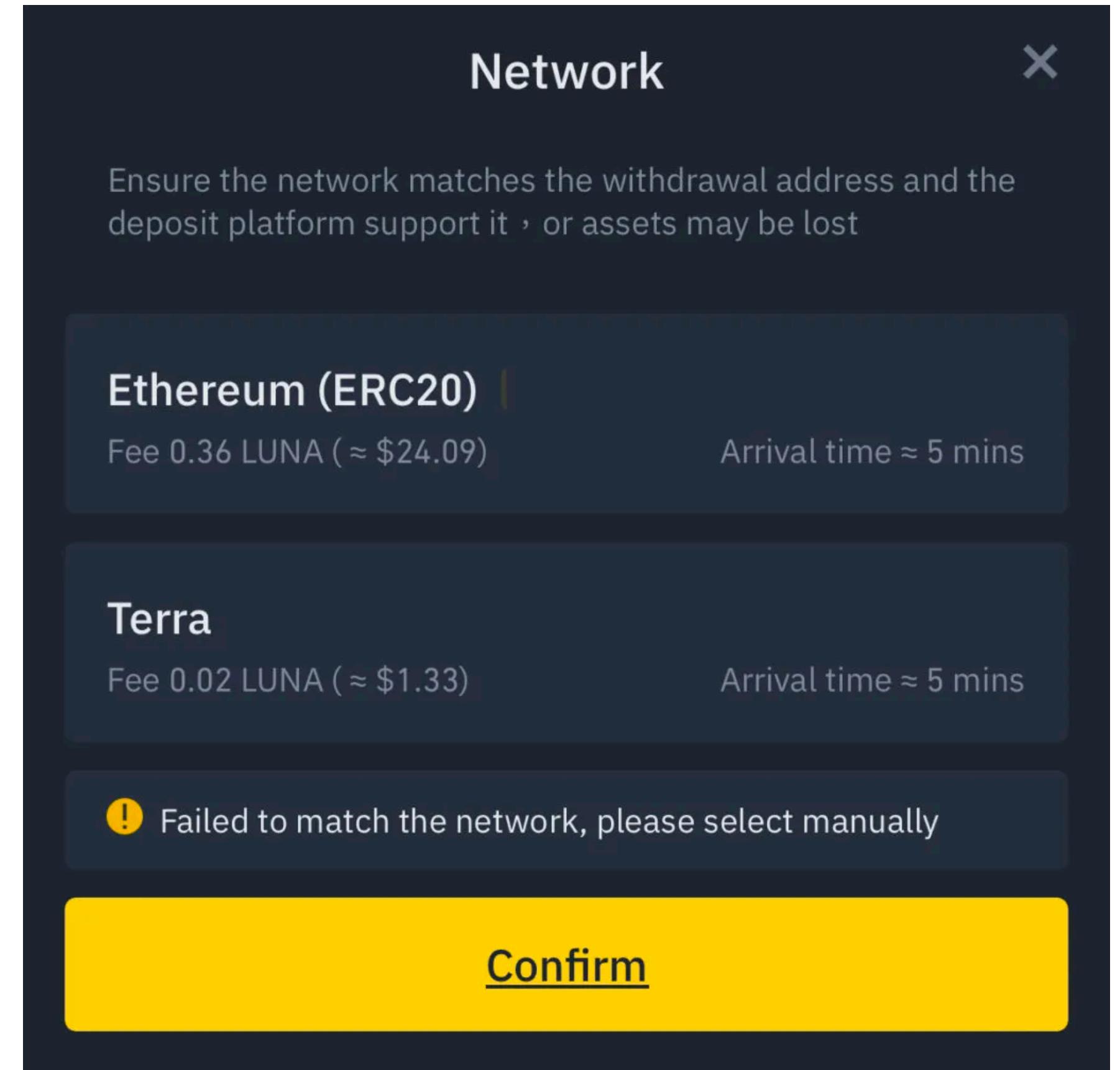
- 크로스체인: 자산을 다른 체인으로 전송하여 체인 간의 결합 발생 솔루션 – **Bridge!**



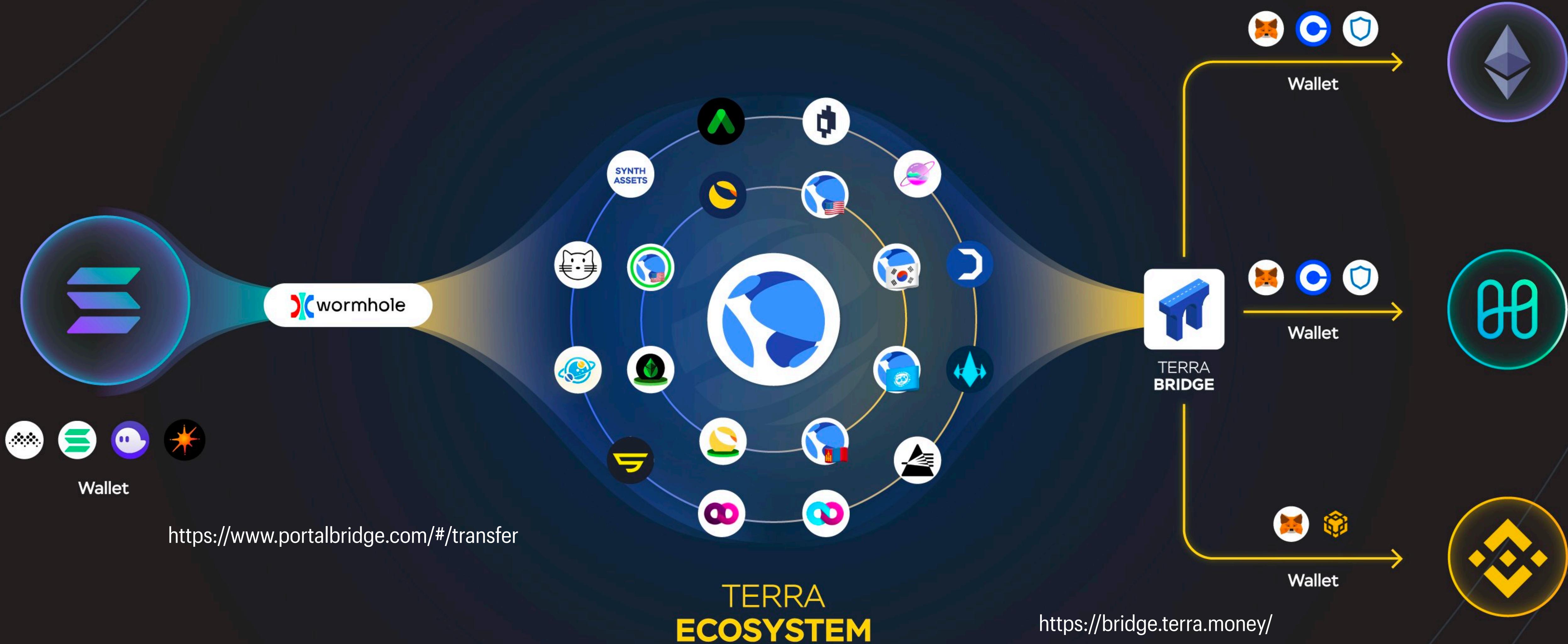
ERC20 토큰 vs 메인체인 코인



[Wrapped LUNA at Ethereum](#)



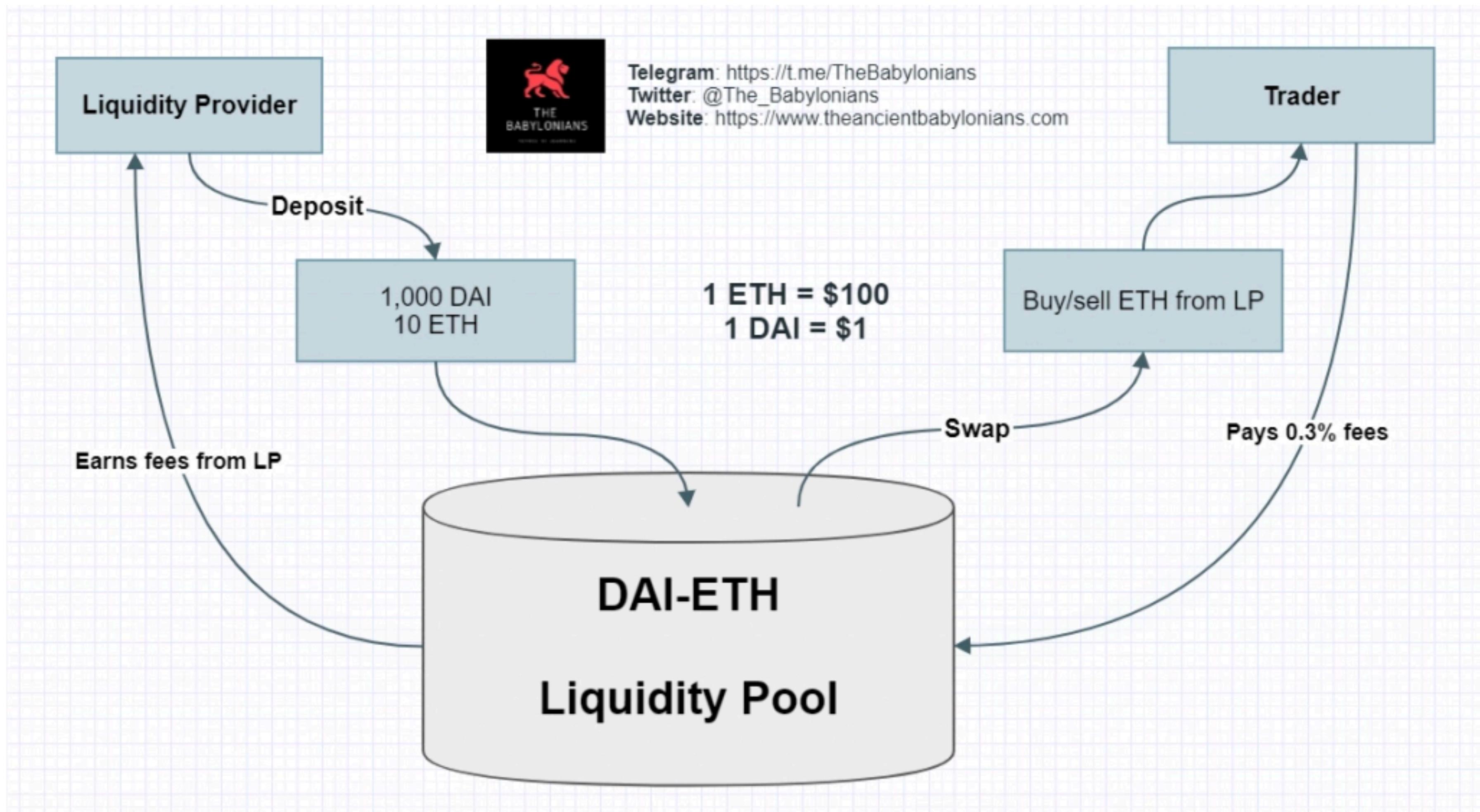
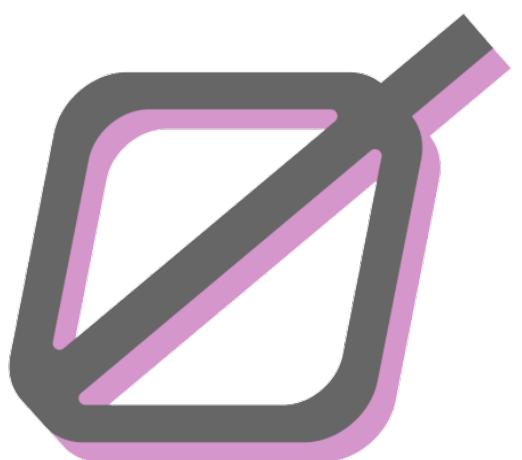
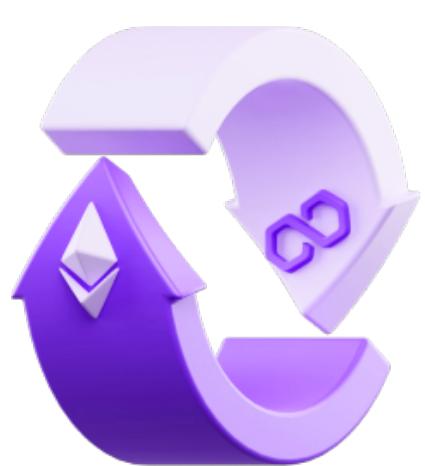
CROSS-CHAIN BRIDGES BETWEEN TERRA AND OTHER BLOCKCHAINS

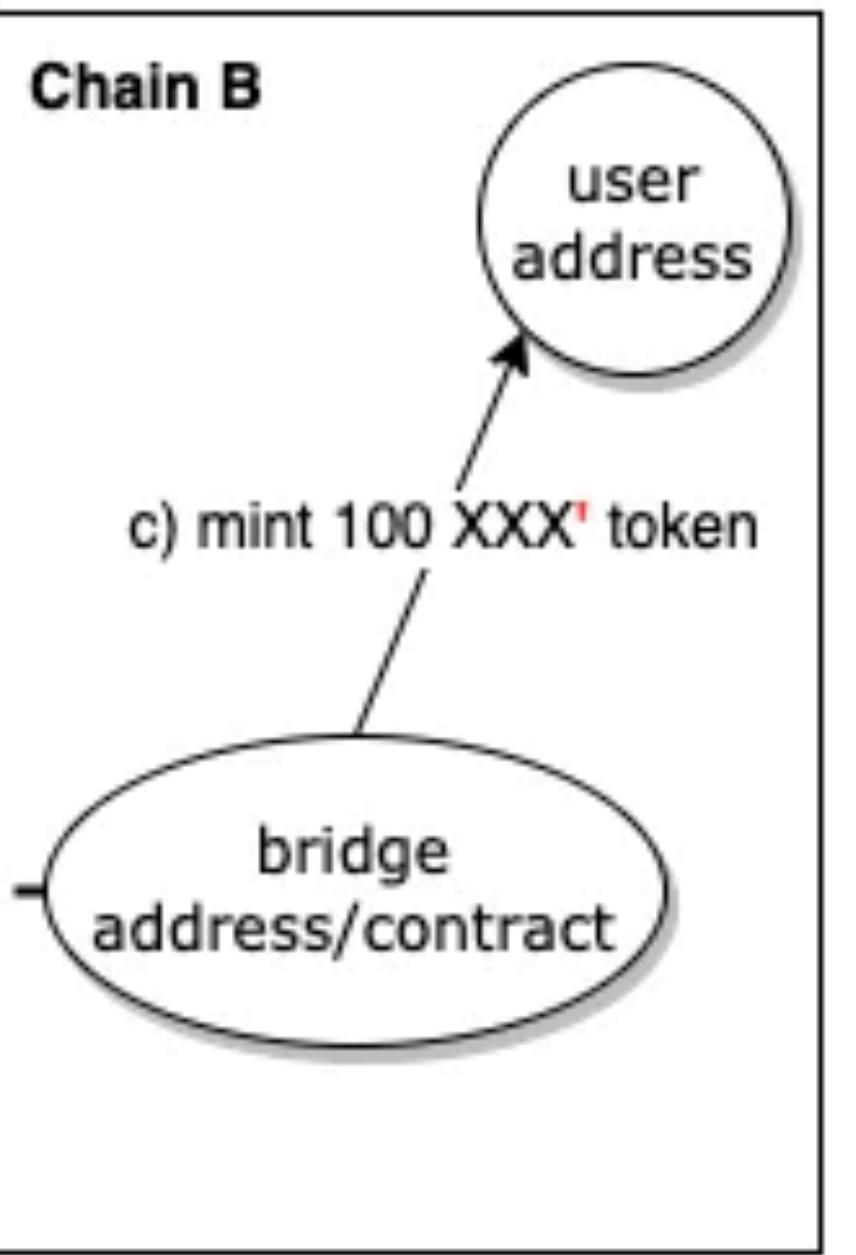
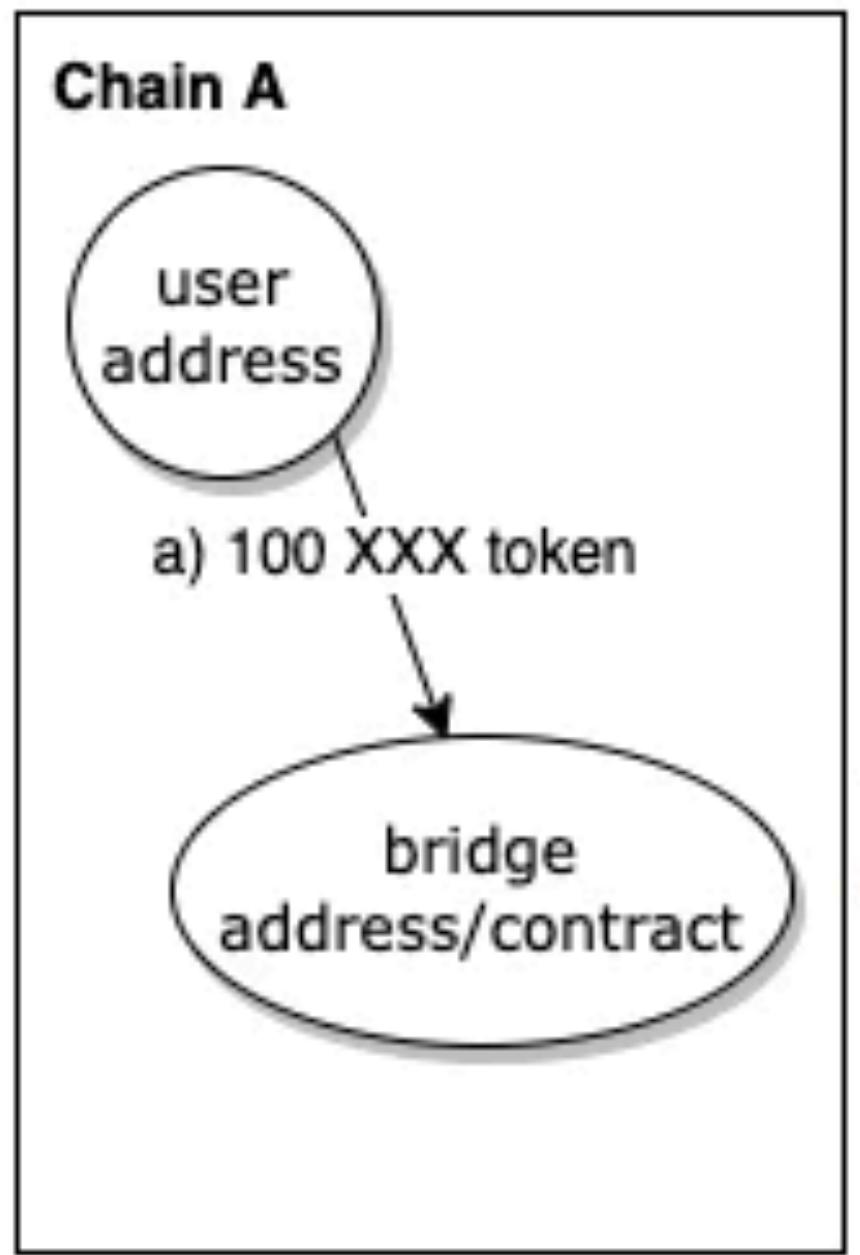


Interoperability is a King

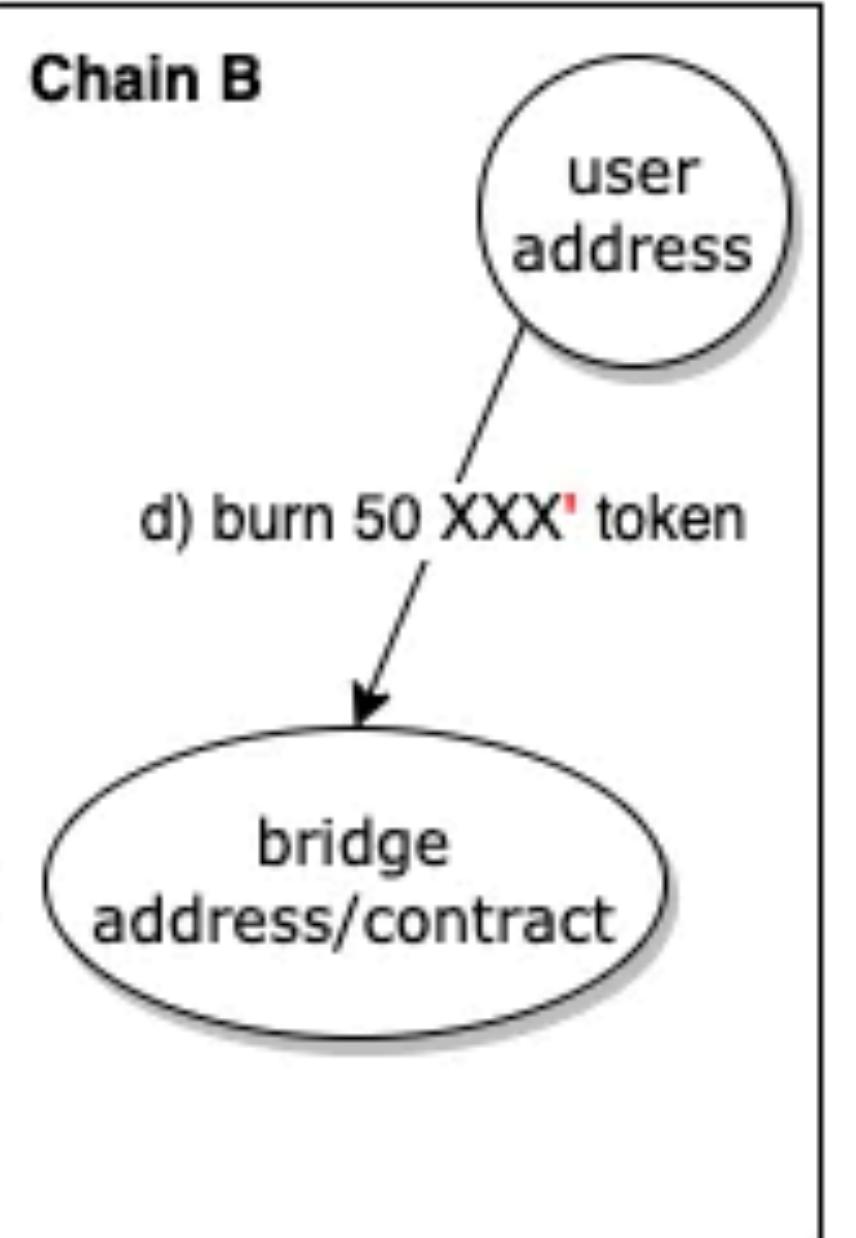
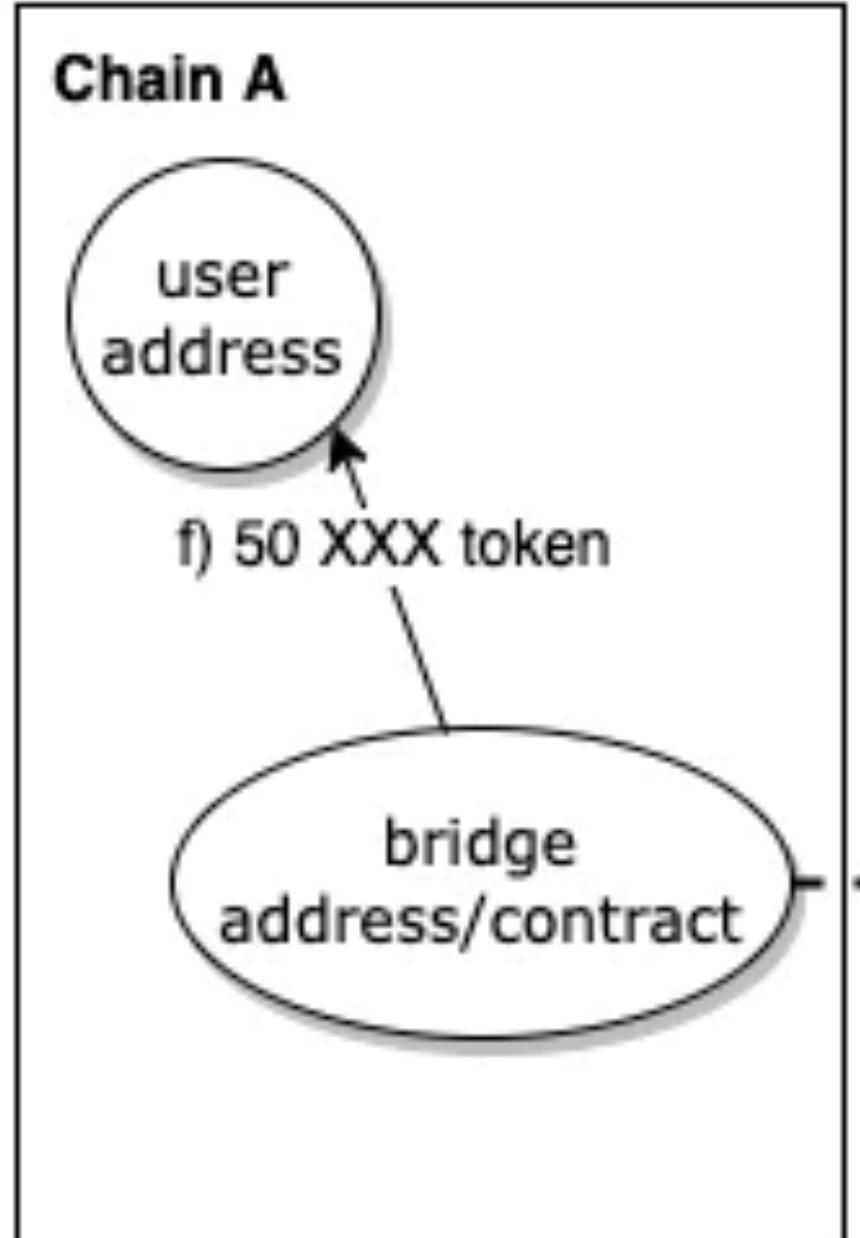
멀티체인 세상에서 상호운용성이 중요하다

- 유동성 파편화로 인한 가격 탐색의 비효율성
 - Ethereum의 경우 확장성 문제를 해결하기 위해 유동성을 Layer 2로 분리
 - Layer 2로 자산 유동성이 분산되다 보니 Layer 2 간의 자산 가격 불균형이 문제됨
 - 멀티체인의 시대가 도래하여 점점 더 많은 체인으로 분기되면 유동성이 얇은 거래 풀의 경우 DEX 간의 가격 불균형이 필연적으로 일어나게 됨
 - 부작용은 같은 종류의 LP pool임에도 불구하고 여러 AMM에 나뉨에 따라서 슬리피지 가 커지는 등의 문제 (해결책: <https://li.fi/>)





- a) 보내는 체인의 토큰을 브리지 주소로 전송합니다. 이 브리지 주소는 보통 스마트 컨트랙트 주소입니다. 브리지 주소로 전송한 토큰은 잠겨서 당분간 풀리지 않습니다.
- b) 브릿지는 토큰이 잠겼는지 확인합니다.
- c) 받는 체인에서 동일한 양의 토큰을 새로 발행합니다(mint). 이더리움에서 100 테더를 브리지 주소로 전송하여 잠그면, 솔라나에서 100 테더를 새로 발행하는 셈입니다.



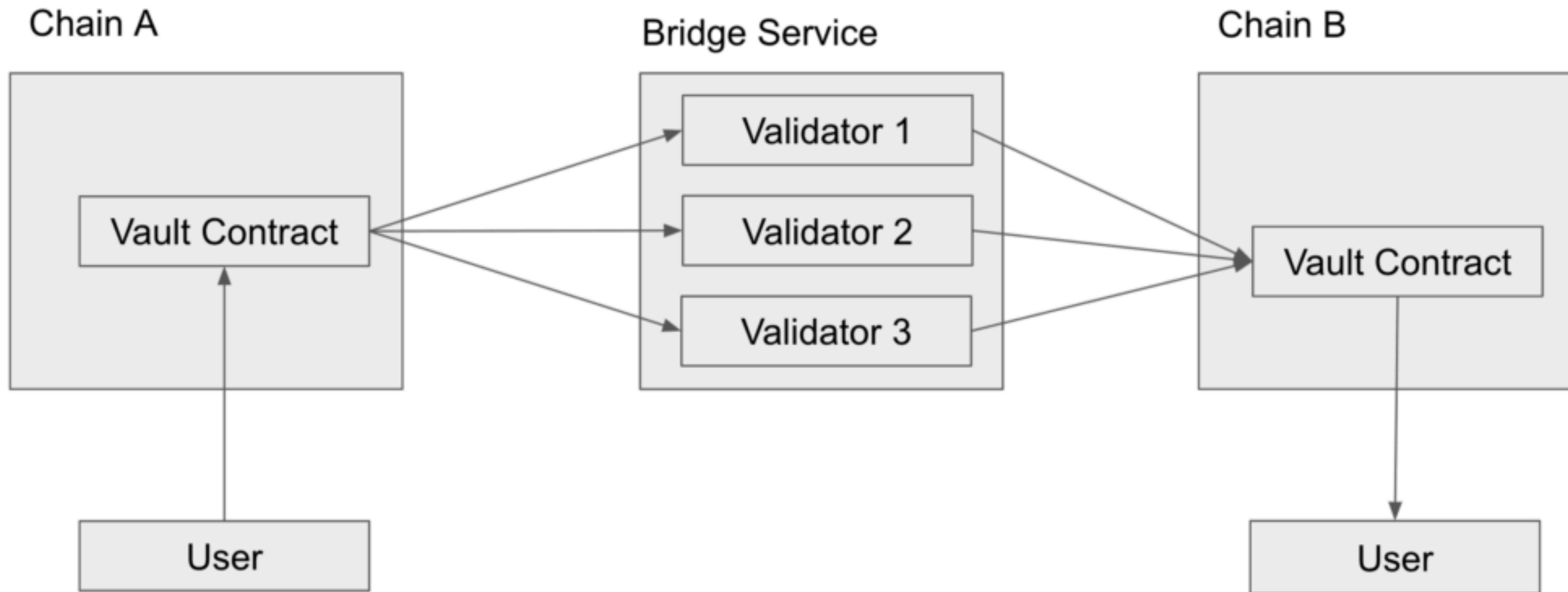
- a) 브리지로 이동한 토큰을 반대로 가져올 수도 있습니다.
- b) 받은 체인에서 토큰을 브리지 주소로 다시 전송하면, 토큰을 소각합니다(burn).
- c) 토큰을 소각했는지 확인한 후, 보내는 체인에 잠긴 토큰을 동일한 양만큼 풁니다. 솔라나에서 50 테더를 반환하면 토큰을 소각하고, 이더리움에 잠긴 50 테더를 인출할 수 있게 됩니다.

API Server that syncs & monitors blocks

NEAR 레인보우 브리지 같은 무신뢰(trustless) 브리지

<https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8>

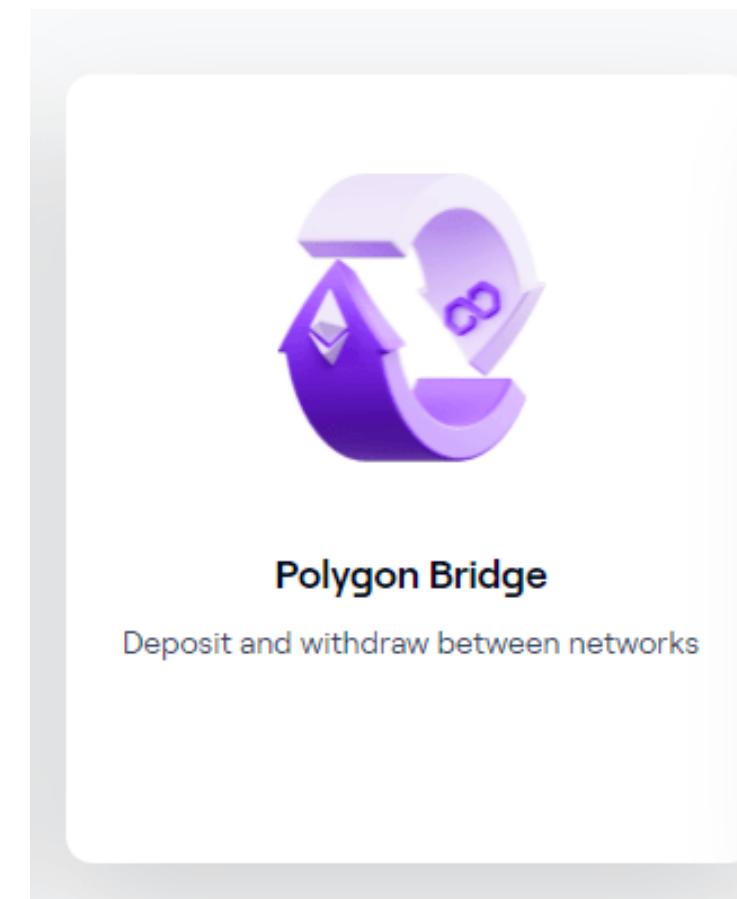
Validating with validators



먼저 외부의 다수의 validator가 트랜잭션을 검증해 주는 방식이 있다. 이 과정에서 브릿지 자체 서비스에 있는 토큰을 보상으로 주며 공개적으로 검증자들을 모집하거나, 신뢰 있는 기관을 검증자로 두어서 유저가 선택하게 하는 등 다양한 방법이 존재한다. 위와 같이 유저가 브릿지를 이용하면 Validator 끼리 체인 밖의 브릿지 서비스에서 따로 검증을 하게 된다. 검증이 끝난 validator는 Chain B의 컨트랙트에 트랜잭션이 문제가 없음을 확인하고 Chain B의 컨트랙트를 통해 유저에게 mint를 해준다. 이러한 방법은 브릿지 서비스마다 모두 다르며 validator에게 보상을 지급하는 방법도 모두 다르지만 오프 체인에서 외부 validator들이 검증을 해준다는 점에서는 다수의 브릿지가 이와 같은 모델을 가지고 있다.

On the whole, third-party cross-chain bridges are faster than official bridges, and there is no 7-day waiting period to withdraw assets from L2 to L1. That said, users need to pay extra to the market makers or protocols that provide cross-chain asset liquidity. This helps discount the time value of assets, reducing the potential loss caused by the 7-day vacancy.

<https://wallet.polygon.technology/>



<https://bridge.umbria.network/>



<https://hackernoon.com/understanding-cross-chain-bridges-under-a-multi-chain-background>



Klayswap

Swap

Pool

Stake & Boost

Dashboard

Learn

Asset

0x420...c887



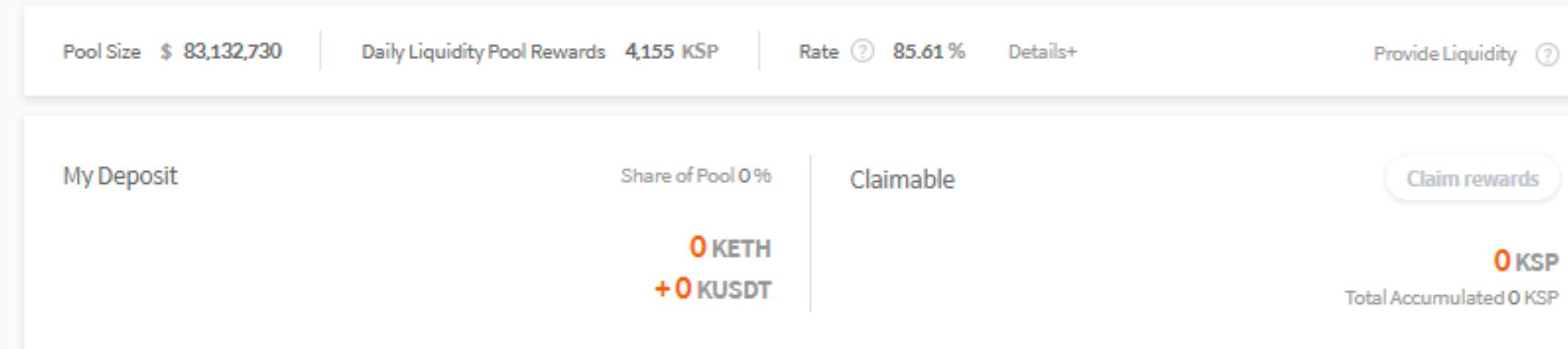
< Back



Ethereum+Tether

Rate

85.61 %



Deposit Withdraw

Assets available for deposit

KETH+KUSDT KETH KUSDT

0 Balance 0.049950 max

0 Balance 0 Deposit Trade

KETH + KUSDT

Deposit

<https://medium.com/klayswap/%EC%9D%B4%EC%A2%85%EC%B2%B4%EC%9D%B8-%EC%9E%90%EC%82%B0%EC%9D%98-%EC%9C%A0%EB%8F%99%EC%84%B1-%EA%B3%B5%EA%B8%89%EB%B0%A9%EB%B2%95-aac5c26b127b>

Orbit Bridge Validators

15 VALIDATORS ACT AS A SAFETY VALVE FOR THE ORBIT BRIDGE.

B-Harvest

B-Harvest provides validation services for multiple dPoS networks and is actively engaging in decentralized governance. Below is the list of networks we are taking part in as validators.

CØSMOSTATION

Cosmostation is an ecosystem leading, highly-secure validator node operator trusted on 35+ networks and chosen by users worldwide.

DSRV.

DSRV is a leading blockchain infrastructure company based in Seoul, South Korea. Our mission is to spearhead the industry's sustainable growth, and in doing so, provide an access point for all.

everstake

Everstake is the biggest decentralized staking provider in the blockchain industry, trusted by 625,000 users.

GBV

GBV Capital is dedicated to the investment, development, and the creation of blockchain projects to shape our future. We aspire to build projects that effect positive change and advance meaningful solutions.

hashQuark

HashQuark provides the most secure, stable and convenient enterprise-level staking services. We have completed the global server deployment and all mainstream PoS blockchains are supported.

iCQN

ICON is a public blockchain protocol building a hyperconnected future with BTP, our chain-agnostic interoperability solution.

GROUND X

Ground X erases the boundaries of digital assets with blockchain and is reliable. We provide the safest and most reliable digital asset experience that anyone can accept, regardless of generation and culture.

NODE A TEAM

Node A-Team is a Top-tier validator based in South Korea with an impressive record of winning awards for its validation services.

Validator Capital

Validator Capital was formed for the purpose of investing in the Celo blockchain ecosystem. We manage a validator group, are a certified Master Validator, and provide price stability for Celo stablecoins.

Huobi Pool

Huobi Pool handles PoW/Staking mining. With many public chain nodes and as the largest staking pool and leading PoW pool, Huobi Pool is devoted to providing one-stop financial services to all the digital users.

Ozys

Ozys' blockchain technology is driving change in various industries and businesses. They are leading changes in the world and presenting innovation.

Stake Bowl

Stake Bowl is a professional crypto operation brand that works toward the vision of maximizing the blockchain value in various areas ranging from node operation to digital asset storage and investment.

KRACKER LABS

Kracker is a team dedicated to promote DeFi business on Klaytn ecosystem with a strong partnership with both Krust and Klaytn Foundation.

AhnLab

AhnLab Provides Industry-Leading Security Solutions and Services through Continuous Development and Differentiated Technology.



Incentivized Pools



Trade



Pools



LBP



Airdrop



Assets



Stake



Vote

**Pool #1**

ATOM/OSMO

APY
1,034.53%Pool Liquidity
\$18,028,921**Pool #2**

ION/OSMO

APY
647.15%Pool Liquidity
\$2,305,667**Pool #3**

AKT/OSMO

APY
1,713.51%Pool Liquidity
\$5,442,499**Pool #4**

AKT/ATOM

APY
1,195.51%Pool Liquidity
\$7,800,638**Pool #5**

DVPN/OSMO

APY
2,181.51%Pool Liquidity
\$2,564,950**Pool #6**

ATOM/DVPN

APY
1,990.53%Pool Liquidity
\$2,811,040**Pool #7**

IRIS/OSMO

APY
1,934.23%Pool Liquidity
\$771,432**Pool #8**

ATOM/IRIS

APY
898.01%Pool Liquidity
\$1,661,578**Pool #9**

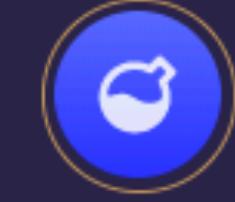
CRO/OSMO

APY
2,004.17%Pool Liquidity
\$744,512**Pool #10**

ATOM/CRO

APY
819.39%Pool Liquidity
\$1,821,013**Pool #13**

ATOM/XPRT

APY
1,285.06%Pool Liquidity
\$5,805,671**Pool #15**

XPRT/OSMO

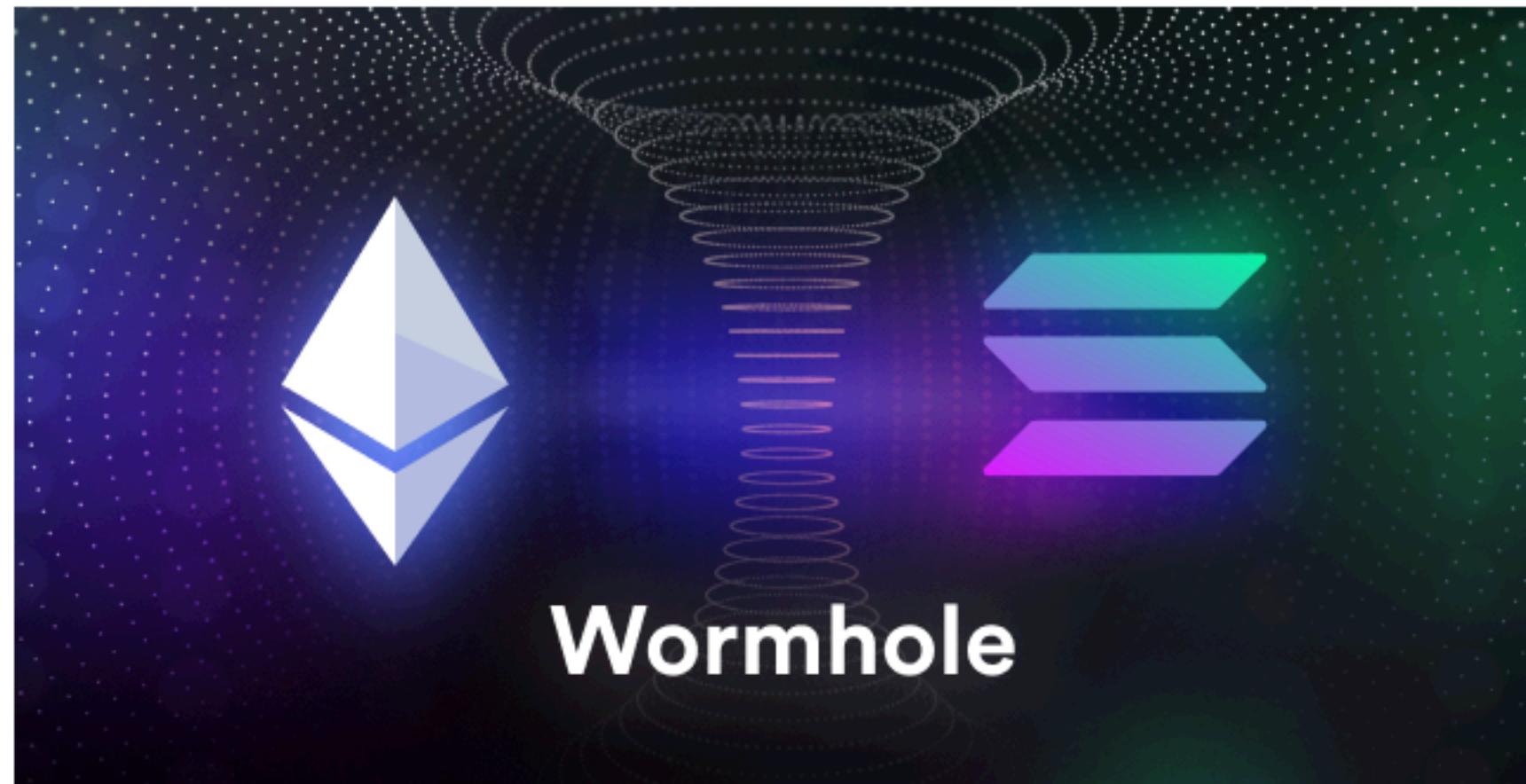
APY
2,139.63%Pool Liquidity
\$3,486,880

솔라나운영 웜홀, 3900억원 해킹···역대 네번째 규모



박범수

© 2022년 2월3일 12:14



출처=솔라나 랩스

솔라나 랩스(Solana Labs)의 크로스 체인 브릿지 서비스인 웜홀(Wormhole)이 3억2400만달러(약 3900억 원) 규모의 자금을 해킹 당했다.

웜홀은 이더리움, 솔라나, 바이낸스 스마트 체인(BSC), 테라 등 서로 다른 블록체인 상의 가상자산 거래를 가능하게 해주는 서비스다.

웜홀은 해킹 가능성으로 인해 네트워크를 일시중단한다고 2일(현지시간) [트윗](#)을 통해 밝혔다.

약 2시간 뒤 웜홀은 “웜홀 네트워크가 12만개의 wETH(랩이더리움)을 탈취 당했다”고 발표했다.

Data Has A Better Idea

Read Post

HIVERY

Open

Most Popular

- [트윗시황] "올여름 알트코인 시즌이 온다"
- "한국 가상자산 시장규모 1000조원, 4만명 고용"···윤석열 정부 의지 있나
- 비트코인, 큰 변동성이 다가오고 있다
- 윤창현 의원 "새 정부 가상자산 정책 뼈대 갖춰졌다"
- "스테픈 다운로드 금지되면, 150만원 운동화 없어지나요?"

작은 미션: DEFI 체험하기

1. (POLYGON) MATIC을 UNISWAP에서 테라 블록체인의 WRAPPED LUNA로 스왑하세요. (단, 이 때 수수료 지불할 MATIC 을 남겨야 합니다.)
2. (POLYGON -> TERRA - 1) WRAPPED LUNA를 TERRA BRIDGE ([HTTPS://BRIDGE.TERRA.MONEY/](https://BRIDGE.TERRA.MONEY/)) 에서
3. (POLYGON -> TERRA - 2) TOKEN BRIDGE에서 REDEEM TOKEN을 합니다. (그냥 기다려도 들어오긴 하는데, 시간이 20 분 걸립니다.)
4. (TERRA -> OSMOSIS) LUNA를 OSMOSIS 블록체인으로 TERRA BRIDGE를 활용하여 보내세요.
5. (OSMOSIS) OSMOSIS에서 WRAPPED LUNA를 OSMO로 절반만 (50%) 바꾸세요.
6. (OSMOSIS) KEPLR WALLET에서 OSMO를 스테이킹하거나, LUNA-OSMO 풀에 넣어서 LP 공급자가 되어 보세요.

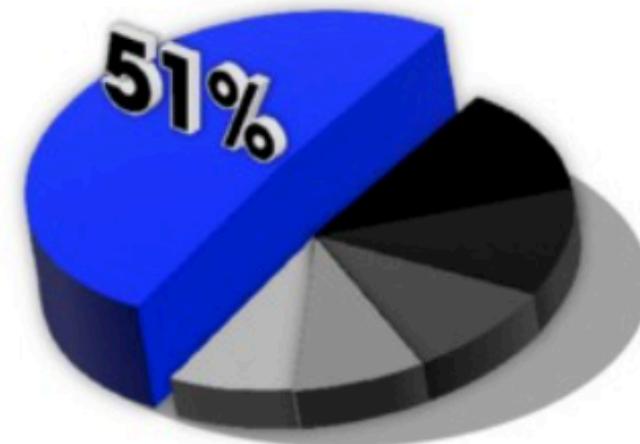
현재 비트코인에서 사용하는 합의 알고리즘인 PoW(Proof of Work, 작업증명, 이하 PoW)에서는 노드들의 컴퓨팅파워인 해시파워를 통한 경쟁으로 블록을 생성하고 블록이 가장 많이 연결된 체인을 정식체인으로 합의합니다. 노드들은 서로 경쟁을 통해 블록을 생성하고 인센티브를 받기 때문에 악의적인 공격이 실패하게되면 그동안 받을 수 있었던 인센티브에 대한 기회비용과 경쟁을 위해 소모한 전기 비용이 패널티로서 작용하게 됩니다. 하지만 악의적인 노드가 해시파워의 51% 이상을 장악하게 된다면 블록을 생성할 확률이 증가하여 유효하지 않은 체인을 정식체인으로 만드는 공격을 성공할 수 있게 됩니다. PoW에서는 네트워크를 유지시키기 위한 해시파워를 점차 높여나가, 악의적인 노드가 전체 해시파워의 51%를 차지하여 공격하기 위한 비용을 증가시킴으로써 네트워크의 보안성을 유지합니다.

PoS(Proof of Stake, 지분증명, 이하 PoS) 합의 알고리즘에서는 블록을 생성할 권한이 보유하고 있는 토큰의 양에 따라 결정됩니다. 노드가 블록의 생성 과정에 참여하기 위해서는 자신의 토큰을 네트워크에 담보물로 예치(스테이킹, Staking)해야 합니다. 노드가 스테이킹된 토큰을 많이 보유하고 있을수록 블록을 생성할 확률도 높아집니다. 이때 노드가 만약 악의적인 행동을 하게 되면, 노드가 보유하고 있는 스테이킹된 토큰의 수량이 삭감되는 패널티가 부여됩니다. PoW와 같이 PoS에서도 전체 네트워크에 스테이킹된 토큰의 51% 이상을 차지하게 되면 네트워크를 장악할 수 있습니다. 이에 따라 PoS에서는 네트워크의 기축 토큰의 시가 총액을 키워, 네트워크를 공격하는데 필요한 비용을 증가시킴으로써 네트워크의 보안성을 유지합니다.

①

PoS로 전환된 이더리움에
51% 공격을 하려면?

{ 약 230조 원 필요
≈ \$185B }



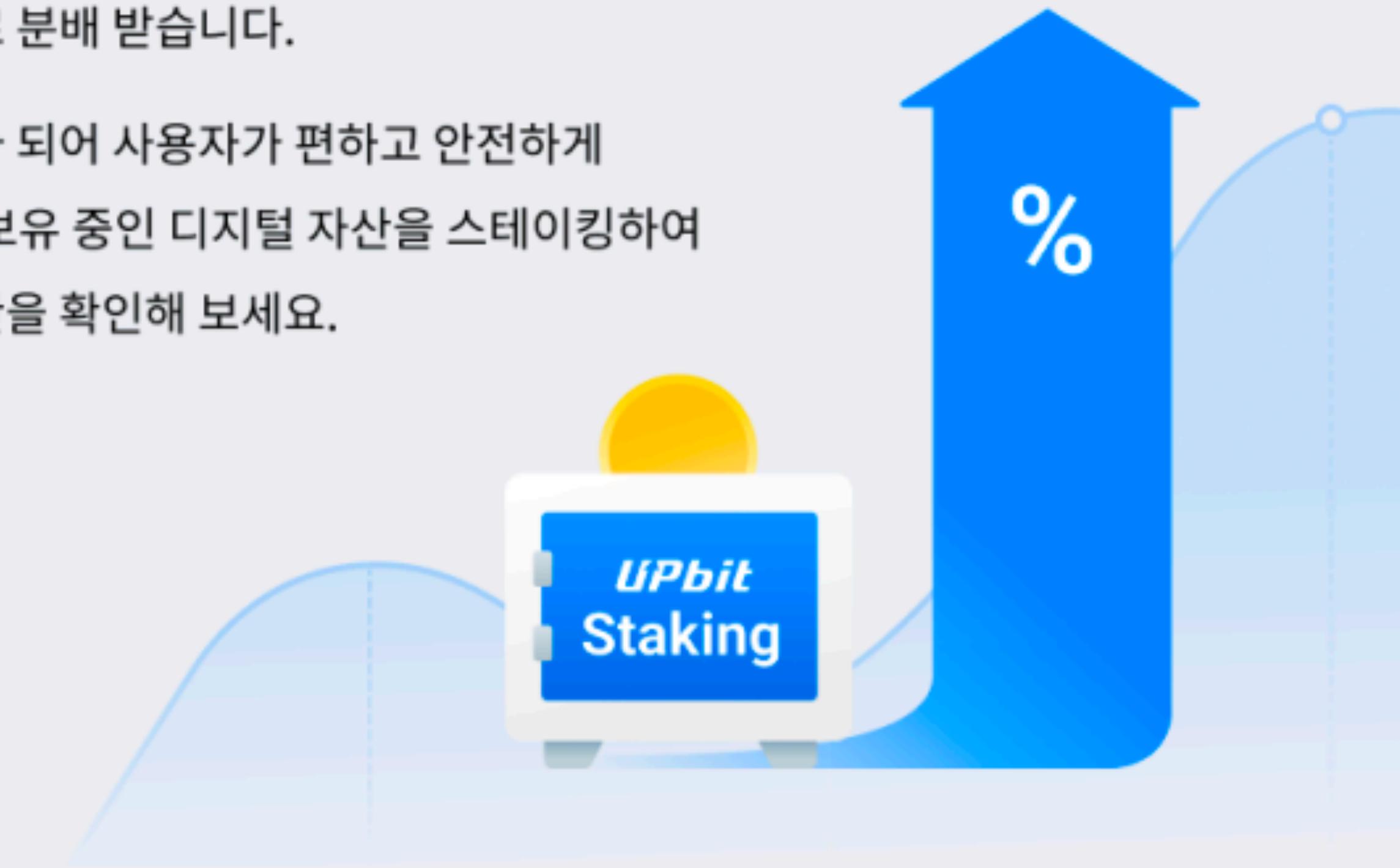
<https://medium.com/dsrv/%ED%8A%B8%EB%A6%B4%EB%A0%88%EB%A7%88-%EC%B2%98%EC%9D%8C-%EB%B5%99%EA%B2%A0%EC%8A%B5%EB%8B%88%EB%8B%A4-a9b68c327702>

스테이킹이란?

보유한 디지털 자산을 블록체인 검증에 활용하도록 맡기는 것을 뜻합니다.

사용자는 그 대가로 디지털 자산을 보상으로 분배 받습니다.

업비트는 복잡한 스테이킹 과정 속 중개자가 되어 사용자가 편하고 안전하게 스테이킹을 이용할 수 있도록 도와줍니다. 보유 중인 디지털 자산을 스테이킹하여 참여한 시간만큼 꾸준히 쌓이는 디지털 자산을 확인해 보세요.



Block Time 1 Hour 6.69s | 1 Day 6.64s | 30 Days 6.67s

Validators

#	Validator Name	Voting Power ↓	Power Change (7d)	Commission	Blocks Proposed	Missed Oracle Votes	Missed Precommits
1	Orion.Money	15,388,023 (5.0%)	14,187	5.0%	190,480	0	2 (0.0%) 
2	DokiaCapital	9,741,502 (3.2%)	(105,694)	5.0%	84,653	0	359 (0.0%) 
3	B-Harvest	9,731,774 (3.2%)	(47,873)	5.0%	135,546	8	281 (0.0%) 
4	DSRV	9,074,340 (3.0%)	228,874	10.0%	58,643	1	275 (0.0%) 
5	everstakeone	8,745,566 (2.9%)	23,678	10.0%	48,858	0	8 (0.0%) 
6	NOD Games	8,594,065 (2.8%)	29,513	0.0%	59,910	1	71 (0.0%) 
7	hashed	8,208,634 (2.7%)	740	10.0%	68,143	0	77 (0.0%) 
8	Smart Stake - terra.smartstake.io	7,960,556 (2.6%)	(52,700)	5.0%	51,574	0	0 (0.0%) 
9	Staking Fund	7,911,826 (2.6%)	(5,506)	10.0%	159,312	12	131 (0.0%) 
10	Figment	7,500,356 (2.4%)	79,888	10.0%	42,568	3	239 (0.0%) 

더 생각해보기



jkb.eth 🎨
@jkb0x

Emails I'm getting.

We are like Aave but on Solana.
We are like Uniswap but on Avalanche.
We are like Synthetix but on Terra.
We are like Yearn but on Fantom.

Can someone point me to some DeFi apps on other L1s that didn't exist on Ethereum first? Genuinely curious

10:09 PM · Sep 22, 2021

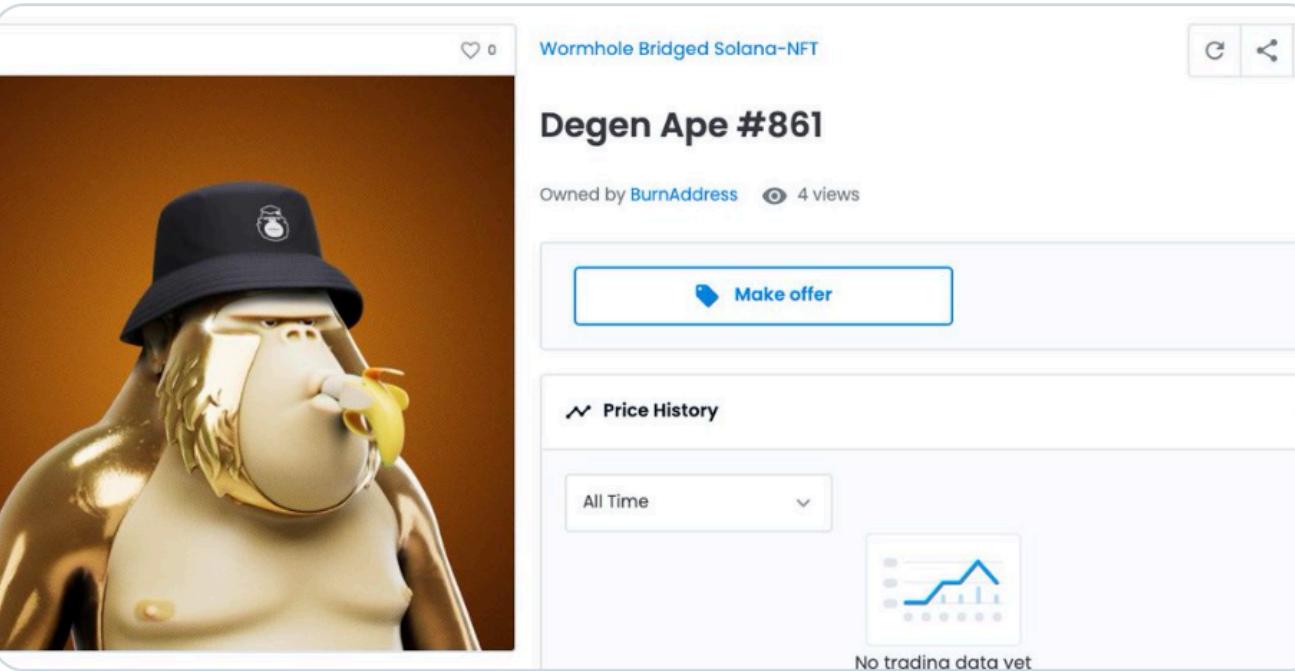
[Read the full conversation on Twitter](#)

- 다양한 디앱들이 각각의 체인에 맞게 설계되어 출시되는 것 자체는 문제라고 볼 수 없다.
- 담보 대출 프로토콜이라도, 이더리움의 아베, 컴파운드에서 제공하는 가치와 솔라나의 포트 퍼센스, 애프리콧 퍼센스 등이 제공하는 기능 사이에는 분명한 차이가 있다.
- 다만, 각 체인들의 고유 강점을 활용하지 않고 단순히 이전에 다른 체인에서 성공한 디앱을 포크만 떠서 출시되는 디앱들이 많다. 과연 이것이 전체 블록체인 생태계의 발전에 도움이 되는 것인지는 고민해 볼 필요가 있다.
- 출처: a41 ventures

더 생각해보기

 Wormhole ⚡ ✅ @wormholecrypto

1/ This is a fake [@DegenApeAcademy](#) bridged from Solana to Eth using Wormhole on [@opensea](#). The Wormhole network cannot prevent the wrapping of fake NFTs, so each user is responsible for independently verifying an NFT's authenticity. Here's how you can use the origin verifier tool ↴



 Wormhole ⚡ ✅ @wormholecrypto

1/ We're excited to see NFTs crossing the bridge already opensea.io/collection/wor...!

To help users verify the authenticity of their NFTs, we've provided a tool called "NFT Origin Verifier" wormholebridge.com/#/nft-origin-v... which shows where the NFT came from.

NFT Origin Verifier

- 만약 상호작용하고 있는 체인에서 블록 재조정(reorg)이 발생하거나, 타임 밴딧 어택 (MEV 공격)이 발생했을 때 어떤 식으로 대처를 해야할지에 대한 해답이 아직 없다.
- 여러 체인을 옮겨다닌 NFT의 출처와 전송 기록을 어떻게 관리할지에 대한 문제도 있다.
- NFT는 디지털 자산에 대한 소유권을 증명하지만, NFT와 연결된 메타데이터/콘텐츠 데이터가 복제되는 것을 막아 주지는 못하며 복제된 파일을 사용해 새로운 NFT를 발행하는 것은 얼마든지 가능하다.
- 다만 최초로 특정 콘텐츠 데이터를 사용해 NFT를 발행한 발행자 주소를 확인할 수 있기 때문에 무엇이 최초 발행자에 의해 발행되었는지 여부는 확인할 수 있다.
- 출처: a41 ventures

작은 미션 2: ERC20 도큰 멀티체인 배포하기

1. 다음 [ALLTHATNODE DOCUMENTATION](#) 링크를 따라하며 실습할 예정입니다.
2. LOCAL HARDHAT NETWORK, ETHEREUM KOVAN TESTNET, POLYGON MAINNET 에 배포하겠습니다.

Any Questions?