아비트럼(Arbitrum)

본 '주요내용설명서'는 가상자산의 발행주체 또는 운영주체가 작성한 가상자산 관련 중요사항을 설명하는 자료 원문의 주요 내용 및 가상자산 관련 중요사항에 대한 최신 변경내용을 기재한 한글 자료이며, 본 설명서가 업로드 되는 시점에 따라 자료 원문과 내용의 차이가 있을 수 있습니다. 보다 자세한 사항 및 최신 변경내용은 반드시 원문을 참고해 주시기 바랍니다.
(원문 링크)

개요

아비트럼(Arbitrum)은 이더리움의 확장성(scalability)을 개선하기 위한 이더리움 기반 레이어 2 블록체인이다. 니트로(Nitro) 업그레이드는 이러한 노력의 일환으로 네트워크 비용을 낮추는 동시에 이더리움 가상 머신과의 호환성(EVM-Compatibility)을 개선하고자 한다. 시퀀서(sequencer)에 의한 트랜잭션(transaction) 검열을 최소화하기 위해 "Delayed Inbox"를 두는 것 역시 특징이다. 또한, 아비트럼은 'BoLD(Bounded Liquidity Delay)' 기반 상호작용적 사기 증명(Interactive Fraud Proof)을 통해 탈중앙화된 방식으로 보안성을 개선하고자 한다. 최근에는 스타일러스(Stylus)를 도입했는데 솔리디티(Solidity)뿐만 아니라 러스트(Rust), C, C++ 등 다양한 프로그래밍 언어를 활용한 개발을 가능하게 하는 것을 주요 목표로 한다. 거버넌스의 경우 아비트럼 다오(Arbitrum DAO)를 중심으로 다양한 이해 관계자의 의사 결정 참여를 이끌어내고자 한다.

기술 및 특징

이더리움 기반 레이어 2 블록체인

레이어 2 블록체인은 오프체인(offchain)에서 트랜잭션(transaction)을 실행 및 처리하는 방식으로 레이어 1 블록체인 속도를 향상시키는 동시에 비용을 줄이고자 한다. 아비트럼의 기본 형태로 채택된 레이어 2 블록체인의 한 형태인 "옵티미스틱 롤업(Optimistic Rollup)"의 경우 트랜잭션 데이터를 레이어 1 블록체인에 제출하고 이를 기반으로 레이어 2 블록체인상 트랜잭션 및 이를 적용한 상태(state)를 둘러싼 잠재적인 분쟁을 해결하는 방식으로 레이어 1 블록체인의 보안을 물려받는다. 이 때, 아비트럼은 이더리움에 제출된 트랜잭션 데이터에 대한 이의 제기가 없는 한 해당 트랜잭션이 유효하다는, "낙관적(optimistic)"인 가정에 기초하고 있다.

아비트럼의 보안은 네트워크를 운영하는 시퀀서를 감시할 수 있는 정직한 검증인(validators)의 존재에 영향을 받는다. 아비트럼에는 1) 블록을 생성해 상태를 업데이트하는 적극적 검증인(active validator), 2) 아비트럼 운영을 감시하면서 필요할 경우 이의를 제기하는 수동적 검증인(defensive validator), 3) 아비트럼 운영을 감시하는 데에만 그치는 감시 검증인(watchower validator)이 존재한다. 적극적 검증인 및 수동적 검증인은 일정량의 이더를 스테이킹해야 한다. 작성 시점 기준으로 시퀀서는 오프체인 랩스(OffChain Labs)가 운영하고 있으며, 적극적 검증인은 오프체인 랩스에, 수동적 검증인은 화이트 리스트에 각각 의존하고 있다. 다만, 감시 검증인이 되는 데에는 특별한 자격이 필요하지 않다.

아비트럼 생태계는 크게 1) 아비트럼 롤업(Arbitrum Rollup), 2) 아비트럼 애니트러스트(Arbitrum Anytrust), 3) 아비트럼 오빗(Arbitrum Orbit)으로 구성된다.
아비트럼 롤업은 여러 개의 트랜잭션을 한 데 묶어(batch) 이더리움에 올리는 롤업 방식을 활용한다.
아비트럼 애니트러스트는 전반적으로 아비트럼 롤업과 비슷하지만 트랜잭션 데이터가 이더리움에 저장되는 대신 데이터 가용성 위원회(Data Availability Committee, DAC)에 의해 관리된다. 이러한 방식으로 다소 중앙화된 집단에 데이터 가용성을 의존한다는 점에서 탈중앙성 및 보안을 일부 희생하는 측면이 있지만, 이더리움의 저장 자원을 쓰지 않기 때문에 트랜잭션 비용을 더욱 낮출 수 있다.
아비트럼 오빗은 사용자의 다양한 니즈를 충족하는 맞춤형 레이어 2 혹은 레이어 3 블록체인을 의미한다. 이를 통해 사용자들은 더욱 효율적이고 다양한 블록체인 환경을 경험할 수 있다.

궁극적으로 아비트럼은 레이어 2 블록체인의 형태를 취해 이더리움의 확장성을 제고하는 것을 목표로 한다.

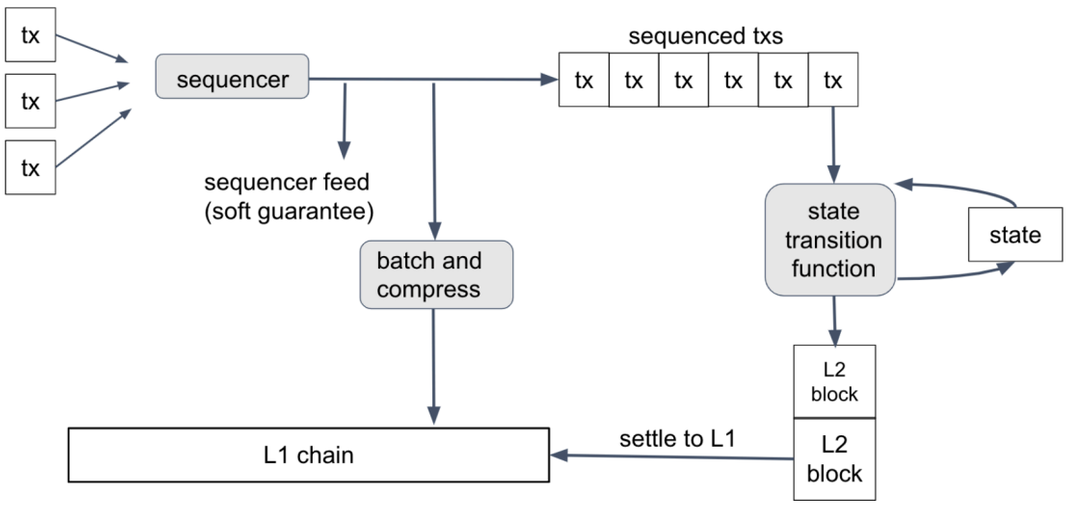
니트로 업그레이드

니트로 업그레이드는 트랜잭션, 롤업 상태 등과 관련해 분쟁이 발생한 상황에서 문제가 되는 부분과 직접적으로 연관된 코드만 컴파일(compile)해 네트워크 효율성을 개선하려고 한다. 여기서 "컴파일"이라 함은 인간 친화적인 고수준 프로그래밍 언어를 컴퓨터 친화적인 저수준 프로그래밍 언어로 변환시키는 행위를 의미한다. 니트로 업그레이드 전에는 분쟁 여부와 상관 없이 대상이 되는 코드를 모두 컴파일했다.

또한, 이더리움에 저장되는 트랜잭션 데이터를 보다 효율적으로 압축함으로써 트랜잭션 비용을 감소시키고자 한다.

여기에 더해 아비트럼 가스(ArbGas)와 이더리움 가스의 일대일 대응, 아비트럼 가상 머신(Arbitrum Virtual Machine, AVM)의 Geth(Go-ethereum) 도입 등을 통해 이더리움 가상 머신과의 호환성을 증진시키고자 한다.
니트로 업그레이드 전에는 단순 전송 트랜잭션의 경우 이더리움 가상 머신 하에서는 21,000 가스가 필요했다. 반면에 아비트럼 가상 머신을 거칠 경우 100,000 아비트럼 가스가 넘게 소모됐다. 따라서, 가스 산정 로직을 포함한 스마트 컨트랙트의 경우 아비트럼에 배포할 때 수정이 불가피하게 된다.
또한, 니트로 업그레이드 전 아비트럼 가상 머신은 자체 프로그래밍 언어인 "미니(mini)"를 활용했는데 고(Go)로 구현된 이더리움 실행 환경인 Geth를 적용함으로써 비효율성을 개선할 수 있게 됐다.

Delayed Inbox



출처: 아비트럼 독스

,

시퀀서(sequencer) 중심으로 네트워크가 운영되는 아비트럼 특성상 악의적인 시퀀서가 특정 사용자의 트랜잭션을 고의로 처리하지 않는 이슈가 발생할 수 있다. 아비트럼은 이를 완화하기 위해 Delayed Inbox를 도입했다.

이를 이해하기 위해서는 아비트럼에서의 일반적인 트랜잭션 생애 주기(transaction lifecycle)를 먼저 이해할 필요가 있다.

① 시퀀서가 사용자로부터 트랜잭션을 수취한다.
② 시퀀서가 수취한 트랜잭션을 정렬한다.
③ 시퀀서가 여러 개의 트랜잭션을 묶어 이더리움에 올린다.
④ 적극적 검증인이 30분~60분을 주기로 "롤업 블록(Rollup Block, Rblock)"을 생성한다. 이 때 롤업 블록은 여러 개의 니트로 블록(L2 block)으로 구성된다.
⑤ 약 일주일 간의 분쟁 기간이 분쟁 없이 지나가거나 모든 분쟁이 해결될 경우 롤업 블록 및 그 안에 포함된 트랜잭션들이 최종 확정된다.

아비트럼에서 사용자가 시퀀서에게 트랜잭션을 제출할 경우 시퀀서는 이를 Core Inbox에 넣고, 그 후 트랜잭션은 정렬된다. 이 때 시퀀서가 트랜잭션을 Core Inbox에 삽입하지 않으면 문제가 발생하는 것인데 이에 대응해 사용자는 트랜잭션을 Delayed Inbox에 보낼 수 있다. 트랜잭션이 Delayed Inbox에 들어가고 난 후 약 24시간이 지나면 임의의 주체가 "ForceInclusion" 메서드를 통해 해당 트랜잭션을 Core Inbox로 보내 정렬시킬 수 있다.

이와 같이 아비트럼은 Delayed Inbox를 통해 검열 저항성을 유지하고자 한다.

BoLD 기반 상호작용적 사기 증명

아비트럼에서 상호작용적 사기 증명은 적극적 검증인의 잠재적인 잘못 혹은 오류에 대해 수동적 검증인이 이의를 제기해

이를 해결하고자 하는 분쟁 과정이다. 상호작용적 사기 증명은 일반적으로 다음과 같이 진행된다. (적극적 검증인 A가 생성한 롤업 블록 "R"에 대해 수동적 검증인 B가 이의 제기를 했다고 가정한다.)

① 적극적 검증인 A가 R에 포함된 N개의 니트로 블록을 k 묶음으로 쪼개는 동시에 각 묶음을 실행한 결과를 산출한다.

② 수동적 검증인 B는 적극적 검증인 A가 산출한 니트로 블록 묶음 리스트 및 실행 결과 중 문제가 있는 것을 골라 해당 묶음 내 니트로 블록들을 다시 k 묶음으로 쪼개는 동시에 각 묶음을 실행한 결과를 산출한다.

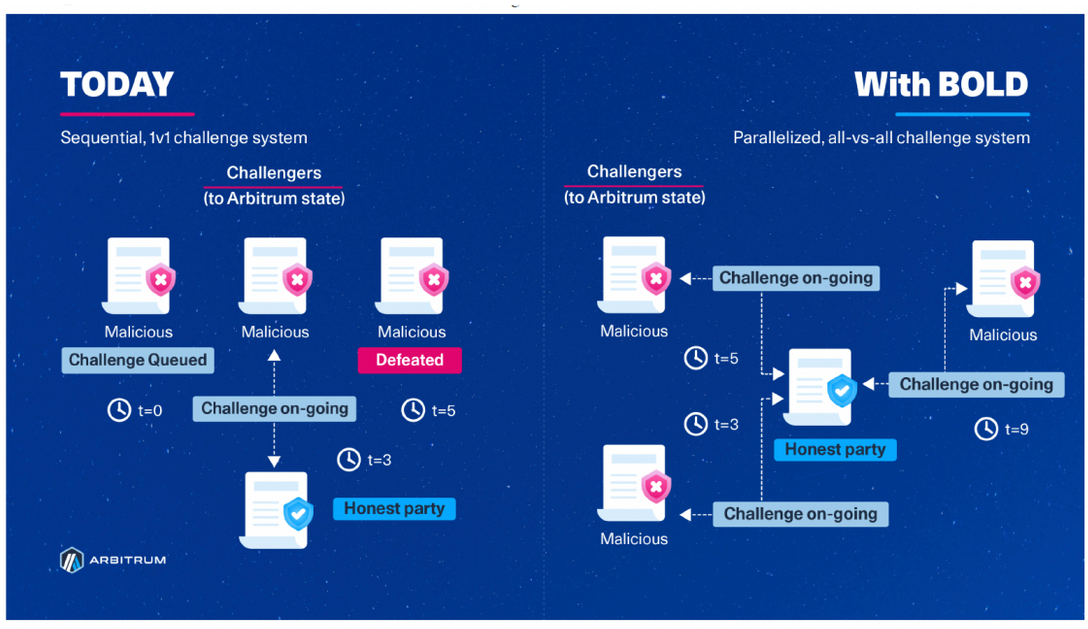
③ 적극적 검증인 A는 수동적 검증인 B가 산출한 니트로 블록 묶음 리스트 및 실행 결과 중 하나를 선정해 해당 묶음 내 니트로 블록들을 다시 k 묶음으로 쪼개는 동시에 각 묶음을 실행한 결과를 산출한다.

④ 한 개의 니트로 블록이 남을 때까지 2. 및 3.을 반복한다.

⑤ 한 개의 니트로 블록이 남을 경우 해당 니트로 블록이 포함한 명령들(Instructions)에 대해 명령이 하나 남을 때까지 명령들을 대상으로 1. ~ 4. 을 진행한다.

⑥ 한 개의 명령이 남을 경우 이더리움 상 검증 컨트랙트를 통해 해당 명령의 실행 결과를 검증한다. R이 유효할 경우 적극적 검증인 A가 임의로 니트로 블록 묶음 혹은 명령 묶음을 선정하더라도 최종적으로 남는 명령을 실행한 결과는 유효하다. R이 유효하지 않을 경우 수동적 검증인 B가 반복적으로 문제가 있는 니트로 블록 묶음 혹은 명령 묶음을 골라내 궁극적으로는 유효하지 않은 명령의 실행 결과를 잡아낼 수 있다.

출처: 아비트럼 독스



출처: 아비트럼 독스

하지만 이와 같은 시스템은 트랜잭션 최종 확정을 사실상 무기한 늦추는 '지연 공격(delayed attacks)'에 취약할 수 있다. 예를 들어, 악의적인 주체가 이의 제기에 필요한 담보금을 잃는 것을 감수하면서 반복적으로 이의 제기를 하는 상황을 생각해볼 수 있다. 잠재적 지연 공격의 가능성은 여태껏 아비트럼의 상호작용적 사기 증명이 중앙화된 화이트리스트 중심으로 운영된 이유기도 했다.

따라서 아비트럼은 BoLD를 통해 지연 공격으로 인한 피해를 최소화하는 동시에 탈중앙화된 상호작용적 사기 증명을 추구하고자 한다. 우선 BoLD는 특정 상태에 대한 이의 제기를 할 수 있는 기간을 6.4일로 제한하는 동시에 여러 건의 이의 제기를 순차적인 방식이 아닌 병렬적인 방식으로 처리할 수 있게 한다. 또한, BoLD 하에서는 현재와 달리 누구나 일정양의 ETH를 스테이킹할 경우 상호작용적 사기 증명에 참여할 수 있다. 물론 이의 제기에 필요한 담보금이 1,110 ETH라는 점에서 절대 작은 금액이라고 볼 수는 없지만 다수의 참여자를 통해 이를 모집할 수 있는 '풀링 컨트랙트(pooling contract)'를 지원해 이를 보완한다.

이와 같이 아비트럼은 BoLD 기반 상호작용적 사기 증명을 통해 탈중앙화된 방식으로 보안성을 개선하고자 한다.

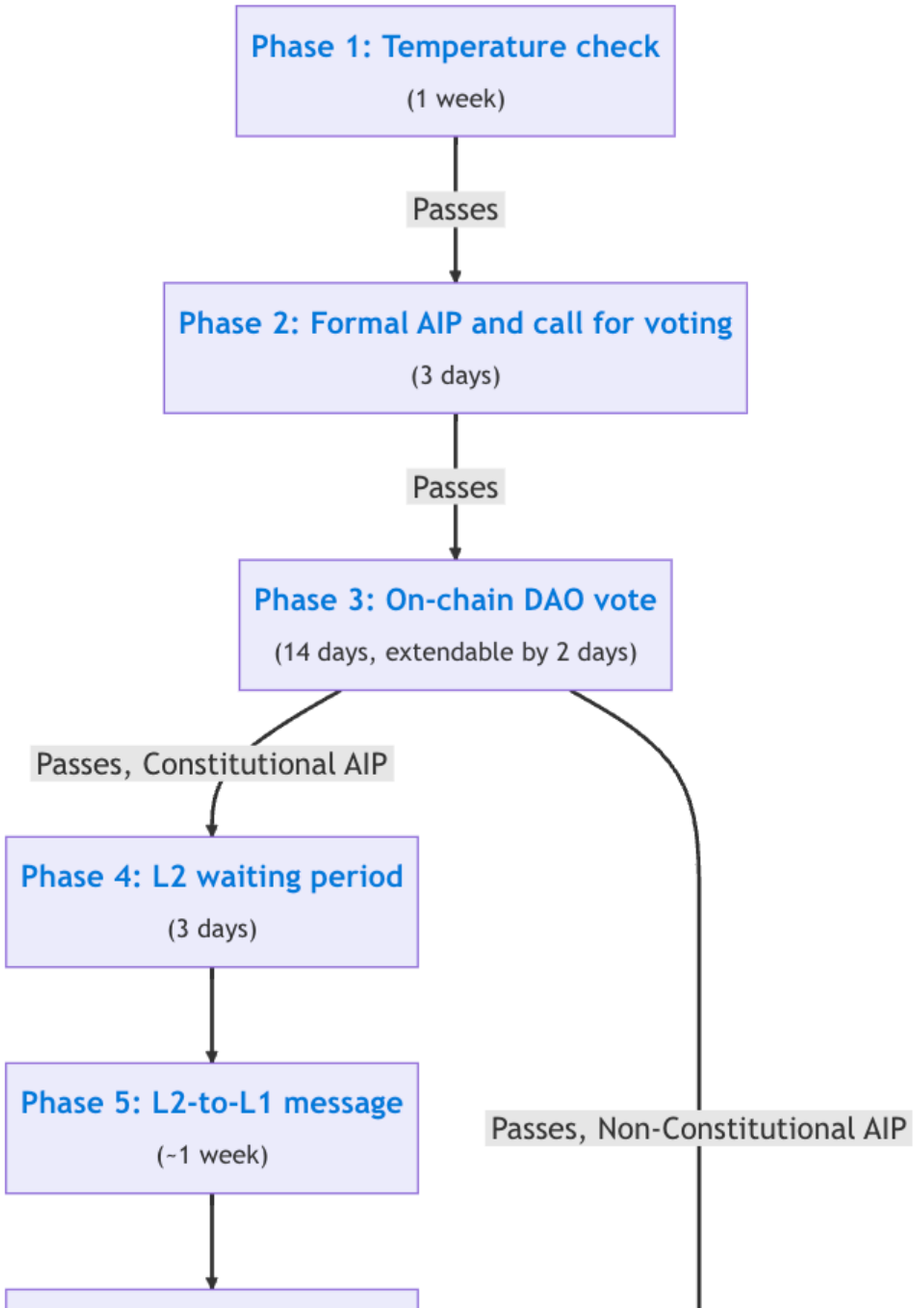
스타일러스

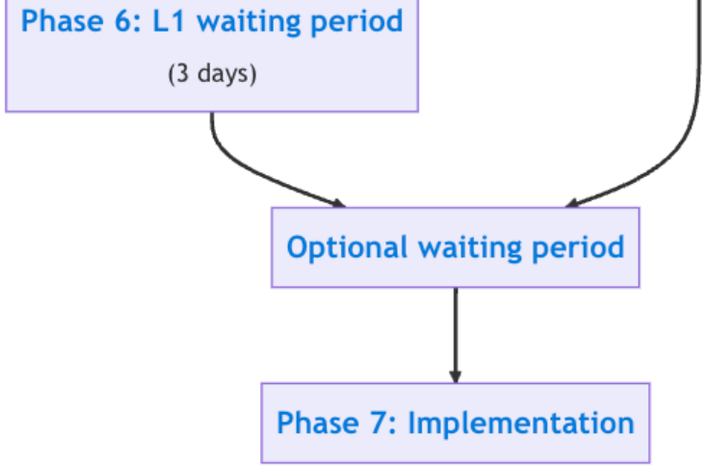
스타일러스는 이더리움 가상 머신에 더해 WebAssembly(WASM)를 지원하는 가상 머신을 추가함으로써 "다중 가상 머신" 환경을 구현하고자 한다. 여기서 WebAssembly라 함은 웹에서 성능이 좋은 다양한 언어를 지원하는 이진 코드 기준을 뜻한다. 이와 같은 모델이 가능한 것은 아비트럼이 이진 계산에 기초한 상호작용적 사기 증명을 통해 보안을 유지하기 때문이다.

결과적으로 스타일러스를 통해 아비트럼에서는 솔리디티뿐만 아니라 WebAssembly 언어에 속하는 러스트, C, C++ 등을 통한 개발이 가능해질 수 있다.

아비트럼 다오

아비트럼 다오는 수수료 조정, 업그레이드, 신규 레이어 2 블록체인 생성 등에 대해 의사 결정을 진행한다. ARB 보유자는 1) 거버넌스 제안에 대해 직접 투표하거나 2) 투표권을 대표(Delegates)에게 위임하는 방식으로 아비트럼 다오에 참여할 수 있다.





출처: 아비트럼 독스

아비트럼 다오를 중심으로 한 거버넌스 프로세스는 일반적으로 다음과 같이 진행된다.

① 커뮤니티 반응 체크(Temperature Check)
: 제안자는 포럼 내 논의, 사전 투표 등을 통해 제안(AIP, Arbitrum Improvement Proposal)에 대한 커뮤니티의 의견을 수렴한다.

② 제안 공식 제출 및 투표 독려(Formal AIP and call for voting)
: 제안자는 최소 100만 ARB를 보유한 계정을 가지고 있어야 한다.

③ 온체인 다오 투표(On-chain DAO vote)
: 제안이 통과되기 위해서는 1) 찬성표가 반대표보다 많아야 하며, 2) Constitutional AIP의 경우 5%, Non-Constitutional AIP의 경우 3%의 투표율을 넘겨야 한다. Consitutional AIP는 아비트럼 거버넌스를 규율하는 "헌법(Constotution)" 변경, 소프트웨어 업데이트, 신규 체인 승인 등에 관한 것이다. Non-Constitutional AIP는 펀딩, 정보 제공 등에 관한 것이다.

④ 레이어 2 대기 기간(L2 waiting period)
: 이해 관계자들이 통과된 제안에 대응할 수 있는 최소한의 기간을 제공한다.

⑤ 레이어 2 ⇒ 레이어 1 메시지(L2-to-L1 message)
: 아비트럼에서 제안이 통과됐다는 메시지를 이더리움에 전달한다.

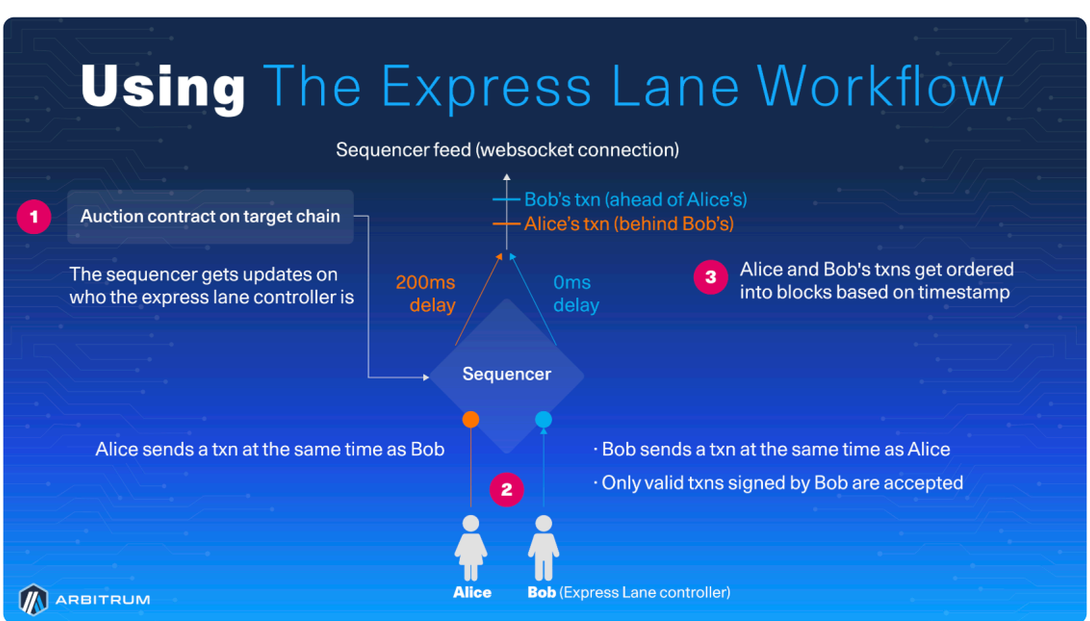
⑥ 레이어 1 대기 기간(L1 waiting period)
: 제안에 영향을 받을 수 있는, 이미 진행 중인 트랜잭션들이 최종 확정되는 것을 기다린다.

⑦ 제안 실행(Implementation)

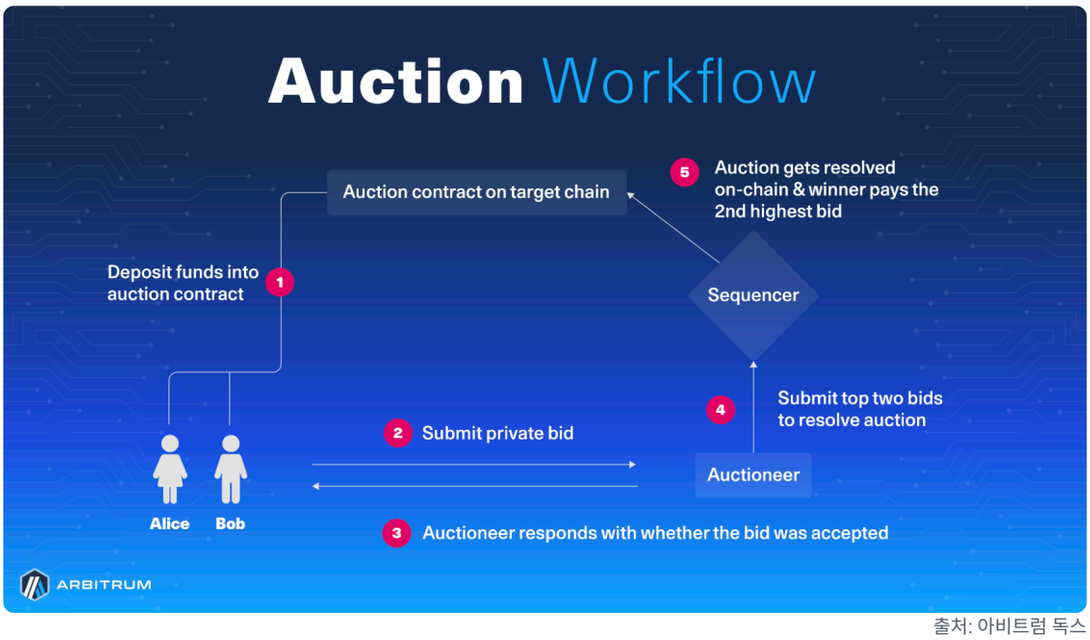
아비트럼 다오와는 별개로 아비트럼 다오에 의해 선정된 12명으로 구성된 보안 위원회(Security Council)라는 기구가 존재하는데 아비트럼 다오를 거치지 않고 보안 등과 관련된 긴급 조치 혹은 정기적인 업데이트와 같은 비긴급조치를 취할 수 있다.

이와 같이 아비트럼은 거버넌스 차원에서 탈중앙화와 효율성 간 균형을 찾고자 한다.

타임부스트



출처: 아비트럼 독스



출처: 아비트럼 독스

아비트럼이 기본적으로 채택한 '선착순' 트랜잭션 정렬 정책은 좋은 사용자 경험을 제공할 수는 있으나 트랜잭션의 네트워크 반영 여부 혹은 그 순서 등에 대한 권리에서 파생되는 MEV를 네트워크 내로 흡수하기 어려울 수 있다는 단점이 있다. 또한, MEV 기회를 전문적으로 찾는 이른바 'seracher'간 심화된 경쟁으로 인해 네트워크 성능이 저하될 수도 있다.

따라서 아비트럼은 이와 같은 이슈에 대응하기 위해 추후 타임부스트를 도입했다. 타임부스트의 핵심 개념은 바로 'express lane' 이다. 사용자가 express lane에 대한 권리를 취득할 경우 시퀀서가 본인의 트랜잭션을 빨리 처리하게끔 할 수 있다. 해당 권리는 경매를 통해 매각되는데 'sealed-bid second-price auction' 방식으로 최고가 입찰자가 2순위 입찰가를 지불하고 권리를 매250829) TICKER 2Q 25 배포입하게 된다.

다만, 타임부스트 구조상 express lane 상 트랜잭션을 먼저 처리한 후 다른 트랜잭션을 처리하기 때문에 일반적인 트랜잭션의 경우 지연(latency)이 발생할 수 있다는 문제가 있다. 아비트럼은 블록 주기를 그대로 유지함으로써 이와 같은 문제로 인해 발생할 불편을 최소화하겠다는 계획이다.

궁극적으로 아비트럼은 타임부스트를 바탕으로 트랜잭션 처리 순서에 대한 일종의 가격 차별 정책을 도입해 MEV를 네트워크 차원에서 최대한 내재화하는 동시에 MEV 경쟁으로 인한 네트워크 성능 하락을 최소화하고자 한다.

토큰 이코노미

토큰 유틸리티

아비트럼의 유틸리티 토큰인 ARB는 주로 다음과 같이 사용된다.

- 거버넌스: 사용자는 ARB를 매개로 거버넌스 제안에 대해 표결권을 행사할 수 있다.

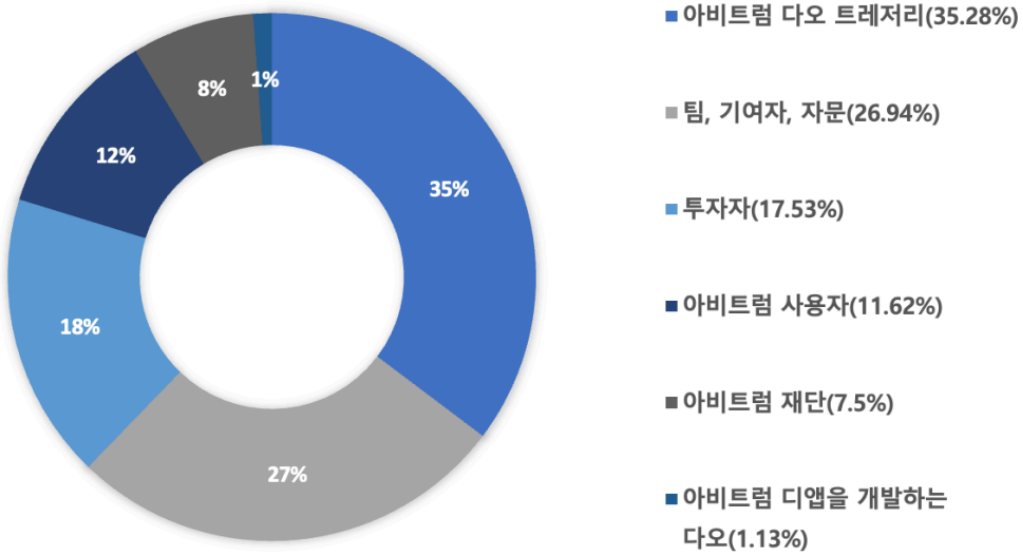
토큰 분배

> 아래 유통량 관련 정보는 프로젝트 팀이 대외적으로 공개하거나 프로젝트 팀이 업비트에 제공한 자료 등에 기초하고 있기 때문에, 차후 프로젝트의 사정에 따라 유통량 계획은 변경될 수 있습니다. 기준일 이후 업데이트 되는 유통량 관련 정보는 반드시 프로젝트의 공식 웹사이트, 커뮤니케이션 채널 등을 확인해주시기 바랍니다.

아비트럼의 유틸리티 토큰인 ARB의 초기 발행량은 100억개로 다음과 같이 분배됐다.

- 아비트럼 다오 트레저리(Arbitrum DAO treasury, 35.28%)
- 팀, 기여자, 자문(Team and Contributors + Advisors, 26.94%)
- 투자자(Investors, 17.53%)
- 아비트럼 사용자(Users of the Arbitrum platform (via airdrop to user wallet addresses), 11.62%)
- 아비트럼 재단(Arbitrum Foundation, 7.5%)

- 아비트럼 디앱을 개발하는 다오(DAOs building apps on Arbitrum (via airdrop to DAO treasury addresses), 1.13%)



출처: 아비트럼 독스, 업비트 재구성

매년 총 공급량 대비 최대 연 2%에 상응하는 ARB가 신규 발행될 수 있다.

참고 문헌

- 아비트럼 독스
- 아비트럼 홈페이지
- 아비트럼 X - BoLD 런칭

2025.08.27 16:34 업데이트

- 본 자료는 두나무(이하 당사)가 거래지원한 가상자산과 관련하여 작성한 것으로 이용자에게 투자를 권장하거나 유도할 목적이 없으며, 이용자의 투자 판단에 참고가 되는 정보 제공을 목적으로 작성되었습니다.
- 본 자료는 제3자로부터 제공받거나 제3자가 작성한 원문을 참고하여 작성 당시의 당사의 신뢰할 수 있는 내용 및 정보를 바탕으로 작성되었으나, 오차가 있을 수 있고 상이한 정보가 포함되어 있을 수 있습니다. 이에 당사는 어떠한 경우에도 정보의 정확성이나 완전성을 보장하지 않으며, 필요한 경우 이용자는 발행인이 직접 작성·공개한 정보를 통해 사실 여부를 확인하여야 합니다.
- 당사는 본 자료가 공개 되기 이전 제3자에게 사전 제공한 사실이 없습니다. 본 자료의 발행인을 포함하여 그 누구도 본 가상자산의 가치 또는 지급을 보증하지 않습니다. 본 가상자산은 시장 상황, 기술적 변화, 규제 동향 등에 따라 가치가 크게 변동할 수 있으며, 가상자산 투자는 원본 손실이 발생할 수 있습니다.
- 당사는 본 자료와 관련한 이용자의 투자 결과 일체에 대하여 어떠한 책임도 지지 않습니다.
- 본 자료는 어떠한 경우에도 이용자의 투자 결과에 대한 법적 책임 소재의 증빙자료로 사용될 수 없습니다. 본 자료의 저작권은 당사에 있고, 국내 코인 마켓거래소가 본 자료의 출처를 정확하게 명기하여 사용하는 경우 외에는 어떤 형태로든 당사의 동의 없이 복제, 변형, 재배포 될 수 없습니다.

UPbit Copyright © 2017 - 2024 Dunamu Inc. All rights reserved.