

폴카닷(Polkadot)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다

아키텍처

릴레이 체인

릴레이 체인은 폴카닷의 중심 체인이다. 모든 밸리데이터는 DOT의 릴레이 체인에 스테이킹되어 릴레이 체인을 검증한다. 릴레이 체인은 거버넌스 메커니즘과 상호 작용하고 NPoS(네트워크 지분 증명)에 참여하는 방식을 포함하여 비교적 적은 수의 거래 유형으로 구성된다. 릴레이 체인은 의도적으로 최소한의 기능만 제공한다. 예를 들어 스마트 계약은 지원되지 않는다. 주된 역할은 파라체인을 포함한 시스템 전체를 조정하는 것이다. 다른 특정 작업은 서로 다른 구현 방식과 기능을 가진 파라체인에 위임된다.

파라체인 슬롯

릴레이 체인은 컴퓨터 프로세서의 코어처럼 여러 개의 실행 코어를 지원할 수 있다(예: 최신 노트북 프로세서는 8개의 코어를 가질 수 있다). 이러한 코어는 한 번에 하나의 프로세스를 실행할 수 있다. 릴레이 체인은 파라체인과 온디맨드 파라체인이라는 두 가지 구독 모델을 사용하여 이러한 코어를 지원한다. 파라체인은 체인 전용 코어를 가지며, 지속적으로 실행되는 프로세스와 같다. 온디맨드 파라체인은 그룹 내에서 (동시에 실행되지는 않지만) 코어를 공유하므로, 깨어나서 덜 자주 실행될 필요가 있는 프로세스와 같다(최신 컴퓨터의 동시성과 유사).

네트워크 전체에서 발생하는 대부분의 연산은 다양한 사용 사례를 처리하는 특정 파라체인 구현에 위임된다. 릴레이 체인은 파라체인이 수행할 수 있는 작업에 제약을 두지 않는다. 단, 파라체인에 할당된 밸리데이터가 검증할 수 있는 증명을 생성할 수 있어야 한다. 이 증명은 파라체인의 상태 전이를 검증한다. 일부 파라체인은 특정 애플리케이션에 특화될 수 있고, 다른 파라체인은 스마트 계약, 개인정보 보호, 확장성과 같은 특정 기능에 중점을 둘 수 있다. 또한, 블록체인의 본질과는 반드시 일치하지 않는 실험적 아키텍처도 있을 수 있다.

릴레이 체인은 특정 기간 동안 파라체인에 대한 코어를 확보하는 다양한 방법을 제공한다. 온디맨드 파라체인은 다른 파라체인과 코어를 공유한다(동시에 공유하지는 않음). 일반 파라체인과 온디맨드 파라체인은 모두 동일한 API를 사용하며, 코어타임을 통해 DOT를 통해 코어에서 시간을 확보해야 한다. 파라체인은 온디맨드와 영구 파라체인 사이를 전환할 수 있다.

공유 보안

릴레이 체인에 연결된 모든 파라체인은 릴레이 체인의 보안을 공유한다. 폴카닷은 릴레이 체인과 연결된 모든 파라체인 간에 공유 상태를 갖는다. 어떤 이유로든 릴레이 체인이 원래 상태로 돌아가야 하는 경우, 모든 파라체인도 원래 상태로 돌아간다. 이는 전체 시스템의 유효성을 유지하고 개별 부분이 손상되지 않도록 하기 위한 것이다.

공유 상태는 파라체인을 사용할 때 신뢰 가정이 릴레이 체인 밸리데이터 세트의 신뢰 가정과 동일하며 다른 가정은 적용되지 않도록 보장한다. 릴레이 체인의 밸리데이터 세트는 이를 뒷받침하기 위해 많은 지분이 투자되어 안전할 것으로 예상되므로, 파라체인은 이러한 보안으로부터 이점을 얻을 수 있다.

상호 운용성

엑스씨엠

XCM은 크로스 컨센서스 메시지(Cross-Consensus Message)의 약자로, 프로토콜이 아닌 형식이다. 이 형식은 수신자 또는 발신자의 컨센서스 메커니즘에 대한 어떠한 가정도 하지 않으며, 오직 메시지가 어떤 형식으로 구성되어야 하는지에만 관심을 둔다. XCM 형식은 파라체인(parachain)들이 서로 통신할 수 있는 방식이다. 크로스 체인 메시징 프로토콜(Cross-chain Messaging Protocol)의 약자인 XCMP와는 달리, XCM은 전달되는 대상이며 XCMP는 전달 메커니즘이다. XCM에 대해 더 자세히 알아보려면 사양을 읽어보는 것이 가장 좋다.

브릿지

블록체인 브릿지는 임의의 데이터를 한 네트워크에서 다른 네트워크로 전송할 수 있도록 하는 연결이다. 이러한 체인은 브릿지를 통해 상호 운용될 수 있지만, 서로 다른 프로토콜, 규칙 및 거버넌스 모델을 사용하는 독립형 체인으로도 존재할 수 있다. 폴카닷에서 브릿지는 릴레이 체인에 연결되며, 콜레이터(collator)가 관리하는 합의 메커니즘을 통해 보안이 유지된다.

폴카닷은 웹 3.0의 미래를 연결하기 위해 브릿지를 사용한다. 브릿지는 고립된 체인 간의 안전하고 견고한 통신 채널 역할을 함으로써 폴카닷의 상호 운용 가능한 아키텍처의 기본이 된다.

밸리데이터

밸리데이터는 밸리데이터 집합에 선출되면 릴레이 체인에서 블록을 생성한다. 또한, 밸리데이터는 콜레이터(collator)로부터 유효한 상태 전환 증명을 받고 그 대가로 스테이킹 보상을 받는다.

밸리데이터는 나중에 사용할 수 있도록 충분한 파라체인 블록을 로컬 저장소에 보관해야 한다. 이러한 블록은 해당 정보가 없는 피어가 파라체인 블록에 대해 발행된 유효성 진술을 신뢰할 수 있게 확인할 수 있도록 검색될 수 있다. 가용성 및 유효성 (AnV) 프로토콜은 이러한 책임을 성공적으로 이행하기 위한 여러 단계로 구성된다.

노미네이터

노미네이터는 특정 밸리데이터에게 지분을 예치하여 해당 밸리데이터가 활성 밸리데이터 세트에 참여하고 체인 블록을 생성할 수 있도록 지원한다. 그 대가로 노미네이터는 일반적으로 해당 밸리데이터가 제공하는 스테이킹 보상의 일부를 받는다.

콜레이터

콜레이터는 파라체인과 릴레이 체인 모두의 완전 노드이다. 콜레이터는 파라체인 거래를 수집하고 릴레이 체인의 밸리데이터를 위한 상태 전이 증명을 생성한다. 또한 XCMP를 사용하여 다른 파라체인과 메시지를 주고받을 수 있다.

파라체인 블록 자체는 수집기에 의해 생성되는 반면, 릴레이 체인 검증기는 유효성(및 나중에는 가용성)만 검증한다.

콜레이터

콜레이터의 역할

롤업 유지 관리자

콜레이터는 사용자 트랜잭션을 수집하고 폴카닷 밸리데이터를 위한 상태 전이 증명을 생성하여 롤업 체인(파라체인)을 유지한다. 다시 말해, 콜레이터는 트랜잭션을 파라체인 블록 후보로 집계하고 밸리데이터를 위한 상태 전이 증명(유효성 증명, PoV)을 생성한다.

콜레이터는 릴레이 체인과 각 파라체인에 대한 풀 노드를 유지한다. 즉, 새로운 파라블록을 작성하고 PoW 블록체인의 채굴자처럼 거래를 실행하는 데 필요한 모든 정보를 보유한다. 일반적인 상황에서 콜레이터는 거래를 수집하고 실행하여 봉인되지 않은 블록을 생성하고 PoV를 Polkadot 코어의 한 명 이상의 밸리데이터에게 제공한다.

콜레이터는 다른 블록체인의 밸리데이터와 유사하다. 하지만 릴레이 체인이 ELVES 프로토콜을 통해 보안을 서비스로 제공하기 때문에 콜레이터는 보안을 보장할 필요가 없다. 파라체인 블록이 유효하지 않으면 밸리데이터는 해당 블록을 거부한다.

롤업 라이브니스 및 검열

롤업 안전성(즉, 유효하지 않은 거래가 롤업에 포함되지 않도록 보장하는 것)은 ELVES 프로토콜을 구현하는 릴레이 체인의 밸리데이터를 통해 달성된다. 하지만 롤업의 활성화(즉, 새로운 블록이 결국 생성됨)와 검열 저항성은 콜레이터의 책임이다. 따라서 충분히 분산된 콜레이터 세트는 활성도를 보장하고 검열 저항성을 완화한다. 이론적으로, 정직한 콜레이터 하나만 있어도 활성도를 보장할 수 있지만 처리량은 감소한다.

교차 합의 메시징

콜레이터는 XCM(Cross-Consensus Message Passing Format)의 핵심 요소이다. 릴레이 체인의 완전 노드이기 때문에 모두 서로를 피어(peer)로 인식한다. 이를 통해 파라체인 A에서 파라체인 B로 메시지를 전송할 수 있다.

야생의 콜레이터들

서브스트레이트를 사용하여 구축된 블록체인은 릴레이 체인에 독립적으로 연결할 수 없다. Parity 팀은 이 문제를 해결하기 위해 Cumulus 라이브러리를 개발했다. Collators는 Paseo 테스트넷에서 사용되고 있으며, Cumulus Rust 문서를 통해 Cumulus에서 Collators를 사용하는 방법에 대해 자세히 알아볼 수 있다. 자세한 내용은 빌드 파라체인 페이지의 Cumulus 섹션에서 확인할 수 있다.

밸리데이터

밸리데이터는 DOT를 스테이킹하고, 콜레이터의 증명을 검증하고, 다른 밸리데이터와 합의에 참여하여 릴레이 체인을 보호한다.

밸리데이터는 릴레이 체인에 새로운 블록을 추가하는 데 중요한 역할을 한다. 또한 각 롤업 체인(또는 파라체인)이 고유한 규칙을 따르고 안전한 환경에서 다른 롤업 체인과 메시지를 주고받을 수 있도록 보장한다.

폴카닷의 밸리데이터는 코어와 체인에서 여러 작업을 수행한다. 이러한 코어 내/체인 내 이중성은 폴카닷의 고유한 특징이며 확장성의 핵심이다.

코어 내 검증기

코어 내 밸리데이터(또는 파라밸리데이터)는 AnV 프로토콜의 파라체인 단계에 참여하고 릴레이 체인 거래 대기열에 후보 영수증을 제출하여 블록 작성자가 릴레이 체인 포크에 롤업 블록에 대한 정보를 포함할 수 있도록 한다.

인코어 밸리데이터는 그룹으로 작동하며, 매 에포크마다 런타임에 의해 선정되어 폴카닷 코어에 연결된 모든 롤업에 대한 롤업 블록을 검증한다. 인코어 밸리데이터는 검증 프로세스에 참여하기 위해 (에포크별로) 무작위로 선정된 활성 검증자의 일부이다.

인코어 밸리데이터는 할당된 롤업 블록 후보 집합에 포함된 정보가 유효한지 검증한다. 밸리데이터는 제출된 후보의 유효성을 확인한 후, 다른 밸리데이터에게 후보의 유효성에 대한 진술을 발행하고 수집해야 한다. 이 과정을 후보 지원 이라고 하며, Polkadot 보안 프로토콜 페이지에 자세히 설명되어 있다. 밸리데이터는 신뢰할 수 없는 콜레이터로부터 관련 PoV가 포함된 임의의 수의 롤업 블록 후보를 수신한다. 할당된 모든 인코어 밸리데이터 중 최소 2/3가 해당 후보에 대한 유효한 진술을 발행하면 후보가 지원 가능한 것으로 간주된

다.

코어 내 검증기는 다음 조건을 다음 순서대로 성공적으로 검증해야 한다.

1. 후보자는 지속된 검증 데이터의 매개변수를 초과하지 않는다.
2. 채점자의 서명이 유효하다.
3. 릴레이 체인에 저장된 롤업 런타임을 실행하여 후보자를 검증한다.

롤업 블록 후보가 지원 기준을 충족하면, 선택된 릴레이 체인 블록 작성자는 각 롤업 체인에 대해 지원 가능한 후보를 선택하여 릴레이 체인 블록에 추가한다.

블록 작성자

릴레이 체인에는 다른 밸리데이터들의 유효성 진술을 기반으로 릴레이 체인 블록을 생성하는 합의 메커니즘에 참여하는 밸리데이터들이 있다. 이러한 밸리데이터들을 블록 작성자라고 한다. 이들은 BABE에 의해 선정되며, 각 롤업 체인에 포함될 최대 하나의 지원 가능한 후보를 기록할 수 있다. 릴레이 체인 블록에 추가된 지원 가능한 후보는 해당 체인 포크에서 지원된 것으로 간주된다.

릴레이 체인 블록에서 블록 작성자는 이전 릴레이 체인 블록에 부모 후보 영수증이 있는 후보 영수증만 포함한다. 이를 통해 롤업 체인이 유효한 릴레이 체인을 따르도록 한다. 또한, 블록 작성자는 데이터 가용성 체계에서 삭제 코딩 청크를 가진 영수증만 포함하여 시스템이 다음 라운드의 가용성 및 유효성 검사를 수행할 수 있도록 한다.

데이터 가용성

후보자가 릴레이 체인 포크에 지원되면, 사용 가능 여부가 아직 결정되지 않은 상태이다. 즉, 사용 가능 여부가 (PoV와 함께) 입증될 때까지 릴레이 체인의 일부로 완전히 포함되지 않는다(잠정적으로만 포함됨). 밸리데이터는 소위 가용성 분배에도 기여한다. 데이터 가용성 체계는 코어 내 밸리데이터가 후보 블록 정보를 삭제 코드 형태로 분배하는 방식으로 구성된다. 후보자의 가용성 정보는 다음 릴레이 체인 블록에 기록된다. 충분한 정보가 있는 경우에만 후보자가 사용 가능한 것으로 간주되어 포함될 수 있다.

2차 체커

밸리데이터는 소위 승인 프로세스에도 참여한다. 파라블록이 사용 가능한 것으로 간주되어 포함되면 여전히 승인 대기 중이다. 코어 내 밸리데이터는 전체 밸리데이터의 일부이기 때문에 코어에 할당된 밸리데이터 대부분이 우연히 부정직할 위험이 있다. 따라서 롤업 블록이 승인된 것으로 간주되기 전에 2차 검증을 실행해야 한다. 2차 검증 단계를 거치면 코어 내 밸리데이터가 더 많이 할당되어 궁극적으로 시스템 처리량이 감소하는 것을 방지할 수 있다. 분쟁이 발생하지 않으면 후보 블록이 승인된다.

분쟁

합의 알고리즘을 준수하지 않는 모든 사례는 밸리데이터가 스테이킹한 토큰의 일부 또는 전부를 제거하여 해당 밸리데이터에게 불이익을 주는 방식으로 분쟁을 야기하여 악의적인 행위자의 활동을 억제한다. 그러나 좋은 성과를 거둔 밸리데이터는 활동에 대한 대가로 네이티브 토큰 형태의 블록 보상(거래 수수료 포함)을 받게 되므로 보상을 받게 된다.

결정론적 최종성

마지막으로 밸리데이터는 GRANDPA 내의 체인 선택 프로세스에 참여하여 최종화된 릴레이 체인 내에서만 사용 가능하고 유효한 블록이 종료되도록 하고 모든 기록이 하나의 정식 체인으로 수렴되도록 보장한다.

한 시대 안에서 역할은 바뀔 수 있다.

같은 시대에 밸리데이터는 코어 또는 블록 작성자에 속할 수 있으며, 가용성 분배 또는 승인 프로세스에 참여할 수 있다. 이러한 역할은 세션마다 변경될 수 있다.

롤업 체인 블록의 경로

새로운 블록 후보의 시작은 블록 생성 시간과 함께 시작된다. 콜레이터는 모든 새로운 거래를 집계하여 롤업 체인 블록 후보에 넣는다. 이 과정에서 콜레이터는 롤업 체인 블록 후보에 서명하고 상태 전이 증명(유효성 증명, PoV)을 생성한다. 이는 후보 블록의 거래로 인해 발생한 최종 계좌 잔액의 요약이다. 콜레이터는 후보 블록과 PoV를 코어타임을 통해 롤업 체인에 의해 예약된 폴카닷 코어의 코어 내 밸리데이터에게 전송한다. 코어 내 밸리데이터는 블록 후보 내의 거래를 검증한다. 검증 후 모든 것이 정상이면 후보는 지원 가능 상태가 되고, 일부 코어 내 밸리데이터는 추가 검증을 위해 후보 블록을 다른 코어 내 밸리데이터와 공유한다. 코어 내 밸리데이터의 2/3가 성공적으로 검증하면 블록 작성자는 후보를 릴레이 체인에 지원할 수 있다. 데이터 가용성 체계는 모든 밸리데이터가 후보의 유효성을 검증할 수 있도록 보장한다. 분쟁이 발생하지 않으면 2차 검사 후 6초마다 블록이 릴레이 체인에 포함될 수 있다.

릴레이 체인의 밸리데이터들은 블록 후보에 대한 합의에 도달하려고 시도한다. 합의에 도달하면, 검증된 블록 후보가 밸리데이터 및 콜레이터와 공유되고, 이 프로세스는 새로운 거래에 대해 반복된다. 새로운 파이프라인 기능(비동기 백업이라고도 함)을 통해 콜레이터는 릴레이 체인 밸리데이터들에게 제안한 이전 블록 후보가 백업되는 동안 롤업 방식으로 새로운 블록을 계속 생성할 수 있다. 블록은 6초마다 릴레이 체인에 추가된다.

노미네이터

추천인은 누구인가요?

노미네이터는 스테이킹 참여자의 한 유형이다. 노미네이터는 밸리데이터에게 자신의 지분을 할당하는데, 밸리데이터는 두 번째 유형의 참여자이다. 지분을 할당함으로써, 밸리데이터는 활동하는 밸리데이터 그룹을 선출하고 지급되는 보상을 공유할 수 있다.

밸리데이터는 블록 생성 및 완결성 메커니즘에 참여하는 네트워크의 적극적인 참여자이지만, 노미네이터는 약간 더 수동적인 역할을 한다. 노미네이터가 된다고 해서 자체 노드를 운영하거나 온라인 가동 시간에 대해 걱정할 필요는 없다. 하지만 유능한 노미네이터는 자신이 선출한 밸리데이터에 대해 실사를 수행한다. 지명할 밸리데이터를 찾을 때, 노미네이터는 특정 밸리데이터를 지명할 때 받는 보상 비율과 밸리데이터가 슬래시될 경우 자신이 감수 해야 할 위험에 주의를 기울여야 한다.

왜 추천해야 하나요?

- 여러분은 전 세계의 다양한 전문가와 열광자들로 구성된 네트워크 참여자가 되어 차세대 인터넷인 Web3(분산화되고, 개인정보 보호에 중점을 두고, 신뢰할 수 있는 인터넷)를 구축하고 육성하고자 열망한다.
- 여러분은 네트워크 보안을 유지하는 데 필수적인 역할을 한다. 보증금 잔액은 Polkadot OpenGov 에서 투표 하고 네트워크의 미래 방향을 형성하는 데 사용될 수 있다.
- 폴카닷의 작동 방식을 기술적인 측면에서 이해하기 시작할 것이다. 지명 기술과 지식에 익숙해지면 지명 풀을 개설하고, 다른 사람들이 네트워크를 안전하게 보호하고 보상을 받을 수 있도록 돕고, 신뢰할 수 있는 지명 풀 운영자로서의 명성을 쌓을 수 있다. 더 적극적으로 참여하고 싶다면 다음 단계는 밸리데이터가 되는 것이다.
- 스테이킹 보상을 받으면 네트워크 인플레이션에 발맞추거나 (가능성상) 앞서 나갈 수 있다.

노미네이터는 네이티브 토큰(폴카닷의 DOT 또는 쿠사마의 KSM) 을 스테이킹하고 밸리데이터를 지명하여 릴레이 체인을 보호한다. DOT 계정이 있고 새로운 DOT를 획득하고 싶을 수도 있다. 밸리데이터로서 노드를 설정하고 24시간 운영 및 유지 관리 경험이 필요하다.

폴카닷에서는 한 명 이상의 검증인을 추천하여 DOT를 획득할 수 있다. 추천을 통해 선택한 검증인의 추천인이 된다. 검증인을 신중하게 선택하세요. 검증 인이 제대로 행동하지 않으면 슬래싱(slashing)을 당하고 DOT를 일부 잃게 된다. 하지만 네트워크 규칙을 준수하는 검증인은 해당 검증인이 생성하는 스테이킹 보상을 공유할 수 있다.

지명을 위해 토큰이 스테이킹되는 동안에는 '잠금'(본딩)된다. 언제든지 지명을 중단 할 수 있지만, 해당 조치는 다음 시대에 적용되며 자금 본딩이 자동으로 해제되지는 않는다. 본딩 해제는 별도의 조치이며, 본딩 해제 기간 이후에 적용된다. 본딩 해제 기간 동안 Polkadot-JS UI에 스테이킹 잠금이 표시되며, 그 이후에는 잠금이 해제되고 본딩된 자금은 자유롭게 이전할 수 있는 잔액이 된다.

빠른 언스테이킹

실수로 토큰을 본딩했거나 본딩된 토큰이 활성 밸리데이터를 지원하지 않은 경우, 이제 즉시 본딩을 해제할 수 있다.

Polkadot에서는 지난 28일 동안(Kusama에서는 7일 동안) 귀하의 본딩 잔액이 밸리데이터를 지원하지 않았다면, 빠른 스테이킹 해제를 진행할 수 있다. 스테이킹 대시보드에서 자동으로 자격 여부를 확인한다. 자세한 내용은 이 지원 문서의 "빠른 스테이킹 해제" 섹션을 참조하세요.

계정 설정

스태시 & 스테이킹 프록시

노미네이터는 별도의 스태시 계정과 스테이킹 프록시 계정을 설정하는 것이 좋다. 이러한 목적으로 별도의 계정을 생성하는 이유와 설명은 키 섹션에서 자세히 설명한다.

스태시 및 스테이킹 프록시 계정은 계정 생성 페이지에 자세히 설명된 권장 방법 중 하나를 통해 생성할 수 있다. 추천인이 되기 전에 가장 먼저 해야 할 일은 스테이킹에 사용할 자금을 이체할 수 있는 스태시 계정이 있는지 확인하는 것이다. 이러한 계정에는 Ledger 또는 Polkadot Vault 와 같은 "콜드 월렛" 솔루션을 사용하는 것이 좋다.

스태시 계정을 설정한 후에는 스테이킹 프록시를 사용하는 것이 좋다. 스태시 계정만으로도 노미네이터가 될 수 있지만, 보안상의 이유로 스테이킹 프록시를 사용하는 것이 좋다.

스태시의 스테이킹 프록시는 모든 스테이킹 관련 거래에도 서명할 수 있다. 스태시는 완전히 격리된다(사용자가 스태시의 스테이킹 프록시를 변경하거나 스태시에 다른 프록시를 연결하기로 결정하는 경우 제외).

보상 지급 계정

추천인은 보상을 지급받을 계정을 선택해야 한다. 다음 옵션 중 하나를 선택하실 수 있다.

- 스테이킹으로 돌아가면 보상은 보증금액에 합산된다.
- 보관: 보상은 무료 잔액으로 보관 계정으로 전송된다.
- 다른 계정으로: 보상은 사용자가 정의한 계정(보관함이 아님)으로 전송된다.

클라이언트 버전 0.8.23에 기본적으로 포함된 런타임 버전 v23부터는 모든 사용자 지정 주소로 지급금을 보낼 수 있다. 스테이킹 프록시나 스태시 계정이 아닌 계정으로 지급금을 리디렉션하려면 해당 계정을 설정해야 한다. 거래소 주소를 스테이킹 보상 수령 주소로 설정하는 것은 매우 안전하지 않다.

위반 행위

폴카닷은 허가가 필요 없는 공개 네트워크이다. 따라서 위법 행위에 대한 인센티브를 줄이고 올바른 행동에 대한 인센티브를 제공하는 메커니즘을 갖추고 있다. 아래에서 특정 위법 행위에 대한 처벌 요약을 확인하실 수 있다.

위반	슬래시 (%)	온체인 비활성화	오프체인 비활성화	평판 변화
백업이 무효된다	100%	예 (높은 우선순위)	예 (높은 우선순위)	아니요
무효 투표	2%	예 (중간 우선순위)	예 (중간 우선순위)	아니요
반대 투표	0%	예 (낮은 우선순위)	예 (낮은 우선순위)	아니요
GRANDPA / BABE / BEEFY 모호함	0.01-100%	예 (우선순위 변동)	아니요	아니요
두 번째 + 유효한 모호함	-	아니요	아니요	아니요
이중 두 번째 모호함	-	아니요	아니요	예

폴카닷에는 아래와 같이 6가지 주요 밸리데이터 위반 사항이 있다.

- 무효한 지원: 밸리데이터가 무효한 블록을 지원하고 있다.
- 무효 투표: 밸리데이터(보조 검사자)가 무효 블록에 찬성 투표한다.
- AgainstValid Vote: 밸리데이터(보조 검사자)가 유효한 블록에 반대표를 던지고 네트워크 리소스를 낭비한다.
- 모호성 : 밸리데이터가 동일한 블록이나 투표를 두 개 이상 생성한다.
- GRANDPA 와 BEEFY 모호함 : 밸리데이터가 동일한 라운드에서 서로 다른 체인에서 두 개 이상의 투표에 서명한다.
- BABE 모호성 : 밸리데이터는 동일한 시간 슬롯에서 릴레이 체인에 두 개 이상의 블록을 생성한다.
- 이중 세컨드 모호성 : 5명의 파라 밸리데이터로 구성된 후원 그룹 내에서 최대 5개의 파라블록이 지원될 수 있다. 각 파라블록은 5명의 잠재적 후원자로부터 정확히 1개의 지지 투표와 최소 2개의 유효 투표를 추가로 받아야 한다. 이는 릴레이 체인 블록 작성자에게 어느 정도 선택권을 제공하면서도 시스템이 처리해야 하는 파라블록 수의 상한선을 정하는 것이다. 후원자는 어떤 파라블록을 지지할지 결정해야 하며, 다른 파라블록을 지지할 수는 없다. 또 다른 지지 투표가 발견되면 처벌을 받게 된다(현재로서는 다소 가볍지만, 이로 인해 얻을 수 있는 이득은 거의 없다). 비동기 후원에서는 이 모든 것이 약간 더 복잡해진다. 후원자가 "미래"에 블록을 낙관적으로 지지할 수 있기 때문에 릴레이 체인 블록당 한 명의 후보가 더 이상 없기 때문이다.
- 재청 + 유효한 모호성 : 악의적인 노드가 먼저 무언가를 재청(절대적인 책임을 지고)한 후, 다른 노드가 책임을 지고 나서야 방금 옳다고 말한 사람인 척하는 경우 발생한다. 이러한 행동은 노드가 두 가지 상충되는 입장을 보이기 때문에 모호성의 명백한 사례이다. 노드는 책임을 회피하기 위해 이러한 전략

을 사용할 수 있지만, 시스템이 두 가지 상충되는 투표를 감지하면 해당 위반 사항이 보고된다.

모호함 (상충되는 진술)

모호함은 밸리데이터가 서로 충돌하는 진술을 생성할 때 발생한다.

예를 들어, BABE 가 임명한 블록 작성자는 주어진 슬롯에 대해 단 하나의 블록만 작성해야 하며, 두 개 이상이 작성되면 서로 충돌하게 된다. 이는 BABE 모호성 위반에 해당한다.

BEEFY & GRANDPA 밸리데이터는 자신이 최고라고 생각하는 블록에 한 표를 행사해야 하지만, 서로 다른 블록에 두 개 이상의 표를 행사한 것으로 밝혀지면 상충되는 진술로 네트워크를 혼란스럽게 하려고 했다는 의미이며, 이 사실이 밝혀지면 BEEFY/ GRANDPA 모호성 위반으로 간주된다.

모호성은 일반적으로 밸리데이터 호스트에 중복된 서명 키가 존재할 때 발생한다. 키가 중복되지 않으면, 정직한 모호성 슬래시가 발생할 확률은 거의 0으로 감소한다.

처벌

폴카닷에서는 네트워크 위반 행위가 심각도에 따라 처벌될 수 있다. 주요 처벌은 세 가지이다. 계정 삭제, 계정 정지, 그리고 평판 훼손이다.

슬래싱

밸리데이터가 네트워크에서 부적절한 행동을 할 경우 슬래싱이 발생한다. 밸리데이터와 노미네이터는 스테이킹된 토큰의 일정 비율을 최소 0.01%에서 최대 100%까지 손실하게 된다.

슬래싱된 토큰은 모두 재무부(Treasury)로 이전된다. 이렇게 하는 이유는 (소각하거나 보상으로 분배하는 것이 아니라) 재무부에서 지급함으로써 슬래싱을 되돌릴 수 있기 때문이다. 이는 잘못된 슬래싱과 같은 상황에서 유용할 것이다. 합법적인 슬래싱의 경우, 재무부 절차에 따라 악의적인 밸리데이터로부터 생태계를 지원하고 강화하는 기여자에게 토큰이 재분배된다.

슬래싱은 특정 노미네이터에 대한 활성 검증에서만 발생하며, 다른 비활성 또는 대기 중인 지명이 있는 경우 슬래싱이 완화되지 않는다. 또한 밸리데이터 운영자가 별도의 노드를 운영하는 경우에도 슬래싱이 완화되지 않는다. 각 노드는 슬래싱 목적으로 별도의 개체로 간주된다.

여러 활성 후보 지명

드물지만, 매우 큰 규모의 본드가 있는 경우, 노미네이터는 한 시대에 여러 밸리데이터를 적극적으로 지명할 수 있다. 이 경우, 슬래시는 해당 밸리데이터에게 스테이킹된 금액에 비례한다. 각 밸리데이터에게 할당되는 스테이킹 비율을 제어하거나 활성 밸리데이터를 선택할 수 없다(단일 밸리데이터를 지명하는 간단한 경우는 제외). 스테이킹 할당은 Phragmén 알고리즘에 의해 제어된다.

밸리데이터가 삭감되면 "적용되지 않은 삭감" 상태로 저장된다. Polkadot-JS UI 를 통해 이를 확인할 수 있다. UI에는 밸리데이터별 삭감 내역과 영향을 받는 모든 노미네이터 및 금액이 표시된다. 삭감이 적용되지 않은 경우, 27일의 유예 기간 동안 거버넌스 제안을 통해 삭감 취소를 요청할 수 있으며, 그 후 삭감이 적용된다.

다음과 같은 상황에서는 슬래시가 발생할 수 있다.

1. 모호함 – 단 한 번의 유발만으로도 0.01%의 삭감이 적용된다. 더 많은 밸리데이터가 모호함을 보일 수록 삭감량은 점진적으로 100%까지 증가한다.
2. 분쟁 – 밸리데이터가 블록 내용을 허위로 표시하려고 시도할 경우 분쟁이 발생할 수 있다. 100%의 슬래싱 페널티가 적용될 수 있다.

모호함을 위한 슬래시

다음과 같은 범죄 수준이 정의되어 있다. 그러나 이러한 특정 수준은 코드나 시스템에 구현되거나 언급되지 않는다. 이는 범죄의 심각도에 따른 다양한 수준에 대한 지침일 뿐이다.

- 레벨 1: 고립된 모호함은 최소한의 지분만을 삭감한다.
- 레벨 2: 우발적인 행위는 아니지만 네트워크 보안에 큰 피해를 주지 않는 부정 행위. GRANDPA에서 동시다발적인 모호 행위나 정당하지 않은 투표가 단발적으로 발생한 사례가 그 예이다. 지분의 상당 부분을 약간 삭감한다.
- 레벨 3: 시스템에 심각한 보안 또는 금전적 위험을 초래하는 부정행위 또는 대규모 공모. 밸리데이터가 보유한 지분의 전부 또는 대부분을 삭감한다.

다음은 모호함 속에서 슬래시를 구축하는 시나리오이다.

1. 서버 복제, 즉 새 하드웨어로 마이그레이션할 때 모든 콘텐츠를 복사하는 행위는 피해야 한다. 이 작업은 피해야 한다. 이미지가 필요한 경우, 키가 생성되기 전에 이미지를 생성해야 한다.
2. 고가용성(HA) 시스템 – 장애가 발생한 서버가 재시작되거나, 오탐지(false positive) 이벤트로 인해 두 서버가 동시에 온라인 상태가 되는 등 동시 작업이 있는 경우 모호성이 발생할 수 있다. HA 시스템은 매우 신중하게 사용해야 하며 권장되지 않는다.
3. 한 인스턴스에서 다른 인스턴스로 데이터베이스를 복사할 때 키 저장소 폴더가 복사된다. 단일 사고에서 슬래시(/)가 모호하게 사용된다는 점에 유의해야 한다. 이는 중복된 키 저장소가 몇 초 동안만 사용되는 경우 발생할 수 있다. 슬래시(/)는 노미네이터와 자금을 잃고, 분산 노드 프로그램에서 제외되며, 평판이 손상될 수 있다.

모호성에 대한 슬래시 금액 계산 방법을 알아보려면 다음 섹션을 참조하세요. 슬래싱에 대해 더 자세히 알아보려면 슬래싱 연구 페이지를 참조하세요.

모호성에 대한 슬래시 계산

GRANDPA, BABE, BEEFY의 모호함은 슬래싱 페널티를 계산하는 데 동일한 공식을 사용한다.

Let x = offenders, n = total number of validators in the active set

$$\min((3 * x / n)^2, 1)$$

예를 들어, 활성 세트에 100명의 밸리데이터가 있고 한 명이 슬롯에서 모호한 행동을 한다고 가정해 보겠다(BABE 든 GRANDPA 든 모호한 행동은 중요하지 않다). 이는 네트워크 공격일 가능성은 낮지만, 밸리데이터의 잘못된 설정일 가능성이 훨씬 높다. 페널티는 $\min(3 * 1 / 100)^2, 1) = 0.0009$, 즉 해당 밸리데이터(즉, 밸리데이터와 그 노미네이터가 보유한 지분)에 대해 0.09%의 삭감이 적용된다.

이제 한 그룹이 여러 밸리데이터를 운영하고 있고, 모두 같은 슬롯에 문제가 있다고 가정해 보겠다. 페널티는 $\min((3 * 5 / 100)^2, 1) = 0.0225$, 즉 2.25%의 슬래시가 적용된다. 만약 20명의 밸리데이터가 모호한 답변을 한다면, 이는 훨씬 더 심각한 위반이며, 네트워크에 대한 조직적인 공격을 시사할 수 있다. 따라서 슬래시가 훨씬 더 커진다. $\min((3 * 20 / 100)^2, 1) = 0.36$, 즉 모든 밸리데이터와 그 노미네이터에게 36%의 슬래시가 적용된다. 슬래시가 적용된 모든 밸리데이터는 또한 강제로 정지된다.

위의 예시는 활성 세트에서 여러 밸리데이터를 지명하거나 운영할 때 발생할 수 있는 위험을 보여준다. 보상은 선형적으로 증가하는 반면(밸리데이터 두 명은 한 명보다 약 두 배 많은 스테이킹 보상을 받음), 슬래시는 기하급수적으로 증가한다. 밸리데이터 한 명이 모호하게 행동하면 0.09%의 슬래시가 발생하고, 밸리데이터 두 명이 모호하게 행동하면 $0.09 * 2 = 0.18\%$ 의 슬래시가 발생하는 것이 아니라 0.36%의 슬래시가 발생하여 밸리데이터 한 명보다 4배 더 커진다.

밸리데이터는 노드 중 하나가 다운되더라도 검증 작업을 계속 수행할 수 있도록 여러 머신에서 노드를 실행할 수 있다. 하지만 밸리데이터 운영자는 이러한 노드를 설정할 때 주의해야 한다. 서명 머신 관리에 대한 원활한 협력이 이루어지지 않으면 모호한 상황 이 발생할 수 있다.

슬래싱을 피하기 위한 좋은 방법

노드 운영자에게는 완벽한 바이너리나 소스 코드를 확보하고 노드의 보안을 보장하기 위해 다음 사항을 권고한다.

1. 항상 공식 Parity 저장소에서 소스 파일이나 바이너리를 다운로드하세요.
2. 다운로드한 파일의 해시를 확인하세요.
3. W3F 보안 검증기 설정을 사용하거나 해당 원칙을 준수하세요.
4. 필수 보안 항목을 확인하고 방화벽을 사용하고 사용자 액세스를 관리하고 SSH 인증서를 사용하세요.
5. 서버를 범용 시스템으로 사용하지 마십시오. 워크스테이션이나 다른 서비스를 호스팅하는 시스템에 검증을 호스팅하면 악의적인 행위의 위험이 커진다.

과거에 일어났던 사소한 모호함의 몇 가지 예는 다음과 같다.

블록 체인	연대	이벤트 유형	세부	취해진 조치
폴 카 닷	774	작은 모호함	밸리데이터가 서버를 마이그레이션하고 키 저장소 폴더를 복제했다. 온체인 이벤트는 여기에서 확인할 수 있다.	밸리데이터가 슬래시 취소 요청을 제출하지 않았다.
쿠사마	3329	작은 모호함	밸리데이터는 복제된 키를 사용하여 테스트 머신을 운영했다. 테스트 머신은 기본 머신과 동시에 온라인 상태였기 때문에 슬래시가 발생했다. 자세한 내용은 여기에서 확인할 수 있다.	밸리데이터는 슬래시 취소를 요청했지만 위원회는 거부했다.
쿠사마	3995	작은 모호함	밸리데이터는 여러 오류를 발견한 후 클라이언트가 충돌하여 슬래시가 적용됐다. 밸리데이터는 모든 이벤트를 기록하고 GitHub 이슈를 공개하여 기술적인 의견을 공유할 수 있도록 했다.	밸리데이터가 슬래시 취소를 요청했다. 위원회는 해당 오류가 운영자와 관련이 없다고 판단하여 요청을 승인했다.

NPoS에서 슬래싱을 적용하는 데에는 세 가지 주요 어려움이 있다.

노미네이터는 여러 밸리데이터를 추천할 수 있으며, 그 중 누구를 통해서든 슬래시를 받을 수 있다. 삭감될 때까지 해당 지분은 시대별로 재사용된다. E 시대 연속으로 N개의 코인을 지명한다고 해서 N*E개의 코인을 삭감할 수 있다는 뜻은 아니다. N개만 가지고 있었던 것이다. 사형에 처할 수 있는 범주는 사후에, 순서 없이 발견될 수 있다. 이러한 균형을 맞추기 위해 시스템은 참가자가 주어진 기간 동안 받을 수 있는 최대 슬래시 값만 적용하며, 총액은 적용되지 않는다. 이를 통해 과도한 슬래시 발생을 방지할 수 있다.

비활성화

비활성화는 밸리데이터가 위법 행위를 저지른 후 특정 작업을 수행하지 못하도록 차단한다. 비활성화는 다음과 같이 세분화된다.

체인상 비활성화는 한 시대 동안 지속되며 밸리데이터가 블록 작성, 지원 및 분쟁 시작을 중단한다. 오프체인 비활성화는 세션 동안 지속되며, 분쟁에서 패배하면 발생하고 밸리데이터가 분쟁을 시작하는 것을 막는다. 오프체인 비활성화는 항상 온체인 비활성화보다 우선순위가 낮다. 오프체인 비활성화는 후원자 비활성화를 먼저, 그다음 승인 확인자 비활성화를 우선시한다.

평판 변경

스팸과 관련된 일부 경미한 위반은 네트워킹 평판 변경(Networking Reputation Changes)을 통해서만 처벌된다. 밸리데이터는 서로 연결될 때 각 피어에 대한 평판 지표를 사용한다. 피어가 귀중한 데이터를 제공하고 적절하게 행동하면 시스템은 평판을 높이고, 잘못된 데이터나 스팸 데이터를 제공하면 시스템은 평판을 낮춘다. 밸리데이터는 평판을 충분히 잃을 수 있으며, 이로 인해 피어는 일시적으로 채널을 닫을 수 있다. 이는 DoS(서비스 거부) 공격에 대응하는 데 도움이 된다. 채널 폐쇄의 결과는 다양할 수 있다. 일반적으로 평판이 낮아진 상태에서 밸리데이터 작업을 수행하는 것은 더 어려워지고, 결과적으로 밸리데이터 보상이 줄어든다.

탈중앙화 컴퓨터

엘프 프로토콜

파라체인 프로토콜은 릴레이 체인에 연결된 각 파라체인에 대해 반복적으로 병렬로 수행될 수 있는 프로세스를 통해 파라체인 블록의 작성부터 포함까지 전달하는 것을 목표로 한다. 이 프로토콜은 강력한 보안을 보장하는 동시에 파라체인 간에 네트워크를 효율적으로 샤딩할 수 있도록 한다. 가용성 및 유효성(AnV) 프로토콜은 가용성과 유효성의 관점에서 파라체인 프로토콜을 설명한다.

주요 배우들

밸리데이터

이들은 제안된 파라체인 블록의 유효성 증명 (PoV) 을 확인하고 지정된 기간 동안 PoV가 사용 가능한 상태로 유지되도록 보장함으로써 블록의 유효성을 검증할 책임이 있다. 이들은 "스킨 인 게임(skin in the game)"을 가지고 있는데, 이는 온체인에 예치된 자금을 보유하고 있으며, 부정 행위 발생 시 네트워크에서 일부 또는 전부를 몰수할 수 있음을 의미한다.

콜레이터들

밸리데이터가 확인할 수 있는 PoV를 생성한다. PoV를 생성하려면 특정 파라체인의 거래 형식과 블록 작성 규칙에 대한 지식이 필요하며, 해당 파라체인의 전체 상태에 접근할 수 있어야 한다.

피셔맨: 더 이상 사용되지 않음

AnV 의정서의 이전 제안과 달리 어부들은 공식적인 시행을 계획하지 않았다.

피셔맨의 기본 아이디어는 콜레이터처럼 파라체인의 전체 노드이지만, 네트워크와 관련하여 다른 역할을 수행한다는 것이다. 콜레이터처럼 상태 전환을 패키징하고 다음 파라체인 블록을 생성하는 대신, 피셔맨은 이 과정을 감시하고 잘못된 상태 전환이 포함되지 않도록 한다.

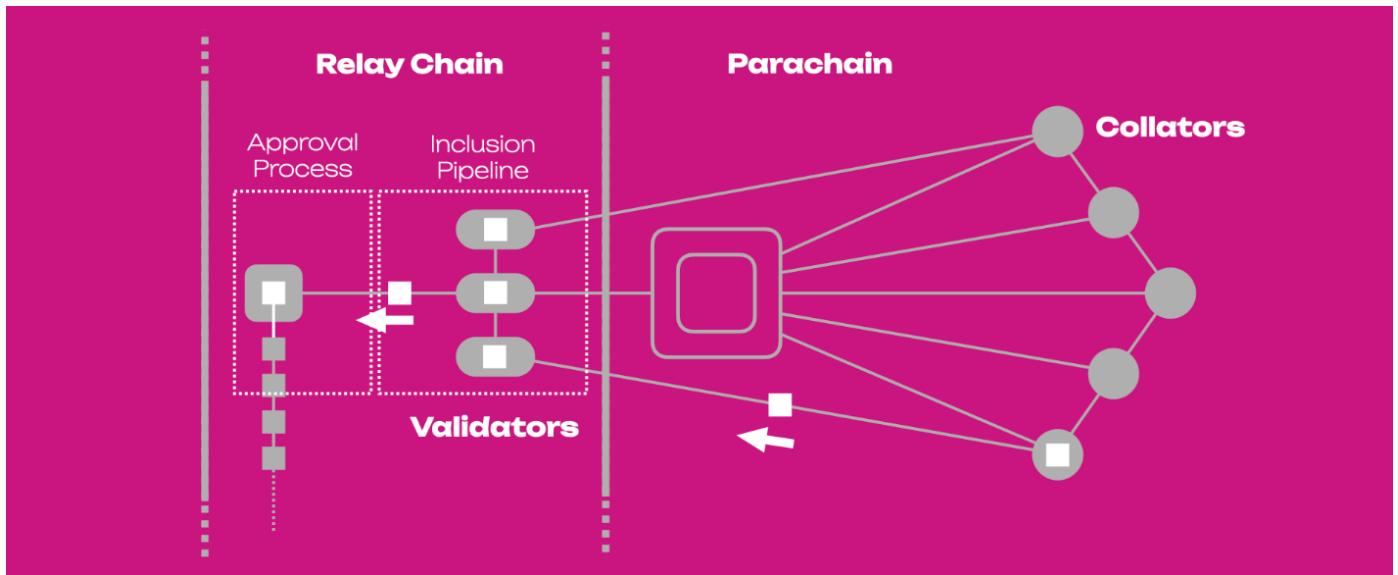
피셔맨 설계 고려 사항의 동기를 설명하기 위해, 현재 보조 밸리데이터(secondary backing checker)는 네트워크와 관련하여 유사한 역할을 수행한다. 보안 관점에서 볼 때, 보안은 파라체인 밸리데이터 또는 보조 밸리데이터 중 최소 한 명 이상의 정직한 밸리데이터를 확보하는 데 기반한다(자세한 내용은 나중에 설명).

프로토콜 요약

파라체인 프로토콜

파라체인 프로토콜은 두 가지 주요 단계로 나뉜다.

- 포함 파이프라인 : 수집자는 PoV가 포함된 파라체인 블록(파라블록)을 밸리데이터에게 전송한다. 밸리데이터는 파라블록이 파라체인의 상태 전환 규칙을 준수하는지 확인하고 긍정적 또는 부정적 결과를 초래할 수 있는 진술에 서명한다. 충분한 양의 긍정적 진술이 있으면 블록은 지지 되고 릴레이 체인에 포함되지만, 아직 승인 대기 중이다.
- 승인 프로세스 : 밸리데이터는 추가 검사를 수행하여 긍정적인 결과가 나오면 파라블록을 승인한다. 아래 그림은 콜레이터와 밸리데이터가 있는 파라체인을 보여준다. 또한, 파라체인 블록(흰색 사각형)이 포함 파이프라인과 승인 프로세스를 거치는 과정도 보여준다.



가용성 및 유효성(AnV) 프로토콜

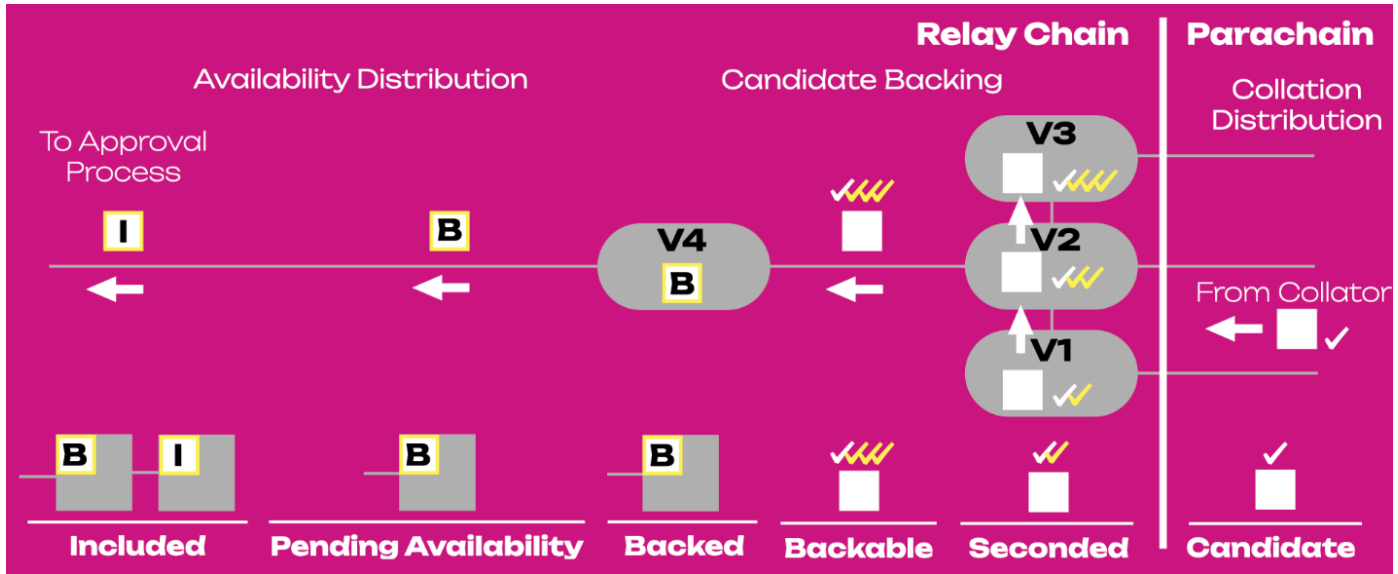
가용성 및 유효성(AnV) 프로토콜은 파라체인 프로토콜을 다른 관점에서 바라보는 방식으로, 최종 릴레이 체인에 포함되기 전에 파라블록이 사용 가능하고 유효한지 확인하는 것의 중요성을 강조한다. 이 프로토콜은 포함 파이프라인 내 3단계와 승인 프로세스 내 2단계, 총 5단계로 나뉜다.

- 포함 파이프라인 1. 파라체인 단계 2. 릴레이 체인 제출 단계 3. 가용성 및 비가용성 단계
- 승인 프로세스 1. 할당 및 2차(유효성) 검사 2. 체인 선택
포괄 파이프라인에서는 파라블록이 사용 가능(또는 사용 불가능)하게 되는 반면, 승인 프로세스에서는 파라블록이 유효한지 여부가 확인된다.

포괄 파이프라인

개요

포함 파이프라인은 파라체인 블록(또는 파라블록)이 생성되어 최종화되지 않은 릴레이 체인(즉, 릴레이 체인의 포크)에 포함되는 경로이다.



위 그림은 후보 블록이 포함 파이프라인을 통과하는 경로를 보여준다. 블록은 이 경로를 통해 다음과 같이 상태를 변경한다.

- 후보 : PoV를 포함한 블록이 콜레이터(collator)에 의해 파라-밸리데이터(이 경우 V1)에게 제출된다. 후보 블록은 흰색 사각형으로 표시되며, 측면에 흰색 체크 표시가 하나 있다(콜레이터의 PoV). 후보 블록은 아직 유효하지 않으며, 릴레이 체인에 포함되지 않을 수 있다.
- 동의: 블록은 보조 밸리데이터 V1에 의해 다른 보조 밸리데이터(이 경우 V2와 V3)에게 제시된다. 동의된 블록은 흰색 사각형 위에 흰색 체크 표시와 노란색 체크 표시가 있는 형태로 표시된다. 노란색 표시는 보조 밸리데이터 V1의 PoV를 나타낸다.
- 지원 가능: 블록의 유효성은 대부분의 준밸리데이터에 의해 입증된다. 지원 가능한 블록은 흰색 사각형 위에 흰색 체크 표시와 그 위에 세 개의 노란색 체크 표시가 있는 형태로 표시된다. 노란색 표시는 준밸리데이터의 PoV를, 흰색 표시는 콜레이터의 PoV를 나타낸다.
- 백업됨: 블록은 릴레이 체인 블록 작성자(이 경우 V4)에 의해 릴레이 체인의 포크에 백업되고 표시된다. 백업된 블록은 흰색 배경과 노란색 테두리로 둘러싸인 "B"가 있는 사각형으로 표시된다. 백업된 블록은 여전히 릴레이 체인에 포함되지 않을 수 있다. 편의상 백업된 파라체인 블록은 릴레이 체인 블록 내에 표시되지만, 실제로 릴레이 체인 블록은 파라블록 자체를 포함하지 않는다(자세한 내용은 나중에 설명).
- 이용 가능 여부 대기 중: 블록은 지원되었지만 아직 이용 가능한 것으로 간주되지 않는다.
- 포함됨: 블록은 지지대가 있고 사용 가능한 것으로 간주된다(파라블록이 있다). 포함된 파라블록은 흰색 배경에 노란색 테두리로 "I"를 둘러싼 정사각형으로 표시된다.

비동기 백킹

파라블록의 백킹과 인클루전은 릴레이 체인에 기록되는 데 12초가 걸린다. 즉, 백킹은 한 릴레이 체인 블록에서 6초 동안 발생하고, 인클루전은 다른 릴레이 체인 블록에서 추가로 6초가 소요된다(위 그림 참조). 비동기 백킹을 사용하면 백킹과 인클루전을 단 하나의 릴레이 체인 블록에만 기록할 수 있다.

파라체인 단계

파라체인 단계에서는 밸리데이터 할당 루틴(Validator Assignment Routine)을 통해 일부 밸리데이터가 파라체인에 할당된다(이러한 밸리데이터를 파라-밸리데이터(Para-validator)라고 함). 파라-밸리데이터는 콜레이터(Collator)와 연결을 설정하며, 콜레이터는 밸리데이터 분배 서브시스템(Collator Distribution Subsystem)을 통해 파라-밸리데이터에게 검증 증명(PoV)과 함께 후보 블록을 제안한다.

파라 밸리데이터는 후보자 지원 하위 시스템에 참여한다. 파라 밸리데이터는 후보 블록이 파라체인의 상태 전환 규칙을 따르는지 확인해야 한다. 상태는 머클 트리에 저장되므로 파라 밸리데이터는 전체 상태에 접근하지 않고도 상태 전환을 검증할 수 있지만, 다음 사항이 필요하다.

- 블록 후보(상태 전환 목록)
- 블록이 수정하는 파라체인 데이터베이스의 값
- Merkle 트리에서 영향을 받지 않은 포인트의 해시

이러한 정보 집합을 유효성 증명(PoV)이라고 한다.

파라 밸리데이터가 PoV를 획득하면, 이 정보를 다른 파라 밸리데이터들에게 공유하고, 다른 파라 밸리데이터들은 후보 블록을 PoV와 비교한다. 서명된 유효성 진술의 절반 이상을 수집한 후보는 지지 가능한 것으로 간주되며(즉, 유효한 상태 전환을 나타내는 것으로 보임), 이를 뒷받침하는 것은 서명된 진술들의 집합이다. 파라 밸리데이터는 후보 영수증(릴레이 체인 블록에 포함되는 것)과 삭제 코딩(파라블록을 사용 가능하게 만드는 것, 나중에 자세히 설명)을 구성하여 네트워크의 모든 밸리데이터에게 전송할 수 있다.

Polkadot은 유효한 상태가 아닌 유효한 상태 전환을 보장한다.

밸리데이터는 파라체인 상태의 모든 값을 검사하지 않고, 수정된 값만 검사한다. 이를 통해 수정된 값이 유효한지 확인할 수 있다.

앞서, 우리는 백업 가능한 블록이 유효한 상태 전환을 나타내는 것처럼 보인다고 언급했다. 파라 밸리데이터는 전체 밸리데이터의 일부이기 때문이다. 따라서 파라 밸리데이터 대부분이 부정직할 수 있다. 나중에는 파라블록의 완전한 유효성을 보장하기 위해 더 많은 밸리데이터가 참여하게 될 것이다.

릴레이 체인 제출 단계

지원 가능한 파라블록의 영수증은 다른 파라체인의 영수증과 함께 릴레이 체인 거래 대기열에 추가된다. 영수증에 대한 소문이 돌고, 릴레이 체인 블록 작성자가 BABE 슬롯 리더십을 획득하면 릴레이 체인 포크의 블록에 포함할 후보 영수증을 선택한다.

블록 작성자는 릴레이 체인 블록에 포함될 각 파라체인에 대해 최대 1개의 지원 가능 후보를 백킹과 함께 표시할 수 있다. 릴레이 체인의 포크에 포함되면 후보는 해당 포크에서 백킹된 것으로 간주된다. 후보는 "사용 가능 여부 대기" 상태 로 간주되며, 사용 가능함이 입증된 후에야 파라체인의 일부로 간주될 수 있다. 이 단계에서 릴레이 체인의 밸리데이터는 해당 파라블록의 삭제 코딩 정보를 이미 수신했음을 기억하십시오.

가용성 및 비가용성 단계

가용성 및 비가용성 단계에서 밸리데이터는 후보의 가용성을 보장하기 위해 가용성 분배 서브시스템 (Availability Distribution Subsystem)에 참여한다. 밸리데이터는 삭제된 코드 조각들을 네트워크 간에 공유한다. 최소 $\frac{1}{3} + 1$ 명의 밸리데이터가 코드워드 조각을 보유하고 있다고 보고해야 한다. 밸리데이터 수가 이 임계값에 도달하면 네트워크는 후보 블록을 사용 가능한 것으로 간주할 수 있다. 해당 블록은 완전한 파라체인 블록으로 분류되고, 헤더는 릴레이 체인의 해당 포크에 포함된다. 후보 가용성에 대한 정보는 해당 포크의 후속 릴레이 체인 블록에 기록된다.

블록 작성자가 수행하는 가용성 검사는 밸리데이터가 삭제 코드화된 청크를 배포한 블록만 릴레이 체인에 포함되도록 보장하지만, 유효성을 보장하지는 않는다. 각 파라체인에 참여하는 파라밸리데이터의 수가 매우 적기 때문에 담합은 합리적인 우려 사항이다. 블록 생성(BABE)과 완결성(GRANDPA)을 분리함으로써, 밸리데이터는 블록 생성 후 완결되기 전에 추가 유효성 검사를 수행할 수 있다.

따라서 파라블록이 사용 가능하고 파라체인의 일부로 간주되면 여전히 "승인 대기 중" 상태이다. 특정 파라체인에 대한 포함 파이프라인이 완료되어야 해당 파라체인에 새 블록이 승인될 수 있다. 포함 후 승인 프로세스가 시작되어 블록의 유효성을 확인하고 여러 파라체인 블록에 동시에 적용될 수 있다.

데이터 가용성 - 파라체인 블록 및 PoV의 삭제 코드

파라체인 블록과 해당 유효성 증명(PoV)을 재구성하는 데 필요한 삭제 코드 청크는 릴레이 체인 밸리데이터의 하드웨어(디스크)에 저장되며 최대 24시간 동안 릴레이 체인 네트워크에서 사용할 수 있다. 이 데이터는 릴레이 체인 블록이나 체인 상태에 저장되지 않는다는 점에 유의해야 한다. 해당 청크의 루트만 후보 영수증에 내장되어 릴레이 체인 블록에 저장된다.

포용 실패

후보자는 다음과 같은 이유로 파라체인에 포함되지 못할 수 있다.

- 수집기는 할당된 밸리데이터에게 블록을 전파할 수 없다.
- 후보자는 후보자 지원 하위 시스템에 참여하는 밸리데이터의 지원을 받지 않는다.
- 릴레이 체인 블록 작성자는 후보자를 선택하지 않는다.
- 후보자의 PoV는 시간 초과 내에 사용할 수 없는 것으로 간주되고, 블록은 릴레이 체인에서 삭제된다.

승인 프로세스

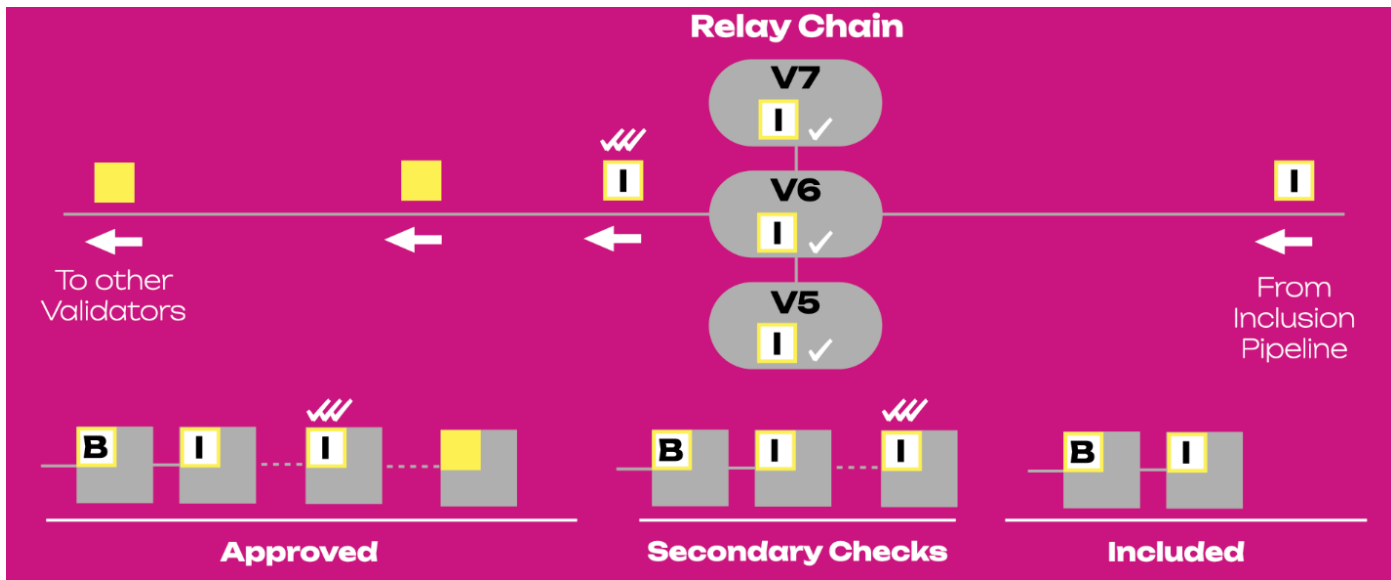
개요

파라블록이 사용 가능하고 파라체인 블록의 일부로 간주되면 여전히 "승인 대기" 상태이다. 이 단계에서 파라블록은 파라체인에 잠정적으로 포함되지만, 추가 확인이 필요하다. 파라체인에 할당된 밸리데이터(즉, 파라체인 밸리데이터)는 최악의 경우 1/3가 부정직하다고 가정되는 밸리데이터 집합에서 샘플링된다. 이 경우, 특정 파라체인에 대해 샘플링된 무작위 파라블록 밸리데이터의 대다수가 부정직하며 후보를 잘못 지지할 가능성이 높다. 이를 해결하기 위해 승인 프로세스는 추가 파라블록 밸리데이터를 할당하지 않고 사후에 부정 행위를 감지할 수 있도록 하며, 이는 궁극적으로 시스템 처리량을 감소시킨다. 파라블록은 사용 가능한 것으로 간주된 후 자식 블록을 허용할 수 있으므로, 승인 프로세스를 통과하지 못하면 파라블록과 그 하위 블록(자식 블록)이 무효화된다. 해당 블록을 지지한 밸리데이터만 슬래시되며, 하위 블록을 지지한 밸리데이터는 슬래시되지 않는다.

승인 파이프라인은 다음 단계로 나눌 수 있다.

1. 포괄 파이프라인에 포함된 파라블록은 2차 확인 기간 이라고 알려진 기간 동안 승인을 기브릿지고 있다.
2. 2차 검사 기간 동안 밸리데이터(2차 검사자)는 VRF 추첨을 기반으로 무작위로 자체 선택하여 각 패러블록에 대한 2차 검사를 수행한다.
3. 2차 검사기는 PoV로 파라블록을 획득하고(PoV를 재구성하려면 삭제 코딩이 필요함) 검증 기능을 다시 실행한다.
4. 2차 밸리데이터들은 자신의 검증 결과에 대해 책임을 진다. 모순되는 결과는 모든 밸리데이터가 블록을 검증해야 하는 상황으로 이어진다. 패배한 측 밸리데이터는 삭감된다.
5. 프로세스가 끝나면 파라블록이 승인되거나 거부된다.

아래 그림은 파라체인 블록이 인클루전 파이프라인을 통과하여 승인 프로세스에 진입할 때의 경로를 보여준다. 파라체인 블록은 지지되고, 사용 가능하며, 이의 제기되지 않을 때 승인된다. 파라체인 블록은 밸리데이터 하위 그룹(V5, V6, V7)에 의해 두 번째 검증을 받고, 모순되는 결과가 없으면 블록이 승인되어 다른 릴레이 체인 밸리데이터들에게 가십(gossiping)된다. 2차 검증 후 파라체인 블록은 흰색 배경, 노란색 테두리 안에 "I" (포함됨을 의미)가 있는 사각형, 그리고 세 개의 흰색 체크 표시(각 2차 검증마다 하나씩)로 표시된다. 승인된 파라체인 블록은 노란색 사각형으로 표시된다.



과제 및 2차 확인

릴레이 체인의 포크에 잘못된 파라블록이 있어도, 해당 블록이 최종 가젯인 GRANDPA에 의해 승인 및 완료되지 않는 한 심각한 문제는 아니다. 블록이 완료되지 않으면, 해당 블록이 포함된 체인의 포크는 무시되고, 대신 좋은 블록이 포함된 다른 포크가 사용된다. 잘못된 파라블록을 처리하는 단계는 다음과 같다.

- 감지: 불량 블록은 정직한 밸리데이터에 의해 감지되어야 한다.
-에스컬레이션: 정직한 밸리데이터가 분쟁을 시작해야 한다.
- 결과: 해당 파라블록의 후원자가 줄어들었다.
분쟁의 결과는 다른 모든 포크에 이식될 수 있어야 하므로 악의적인 밸리데이터는 가능한 모든 기록에서 삭제되고 정직한 밸리데이터는 해당 파라블록이 포함된 모든 포크를 무시하게 된다.

파라블록 vs. 릴레이 체인 블록

릴레이 체인 블록은 파라블록이 아니라 파라헤더를 포함한다는 점을 이해하는 것이 중요하다. 파라체인 블록은 파라체인 내부에 있다. 따라서 승인된 파라블록 대신 릴레이 체인 블록이 승인되었다고 생각하는 것이 더 합리적이다. 승인된 파라블록에 대한 정보를 포함하는 릴레이 체인 블록은 상위 릴레이 체인 블록도 승인된 경우 승인된 것으로 간주될 수 있다. 따라서 릴레이 체인 블록의 유효성은 상위 체인 블록의 유효성에 따라 달라진다.

밸리데이터는 승인 프로세스에서 두 가지 주요 작업을 수행한다.

- 할당은 어떤 밸리데이터가 어떤 후보자에 대해 승인 확인을 수행할지 결정하여 각 후보자가 충분한 무작위 검사기를 받도록 한다. 이 단계는 승인 투표를 추적하여 미참석 승인 확인에 의심스러운 정도로 오랜 시간이 걸리는 경우를 파악한다. 또한, 릴레이 체인 모호성을 추적하여 공격자가 할당에 대한 사전 지식을 얻었을 가능성을 파악하고 그러한 경우 추가 검사를 추가한다. 할당자는 후보자를 포함하는 릴레이 체인 블록에 대한 두 가지 가능한 스토리 (즉, 후보를 사용 가능으로 선언) 를 기반으로 두세 가지 할당 기준을 사용하여 특정 후보자를 확인하는 자체 할당을 결정 한다. 할당 알림은 노드 간에 소문으로 퍼져 모든 밸리데이터가 어떤 밸리데이터가 어떤 후보자를 확인해야 하는지, 그리고 후보자에게 추가 검사기가 필요한지 여부를 알 수 있도록 한다.
- 승인 확인은 후보자 확보, 유효성 검증, 승인 투표 발송 또는 분쟁 제기를 통해 확인을 수행한다. 승인 확인에는 후보 블록 재구성, 후보 수신 확인을 위한 삭제 코딩 재실행, 후보 블록 자체 재확인을 위한 미출석(no-show) 제한 시간(즉, 릴레이 체인 슬롯 하나 이상)이 있다. 밸리데이터가 미출석 제한 시간 내에 승인 또는 분쟁을 제기하지 않으면 미출석으로 분류된다. 밸리데이터는 할당 작업으로 과부하될 수 있으므로, 미출석을 방지하기 위해 할당 알림 발송을 의도적으로 지연할 수 있다(자세한 내용은 할당 연기 참조).

이 두 단계는 먼저 모든 밸리데이터 간에 주고받은 메시지를 사용하는 오프체인 합의 프로토콜로 실행되고, 그 후 해당 프로토콜의 진행 상황을 온체인에 기록한다. 온체인 프로토콜은 오프체인 프로토콜에 보상을 제공하는 데 필요하다. 온체인 검증은 두 단계로 구성된다. a) 할당 알림과 승인 투표는 릴레이 체인 블록에 기록되고, b) 다른 릴레이 체인 블록의 메모는 승인 코드에 입력된다.

가십 메시지는 할당 알림과 승인 투표의 두 가지 유형으로 구성되며, 승인 키로 서명된다. 이러한 키는 밸리데이터가 사용하는 세션 키의 일부이다. 간단히 말해, 승인 키는 다음과 같다.

- VRF 할당 기준에만 사용되는 sr25519 키인 승인 할당 키이다.
- ed25519인 승인 투표 키는 후보자 파라블록 유효성에만 서명한다.

파라블록을 수용하는 것은 분쟁 없이 감지 단계를 통과했거나, 긍정적인 결과로 확대/분쟁 단계를 통과한 결과이다.

체인 선택

블록 내 모든 후보 영수증에 대해 충분한 2차 검증이 수행된 후, 밸리데이터는 GRANDPA에서 해당 블록(및 이전 모든 블록)에 투표할 수 있다. 블록이 $\frac{2}{3}$ 이상의 찬성표를 얻으면 해당 블록은 체인에서 확정된다.

체인 선택은 블록을 생성하고 완료할 블록을 선택하는 데 사용된다. 이러한 프로세스는 노드 간에 일관성을 유지해야 하며, 악성 노드의 최대 비율에 대한 복원력을 가져야 한다. 파라체인 호스트는 블록 작성 시스템과 완료 가젯을 사용한다. 체인 선택 전략은 리프 선택 규칙과 일련의 완료 제약 조건을 포함한다.

후보자 영수증

PoV는 일반적으로 크기가 1MB에서 10MB 사이이며 릴레이 체인 블록에 포함되지 않는다. 폴카닷이 수백 개의 파라체인으로 확장하려면, PoV는 릴레이 체인에서 더 작은 단위인 후보 영수증으로 표현되어야 한다. 파라체인 밸리데이터는 다음을 서명하여 파라체인 블록에 대한 후보 영수증을 생성한다.

- 파라체인 ID.
- 수집자의 신분증과 서명.
- 부모 블록의 후보 영수증의 해시이다.
- 블록의 삭제 코드화된 조각의 머클 루트이다.
- 모든 발신 메시지의 머클 루트이다.
- 블록의 해시.
- 블록 실행 전 파라체인의 상태 루트이다.
- 블록 실행 후 파라체인의 상태 루트이다.

이 정보는 크기가 일정하지만, 파라체인의 실제 PoV 블록은 길이가 가변적일 수 있다. 이는 전체 PoV 블록을 획득한 사람이라면 누구나 블록 내부에 포함된 상태 전이를 검증하기에 충분한 정보이다.

삭제 코드

후보 영수증을 릴레이 체인 거래 대기열로 보내기 전에, 영수증을 구성하는 파라밸리데이터는 파라체인 블록의 삭제 코딩도 구성해야 한다.

삭제 코딩은 메시지(이 경우 파라체인 블록과 PoV)를 사용하여 더 작은 메시지 집합을 생성한다. 이 작은 메시지들의 일부를 얻어 원본 메시지를 재구성할 수 있다. 폴카닷의 경우, 작은 메시지의 총 개수는 밸리데이터 수와 같으며, 그 비율은 $\frac{1}{3}$ 이다.

파라-밸리데이터는 삭제 코딩 청크를 생성하여 머클 트리에 저장하고, 각 청크를 후보 영수증과 함께 릴레이 체인의 해당 밸리데이터에게 전송한다. 삭제 코딩 청크가 포함된 영수증을 수신한 밸리데이터는 해당 영수증을 릴레이 체인 대기열에 포함하며, 작성자는 해당 영수증을 블록에 포함할 수 있다.

폴카닷의 가용성 체계에서 사용하는 삭제 코드 유형은 리드-솔로몬 코드로, 블록체인 산업 외의 기술 분야에서 이미 실전 테스트를 거친 적용 사례가 있다. CD 산업에서 한 가지 예를 찾아볼 수 있다. CD는 리드-솔로몬 코드를 사용하여 먼지 입자나 긁힘과 같은 디스크 표면의 불일치로 인해 손실된 데이터를 수정한다.

폴카닷에서는 삭제 코드를 사용하여 모든 밸리데이터가 모든 파라체인을 추적할 필요 없이 시스템에서 파라체인 상태를 사용할 수 있도록 한다. 대신, 밸리데이터는 작은 데이터 조각들을 공유하고, 밸리데이터 중 $\frac{1}{3}+1$ 명이 데이터 조각을 제공할 수 있다는 가정 하에 나중에 전체 데이터를 재구성할 수 있다.

메모

전체 파라체인 상태 데이터를 구성하는 데 반응해야 하는 밸리데이터의 임계값 $\frac{1}{3}+1$ 은 비잔틴 노드에 대한 폴카닷의 보안 가정에 해당한다.

분쟁

최종 릴레이 체인에 포함된 모든 파라체인 블록은 유효해야 한다. 이는 포함되지 않은 백업 블록에는 적용되지 않는다. 최종 릴레이 체인에 유효하지 않은 블록이 포함되지 않도록 승인 확인(위에서 설명)과 분쟁이 있다. 분쟁은 유효하지 않은 블록을 포함하려는 모든 시도를 적발하고 위반한 밸리데이터를 처벌한다.

거짓 긍정이 발생할 수 있으며, 이에 책임이 있는 행위자는 삭감 될 것이다. 거짓 긍정을 감지하려면 가용성 체계를 통해 블록이 릴레이 체인에 포함된 후 PoV 정보를 사용할 수 있어야 한다.

분쟁은 특정 포크와는 별개로 처리되지만, 지원 및 승인은 특정 포크에서 작동한다. 다른 포크(현재 승인된 후보가 포함되지 않을 수 있음)가 확정되면 승인 투표가 중단된다. 승인 절차의 유일한 목적은 유효하지 않은 블록이 확정되지 않도록 하는 것이다. 그러나 위험이 지나갔고 문제가 있는 밸리데이터가 유효하지 않은 블록을 승인하지 못했더라도, 해당 밸리데이터는 시도에 대해 슬래시를 받아야 한다.

분쟁은 두 명 이상의 밸리데이터 간의 의견 불일치에서 발생한다. 이를 위해서는 악의적인 행위자가 정직한 밸리데이터에게 유효하지 않은 블록을 배포해야 한다. 분쟁으로 이어지는 시나리오는 다음과 같다(중요도가 높은 것부터 낮은 것 순).

- 릴레이 체인의 분기에 포함된 파라블록이 불량이다.
 - 릴레이 체인의 가지에 뒷받침된 파라블록은 좋지 않다.
 - 릴레이 체인의 어느 지점에도 지지되지 않고 보조되는 파라블록은 좋지 않다.
- 파라체인 블록을 확인하려면 파라체인 밸리데이터 코드, 데이터 가용성, 그리고 후보 영수증이라는 세 가지 데이터가 필요하다. 밸리데이터 코드는 온체인에서 사용 가능하며 사전에 공개된다. 따라서 분쟁

절차는 데이터 가용성을 보장하기 위한 가용성 확인부터 시작된다. 데이터가 이미 사용 가능한 경우 이러한 절차는 신속하게 완료되지만, 그렇지 않은 경우 분쟁 제기자는 데이터를 제공해야 한다.

분쟁은 온체인과 오프체인 모두에 존재한다. 슬래싱은 온체인에서 처리되므로, 분쟁 양측의 밸리데이터의 투표는 온체인에 반영되어야 한다. 또한, 체인의 한 지점에서 발생한 분쟁은 모든 활성 지점으로 이관되어 모든 가능한 이력에서 부정행위를 처벌할 수 있어야 한다. 따라서 릴레이 체인의 특정 지점과 관련하여 로컬 분쟁(현재 우리가 살펴보고 있는 분쟁)과 원격 분쟁은 구분된다.

분쟁은 세 가지 단계로 나눌 수 있다.

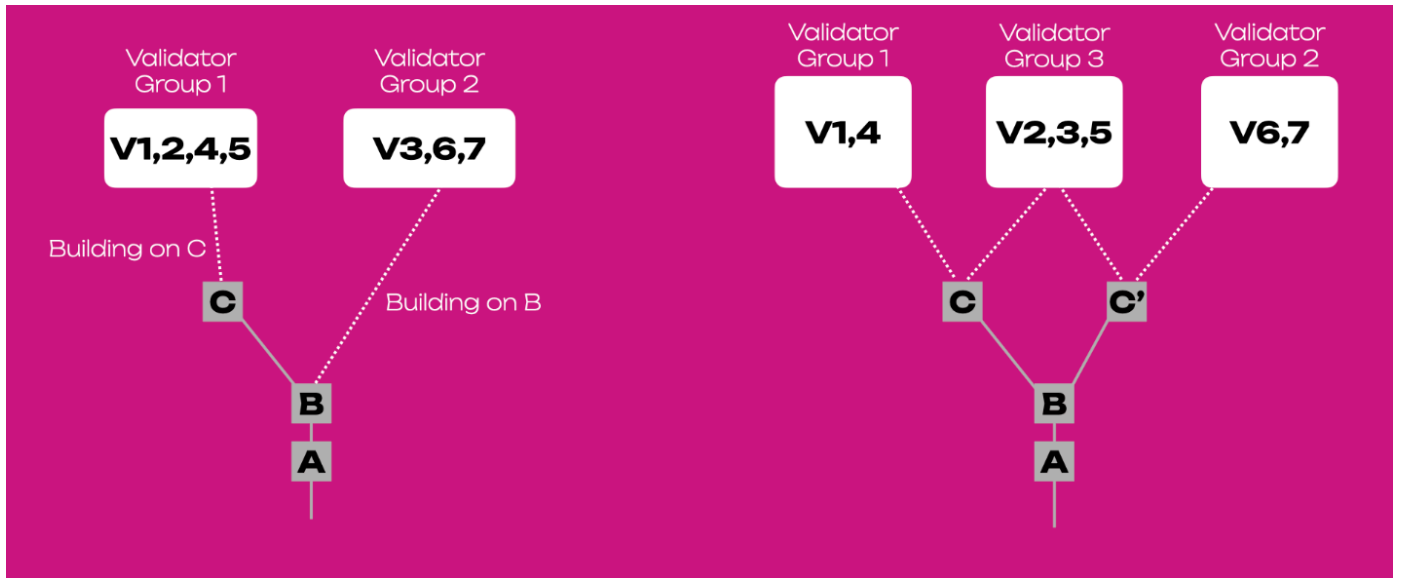
- **분쟁 발생** : 분쟁은 다른 발행된 의견과 상반되는 파라블록의 유효성에 대한 자신의 의견을 제시하는 밸리데이터에 의해 시작된다. 분쟁은 파라블록이 잘못되었다고 판단하는 노드들만 오프체인에서 시작된다. 밸리데이터는 파라블록 밸리데이터(즉, 지지자 중 한 명) 중 한 명이거나 승인 확인자 중 한 명일 수 있다. 지지 단계에서 분쟁이 발생하는 경우, 개시자는 데이터를 제공해야 하지만, 승인 과정에서 분쟁이 발생하는 경우 데이터는 이미 사용 가능하다.
- **분쟁 참여** : 분쟁을 인지하게 되면 모든 밸리데이터가 참여해야 한다.
- **분쟁 종결** : 양측의 $\frac{2}{3}$ 의 압도적 다수가 합의에 도달하면 분쟁이 종결된다. 분쟁은 타임아웃 이후에도 종결될 수 있다. 이는 과반수의 밸리데이터가 어떤 이유로든 투표에 참여할 수 없는 경우에만 발생한다.

분쟁의 온체인 구성 요소는 두 개의 상충되는 투표를 제공하여 시작될 수 있으며, 양측 모두 $\frac{2}{3}$ 의 압도적 다수를 기다린다. 또한 이 구성 요소는 이미 분쟁이 발생한 파라블록을 추적하여 릴레이 체인의 어느 지점에서든 동일한 파라블록에 대해 한 번만 분쟁을 제기할 수 있도록 한다. 분쟁이 해결될 때까지 해당 파라블록의 포함은 중단된다.

네트워크 비동기

릴레이 체인 블록 작성자가 후보를 선택하고 릴레이 체인에 기록해야 하는 방식(블록이 지지된다고 함)을 이미 언급했다. 릴레이 체인 블록 작성자는 포크풀 알고리즘인 BABE에 의해 선택된다. 즉, 여러 블록 작성자가 동시에 선택되며, 동일한 부모 블록에서 작업하지 않을 수 있다(즉, 이전 그림의 표현은 단순화된 것이다). 또한, 밸리데이터와 파라체인은 집합은 고정되어 있지 않으며, 밸리데이터가 파라체인에 할당되는 방식 또한 유연하다.

네트워크가 비동기적이 라고 하는 이유는 블록을 받은 밸리데이터와 받지 못한 밸리데이터가 있기 때문이다. 따라서 네트워크는 가변적이며 여러 상태로 존재한다. 아래 그림(왼쪽)에서 그룹 1은 블록 C를 받았지만 네트워크 비동기로 인해 그룹 2는 받지 못했다. 그룹 2의 밸리데이터는 B 위에 C'라는 또 다른 블록을 만들 수 있다. 그 후에 일부 밸리데이터는 C와 C'를 모두 알게 되고 다른 밸리데이터는 그 중 하나만 알게 된다고 가정해 보겠다(오른쪽). 그룹 3의 밸리데이터는 각 헤드(C와 C')의 네트워크 상태를 알아야 하며, 둘 다에 어느 정도 또는 전부 기여할 수 있다. 네트워크 비동기로 인해 두 개의 포크가 한동안 병렬로 성장할 수 있지만 결국에는 최종성 가젯에 의해 하나의 포크가 선택될 수 있다. 적대적 네트워크가 없는 경우 두 체인 헤드를 모두 알고 있는 밸리데이터가 있을 것이므로 두 개의 포크가 한동안 공존할 가능성은 낮다.



파이프라인

파이프라인은 작업의 여러 단계를 더 작은 단계로 나누어 동시에 처리하는 기술이다. 이를 통해 이전 단계가 완전히 완료되기 전에 다음 단계를 시작할 수 있다. 파이프라인은 프로세서와 컴퓨터 아키텍처에서 처리량을 높이기 위해 자주 사용된다.

폴카닷은 비동기식 백킹을 통해 파라체인 블록 생성, 백킹 및 포함에 파이프라인을 도입한다. 이는 기존 아키텍처에서 프로세서 명령어의 논리적 파이프라인과 유사하며, 일부 명령어는 다른 명령어가 완료되기 전에 실행될 수 있다.

블록으로 표현된 상태 전환 묶음도 유사하게 처리될 수 있다. 폴카닷(Polkadot)의 맥락에서, 파이프라이닝은 여러 블록에 대한 백킹(backing) 및 포함(inclusion) 단계를 동시에 완료하여 전체 네트워크의 처리량을 높이는 것을 목표로 한다. 비동기 백킹은 단일 파이프(또는 코어) 내에서만 파이프라인을 허용하는 것이 아니라, 동일한 파라체인(parachain)에 대해 여러 파이프(또는 코어)가 동시에 실행될 수 있는 기반을 마련한다.

폴카닷에서는 파라블록이 파라체인 측의 콜레이터에 의해 생성되고, 지원을 위해 릴레이 체인 측의 밸리데이터에게 전송된다.

백킹이란 무엇인가요?

백킹(Backing)은 파라블록(parablock)이 밸리데이터 또는 백킹 그룹의 하위 집합에 의해 검증되는 과정을 의미한다. 이는 검열 저항성을 보장하는 최전선 방어선이므로 파라블록 검증 과정에서 중요한 단계이다. 파라블록은 단 하나의 밸리데이터만 지지하면 되므로, 백킹만으로는 파라블록의 유효성을 보장할 수 없다.

백업된 파라블록은 릴레이 체인에 포함되도록 다른 밸리데이터에게 전송된다. 밸리데이터가 파라블록 데이터의 삭제 코딩된 청크를 수신했음을 증명하면 파라블록이 포함된다. 파라블록 자체가 아닌 후보 수신 이 릴레이 블록에 포함된다는 점에 유의하십시오(단, 편의상 파라블록을 포함되는 것으로 지칭한다). 파라블록이 생성되면 릴레이 부모(relay parent)라는 릴레이 체인 블록에 앵커링되어야 한다. 릴레이 부모는 파라블록 후보 생성의 입력이다. 다음 파라블록을 생성하는 데 필요한 컨텍스트를 제공한다. 파라블록의 릴레이 부

모와 해당 파라블록을 포함하는 릴레이 블록은 항상 다르다.

동기식 백업

비동기 백킹을 살펴보기 전에 동기 백킹의 정의와 주요 한계를 이해하는 것이 중요하다. 동기 백킹에서 파라블록 생성은 릴레이 체인의 진행과 밀접하게 결합된다.

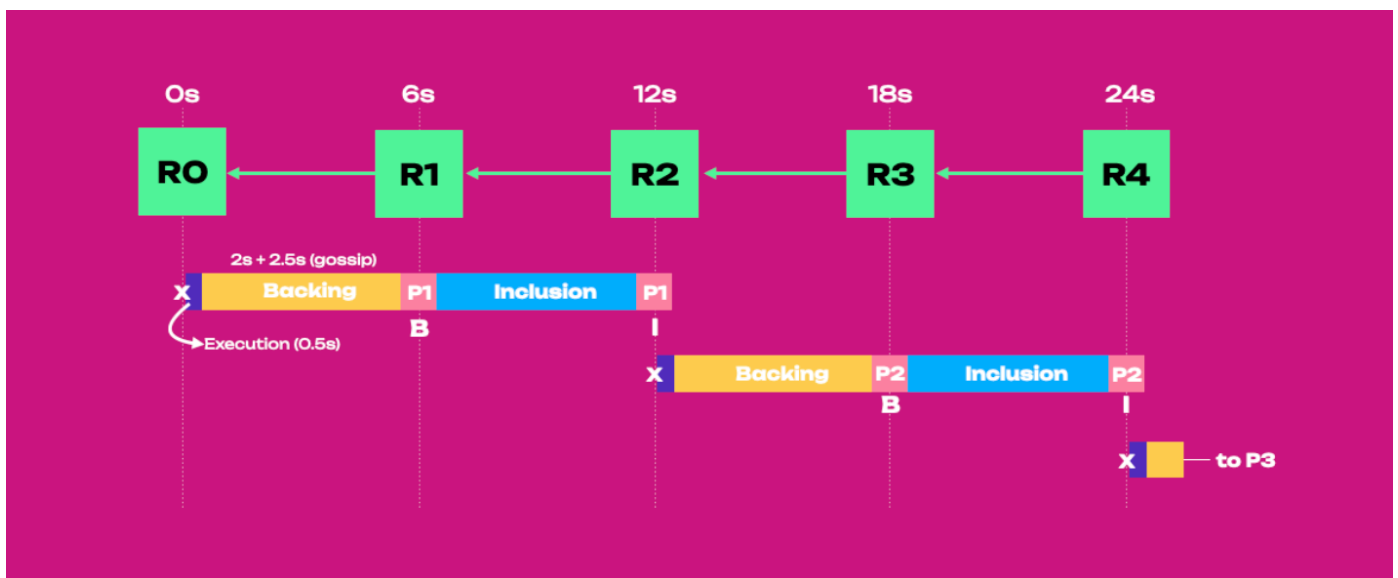
이전 패러블록을 포함한 후에(즉, 12초마다) 새로운 패러블록을 생성할 수 있다.

다음 파라블록을 구축하기 위한 컨텍스트는 포함된 최신 파라블록 조상에서 가져온다.

릴레이 부모는 최신 릴레이 체인 블록이어야 한다.

(1) 파라블록은 릴레이 체인 블록 하나(즉, 12초마다)마다 생성될 수 있다. (2) 파라블록 생성은 파라블록이 포함될 P때만 시작할 수 있다 P - 1(파이프라인 없음). (3) 파라블록이 P다음 5.5초 안에 백업되기 위해 서 두르기 때문에 실행 시간은 최대 0.5초가 걸릴 수 있다(백업에 2초, 나머지는 가십에 필요). 모든 파라블록은 6초(하나의 릴레이 체인 블록) 안에 백업되고 다음 6초(다음 릴레이 체인 블록) 안에 포함된다. 생성부터 포함까지 걸리는 시간은 12초이다. 이는 콜레이터가 각 파라블록에 추가할 수 있는 데이터 양을 제한한다.

파라블록 생성은 가장 최근에 수신된 릴레이 블록을 릴레이 부모로 선택하지만, 불완전한 네트워크에서는 실제 가장 최근 릴레이 블록과 다를 수 있다. 따라서 일반적으로 릴레이 블록 R이 파라블록 P의 릴레이 부모라면, P는 R + 1에 백업되고 R + 2에 포함될 수 있다.



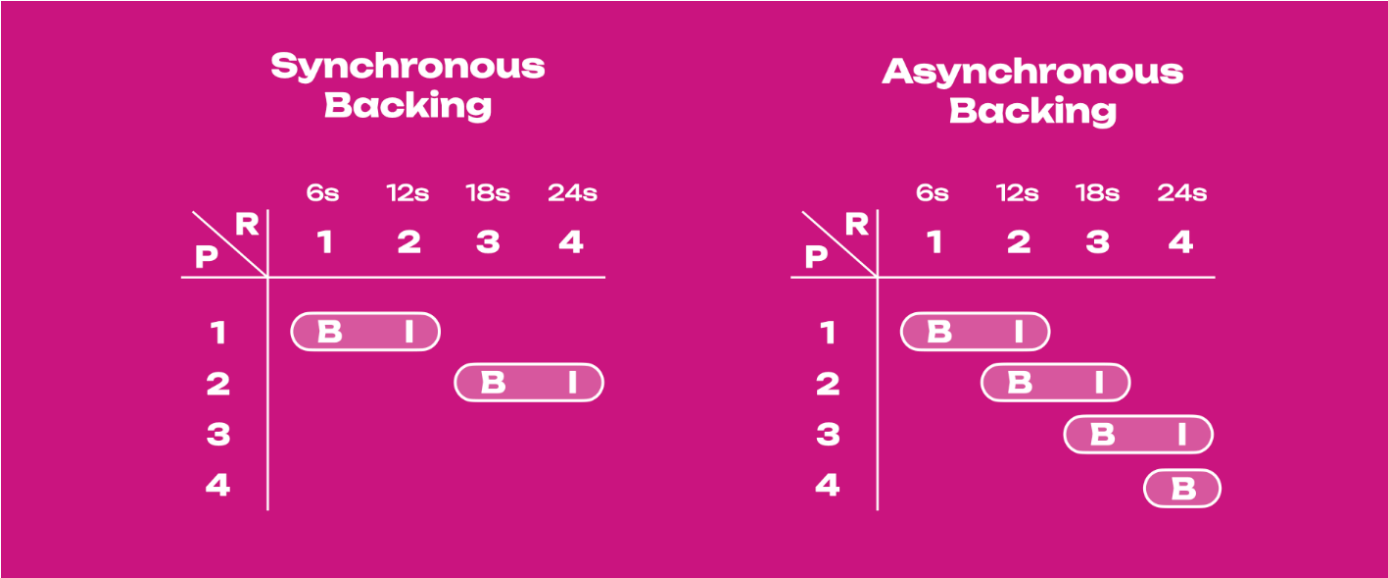
왼쪽에서 오른쪽으로, 파라블록 P1은 릴레이 부모 R0(로 표시 x)에 앵커링되고, 릴레이 체인 블록 R1에 백업되어 R2에 포함된다. P1을 포함한 후, 콜레이터는 릴레이 부모 R2에 앵커링되어야 하는 P2를 생성할 수 있다. R2가 릴레이 체인에 포함되고 P2를 생성하는 콜레이터에 가십(gossiping)되면 R2가 P2의 릴레이 부모가 된다.

각 콜레이터는 또한 연결된 릴레이 체인 전체 노드를 실행한다.

연결된 릴레이 노드는 가십을 통해 릴레이 블록을 수신한다. 그런 다음, 릴레이 노드는 CollationGeneration서브시스템을 통해 파라체인 노드와 통신한다. R2는 콜레이터에 연결된 릴레이 풀 노드로 가십을 전송하여 P2를 생성한다. 그런 다음, CollationGenerationR2에 대한 정보를 콜레이터 노드로 전달한다. 마지막으로, R2의 릴레이 부모 정보는 후보 P2 생성에 정보를 제공한다.

P2가 R3에서 6초 안에 백업을 받기 위해 서두르고 있기 때문에 밸리데이터는 실행에 0.5초만 할애할 수 있다. 백업 그룹은 P2를 백업하는 데 약 2초가 걸리고, 가십(gossiping)에 추가 시간이 필요하다(데이터 대조부터 백업까지 전체 과정은 6초가 걸린다). P2는 R4에 포함되며, R4는 P3의 릴레이 부모 노드로 사용될 수 있다(그림에는 표시되지 않음). 24초 후 P1과 P2는 릴레이 체인에 포함된다. 콜레이터는 12초마다 새로운 파라블록을 시작할 수 있지만 실행에 0.5초만 할애할 수 있다는 점에 유의하십시오.

비동기 백킹



비동기 백킹에서는 6초마다 파라블록(P)이 포함되고, 백킹(B)과 포함(I)은 동일한 릴레이 체인 블록(R) 내에서 발생할 수 있다.

동기식 vs. 비동기식 백킹

아래는 동기식 백킹과 비동기식 백킹의 주요 차이점을 보여주는 표이다.

항목	동기화 백업	비동기 지원	비동기 백업의 장점
모든 파라블록이 포함되어 있다	12초	6초	처리량 2배 증가 또는 대기 시간 2배 감소
Parablock의 최대 실행 시간	0.5초	2초	파라블록에 4배 더 많은 데이터
릴레이 부모	최신 릴레이 체인 블록이다	반드시 최신 릴레이 체인 블록이 아니다	수집자는 사전에 지원 그룹에 파라블록을 제출할 수 있다
수집자는 다음을 기반으로 구축할 수 있다	최신 릴레이 체인 블록에 포함된 가장 최근의 조상	릴레이 체인 블록에 포함된 조상(반드시 최신일 필요는 없음)으로 포함되지 않은 세그먼트의 최신 조상으로부터 증명된 정보를 포함한다	수집자는 미리 파라블록을 만들기 시작할 수 있다
포함되지 않은 파라블록의 수	단 하나	하나 또는 둘 이상 (구성 매개변수에 따라 다름)	더 높은 효율성과 확장성
포함되지 않은 파라블록	재제안 불가	첫 번째 시도에서 성공적으로 포함되지 않은 경우 우 재제안할 수 있다	사용되지 않은 블록 공간 낭비 감소
Parablock의 Backing-to-inclusion 시간	12초	12초	변화 없음
Parablock의 포함에서 최종성까지의 시간	30초	30초	변화 없음

동기식 백킹에서는 콜레이터가 릴레이 체인에서 완전히 가져온 컨텍스트를 사용하여 파라블록을 생성한다. 반면 비동기식 백킹에서는 콜레이터가 미포함 세그먼트의 추가 컨텍스트를 사용한다. 파라블록은 6초마다 포함된다. 이는 파라블록 N+1의 백킹과 파라블록 N의 포함이 동일한 릴레이 체인 블록에서 발생할 수 있기 때문이다(파이프라인 처리). 그러나 동기식 백킹의 경우, 패러블록이 백킹되고 포함되기까지 12초가 소요되며, 포함부터 최종 확정까지 추가로 30초의 시간 차이가 존재한다.

처리량이 2배 증가하고 파라체인의 실행 시간이 4배 더 길어지기 때문에 비동기 백업은 파라체인에 8배 더 많은 블록 공간을 제공할 것으로 예상된다.

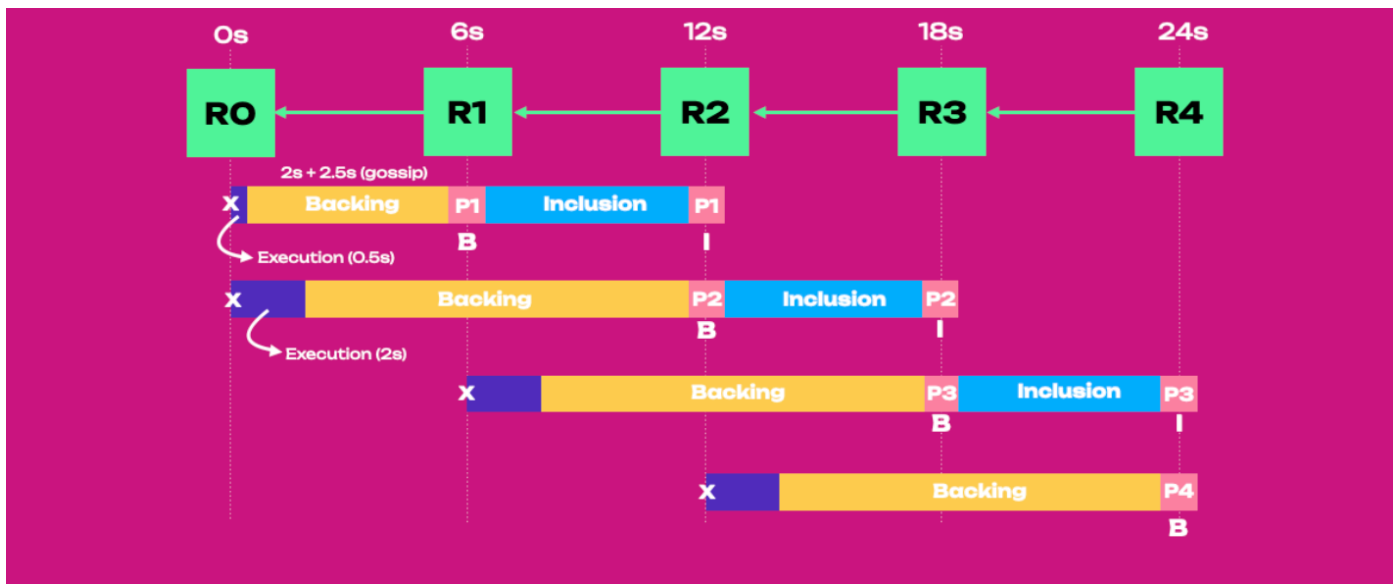
비동기 백업의 특수한 경우로서의 동기화 백업

비동기 백업의 두 가지 매개변수는 거버넌스에 의해 제어될 수 있다.

- `max_candidate_depth`: 릴레이 체인에 아직 포함되지 않은, 콜레이터가 생성할 수 있는 파라체인 블록의 수이다.
- `allowed_ancestry_len`: 파라체인 블록을 위에 만들 수 있는 가장 오래된 릴레이 체인 부모이다.

두 값 모두 0일 경우 동기식 백킹에 해당한다.: `max_candidate_depth = 0`은 항상 하나의 미포함 패러블록만 존재할 수 있음을 의미하며, `allowed_ancestry_len = 0`은 패러블록이 해당 패러체인에 대한 최신 릴레이 부모 위에서만 구축될 수 있음을 의미한다. 초기값은 각각 3(항상 4개의 미포함 패러블록 허용)과 2(릴레이 부모는 세 번째 마지막까지 허용)로 설정된다.

비동기 백킹 다이어그램



이 다이어그램은 다음을 가정한다.

- `max_candidate_depth = 2`즉, 항상 포함되지 않은 파라블록이 최대 3개까지 있을 수 있음을 의미한다.
- `allowed_ancestry_len = 1`즉, 파라블록은 마지막 또는 두 번째 마지막 릴레이 부모에 고정될 수 있다(즉, 수집기는 6초 전에 파라블록 준비를 시작할 수 있음)

왼쪽에서 오른쪽으로, 파라블록 P1은 릴레이 체인 블록 R1에 백업되고 R2에 포함된다. P1이 백업을 받는 동안 콜레이터는 이미 P2를 생성할 수 있으며, P2는 R0을 릴레이 부모로 갖(x로 표시). 포함되지 않은 세그먼트에 포함되지 않은 파라블록이 최대 3개 있는 한 R0도 P1의 릴레이 부모가 될 수 있다. 파라블록 P2는 R2(P1이 포함된 동일한 릴레이 블록)에 백업되고 R3에 포함될 수 있다. 콜레이터는 이제 실행에 최대 2초를 사용할 수 있다. 이런 식으로 백업 그룹이 P2를 확인하는 동안 P3을 생성할 수 있고, P3이 백업을 받는 동안 P4를 생성할 수 있다. 24초 안에 P1~P3이 릴레이 체인에 포함된다.

항상 세 개의 미포함 파라블록이 존재한다는 점에 유의하세요. 즉, 동기식 백킹과 비교했을 때 여러 개의 미포함 파라블록(즉, 파이프라이닝)이 존재할 수 있다. 예를 들어, P1이 포함되는 동안 P2와 P3은 백킹을 받는다. 콜레이터는 미포함 세그먼트를 통해 여러 개의 미포함 파라블록을 생성할 수 있었다. 미포함 세그먼트는 포함되지 않은 파라블록 조상의 로컬 저장소로, 새로운 파라블록을 생성하기 위한 정보를 가져오는 데 사용할 수 있다. 릴레이 체인 측면에서, 원근 파라블록은 각 미포함 세그먼트가 후보를 추적하는 작업을 반복한다(밸리데이터는 파라체인에 보관된 레코드를 신뢰할 수 없기 때문이다).

6초 릴레이 체인 블록 지연에는 백킹 실행 시간 초과(2초)와 네트워크 지연 시간(전체 네트워크에서 메시지를 주고받는 데 걸리는 시간)이 포함된다. 콜레이터가 파라블록을 생성하는 데 걸리는 제한 시간은 백킹에 걸리는 시간(즉, 2초)이다. 콜레이션 생성은 보수적으로 항상 동일한 시간 제한을 둔다. 콜레이션 생성 및 백킹에 추가 시간이 있는 경우(즉, 2초 + 6초 이상), 추가 시간은 모두 백킹에 할당된다(그림 참조). 이로 인해 백킹 단계가 끝나고 다음 릴레이 블록이나 이후 릴레이 블록에서 해당 블록을 백킹할 코어가 확보될 때까지 백킹 가능한 블록이 몇 초 동안 차례를 기다릴 수 있다. 백킹 후, 그리고 포함되기 전에 코어가 점유된다는 점에 유의하세요.

따라서 2초의 실행 시간은 시스템 제약이 아닌 제한 요소이다. 파라블록 생성에 2초 이상이 소요되면 포함되지 않은 세그먼트는 줄어들고(포함되지 않은 파라블록이 줄어듦), 2초 미만이 소요되면 세그먼트는 늘어난다(백업 및 포함해야 할 포함되지 않은 파라블록이 늘어남). 파라체인 측에서 이러한 유연성은 릴레이 체인 측에서 탄력적인 확장(즉, 민첩한 코어 사용 및 코어 시간 할당)이 가능할 때 가능하다.

용어

후보자 영수증

파라블록이 릴레이 체인 부모 블록에 포함되었다고 해서 파라블록 전체가 릴레이 체인 블록에 있다는 것을 의미하지는 않는다. 대신, 파라블록의 해시, 상태 루트, ID 정보로 구성된 후보 수신(candidate receive)이 릴레이 체인의 부모 블록에 배치된다. 릴레이 체인은 파라블록의 전체 상태에 접근하지 않고, 해당 블록에서 변경된 값과 변경되지 않은 값의 머컬화된 해시 값에만 접근한다.

포함되지 않은 세그먼트

포함되지 않은 세그먼트는 릴레이 체인에 아직 포함되지 않은 후보 파라블록 체인이다. 즉, 포함 전 어느 단계에서든 파라블록을 포함할 수 있다. 따라서 포함되지 않은 세그먼트에는 지지되거나, 지지 가능하거나, 지지된 후보가 포함될 수 있다. 포함되지 않은 세그먼트에 기록된 모든 파라블록 후보는 즉시 밸리데이터에게 광고되어 지지 프로세스를 시작한다.

백킹 프로세스는 릴레이 체인에서 발생하는 반면, 포함되지 않은 세그먼트는 파라체인 콜레이터의 런타임에 존재한다. 비동기 백킹의 핵심 기능은 릴레이 체인 상태에 포함된 조상만을 기반으로 하는 것이 아니라, 블록 조상의 포함되지 않은 세그먼트를 기반으로 구축할 수 있다는 것이다.

포함되지 않은 각 세그먼트의 목적은 두 가지이다.

- 각 파라체인이 릴레이 체인에서 거부되지 않는 블록을 언제, 어느 깊이에서 구축할 수 있는지 인식하도록 한다.

- 아직 포함되지 않은 부모 블록을 사용하여 파라블록을 만드는 데 필요한 중요한 맥락을 제공한다. 포함되지 않은 부분은 모두 파라블록 만들기에 관한 것이다.

잠재적인 파라체인

미래 파라체인 의 목적은 두 가지이다.

- 후원자에게 제출되었지만 아직 포함되지 않은 파라블록을 추적한다. 여기에는 각 파라블록의 포함되지 않은 전체 조상을 추적하는 것이 포함되며, 이러한 정보가 없으면 해당 파라블록의 진위 여부를 확인할 수 없다.
- 각 파라체인에 대해 가장 최근에 포함된 파라블록의 자식 후보들을 찾아 제공한다. 이는 가용성 프로세스의 입력으로 사용된다. 유망 파라체인은 후보들을 추적, 저장하고 가용성/포함 단계에 제공하는 것을 핵심으로 한다.

예비 파라체인은 기본적으로 각 미포함 세그먼트가 후보 추적 과정에서 수행하는 작업을 반복한다. 밸리데이터는 파라체인에 보관된 레코드의 가용성이나 유효성을 단순히 신뢰할 수 없다. 예비 파라체인은 지원 및 포함 과정을 거치는 모든 파라블록 후보에 대한 릴레이 체인의 레코드이다. 파라블록 유효성을 위한 권위 있는 게이트키퍼이다. 반면, 미포함 세그먼트는 파라체인이 나중에 예비 파라체인이 시행하는 규칙을 준수하는 블록을 생성할 수 있도록 하는 로컬 레코드이다.

포함되지 않은 세그먼트는 파라체인 런타임에 존재하므로 포크/다른 파라체인에 대해 알지도, 신경 쓰지도 않는다. 잠재적 파라체인은 릴레이 체인 클라이언트에 존재한다. 따라서 모든 파라체인의 모든 포크에서 후보들을 동시에 추적해야 한다. 이는 마치 모든 파라체인의 모든 포크에서 포함되지 않은 세그먼트들을 하나의 거대한 데이터 구조로 접은 것과 같다. 서로 다른 체인 포크를 나타내는 포함되지 않은 세그먼트들을 함께 접으면 트리 구조가 생성된다. 따라서 "프래그먼트 트리" 라는 용어가 사용된다.

단일 미포함 세그먼트는 콜레이터에게 특정 파라체인의 특정 포크 위에 블록을 생성할 수 있는지 여부를 알려준다. 잠재 파라체인은 밸리데이터에게 모든 파라체인의 모든 포크 위에 생성된 블록을 허용해야 하는지 여부를 알려준다.

파라블록은 체인에 포함되면 더 이상 예비 파라블록이 아니다. 이 시점부터 예비 파라체인은 더 이상 해당 파라블록에 신경 쓸 필요가 없다. 반대로, 파라블록의 릴레이 부모가 파라블록이 포함되기 전에 너무 오래될 경우, 예비 파라체인은 후보 파라블록을 버릴 수 있다.

스케줄링

스케줄링은 특정 시간이나 특정 조건에서 CPU 코어와 같은 리소스에 작업을 할당하는 프로세스이다. 효과적인 스케줄링은 리소스가 효율적으로 사용되고 작업이 적시에 완료되도록 보장한다.

폴카닷은 Agile Coretime을 활용한 스케줄링을 도입하여 폴카닷 네트워크 리소스를 효율적으로 활용하고 개발자에게 경제적 유연성을 제공하며, 폴카닷을 백서에서 처음 제안하고 구상했던 것 이상으로 일반화한다. 코어타임 도입으로 멀티스레딩이 가능해졌다.

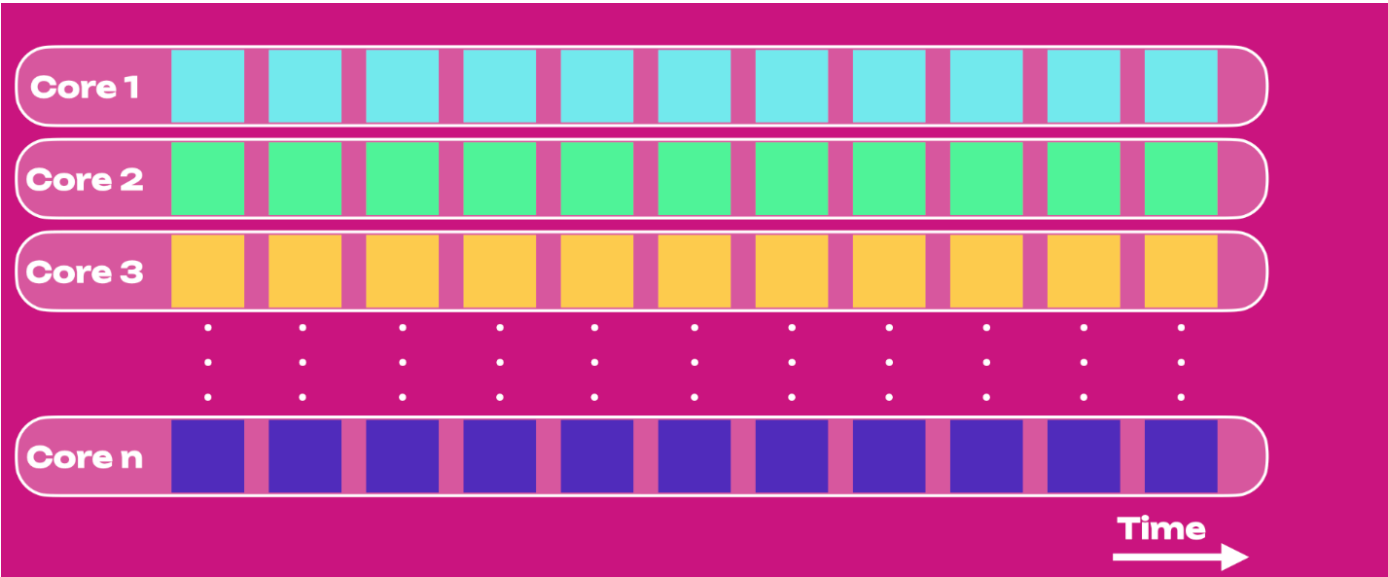
멀티스레딩(Multi-threading)은 단일 프로세스 내에 여러 스레드(프로그래밍된 명령어들의 작은 시퀀스)를 생성하여 여러 작업을 동시에 수행하는 프로그래밍 모델이다. 멀티스레딩은 일반적으로 프로그램의 여러 부분을 동시에 실행하여 애플리케이션의 성능을 향상시키는 데 사용된다. 동시성은 병렬 실행을 의미하는 것이 아니라, 시스템이 여러 프로세스 간을 빠르게 전환하여 관리할 수 있도록 하는 것이다.

Polkadot은 Coretime을 분할하고 인터레이싱하여 멀티스레딩을 구현한다.

Agile Coretime 소개

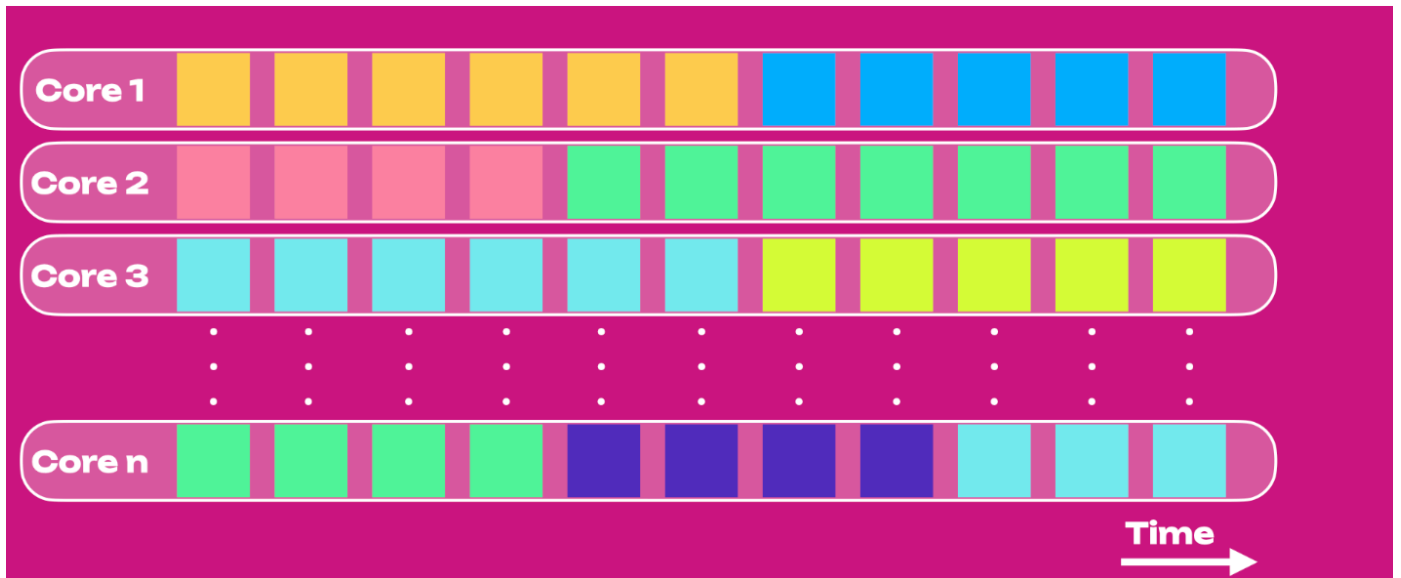
폴카닷 1.0에서는 폴카닷이 파라체인을 보호하는 유일한 방법은 경매를 통해 임대하는 것이었는데, 이를 통해 파라체인 블록 검증이 최대 2년 동안 보장됐다. 이 과정에서 상당한 양의 DOT 토큰을 잠가야 했기 때문에 중소 규모 블록체인 프로젝트의 진입 장벽이 높았다. 파라체인은 네트워크 활동과 관계없이 12초 간격으로 블록을 생성했다. 이로 인해 비효율적인 자원 할당과 잘못된 경제적 인센티브가 발생했고, 트래픽이 적을 때는 거의 빈 블록이 생성되었으며, 블록 한도를 초과하는 트래픽이 발생하면 이를 감당할 수 없었다. Agile Coretime은 이러한 모든 단점을 해결한다.

아래 그림은 Polkadot 1.0의 핵심 사용 방식을 보여준다. 가로축은 시간을, 각 행은 핵심을 나타낸다. 색상은 각각 하나의 핵심을 사용하는 여러 개의 파라체인을 나타낸다(즉, 파라체인 하나당 핵심 하나).



Agile Coretime은 한 달 동안 할당된 코어타임을 "대량"으로 구매할 수 있도록 한다. 12초마다(또는 비동기 백업을 사용하는 경우 6초마다) 블록을 작성해야 하는 고성능 파라체인은 매달 코어타임을 원활하게 "갱신"할 수 있다. 코어타임 갱신 주문은 신규 주문보다 우선하며 가격 변동으로부터 보호해 파라체인이 프로젝트 예산과 비용을 더욱 효과적으로 계획할 수 있도록 한다.

구매한 코어타임을 한 달에 한 블록씩 분할하여 판매할 수 있으며, 이를 통해 2차 시장이 활성화되고 코어타임 배분 효율성이 향상된다. 또한, Agile Coretime은 온디맨드 코어타임 기능을 제공하여 필요에 따라 파라체인 블록을 생성할 수 있다.



Agile Coretime 용어

핵심

"코어"라는 용어는 릴레이 체인이 파라체인의 블록을 보호하기 위해 제공하는 계산 리소스의 가상 추상화를 포착하며, 여기에는 릴레이 체인 밸리데이터의 무작위 집합이 포함된다.

코어타임

릴레이 체인 블록으로 측정된 코어 활용에 할당된 시간이다.

대량 코어타임

분할, 공유 또는 재판매가 가능한 NFT로 표현되는 고정된 기간의 연속 코어타임이다. 현재 대량 코어타임의 기간은 28일로 설정되어 있다.

지역

NFT는 단일 단위의 대량 코어타임을 나타낸다.

주문형 코어타임

이전에는 즉각적인 코어타임으로 알려졌던 주문형 코어타임은 주문형 주문에 특별히 예약된 코어 중 하나에서 단일 파라체인 블록의 검증을 위해 거의 실시간으로 입찰을 통해 획득한 코어타임을 말한다.

주문형 코어타임 풀

주문형으로 사용 가능한 코어 집합이다. 대량 코어타임을 통해 예약된 코어는 주문형 코어타임 풀에서 일부 또는 전체로 사용 가능할 수도 있다.

코어타임 체인

대량 코어타임의 판매, 조작, 그리고 궁극적으로는 주문형 코어타임 크레딧 구매를 담당하는 시스템 파라체인이다. 또한 릴레이 체인의 각 코어를 파라체인에 스케줄링하는 역할도 한다.

타임슬라이스

타임슬라이스는 코어타임 체인이 릴레이 체인에서 코어를 스케줄링하는 세분성을 나타낸다. 코어타임 체인은 각 코어에 대한 스케줄을 미리 발표하며, 이는 다음 80개의 릴레이 체인 블록으로 구성된다. 5,040개의 타임슬라이스는 28일(벌크 코어타임의 초기 구성 설정)의 리전 길이에 해당한다.

태스크

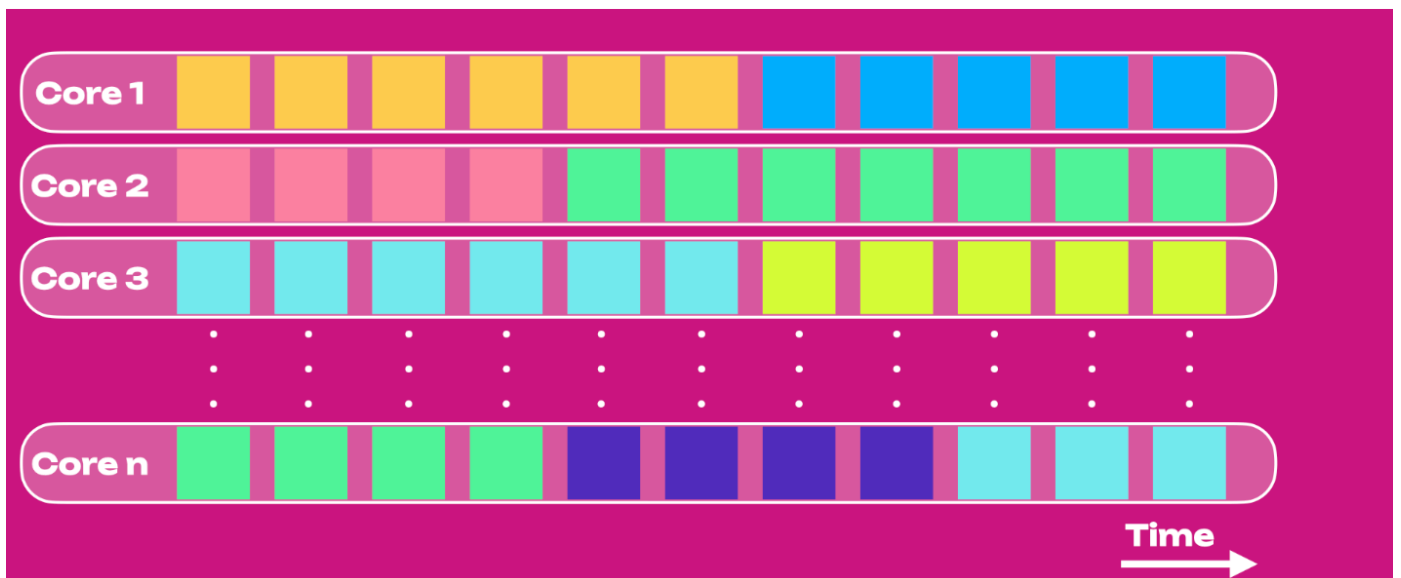
"태스크"라는 용어는 코어의 유용성을 추상화하여 표현한다. 코어의 작업은 단순히 파라체인을 확보하는 데 국한되지 않는다.

Agile Coretime 구현

코어타임은 코어타임 체인에 구축된 브로커 팔레트를 통해 관리된다. 이론적으로 폴카닷 릴레이 체인은 약 100개의 코어를 원활하게 지원할 수 있으며, 최적화를 통해 수백 개 이상의 코어를 지원할 수 있다. 예비 테스트는 12초 블록 시간으로 80개의 코어를 사용하여 성공적으로 진행됐다. 코어타임 매출은 소각됐다.

코어타임 세일즈

코어타임 체인 의 판매는 timeslice기간이 정해져 있다. 이러한 판매는 크게 갱신 기간과 판매 기간으로 나뉜다.



- 갱신 기간은 `interlude_length` 블록으로 구성되며, 대량 코어타임이 갱신될 수 있는 시기이다.
- 판매 기간 역시 가격 발견 기간과 고정 가격 기간으로 나뉜다. 갱신 기간 이후 코어타임 체인에 의해 새로운 시작 가격이 설정되고, 리드인 길이 블록의 네덜란드식 경매가 시작되어 가격에 하방 압력을 가해 적절한 균형점을 찾는다. 이 과정을 통해 고정 가격 기간에 제시될 정규 가격이 결정된다.

분할 및 인터레이싱

분할 및 인터레이싱은 지역 내에서 수행할 수 있는 작업이다. 이러한 작업 중 하나를 수행하면 가격 상한이 적용된 갱신 권한을 잃게 된다.

- 분할 : 하나의 지역을 서로 다른 시작 및 종료 타임슬라이스를 갖는 여러 지역으로 나누는 작업이다.
- 인터레이싱: 한 영역을 타임슬라이스의 각 블록에 대해 여러 작업을 실행하도록 분할하는 동작이다. 결과 영역은 부모 영역과 동일한 시작 및 종료 타임슬라이스를 갖지만, 각 블록마다 서로 다른 작업이 실행된다.

탄력적 스케일링

탄력적 확장(아직 개발 중)을 통해 프로젝트는 이전에 할당된 리소스에 제한받지 않고 원활하게 확장할 수 있다. 탄력적 확장은 하나의 작업에 여러 코어를 할당하는 과정이다. 이를 통해 파라체인은 단위 시간당 더 많은 블록을 포함하고(릴레이 체인 측), 단위 시간당 더 많은 블록을 생성할 수 있다(파라체인 측 비동기 지원). 탄력적 확장은 온디맨드 코어타임과 함께 사용하여 대역폭을 원활하게 늘릴 수 있다.

병렬 컴퓨팅

병렬 컴퓨팅은 작업을 여러 프로세서 또는 코어에서 실행되는 하위 작업으로 나누어 여러 계산이나 프로세스를 동시에 수행하는 것을 의미한다. 이는 처리 속도를 높이기 위해 많은 연산을 병렬로 실행하는 고성능 컴퓨팅 작업에 필수적이다.

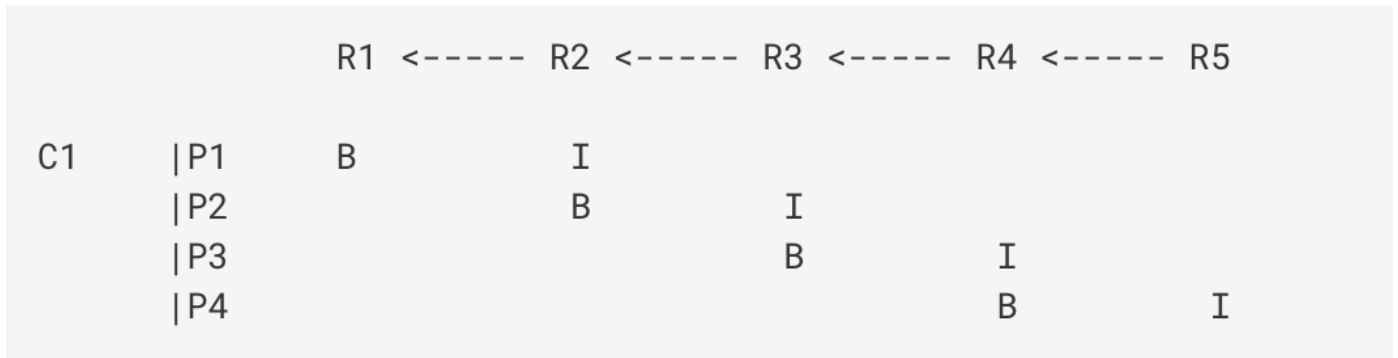
폴카닷은 파이프라인과 멀티스레딩을 사용하여 처리량을 높이고 동시성을 구현한다. 폴카닷은 또한 탄력적인 확장성을 통해 단일 작업에 대한 병렬 계산을 통해 처리량을 향상시킨다. 파라체인은 여러 코어를 사용하여 동일한 릴레이 체인 블록 내에 여러 파라블록을 포함할 수 있다.

탄력적 확장 기능은 2024년 12월 쿠사마(Kusama)에서 스팸밍 이벤트(Spamming Event)를 통해 라이브로 테스트됐다. 이 이벤트 동안 100개 코어 중 23개(용량의 23%)에서 143,343 TPS가 기록되었으며, 평균 블록 시간 6.3초와 최종성 16.5초를 지속적으로 달성했다.

폴카닷 2.0

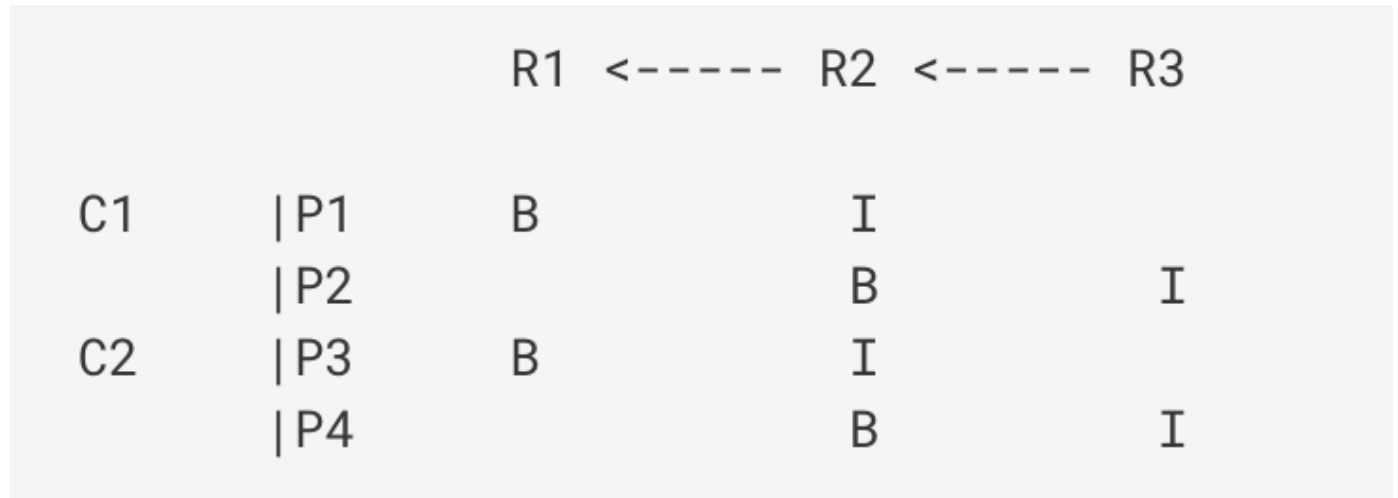
탄력적 확장은 파이프라인, 민첩한 스케줄링, 그리고 이제 병렬 컴퓨팅을 포함하는 Polkadot 2.0의 마지막 기술 업그레이드이다. 이를 통해 Polkadot은 안전한 컴퓨팅을 제공하는 진정한 분산형 컴퓨터가 된다.

예를 들어, 릴레이 체인에 네 개의 파라블록을 제출하려는 파라체인을 생각해 보겠다. 탄력적 확장이 없다면 하나의 코어를 통해 모든 파라블록을 포함하는 데 24초가 걸린다. 코어는 백킹 후 포함되기 전, 즉 전체 데이터 가용성 프로세스 동안 점유된다는 점을 기억하십시오. 블록은 이전 블록이 사용 가능하다고 선언되기 전에는 코어에 진입할 수 없다.



위 그림은 동일한 릴레이 체인 블록(R) 내에서 파라블록(P)의 백킹과 인클루전이 어떻게 이루어지는지 보여 준다. 코어(C1) 하나가 있으면 6초마다 파라블록이 하나씩 추가된다. P4가 30초(24초가 아님) 후에 포함 되는 것에 주목하세요. P1이 백킹을 위해 릴레이 체인으로 푸시되었을 때 이전에 파라블록이 없었기 때문이다.

탄력적 확장을 사용하면 두 개의 코어를 사용하여 4개의 파라블록을 모두 포함하는 데 불과 12초(블록 시간 3초)가 걸린다.



위 그림은 두 개의 코어(C1과 C2)를 사용하여 네 개의 파라블록이 어떻게 백업되고 릴레이 체인에 포함되는 지 보여준다. P2와 P4가 12초가 아닌 18초 후에 포함되는 것을 볼 수 있다. P1과 P3이 백업을 위해 릴레이 체인으로 밀려났을 때, 그 앞에 다른 파라블록이 없었기 때문이다.

릴레이 체인은 여러 코어에서 일련의 파라체인 블록을 수신하며, 이 블록들은 포함 과정에서 모든 상태 루트가 일치하는지 검증되고 확인된다. 하지만 백업, 가용성 및 승인 과정에서는 서로 관련 없는 파라체인 블록으로 간주된다. 탄력적 확장이 구현된 파라체인의 처리량은 콜레이터 인프라에 따라 달라진다.

릴레이 체인의 코어당 속도가 변하지 않으면(코어당 6초마다 백업 및 포함), 파라체인 측에서 수집자는 파라블록 생산 속도를 높여 P1과 P3을 두 릴레이 체인 코어로 밀어야 한다.

탄력적 확장의 이점

- 더 높은 처리량 : 파라체인은 여러 코어를 동시에 활용하여 훨씬 빠른 트랜잭션 처리를 가능하게 한다. 이전에는 파라체인이 릴레이 체인 블록당 하나의 블록으로 제한됐다. 이제 파라체인은 탄력적인 확장을 통해 훨씬 더 큰 용량을 처리할 수 있어 전반적인 성능이 크게 향상된다.

- 지연 시간 : 탄력적 확장은 지연 시간을 크게 줄여 블록 생성 및 처리 속도를 높인다. 예를 들어, 쿠사마(Kusama)의 파라체인(parachain)은 현재 3개의 코어로 지연 시간을 2초로 단축할 수 있으며, 2025년에는 12개의 코어로 500ms의 지연 시간을 달성하여 실시간 애플리케이션의 응답 시간을 더욱 빠르게 보장한다.
- 애플리케이션 비용 효율성 : 애플리케이션은 사용하는 리소스에 대해서만 비용을 지불하므로 비용을 절감하고 초기 비용을 절감할 수 있다. 코어타임은 블록, 시간 또는 월 단위로 동적으로 구매할 수 있다. 이는 온라인 경매나 갑작스러운 소셜 미디어 사용량 급증처럼 활동량이 급증하는 앱에 적합하다.
- 새로운 애플리케이션을 위한 유연한 확장 : 탄력적인 확장을 통해 온디맨드 코어타임을 통해 소규모로 애플리케이션을 시작 하고, 수요가 증가하면 코어 수를 초과하여 원활하게 확장할 수 있다. 이를 통해 기존 설정에서 흔히 발생하는 과도한 할당(사용되지 않는 리소스에 비용 낭비)이나 부족한 할당(성능 문제 발생)을 방지할 수 있다.
- 리소스 최적화 : 파라체인은 수요가 증가하면 추가 코어를 임대하고 활동이 감소하면 코어를 해제하여 코어 사용량을 부하 분산할 수 있다. 또한 코어타임 보조 시장은 사용되지 않는 리소스가 효율적으로 재활당되도록 하여 전반적인 시스템 성능을 최적화한다.
- 향상된 사용자 경험 : 최종 사용자는 최대 트래픽 상황에서도 원활하고 안정적인 성능을 경험할 수 있다. 애플리케이션은 더 이상 수요 급증 시 속도 저하나 정지 위험에 노출되지 않으므로 일관되고 고품질의 사용자 경험을 보장한다.

탄력적 확장은 파라체인의 처리량을 증가시킨다. 폴카닷의 확장 방식은 전통적으로 여러 파라체인을 통해 확장하는 방식, 즉 교차 합의 메시징(XCM)을 통한 "수평적 확장" 또는 "수평적 샤딩"을 사용해 왔다. 그러나 여러 파라체인에 프로세스를 설정하고 병렬화하고 XCM을 통해 채널을 여는 데는 시간과 노력이 필요하다. 탄력적 확장을 사용하면 프로젝트는 여러 파라체인에 프로세스를 병렬화하기 전에 더 높은 처리량을 얻을 수 있다.

탄력적 확장 사용 사례

- "폭발적인" 애플리케이션 : 게임, DeFi, 경매, 메시징, 소셜 미디어 등 많은 애플리케이션은 지속적인 수요보다는 산발적인 활동 급증을 경험한다. 탄력적인 확장을 통해 이러한 애플리케이션은 최대 사용량 중에 추가 코어 타임을 확보하고 사용량이 적은 시간에 이를 해제하여 비용을 절감하는 동시에 성능을 최적화할 수 있다.
- 성장하는 애플리케이션 및 스타트업 : 스타트업과 신규 프로젝트는 예측 불가능한 사용자 증가에 직면하는 경우가 많습니다. 탄력적인 확장을 통해 최소한의 리소스(예: 단일 코어)로 시작하여 사용자 수요 증가에 따라 원활하게 확장한 후 수평 확장할 수 있으므로, 초기 리소스 과다 할당을 방지할 수 있다. 이를 통해 성능과 비용 효율성을 유지하면서 애플리케이션을 효율적으로 확장할 수 있다.
- 대규모 IoT 애플리케이션 : IoT 시스템은 수백만 대의 기기에서 데이터를 처리하기 위해 엄청난 확장성을 필요로 한다. 탄력적인 확장성을 통해 파라체인은 대량의 거래를 비용 효율적으로 처리할 수 있으며, 폴카닷 모델은 IoT 환경에 필요한 개인정보 보호 및 보안을 보장한다.
- 실시간 애플리케이션 : 일부 애플리케이션은 낮은 지연 시간과 실시간 성능을 요구한다(예: 게임, 결제/금융 서비스, 데이터 피드). 이러한 애플리케이션은 지연 시간을 2초까지 단축하는 탄력적 확장 기

능을 통해 이점을 얻을 수 있다. 이를 통해 수요가 높은 상황에서도 원활하고 안정적인 성능을 보장한다.

탄력적 확장 로드맵

탄력적 확장 구현은 여러 단계로 진행된다. 첫 번째 단계에서는 탄력적 확장이 신뢰/권한이 부여된 콜레이터 세트를 사용하는 파라체인에서 작동하도록 설정된다. 이러한 제한을 통해 후보 영수증을 변경하지 않고도 탄력적 확장을 실행할 수 있다. 첫 번째 단계를 성공적으로 구현한 후에는 후보 영수증을 변경하여 콜레이터 세트를 다시 신뢰/권한이 부여되지 않은 상태로 만들 수 있다. 마지막 단계에서는 Cumulus 프레임워크와 완벽하게 통합되어 파라체인이 여러 코어에 지속적으로 액세스하도록 구성할 수 있다.

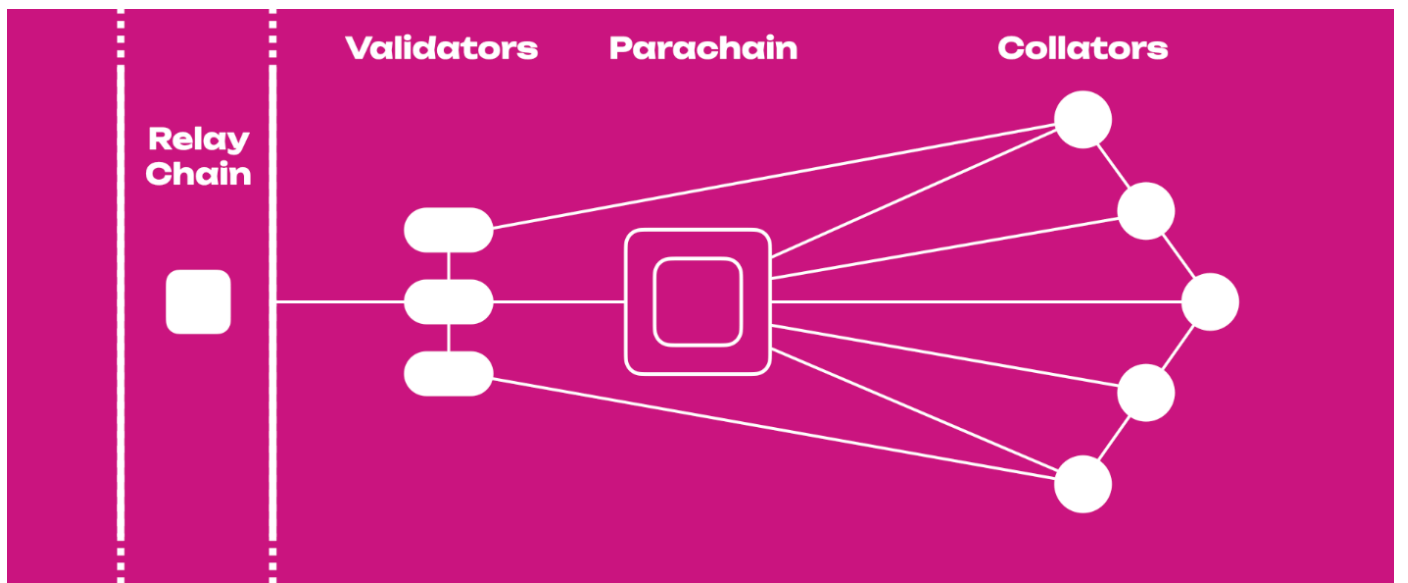
기술적 고려 사항

릴레이 체인 측면에서 코어 수가 일정하다고 가정할 때, 탄력적 확장은 파라체인이 기존 코어를 하나만 사용하는 대신 여러 개를 사용하므로 큰 업그레이드가 필요하지 않다. 그러나 파라체인 측면에서 콜레이터는 단위 시간당 더 많은 파라블록을 생성해야 하므로 콜레이터의 기술 사양이 높아질 가능성이 높다.

파라체인

파라체인 의 정의

파라체인은 전역적으로 일관성을 유지하며 릴레이 체인의 밸리데이터가 검증할 수 있는 애플리케이션별 데이터 구조이다. 파라체인의 이름은 릴레이 체인과 병렬로 실행되는 병렬 체인이라는 개념에서 유래했다. 파라체인은 일반적으로 블록체인 형태를 띠지만, 반드시 실제 블록체인일 필요는 없다.



병렬적 특성 덕분에 트랜잭션 처리를 병렬화하고 프로토콜의 확장성을 확보할 수 있다. 또한 전체 네트워크의 보안을 그대로 이어받으며 XCM 형식을 통해 다른 파라체인과 통신할 수 있다.

파라체인은 콜레이터(collator) 라고 하는 네트워크 유지 관리자에 의해 유지된다. 콜레이터 노드의 역할은 파라체인의 전체 노드를 유지하고, 파라체인에 대한 모든 필수 정보를 보관하며, 검증 및 공유 상태에 포함되도록 릴레이 체인 밸리데이터에게 전달할 새로운 블록 후보를 생성하는 것이다. 콜레이터 노드의 인센티브 제공은 파라체인의 구현 세부 사항이다. 파라체인 구현에 명시되지 않는 한, 콜레이터 노드는 릴레이 체인에 스테이킹하거나 네이티브 토큰을 소유할 필요가 없다.

국가 전환

다른 블록체인과 마찬가지로, 파라체인은 결정론적 상태 머신이다. 각 파라체인은 상태를 가지고, 블록으로 그룹화된 일련의 거래를 실행하고, 새로운 상태를 달성한다. 조 페트로프스키는 이 글에서 켜지거나 꺼질 수 있는 전등 스위치가 있는 상태에 대한 좋은 비유를 제공했는데, 이는 상태 머신이 기능하는 가장 간단한 예 중 하나이다. 각 파라체인은 자체 상태를 가지고 있으며, 릴레이 체인은 모든 상태를 하나의 상태, 즉 상태의 상태로 연결한다. 폴카닷과 같은 멀티체인 네트워크는 상태 전환 함수가 어떤 스위치를 전환해야 하는지 결정하는 논리인 여러 개의 전등 스위치가 있는 한 대의 컴퓨터 상태와 같이 볼 수 있다. 파라체인은 자체 전환 규칙, 별도의 경제, 거버넌스 메커니즘 및 사용자를 가지고 있다.

파라체인의 상태는 머클 트리에 저장된다. 머클 트리는 트리 내의 일부 값이 변경되면 머클 루트(이 경우 상태 루트)에 반영되는 편리한 특성을 가지고 있다. 트리 내에서 변경된 값과 영향을 받는 경로만 확인하면 변경 사항을 확인할 수 있다.

폴카닷 호스트는 파라체인에서 수행되는 상태 전이를 Wasm 실행 파일로 지정하도록 요구한다. 파라체인에서 발생하는 새로운 상태 전이 증명은 릴레이 체인이 파라체인에서 상태 전이가 발생했음을 확인하기 전에 밸리데이터가 릴레이 체인에 저장된 등록된 상태 전이 함수(STF)를 통해 검증해야 한다. 파라체인의 논리와 관련된 핵심 제약 조건은 릴레이 체인 밸리데이터가 검증할 수 있어야 한다는 것이다. 검증은 일반적으로 검증 증명(PoV) 블록이라고 하는 상태 전이 증명의 묶음 형태로 이루어지며, 이는 하나 이상의 파라체인 수집기에서 밸리데이터에게 검증을 위해 제출된다.

왜 파라체인을 사용해야 할까요?

파라체인은 블록체인의 두 가지 근본적인 문제를 해결하는 솔루션이다.

- 확장성 : 여러 용도로 하나의 블록체인을 사용하는 것은 향후 구현 및 업그레이드가 특정 용도에는 유리하지만 다른 용도에는 불리할 수 있으므로 확장성 확보가 어렵다. 반대로, 여러 블록체인을 사용하면 다른 체인에 영향을 미치지 않고 기능을 구현할 수 있다.
- 유연성 : 블록체인은 하나의 문제를 해결하는 데 매우 능숙할 수도 있고, 여러 문제를 해결하는 데는 그다지 능숙하지 않을 수도 있다. 특정 문제 해결에 특화된 블록체인은 자체적으로 그리고 사용자에게 더 큰 영향력을 행사할 수 있다. 파라체인은 특수 목적으로 구축된 블록체인으로, 고도로 전문화되어 있으며 협력을 통해 서로의 장점을 활용할 수 있다.

파라체인 혜택

파라체인은 자체 런타임/STF 로직을 포함하고 있으며, 릴레이 체인이 제공하는 공유 보안 및 교차 합의 메시징의 이점을 활용한다. 파라체인은 높은 유연성과 맞춤 설정을 제공하지만, 시간이 지남에 따라 생성 및 유지 관리에 더 많은 노력이 필요하다. 프로덕션급 파라체인은 블록체인 네트워크의 기술적 및 경제적 측면과 관련된 복잡성으로 인해 일반적으로 생성 과정이 더 복잡한다.

파라체인은 개발자에게 화폐 시스템 및 기타 체인 관련 요소를 처음부터 구축할 수 있는 더 많은 공간을 제공한다. 스마트 컨트랙트 플랫폼보다 복잡한 로직을 더 간결하고 효율적으로 실행할 수 있다. 또한 파라체인은 거버넌스 측면에서 더 큰 유연성을 제공하며, 현재의 하드 포크 방식보다 논란의 여지가 적은 방식으로 완전한 업그레이드를 수행할 수 있다.

파라체인이나 파라스레드에 적용할 수 있는 기능의 몇 가지 예는 다음과 같다.

- 사용자 정의 수수료 구조(예: 정액 거래 수수료 지불 또는 바이트당 지불).
- 릴레이 체인(폴카닷 또는 쿠사마)을 통한 공유 보안 및 완료.
- 토착 토큰과 지역 경제를 위한 맞춤형 통화 정책.
- 주정부 기능의 전환을 통해 재정이 조달된다.
- 온체인 재무를 할당하는 DAO를 관리할 수 있는 거버넌스 메커니즘이다.

공유 보안

공유 보안(때로는 풀 보안 이라고도 함)은 파라 체인 으로 전환하여 네트워크에 가입 하려는 체인에게 고유한 가치 제안 중 하나이다. 높은 수준에서 공유 보안은 코어에 접근하여 릴레이 체인에 연결된 모든 파라체인이 릴레이 체인 밸리데이터가 제공하는 경제적 보안의 혜택을 누릴 수 있음을 의미한다.

공유 보안의 개념은 브릿지 아키텍처를 기반으로 하는 체인 간 프로토콜과 다르다. 브릿지 프로토콜의 경우 각 체인은 주권자로 간주되며 자체 밸리데이터 세트와 경제적 보안을 유지해야 한다. 이러한 프로토콜의 한 가지 우려 사항은 보안의 확장성이다. 예를 들어 블록체인을 확장하기 위한 한 가지 제안은 알트코인에 따른 확장으로, 더 큰 알트코인이 블록을 채우면서 거래량이 시가총액이 낮은 알트코인으로 필터링된다는 것을 의미한다. 이 아이디어의 주요 결함은 시가총액이 낮은 코인은 경제적 보안이 덜하고 공격하기 쉽다는 것이다. 51% 공격의 실제 사례가 최근에 발생했다(2019년 1월 10일 Ethereum Classic 공격). 알려지지 않은 공격자가 219,500 ETC(약 110만 달러)를 두 배로 지출했다. 그 후 ETC에 대한 51% 공격이 두 번 더 발생했다.

풀카닷은 모든 경제적 인센티브를 릴레이 체인에 집중시키고 파라체인이 제네시스 시점에 더 강력한 보장을 활용할 수 있도록 함으로써 보안 확장성 문제를 해결한다. 소버린 체인은 자금력이 풍부한 공격자로부터 충분히 안전할 수 있도록 코인 가치를 높이기 위해 훨씬 더 많은 노력을 기울여야 한다.

PoW 대 Parachain 모델

현재 작업증명(PoW) 체인에 존재하는 표준 주권 보안 모델과 풀카닷의 공유 보안 모델을 비교해 보겠다. 비트코인, 제트캐시, 그리고 그 파생 상품들은 독립적인 채굴자 네트워크를 구축하고 정직한 해시 파워의 경쟁력 있는 부분을 유지해야 한다. 채굴 산업이 핵심 참여자들을 점점 더 중앙화하는 거대 산업으로 성장함에 따라, 단일 행위자가 체인을 공격할 만큼 충분한 해시 파워를 통제할 수 있다는 사실이 점점 더 현실화되고 있다.

즉, 네트워크에서 안전한 양의 해시 파워를 유지할 수 없는 소규모 체인은 해시 파워를 비트코인에서 다른 덜 안전한 체인으로 옮기려는 대규모 채굴 카르텔의 공격을 받을 가능성이 있다. 오늘날 51% 공격은 실행 가능하며, Ethereum Classic(위 참조), Verge, Bitcoin Gold 및 기타 암호화폐에 대한 공격이 보고됐다.

풀카닷에서는 체인 보안 간의 이러한 불균형이 발생하지 않는다. 파라체인이 릴레이 체인에 연결되면 밸리데이터는 해당 파라체인의 상태 전환을 안전하게 보호한다. 파라체인은 밸리데이터에게 최신 상태 전환 및 증명/증명 정보를 제공하기 위해 몇 개의 콜레이터 노드를 운영하는 오버헤드만 발생시킨다. 밸리데이터는 자신에게 할당된 파라체인에서 이러한 정보를 확인한다. 이러한 방식으로 새로운 파라체인은 출시된 지 얼마 안 되었더라도 릴레이 체인이 제공하는 전반적인 보안의 이점을 즉시 누릴 수 있다.

파라체인 경제

파라체인은 자체 토큰을 통해 자체적인 경제 구조를 가질 수 있다. 지분증명(PoS)과 같은 방식은 일반적으로 검증 및 확정을 처리할 밸리데이터 집합을 선택하는 데 사용되지만, 파라체인은 이러한 작업을 수행할 필요가 없다. 그러나 풀카닷은 파라체인이 구현할 수 있는 기능에 대해 지나치게 까다롭지 않으므로, 스테이킹 토큰을 구현하는 것은 파라체인의 선택일 수 있지만, 일반적으로 필수적인 것은 아니다.

콜레이터는 네이티브 파라체인 토큰의 인플레이션을 통해 인센티브를 받을 수 있다. 네이티브 파라체인 토큰을 인플레이션하지 않고도 콜레이터 노드에 인센티브를 제공하는 다른 방법이 있을 수 있다.

네이티브 파라체인 토큰의 거래 수수료는 파라체인의 구현 방식 선택 사항일 수 있다. 폴카닷은 파라체인이 거래의 원래 유효성을 결정하는 방식에 대해 엄격한 규칙을 정하지 않는다. 예를 들어, 파라체인은 거래가 유효하려면 콜레이터에게 최소 수수료를 지불해야 하도록 구현될 수 있다. 릴레이 체인은 이 유효성을 강제한다. 마찬가지로, 파라체인은 구현에 이러한 내용을 포함하지 않을 수 있으며, 릴레이 체인은 여전히 유효성을 강제한다.

파라체인은 토큰을 보유할 의무가 없다. 토큰을 보유하는 경우, 해당 토큰의 경제적 타당성을 입증하는 것은 파라체인(릴레이 체인이 아닌)의 몫이다.

코어타임

파라체인은 코어를 통해 릴레이 체인에 접근할 수 있다.

릴레이 체인 코어를 할당하는 방법에는 두 가지가 있다.

- 시스템 체인에만 거버넌스를 통해 제공된다.
- 비시스템 체인의 경우 DOT (Kusama의 KSM)를 통해 코어타임을 구매한다. 코어타임은 릴레이 체인 코어에서 연산 시간을 임대하는 데 사용된다. 이는 Polkadot의 공유 보안 및 상호 운용성에 접근할 수 있는 유일한 방법이다.

시스템 파라체인은 폴카닷의 온체인 거버넌스에 의해 할당되며, 다른 네트워크 또는 체인과의 브릿지 역할을 하는 네트워크 프로토콜의 일부이다. 이러한 파라체인은 일반적으로 경제 모델이 없으며, 릴레이 체인에서 트랜잭션을 제거하여 파라체인 처리 효율을 높이는 데 도움을 준다.

비시스템 체인은 DOT (또는 Kusama의 KSM)에서 구매한 대량 또는 주문형 코어타임을 통해 릴레이 체인의 코어에 액세스할 수 있다.

코어타임 만료

코어타임 구매에 사용된 DOT (또는 쿠사마의 KSM)는 소각된다. 코어타임이 만료되기 전에 파라체인은 대량 코어타임 구매를 통해 고정 비용으로 코어타임을 갱신할 수 있다. 파라체인이 대량 코어타임을 구매하지 않는 경우, 릴레이 체인에 접근해야 할 때 필요에 따라 코어타임을 온디맨드(수요 및 기타 시장 상황에 따라 블록당 가변 가격)로 구매할 수 있다. 릴레이 체인 코어의 시간을 연장하기 위한 코어타임이 없는 파라체인은 파라스레드(등록은 되었지만 ParaID코어에 접근할 수 없는 체인) 상태로 더 이상 사용되지 않는다.

시스템 파라체인

시스템 파라체인은 네트워크 거버넌스에서 할당한 실행 코어를 사용하는 파라체인이다. 이러한 체인은 릴레이 체인에서 트랜잭션을 제거하여 네트워크 밸리데이터가 검증 파라체인에 리소스를 할당할 수 있도록 한다. 시스템 체인은 폴카닷이 자체 확장 기술을 사용하여 호스팅하는 체인이다.

주문형 파라체인

온디맨드 파라체인은 전용 릴레이 체인 코어를 임대할 필요 없이 (블록 단위로) 일시적으로 네트워크 보안에 참여한다. 이는 여러 경쟁 리소스(파라체인)가 코어라는 희소한 리소스를 경제적으로 공유함으로써 이루어진다. 코어를 완전히 확보할 수 없거나 확보하는 것이 경제적으로 합리적이지 않다고 판단되는 체인도 공유 보안에 참여할 수 있다. 온디맨드 코어타임은 더 이상 전용 코어가 필요하지 않지만 릴레이 체인을 계속 사용하고자 하는 파라체인에게 적절한 오프램프를 제공하기 때문이다.

온디맨드 파라체인의 역사적 맥락

2019년 청두에서 있었던 이 강연에 따르면, 온디맨드 파라체인 아이디어는 80년대 후반과 90년대 초창기 개인용 컴퓨터의 제한된 메모리 자원에서 비롯되었다고 한다. 컴퓨터의 물리적 메모리 용량이 제한되어 있기 때문에, 애플리케이션에 더 많은 메모리가 필요할 때 컴퓨터는 하드 디스크의 스왑 공간을 활용하여 가상 메모리를 생성할 수 있다. 스왑 공간을 통해 컴퓨터 메모리 용량을 확장하고 더 많은 프로세스를 동시에 실행할 수 있지만, 일부 프로세스의 처리 속도가 느려지는 단점이 있다.

파라체인 vs. 주문형 파라체인

파라체인과 온디맨드 파라체인은 개발 관점에서 매우 유사하다. 서브스트레이트로 개발된 체인은 수명 주기의 여러 시점에서 다음 세 가지 상태 중 하나를 가질 수 있다고 상상해 볼 수 있다.

보안된 브릿지가 있는 독립적인 체인
릴레이 체인에 지속적으로 연결된 파라체인,
또는 릴레이 체인에 간헐적으로 연결된 파라체인(즉, 주문형)
이러한 상태 간 차이는 기술적인 차이보다는 경제적인 차이에 가깝기 때문에 비교적 최소한의 노력으로 이러한 상태를 전환할 수 있다.

온디맨드 파라체인은 릴레이 체인 연결에 있어 폴 파라체인과 동일한 이점을 제공한다. 즉, XCMP를 통해 다른 파라객체에 메시지를 전송할 수 있으며, 릴레이 체인 밸리데이터 세트의 완전한 경제적 보안을 통해 보호된다.

파라체인의 사용 사례

우리는 아직 파라체인의 진정한 잠재력을 알아내야 하며, 아래에 나열된 내용은 단지 몇 가지 예일 뿐이다.

- 암호화된 컨소시엄 체인 : 이는 대중에게 정보를 유출하지 않는 개인 체인일 수 있지만 XCMP 프로토콜의 특성으로 인해 여전히 신뢰 없이 상호 작용할 수 있다.
- 고주파 체인 : 이러한 체인은 특정한 균형을 취하거나 최적화를 통해 짧은 시간 안에 많은 거래를 계산할 수 있다.
- 개인정보 보호 체인 : 이러한 체인은 새로운 암호화를 통해 대중에게 어떠한 정보도 유출하지 않는다.
- 스마트 계약 체인 : 이러한 체인은 스마트 계약 이라고 알려진 코드의 배포를 통해 구현된 추가 논리를 가질 수 있다.

파라체인 호스트

블록체인은 상태 전이의 방향성 비순환 그래프 (DAG)로, 추가된 모든 블록은 누적 상태를 갖는 체인의 헤드 또는 포크로 볼 수 있다. DAG를 통과하는 모든 경로는 제네시스 블록에서 끝난다. 블록체인은 각 블록이 하나의 부모 블록만 가질 수 있으므로 트리 구조이다.

블록체인 네트워크는 체인의 여러 포크(fork)를 볼 수 있는 노드들로 구성되며, 어떤 포크를 따를지 결정해야 한다. 파라체인 호스트를 구성하려면 두 가지 구성 요소가 다루는 두 가지 범주의 질문에 답해야 한다.

- 블록체인의 상태 전환 함수는 무엇인가요? 이는 체인의 상태 전환 로직을 정의하는 런타임에 의해 처리된다. 런타임 로직은 다음과 같이 구분된다.
- 모듈은 프로토콜의 특정 동작을 캡슐화하며 다음으로 구성된다.
 - 저장
 - 루틴은 블록 초기화 또는 종료 시 진입점 및 다른 모듈에 의해 호출된다. 루틴은 모듈의 저장 공간을 변경할 수 있다.
 - 진입점은 모듈에 새로운 정보가 도입되는 방식을 정의하고, 정보가 호출되는 출처(사용자, 루트, 파라체인)를 제한할 수 있다.
- API는 노드 측 동작이 단일 포크의 상태에서 의미 있는 정보를 추출할 수 있는 수단을 제공한다.
- 블록체인의 다양한 포크를 인지할 때, 노드는 어떤 행동을 취해야 할까? 노드는 어떤 포크의 상태에서 어떤 정보를 추출해야 하며, 그 정보는 어떻게 사용되어야 할까? 이는 노드 측 행동(Node-side behavior)에 의해 처리되며, 이는 노드가 블록체인을 인식하는 관점에 따라 수행하는 모든 활동을 정의한다. 노드 측 행동은 두 가지 범주로 나눌 수 있다:
- 네트워킹 행동은 정보가 노드 간에 어떻게 분배되는지와 관련이 있지만, 정보가 나중에 어떻게 사용되는지는 관련이 없다.
- 핵심 동작은 특정 노드가 수행하는 내부 작업과 관련이 있다. 이러한 동작은 정보가 배포 되고 수신 되는지에만 관심이 있을 뿐, 이 두 가지가 어떻게 달성되는지에는 관심이 없다.

이 두 범주는 종종 상호 작용하지만, 서로 크게 추상화될 수 있다. 노드 측 동작은 특정 작업 범주를 수행하는 다양한 하위 시스템 으로 나뉜다. 하위 시스템은 경합 상태를 방지하는 오버시어(Overseer)를 통해 서로 통신할 수 있다.

- [Collator subsystem](#)
- [Backing subsystem](#)
- [Availability subsystem](#)
- [Approval subsystem](#)
- [Dispute subsystem](#)
- [Utility subsystem](#)

런타임과 노드 측 동작은 서로 종속된다. 런타임은 블록 을 작성하고 올바른 진입점을 트리거하는 외부

요소를 포함하기 위해 노드 측 동작에 의존한다. 노드 측 동작은 런타임 API를 사용하여 수행할 작업을 결정하는 데 필요한 정보를 추출한다.

파라체인 허브

릴레이 체인은 파라체인 간 크로스체인 기능을 가능하게 하지만, 한 파라체인에서 메시지를 전송한 후 목적지 파라체인이 메시지를 수신할 때까지 약간의 지연 시간이 필요하다. 낙관적인 시나리오에서, 이 메시지의 지연 시간은 최소 두 블록 이상이어야 한다. 한 블록은 메시지를 전송하는 데 소요되고, 다른 한 블록은 수신 파라체인이 메시지를 처리하고 블록을 생성하는 데 소요된다. 그러나 경우에 따라 처리 대기 중인 메시지가 많거나, 두 파라체인 네트워크 모두에서 메시지를 빠르게 주고받을 수 있는 노드가 없는 경우, 메시지 지연 시간이 더 길어질 수 있다.

크로스체인 메시지 전송 시 필요한 지연 시간으로 인해 일부 파라체인은 전체 산업의 허브 역할을 계획하고 있다(자산 허브 및 브릿지 허브 참조). 예를 들어, 많은 DeFi 애플리케이션은 '결합성'이라는 속성을 활용할 수 있다. 결합성은 한 애플리케이션의 기능을 다른 애플리케이션과 시너지 효과를 내어 결합하여 새로운 애플리케이션을 만들 수 있음을 의미한다. 이러한 예로는 거래 종료 시 대출금을 상환하는 조건으로 자금을 빌려 온체인 로직을 실행하는 플래시 대출이 있다.

크로스체인 지연 시간 문제는 단일 블록체인에 비해 파라체인 간의 결합성(composability)이 약화된다는 것을 의미한다. 이는 폴카닷(Polkadot), 이더리움(Ethereum) 등을 포함한 모든 샤딩 블록체인 설계에서 공통적으로 나타나는 현상이다. 이에 대한 해결책은 단일 블록 결합성이라는 강력한 특성을 유지하는 파라체인 허브(parachain hub)를 도입하는 것이다.

시스템 체인

릴레이 체인의 주요 기능은 파라체인(parachain)을 보호하고 파라체인 간의 안전한 통신을 촉진하는 것이다. 자산 이전, 거버넌스, 신원, 브리징(잠재적으로 리소스 집약적인 작업)과 같은 다른 모든 기능은 시스템 체인에서 별도로 운영함으로써 이점을 얻을 수 있다. 시스템 체인은 성능상의 이유로 릴레이 체인에서 기능을 위임하여 폴카닷 아키텍처가 제공하는 고유한 병렬화 기능을 활용한다.

개요

시스템 파라체인은 폴카닷 프로토콜의 핵심 기능을 포함하지만, 릴레이 체인이 아닌 파라체인에 존재하는 시스템이다. 마켓플레이스에서 코어타임을 구매하는 대신, 시스템 체인의 실행 코어는 네트워크 거버넌스를 통해 할당된다.

폴카닷은 릴레이 체인 대신 파라체인에 핵심 프로토콜 로직을 호스팅함으로써, 자체적인 확장 기술, 즉 병렬 실행을 사용하여 스스로를 호스팅한다. 시스템 파라체인은 릴레이 체인에서 트랜잭션을 제거하여 폴카닷의 주요 목적인 파라체인 검증에 더 많은 릴레이 체인 블록 공간을 사용할 수 있도록 한다.

시스템 파라체인은 업그레이드 및 기타 민감한 작업을 관리하기 위해 항상 온체인 거버넌스를 따른다. 즉, DOT KSM과 별도로 자체 토큰이나 거버넌스 시스템을 보유하지 않는다. 실제로 네트워크 거버넌스를 위한 시스템 파라체인이 존재할 가능성이 높다.

기존 시스템 체인

폴카닷

자산 허브

폴카닷과 쿠사마의 자산 허브는 최초의 시스템 파라체인이다.

자산 허브는 전체 네트워크를 위한 자산 포털이다. 자산 생성자(예: 준비금 기반 스테이블코인 발행자)가 네트워크 내 자산 총 발행량을 추적할 수 있도록 지원하며, 여기에는 다른 파라체인으로 이체된 금액도 포함된다. 또한, 자산 허브를 통해 거래, 채굴 및 소각을 수행하고 온체인 자산을 관리할 수 있다.

자산 허브는 유니크 팔레트와 NFT 팔레트를 통해 대체 불가능한 자산(NFT)도 지원한다. NFT에 대한 자세한 내용은 관련 위키 페이지를 참조하세요.

자산 관리 로직은 스마트 컨트랙트에 인코딩되지 않고 체인 런타임에 직접 구현된다. 파라체인에서 로직을 실행하는 효율성 덕분에 수수료와 예치금은 릴레이 체인에서 각각 가치의 약 1/10 수준이다.

수수료 수준이 낮기 때문에 Asset Hub는 잔액과 이체를 처리하는 데 적합할 뿐만 아니라 체인상 자산을 관리하는 데도 적합하다.

집단

폴카닷 콜렉티브스 파라체인은 제81차 국민투표에서 추가되었으며 폴카닷에만 존재한다(즉, 쿠사마에는 존재하지 않는다). 콜렉티브스 체인은 폴카닷 네트워크를 지원하는 온체인 콜렉티브들을 호스팅한다.

이러한 단체로는 폴카닷 얼라이언스(Polkadot Alliance)와 폴카닷 기술 펠로우십(Polkadot Technical Fellowship)이 있다. 이러한 온체인 단체들은 네트워크 관리 및 탈중앙화 거버넌스의 미래에서 중요한 역할을 수행할 것이다.

네트워크 자체는 집단으로서의 역할을 수행할 수 있으며, 다른 네트워크 내에서 입법적 목소리를 단일 의견으로 표현할 수 있다. 이는 브릿지 허브의 지원을 통해 실현된다.

브릿지 허브

폴카닷과 쿠사마가 첫 번째 파라체인을 지원하기 전에는 브릿지를 설계하는 유일한 방법은 릴레이 체인 자체에 로직을 적용하는 것이었다. 이제 두 네트워크 모두 파라체인을 지원하므로, 각 네트워크에 브릿지 전용 파라체인을 두는 것이 합리적이다. 파라체인이 제공하는 실행 격리성 때문이다.

브릿지 허브 시스템 파라체인은 릴레이 체인에서 작동하며, 더 넓은 웹 3.0 공간으로의 브릿지를 용이하게 한다. 브릿지 허브는 런타임에 폴카닷, 쿠사마, 이더리움과 같은 다른 블록체인 네트워크와의 신뢰 없는 브리징을 가능하게 하는 필수 브릿지 팔레트를 포함한다. 브릿지 허브는 릴레이 체인의 네이티브 토큰을 사용한다.

최신 교량 프로젝트에 대한 정보는 교량 페이지에서 확인하세요.

피플 체인

People Chain을 사용하면 사용자가 자신의 계정 신원을 관리할 수 있다.

코어타임 체인

코어타임 시스템 체인을 통해 사용자는 코어타임을 구매하여 폴카닷 컴퓨팅에 접근할 수 있다. 코어타임 마켓플레이스는 코어타임 체인을 기반으로 운영된다. 애자일 코어타임에 대한 자세한 내용은 [여기를 참조하세요](#).

브릿지

브릿지는 폴카닷이나 이더리움처럼 기술적으로 다양한 네트워크 간의 크로스 체인 통신을 가능하게 하는 필수 인프라이다. 브릿지를 통해 이러한 체인들은 서로의 최종 상태를 확인하고 신뢰할 수 있으며, 자산 스왑이나 체인 마이그레이션과 같은 다양한 애플리케이션의 기반을 마련한다.

현재의 브릿지 아키텍처는 다중 서명 릴레이와 같은 중앙 집중식 중개자를 사용하여 체인 간에 전달되는 정보의 유효성을 검사한다. 이러한 접근 방식은 추가적인 신뢰 가정을 도입하고 단일 장애 지점을 생성하여 검열과 같은 공격 경로를 제공한다. 최근의 역사는 이러한 접근 방식이 얼마나 위험한지 보여주었다. 중앙 집중식 기관은 침해되거나 악의적인 행동을 할 수 있다. Chainalysis 보고서에 따르면, 중앙 집중식 브릿지의 장애는 전체 암호화폐 해킹의 60% 이상을 차지하며, 이로 인한 손실액은 20억 달러를 초과한다. rekt 순위표 상위 5개 사건 중 4개가 브릿지 관련 해킹이다. 시스템의 보안은 가장 약한 연결 고리에 따라 결정되며, 브릿지는 심각한 취약점임이 입증됐다.

브리징의 목적

브릿지를 통해 폴카닷은 비트코인 및 이더리움과 같은 외부 블록체인과 통신할 수 있다. 폴카닷 내에서 체인들은 이미 안전한 상호운용성의 이점을 누리고 있다. 파라체인 간의 신뢰 없는 통신을 가능하게 하는 기본 상호운용성 기술에 대한 자세한 내용은 위키의 교차 합의 페이지를 참조하십시오.

따라서 브릿지 디자인은 중앙집중형 및 신뢰형부터 탈중앙화 및 신뢰가 필요 없는 형태까지 다양한 형태를 띠고 있다. 폴카닷은 자사 생태계에서 후자의 브릿지 디자인을 선호한다.

신뢰 불필요 브릿지

체인 A와 B 사이의 양방향 무신뢰 브릿지는 두 개의 단방향 브릿지($A \rightarrow B$, $B \rightarrow A$)로 볼 수 있다. 따라서 양방향 브릿지의 설계는 소스 체인과 타겟 체인을 갖는 단방향 브릿지의 관점에서 설명할 수 있다. 모든 무신뢰 브릿지는 온체인 및 오프체인 구성 요소를 갖는다.

신뢰 없음은 사용자가 특정 개인이나 조직을 신뢰할 필요가 없다는 것을 의미한다. 수학, 코드, 암호, 프로토콜만 신뢰하면 된다. 높은 수준의 신뢰를 요구하는 시스템의 예로는 다중 서명 방식을 통해 제어되는 브릿지가 있는데, 이 경우 공동 서명자를 신뢰해야 한다.

신뢰할 수 없는 시스템을 정의할 때는 원칙적으로 항상 기본적인 가정이 필요하다. 완전히 신뢰할 수 없는 설정이 항상 보장될 수는 없기 때문이다.

온체인 브릿지 구성 요소

신뢰할 수 없는 브릿지를 구축하려면 다음과 같은 온체인 구성 요소를 구현해야 한다(제안된 방법론에 따라 정렬).

- 브릿지 팔레트 - 서브스트레이트 기반 체인의 경우 브릿지 팔레트를 사용한다(예: Kusama <->Polkadot 브릿지, 두 네트워크의 파라체인 모두 서브스트레이트를 사용함).
- 스마트 계약 - 체인이 서브스트레이트에 없는 경우 서브스트레이트가 아닌 체인에 스마트 계약을 맺어 브릿지 해야 한다 (예: 스노우 브릿지, Ethereum 메인넷에는 수신 XCMP 메시지를 기반으로 Eth 트랜잭션을 시작하는 브릿지 스마트 계약이 있음).
- 고차 프로토콜 - 체인이 스마트 계약을 지원하지 않는 경우(예: 비트코인), XClaim 이나 유사한 프로토콜을 사용하여 연결해야 한다.

온체인 브릿지 구성 요소는 체인 런타임에 배포되는 모듈(일반적으로 팔레트 또는 스마트 계약)이다. 소스 체인의 완결성을 추적하는 모듈은 대상 체인에 배포되어야 하며, 크로스 체인 메시징을 처리하는 모듈은 소스 체인과 대상 체인 모두에 배포되어야 한다.

소스 체인에서 메시지를 큐에 넣고 대상 체인에서 메시지 증명을 수신하는 온체인 구성 요소도 있다. 메시지는 특정 레인을 통해 전송되며, 전송된 순서대로 수신이 보장된다. 브릿지 허브에서 메시지는 XCM 형식이며, XCM 실행기를 사용하여 메시지를 전송한다.

브릿지 팔레트를 통해

GRANDPA 합의를 통해 완결되는 체인 간 브릿지를 운영하는 것은 간단하다. 대상 체인의 런타임에 내장된 소스 체인의 GRANDPA 라이트 클라이언트는 소스 체인의 완결성에 대한 "진실의 원천"을 제공한다. 예를 들어, Bridge Hub는 GRANDPA 합의를 사용하고 Kusama와 그 파라체인에서 발생하는 모든 거래의 완결성을 추론하는 Kusama의 온체인 라이트 클라이언트를 실행한다.

서브스트레이트 팔레트를 통해 외부의 비-파라체인 블록체인에서 Polkadot으로 메시지를 수신할 수 있다. 서브스트레이트 인스턴스는 Polkadot 핵심 소프트웨어의 네이티브 확장인 시스템 수준 파라체인 또는 커뮤니티 운영 파라체인으로 Polkadot에 배포될 수 있다.

브릿지 전용 팔레트를 엄격히 사용하는 예로는 쿠사마(Kusama)와 폴카닷(Polkadot) 간 브릿지가 있다. 양쪽 모두 서브스트레이트 기반의 패러체인(parachain)을 사용하기 때문이다.

패러체인 브리징 모듈이 없는 독립형 체인(비-서브스트레이트)의 경우, 브릿지 계약을 배포해야 한다.

스마트 계약을 통해

튜링 완전 스마트 컨트랙트 언어를 사용하는 블록체인 플랫폼의 보편성을 고려할 때, Polkadot과 다른 스마트 컨트랙트 지원 블록체인을 연결하는 것이 가능하다. 예를 들어, 스노우 브릿지는 Polkadot Bridge Hub를 사용하여 이더리움의 온체인 라이트 클라이언트를 실행하여 이더리움 체인에서 거래의 완결성을 추론한다. 이더리움의 스마트 컨트랙트를 통해 GRANDPA 라이트 클라이언트를 실행하는 것은 가능하지만 비용이 많이 든다. 따라서 GRANDPA 위에 구축된 BEEFY 합의 계층은 이더리움 및 기타 프로토콜을 사용하여 신뢰할 수 없는 브릿지를 운영하는 비용 효율적인 솔루션을 제공한다. Cosmos, Avalanche, NEAR 등과 같은 체인에 대한 신뢰할 수 없는 브릿지를 구현하려면 Bridge Hub에 맞춤형 팔레트를 배포해야 한다.

고차 프로토콜을 통해

XCLAIM과 같은 고차 프로토콜을 사용하여 브릿징할 수 있지만, 다른 옵션을 사용할 수 없는 경우에만 사용해야 한다. 특히 XCLAIM은 스왑 가능 자산이 스왑 가능 자산보다 높은 가치의 담보로 뒷받침되어야 하므로 추가적인 오버헤드가 발생한다.

고차원 프로토콜에 적합한 네트워크의 예로는 비트코인이 있다. 비트코인은 스마트 계약을 지원하지 않고 서브스트레이트에 기반하지 않기 때문이다.

비트코인 브릿지 (XCLAIM <-> 기판 <-> 폴카닷)

Interlay 팀은 XCLAIM 설계 문서를 기반으로 비트코인 브릿지에 대한 사양을 작성했다. 이 프로토콜은 폴카닷과 비트코인 간의 양방향 브릿지를 가능하게 한다. BTC 보유자는 폴카닷에서 iBTC를 발행하고, iBTC 보유자는 비트코인 체인에서 BTC를 상환할 수 있다.

사양에 명시된 대로 비트코인 브릿지는 논리적으로 서로 다른 두 가지 구성 요소로 구성된다.

- XCLAIM 구성 요소는 iBTC를 소유한 모든 계정을 유지 관리한다.
- BTC-Relay는 새로운 거래가 제출될 때 비트코인 상태를 검증한다.
자세한 작동 방식은 사양을 참조하세요.

이제 작동 가능한 구현과 메인넷 브릿지가 제공된다.

오프체인 브릿지 구성 요소

오프체인 브릿지 구성 요소는 릴레이어(relayer)라고 불리는 별도의 프로세스이다. 릴레이어는 소스 체인과 타겟 체인 노드 모두에 연결된다. 예를 들어, GRANDPA 합의 기반 체인 간 릴레이어의 역할은 소스 체인의 GRANDPA 정당화와 해당 헤더를 타겟 체인에 배치된 브릿지 GRANDPA 최종성 팔레트(Bridge GRANDPA Finality Pallet)에 제출하는 것이다. 이를 위해 릴레이어는 소스 체인의 GRANDPA 정당화 스트림을 구독하고 모든 새로운 정당화를 타겟 체인의 GRANDPA 라이트 클라이언트에 제출한다.

체인 간의 메시지는 릴레이어를 통해 전달되는데, 여기에는 메시지 전달 릴레이와 전달 확인 릴레이가 포함된다. 릴레이어 및 브릿지 허브 설계에 대한 자세한 내용은 Polkadot-SDK 저장소의 고급 브릿지 문서를 참조하세요.

브릿지 비교

스노우 브릿지와 Hyperbridge는 Polkadot을 다른 생태계와 연결하는 두 가지 신뢰할 수 없는 브릿지이다. 아래에서 두 브릿지의 주요 기술 비교를 살펴보겠다.

스노우브릿지

하이퍼브릿지

이더리움은 1개만 있다.

멀티체인.

Bridge Hub System Chain의 Ethereum 라이트 클라이언트와 Ethereum 스마트 계약의 Polkadot 라이트 클라이언트.

자신의 파라체인.

DOT 토큰.

하이퍼브릿지 네이티브 토큰.

증명자를 위한 무작위 샘플링 BEEFY.

영지식 증명.

코드베이스는 간단하지만 밸리데이터에 의한 분석은 복잡한다.

코드베이스는 복잡하지만 밸리데이터에 의한 분석은 간단하다.

증명용 저사양 하드웨어, 허가 불필요.

증명을 위한 고사양 하드웨어, 허가는 필요 없지만 ZK 기반 특성으로 인해 어느 정도 허가가 필요하다.

증명자에 대한 높은 수준의 분산화가 가능하다.

증명자 분산화가 가능하지만 아마도 BEEFY의 BLS (Boneh-Lynn-Shacham) 버전과 Ethereum에서 BLS 사전 컴파일을 통해 ZK 회로에 대한 증속성을 제거함으로써 가능할 것이다.

이더리움 ↔ 폴카닷: 수십 분 정도 소요. 폴카닷 → 이더리움: 폴카닷 상태를 업데이트하는 데 예측 불가능한 무작위성을 구현하려면 이더리움에서 커밋 애플로치가 필요하므로 지연 시간이 길다(30분).

이더리움 ↔ 폴카닷: 10~20분 정도 소요(폴카닷의 경우 두 브릿지 모두 동일한 지연 시간을 가짐). 폴카닷 → 이더리움: 낮은 지연 시간, 기존 하드웨어에서 5~7분.

BLS 서명 검증을 위한 외부 라이브러리에 대한 종속성 (Last Ethereum 합의 클라이언트인 Lighthouse에서 사용되는 Milagro BLS).

ZK 기반 특성으로 인해 외부 라이브러리에 대한 의존성이 있다. 이러한 라이브러리에는 PLONK가 포함된다.

크로스체인 메시지 포맷으로서의 XCM.

브릿지 통합 프로토콜로서의 ISMP.

- 서로 다른 브릿지를 통해 전송된 WETH는 서로 다르다. 특정 로직이 구현되지 않으면 스노우 브릿지를 통해 전송된 WETH는 Hyperbridge를 통해 다시 전송할 수 없다.
- 스노우 브릿지는 시스템 체인에 배포되므로 스노우 브릿지 WETH는 Polkadot의 "공식" WETH로 간주될 수 있다(다만, 이는 스노우 브릿지에 대해서는 긍정적인 신호이고 Hyperbridge에 대해서는 부정적인 신호로 해석되어서는 안 된다).

스노우 브릿지

Snowfork의 스노우 브릿지는 폴카닷과 이더리움을 연결하는 범용 신뢰 없는 브릿지이다. 브릿지 허브 시스템 파라체인을 활용하여 릴레이어와 연결을 구축하여 이더리움과 폴카닷 간의 허가 및 신뢰가 필요 없는 메시지를 가능하게 한다.

스노우 브릿지를 사용하면 발신자는 크로스체인 거래의 성공을 보장하기 위해 릴레이어를 실행할 수 있다(하지만 반드시 그럴 필요는 없다). 발신자는 다른 사람이 제공한 릴레이어를 사용하는 사용자이다.

스노우 브릿지는 현재 Ethereum과 Polkadot 파라체인 간의 양방향 토큰 전송을 지원한다.

무작위 샘플링 BEEFY

신뢰가 필요 없는 브릿지는 항상 증명자 (증명 계산 필요), 밸리데이터 (증명자에게 증명 계산을 요청하고 검증), 그리고 메시지를 전달하는 중계자를 갖는다. 스노우 브릿지 증명자는 보안을 손상시키지 않으면서 운영 비용을 대폭 절감하는 혁신적인 브릿지 프로토콜인 BEEFY를 사용한다.

BEEFY가 도입한 간소화에도 불구하고, 이더리움에서 폴카닷의 상태를 업데이트하는 스마트 컨트랙트는 폴카닷에 약 300개의 밸리데이터가 있기 때문에 매 업데이트마다 201번의 서명 확인을 수행해야 한다. 이는 특히 밸리데이터 수가 증가함에 따라 여전히 비용(가스비)이 많이 든다. 해결책은 RANDAO 난수 비콘을 활용하는 BEEFY를 다음과 같이 무작위 샘플링하는 것이다.

- 커밋: 릴레이어는 폴카닷에서 최근 완료된 블록에 대한 상태 커밋을 제출하고, 이더리움에 배포된 라이트 클라이언트에 대한 밸리데이터 서명의 절대 다수를 보유하고 있다고 주장한다. 또한 커밋을 뒷받침하는 밸리데이터 서명 하나를 제공하는데, 이는 필요한 경우 슬래싱될 수 있다.
- 과제: 경량 클라이언트가 체인상 무작위성(RANDAO)을 쿼리하여 mRelayer가 주장한 목록에서 서명(~25개)을 하위 샘플링한다.
- 응답: Relayer는 무작위로 샘플링된 서명을 정확히 공유하여 응답하고 m, 라이트 클라이언트는 이를 검증한다. 모든 내용이 확인되면 최종 블록이 승인된다.
필요한 서명 확인 횟수가 크게 줄어들고 밸리데이터 세트 크기에 영향을 받지 않아 프로토콜의 효율성이 향상된다. 하위 샘플링된 서명의 수는 m, 보안과 효율성의 균형을 이루는 매개변수(즉, 보안 매개변수)이다. 이 매개변수의 값은 암호경제적 논증을 사용하여 도출된다.

스노브릿지 암호경제 보안

검증자의 최대 1/3이 악의적일 경우, 표본 추출된 m개의 서명이 모두 이 악의적 행위자들로부터 나온 확률은 $(1/2)^m$ (지수적으로 낮음)이다. 악의적 커밋먼트를 지지하는 검증자는 심각한 제재를 받는다. 공격의 기대값 $E(A)$ 는 다음과 같다:

$$E(A) = p * V + (1 - p) * (-S)$$

여기서 V는 공격 가치(시가총액으로 상한이 정해짐), S는 검증자의 벌금 부과 대상 지분, p는 공격 성공 확률이다.

스노브릿지 가정

스노우 브릿지는 두 가지 주요 가정에 의존한다.

- 공격자가 합리적이라는 암호경제적 가정, 즉 공격은 공격의 기대값이 양수일 때만 실행된다는 가정이다. 따라서 m공격의 기대값이 음수, 즉 $E(A) < 0$. 가 되도록 하여 보안 매개변수를 도출한다.
- RANDAO의 예측 불가능성. Web3 Foundation 연구팀은 RANDAO 편향에 대한 철저한 분석을 수행하고, RANDAO에 대한 마지막 공개자 공격(last-revealer attack)을 분석하는 데 최첨단 기술을 적용했다. 이더리움 밸리데이터의 1/3이 악의적이라고 가정할 때, 보안 매개변수를 비례적으로 증가시킴으로써 이러한 편향의 영향을 완화할 수 있다.

하이퍼 브릿지

상호운용성은 풀카닷 기술의 핵심 비전이다. 수년간의 블록체인 개발을 통해 블록체인 간 안전한 상호운용성 솔루션을 구축하기 위해 많은 노력이 기울여져 왔다. 풀카닷은 크로스 합의 메시징(XCM) 및 크로스 체인 메시지 전달(XCMP) 프로토콜을 통해 파라체인(parachain) 간의 안전한 상호운용성을 제공한다. 그러나 이러한 솔루션은 공유 보안이 있을 때만 작동한다. 동일한 풀카닷의 공유 보안에 속하지 않는 체인 간의 상호 작용의 경우, 브릿지가 필요하다.

하이퍼브릿지(Hyper-Scalable Bridge의 약자)는 상호 운용성 보조 프로세서로 구축된 크로스체인 솔루션으로 혁신을 이루었다. 하이퍼브릿지는 모든 블록체인에서 암호화 보안, 합의 및 상태 증명 기반 상호 운용성을 확장하도록 설계됐다.

코프로세서 모델

안전한 크로스체인 통신을 보장하려면 합의 메커니즘, 합의 오류, 상태 증명 및 상태 전환을 포함한 다양한 측면에 대한 세심한 검증이 필요하다.

코프로세서란 무엇인가요?

하드웨어 측면에서 코프로세서는 주 프로세서의 기능을 보완하도록 설계된 마이크로프로세서라고 할 수 있다. 예를 들어, GPU는 그래픽 및 동시 연산에 최적화되도록 CPU의 보조 프로세서이다.

온체인 검증 프로세스의 복잡성과 비용 부담으로 인해, 코프로세서 모델에서는 연산이 오프체인으로 수행된다. 실행 결과와 그 정확성을 검증하는 암호화 증명은 이후 온체인에 제공된다.

보조 프로세서 모델에 대해 더 자세히 설명하면, 암호화 계산을 오프로드하는 다른 솔루션에도 적용되었는데, 특히 제로 지식(ZK) 보조 프로세서 나 SNARK 회로에 적용됐다.

공동 프로세서로서의 Parachain

BEEFY 가 제공하는 비용 효율적인 합의 증명을 활용하여 Hyperbridge는 네트워크에서 보호되는 모든 파라체인 상태 전환의 적법성을 확인한다.

이 기능을 통해 합의, 상태 증명 및 상태 전환 재실행을 위한 검증 워크로드를 여러 지정된 코어에 분산할 수 있다. 따라서 하이퍼브릿지는 폴카닷을 검증 가능한 연산 계층으로 활용하여 크로스 체인 브릿지에서 "전체 노드 보안"을 제공한다.

따라서 추가적인 보안 계층이 제공되어 Hyperbridge가 연결된 체인 전반에서 비잔틴 행위를 감지하고 방지할 수 있다.

상호 운용 가능한 상태 머신 프로토콜(ISMP)

상호운용성 상태 머신 프로토콜(ISMP)은 상대방 체인에서 특정 로직을 트리거하기 위해 크로스체인 요청을 생성하려는 개발자에게 익숙한 HTTP 유사 API를 제공한다. POST 요청을 통해 연결된 체인에 임의의 데이터를 전송하고, GET 요청을 통해 연결된 체인에 있는 애플리케이션의 저장 공간(상태 증명을 통해 검증됨)을 읽을 수 있다.

ISMP는 연결된 체인 간의 크로스 체인 메시지 전달을 용이하게 할 뿐만 아니라, Hyperbridge 내부 상태 머신 간의 동기화 기본 요소 역할도 수행한다. 이를 통해 Parachain 코어들이 서로 통신하고 작업을 위임할 수 있다.

기반 기술

Hyperbridge의 기반 기술은 다음과 통합되어 있다.

- PLONK 검증기 : Hyperbridge의 PLONK 검증기는 정교한 보안 장치에 비유할 수 있다. 전문 탐정처럼 작동하여 개인 정보를 침해하지 않고 모든 거래의 적법성을 꼼꼼하게 확인한다. 특히 UltraPLONK와 같은 기술 발전을 통해 지속적으로 기능이 향상되고 있는 이 필수 구성 요소는 크로스체인 통신의 최고 수준의 무결성과 기밀성을 유지하는 데 핵심적인 역할을 한다.
- BEEFY 합의 : BEEFY(Bridge Efficiency Enabling Finality Yielder) 프로토콜은 GRANDPA를 보완하는 시스템으로, 폴카닷 네트워크의 릴레이 체인과 이더리움과 같은 외부의 고립된 블록체인 간의 효율적인 연결을 용이하게 하도록 특별히 설계됐다. 특히, BEEFY는 폴카닷 인터체인 프레임워크와 원활하게 통합되도록 설계되지 않은 블록체인의 상호운용성 문제를 해결한다.
- Barretenberg 백엔드 : Hyperbridge 영역 내에서 Barretenberg는 강력한 엔진 역할을 하며 복잡한 수학적 계산을 능숙하게 처리한다. 백엔드 인프라로서, Hyperbridge 생태계 내 모든 암호화 작업의 빠르고 안전하며 안정적인 실행을 보장한다.

용어

국가 증명

상태 증명은 무신뢰 브릿지와 같은 기능을 가능하게 하는 블록체인의 핵심 요소이다. 이러한 오프체인 라이트 클라이언트는 허가 없이 안전하게 온체인 데이터에 접근할 수 있으며, 실행 계층과 합의 계층을 분리할 수 있는 모듈식 블록체인 아키텍처를 제공한다.

합의 증명

블록체인 시스템에서 합의 증명은 참여자(종종 노드 또는 밸리데이터)가 새로운 거래나 블록의 유효성에 대해 집단적으로 동의하는 메커니즘을 의미한다. 합의 증명의 특성은 작업 증명, 지분 증명 또는 기타 합의 알고리즘과 같은 다양한 블록체인 아키텍처에 따라 다르다.

궁극적인 목표는 네트워크 참여자 간에 광범위하고 검증 가능한 합의를 보장하여 분산원장의 보안과 안정성을 강화하는 것이다.

예를 들어, 지분 증명 시스템에서 합의 증명은 전체 권한 집합의 초대다수(3분의 2 + 1) 하위 집합에서 체인의 최신 블록 헤더에 대한 서명으로 제공된다.

DOT - KSM 브릿지

폴카닷과 쿠사마 블록체인 네트워크는 모두 GRANDPA 합의를 통해 완결성을 확보하며, 이는 각각의 브릿지 허브를 통해 두 네트워크 간의 무신뢰 연결(trustless bridging)을 가능하게 한다. 폴카닷 브릿지 허브는 쿠사마 네트워크의 라이트 클라이언트를 실행하고, 쿠사마 브릿지 허브는 폴카닷 네트워크의 라이트 클라이언트를 실행하며, 두 네트워크 모두 OpenGov 국민투표를 통해 활성화됐다. 이 무신뢰 연결은 폴카닷 자산 허브가 래핑된 KSM 토큰을, 쿠사마 자산 허브가 래핑된 DOT 토큰을 브릿징할 수 있도록 하여, 모든 쿠사마 파라체인에서 DOT를, 모든 폴카닷 파라체인에서 KSM을 사용할 수 있도록 한다.

Polkadot 및 Kusama Bridge Relayers

릴레이어의 역할은 Kusama/Polkadot GRANDPA 정당성을 한쪽 브릿지 허브에서 다른 쪽 브릿지 허브로 전달하는 것이다. 또한 최종화된 Kusama Bridge Hub와 Polkadot Bridge Hub 블록 헤더를 릴레이한다. 릴레이어는 브릿지 허브에 메시지가 대기열에 있을 때만 작동한다. 대기열에 메시지가 없으면 릴레이어는 유휴 상태를 유지한다.

Polkadot 및 Kusama Bridge Relayer 실행

누구나 Polkadot < > Kusama Bridge에서 릴레이어를 실행할 수 있다. 자세한 내용은 Polkadot-SDK 저장소의 릴레이어 문서를 참조하세요. 물론 릴레이어 실행에는 비용이 발생한다. CPU와 네트워크 비용 외에도 릴레이어는 브릿지 양쪽에서 발생하는 거래에 대한 비용을 지불한다.

릴레이어 보상

릴레이어에게 지급되는 보상은 정적 보상과 동적 보상, 두 가지로 구성된다. 정적 보상은 온체인 거버넌스를 통해 설정된다. 릴레이어는 미리 설정된 수의 유효 메시지를 전송하여 미리 설정된 수의 DOT 또는 KSM을 획득해야 한다. 다른 보상은 동적 보상으로, 한 브릿지허브에서 다른 브릿지허브로 XCM 메시지를 전송하는 것을 포함한다. 릴레이어는 두 브릿지허브 모두에 트랜잭션을 제출해야 하며, 각 트랜잭션에는 다음과 같은 비용이 발생한다.

동적이기 때문에 메시지 크기가 변경될 수 있고 대상 체인의 수수료 요소가 변경될 수 있다.

중요한 점은 브릿지 거래의 규모가 임의로 정해질 수 있다는 것이다.

릴레이어는 유효하고, 최소이며, 유용한 브릿지 관련 거래를 제출하는 데 드는 비용에 대해 보상을 받는다. 여기서 '유효'는 거래가 실패하지 않음을 의미한다. '최소'는 거래 호출 내의 모든 데이터가 실제로 거래 성공에 필요함을 의미한다. '유용'은 거래에 제공된 모든 데이터가 새로운 데이터이지만 대상 체인에는 알려지지 않았음을 의미한다.

릴레이어에 대한 보상은 항상 전송 체인에서 지불한다. 전송 체인은 각 브릿지 허브의 소버린 계정에서 브릿지의 양쪽 끝에서 지불한다. 예를 들어, 폴카닷 자산 허브 (PAH) → 쿠사마 자산 허브 (KAH) 전송은 릴레이어가 폴카닷 브릿지 허브(PBH)에 있는 PAH의 소버린 계정에서 일부 보상을 받고, 쿠사마 브릿지 허브(KBH)에 있는 PAH의 소버린 계정에서 일부 보상을 받는 것을 포함한다. 폴카닷 오픈거브는 두 브릿지 허브(PBH 및 KBH)에 있는 PAH의 소버린 계정의 자금을 보충할 책임이 있다. 마찬가지로, KAH → PAH 전송은 PBH 및 KBH에 있는 KAH의 소버린 계정에서 보상을 받으며, 이는 쿠사마 오픈거브를 통해 보충해야 한다.

릴레이어 보상에 대한 자세한 내용은 Polkadot-SDK 저장소의 릴레이어 문서에서 릴레이어 보상 제도 섹션을 확인하세요.

롤업 및 상호 운용성

롤업 비교

롤업은 L2 확장 솔루션이다. 가장 기본적인 수준에서 롤업 L2 솔루션은 일반적으로 시퀀서 네트워크를 통해 L1 체인에 게시하기 전에 트랜잭션을 일괄 처리하여 "롤업"하는 역할을 한다. 이론적으로는 별도의 엔티티가 트랜잭션을 시퀀싱하고 게시하는 역할을 수행할 수 있다. 실제로는 동일한 머신이지만, 롤업의 분산화가 심화됨에 따라 이러한 방식은 변경될 가능성이 높다. 이 메커니즘은 단일 롤업에 수천 개의 트랜잭션을 포함할 수 있다.

2계층 정의

2계층(L2) 네트워크는 블록체인 확장성을 위한 핵심 접근 방식으로, 1계층(L1) 네트워크의 연산 부담을 대부분 덜어준다. 이러한 솔루션은 L1의 보안을 활용하여 더 빠르고, 수수료를 절감하며, 플랫폼별 과제를 해결하는 추가 계층을 구축한다. 또한 L2 솔루션은 L1 블록 공간을 효율적이고 비용 효율적으로 활용하는 데 중점을 둔다.

L2 네트워크는 모듈식 설계를 채택하고 기능을 재사용함으로써 이더리움 가상 머신(EVM), 솔라나 가상 머신(SVM), 무브 기반 시스템을 포함한 다양한 가상 머신 환경에 확장 가능한 롤업을 구축할 수 있도록 지원한다. 이러한 롤업은 이더리움으로 다시 통합되어 다양한 블록체인 생태계를 위한 견고하고 안전한 기반을 보장한다.

이 섹션에서는 다음 간의 롤업 기술의 주요 차이점을 살펴보겠다.

- 제로 지식 롤업,
- 낙관적 롤업 및
- 폴카닷 롤업(즉, 파라체인).

이러한 롤업 기술의 차이점을 살펴보기 전에, 비대화형과 대화형 방법의 차이점을 이해하는 것이 중요하다.

사기 증명 vs. 유효성 증명

롤업 맥락에서, 롤업 계층과 메인 블록체인(L1) 간의 트랜잭션 또는 상태 변경의 유효성을 확립하는 방식을 설명하기 위해 대화형 및 비대화형 방식이 일반적으로 사용된다. 이러한 용어는 표준 용어인 사기 방지 및 유효성 증명 메커니즘과 매우 유사하다.

(사기 방지와 관련된) 상호 작용 방식은 거래 검증을 위해 양방향 프로세스를 사용한다. "증명자"는 거래 데이터 또는 상태 변경 사항이 유효하다고 가정하고 L1에 제출한다. 분쟁이 발생하면 이의 제기 메커니즘이 작동하여 참여자는 무효성을 입증하는 증거(사기 방지)를 제공해야 한다. 이 프로세스는 정확성을 보장하지만, 구현 방식에 따라 달라질 수 있는 분쟁 해결 기간으로 인해 지연이 발생한다. 예를 들어, 낙관적 롤업은 종종 몇 시간에서 최대 7일까지 이의 제기 기간을 갖는다.

비대화형 방식 (유효성 증명과 관련됨)은 SNARK 또는 STARK와 같은 암호화 메커니즘을 사용하여 거래를 사전에 검증한다. 이러한 증명은 오프체인으로 생성되어 분쟁 해결 없이 검증을 위해 L1에 제출된다. 이러한 방식은 롤업 자체에 거의 즉각적인 완결성을 제공할 수 있지만, 궁극적으로는 L1의 완결성에 의해 제한된다(주권 롤업의 경우, 완결성은 다를 수 있음). 실제로는 안전장치로서 의도적으로 지연을 도입하는 경우가 있다. 예를 들어, zkSync 롤업은 기술적 한계 때문이 아니라, 기술이 성숙해지고고가 자산을 보호하는 동안의 예방 조치로서 거래를 완료하는 데 최대 하루가 걸릴 수 있다.

두 가지 메커니즘을 비교한 내용은 다음과 같다.

측면	사기 증거(대화형)	유효성 증명(비대화형)
기 구	분쟁이 대화형으로 해결되는 챌린지 기반 시스템이다.	암호화 증명을 통해 모든 거래를 사전에 검증하여 분쟁을 제거한다.
숨 어 있 음	최종 확정까지 걸리는 시간은 챌린지 기간에 따라 다르다. 낙관적 롤업은 확정하는 데 몇 시간 또는 며칠이 걸리는 경우가 많다. Polkadot 롤업은 이 시간을 약 30분으로 단축한다.	이론상으로는 거의 즉각적인 완료가 가능하다. 실제로 zkSync와 같은 시스템은 완료까지 최대 하루가 걸릴 수 있는데, 이는 내재적인 기술적 한계 보다는 인위적인 안전 장치로 인해 발생하는 경우가 많다.
보 안 기 반	암호경제적 인센티브와 참여자 모니터링을 통해 유효성이 보장된다.	암호화 보장을 통해 사전에 정확성을 보장하여 외부 모니터링의 필요성을 줄인다.
복 잡 성	구현하기는 간단하지만 적극적인 모니터링과 문제 해결이 필요하다.	특히 ZK 시스템의 경우, 계산 집약적이고 구축이 복잡한다.
사 용 사 례	기존 시스템과의 광범위한 호환성이 필요하고 최종성을 위해 어느 정도의 지연 시간을 허용하는 애플리케이션에 적합하다.	고도의 보안이 필요한 애플리케이션이나 사전 검증 및 빠른 확정이 중요한 시나리오에 이상적이다.

제로 지식 롤업

영지식 롤업(일반적으로 ZK 롤업이라고 함)은 특정 상태 변경 집합의 유효성을 계산하기 위해 SNARK 형태의 암호화 증명을 활용하는 비대화형 방법이다. 업계에서는 "ZK 롤업"이라는 용어를 채택했지만, 많은 구현 방식이 영지식 속성을 엄격하게 포함하지 않는다는 점에 유의해야 한다. 증명이 반드시 정보를 숨기는 것은 아니기 때문이다. 이러한 롤업은 간단히 SNARK 기반 롤업이라고 부르는 것이 더 적절하지만, "ZK 롤업"이라는 용어는 여전히 널리 사용되고 있다.

사기 방지 및 상호작용적 검증 메커니즘에 의존하는 낙관적 롤업과 달리, ZK 롤업은 전적으로 암호화 검증에 의존하며, SNARK는 정확성에 대한 사전 증명을 제공한다. 이러한 접근 방식을 통해 ZK 롤업은 검증 기간 없이 모든 상태 전환의 정확성을 보장하는 유효성 증명을 통해 훨씬 빠른 완료를 달성할 수 있다.

그러나 ZK 롤업은 증명 생성에 수반되는 계산 복잡성과 리소스가 제한된 환경에서 이러한 증명을 구현하는 어려움으로 인해 성능 문제에 직면한다. 또한 이러한 복잡성은 튜링 완전성 달성을 더욱 어렵게 만들어 블록 공간 사용 측면에서 일반화 가능성을 제한할 수 있다. 이러한 어려움에도 불구하고 ZK 롤업은 특수 애플리케이션에서 점점 더 활용도가 높아지고 있다. 예를 들어, Hyperbridge는 Polkadot 기반의 SNARK 기반 롤업으로, 확장 가능하고 신뢰할 수 있는 브릿지 역할을 한다. 여러 블록체인에 대한 단일 증명을 생성하여 Polkadot에서 즉시 검증할 수 있으므로, 틈새 시장에서 이러한 롤업의 잠재력을 보여준다.

낙관적 롤업

낙관적 롤업은 L1 블록체인을 위한 상호작용적 확장 방식이다. 제안된 모든 거래가 기본적으로 유효하다고 낙관적으로 가정한다.

잠재적으로 무효한 거래를 완화하기 위해 낙관적 롤업은 참여자가 의심스러운 롤업에 이의를 제기할 수 있는 이의 제기 기간을 도입한다. 사기 입증 체계를 통해 여러 사기 증거를 제출할 수 있다. 이러한 증거는 롤업의 유효성을 결정하거나 무효화할 수 있다. 이의 제기가 없고 필요한 증거가 있는 경우, 이의 제기 기간 동안 상태 변경 사항에 대한 이의 제기, 해결 또는 이의 제기가 이루어질 수 있다.

낙관적 롤업은 이더리움 생태계에서 자주 사용된다. 낙관적 EVM 기반 롤업의 예로는 낙관적 롤업과 아비트리움에 있다.

폴카닷 롤업

폴카닷 롤업은 낙관적 롤업과 유사하게 작동한다. 사기 방지 메커니즘을 갖춘 상호작용 방식이다. 낙관적 롤업과 ZK 롤업이 이더리움으로 보안되는 것처럼, 폴카닷 롤업은 폴카닷 릴레이 체인으로 보안된다. 검사 및 사기 방지 메커니즘은 폴카닷에 기본적으로 구현되어 있다. 콜레이터는 릴레이 체인과의 통신 및 활성 상태를 위해 유효성 증명(PoV) 기능을 통해 데이터를 전달한다는 점에서 시퀀서와 원칙적으로 유사하다.

또한, 폴카닷은 롤업의 상태 비저장 클라이언트 로 작동한다. 즉, 릴레이 체인은 각 파라체인의 전체 상태를 유지하지 않는다. 대신, 콜레이터가 제출한 PoV 블록을 사용하여 상태 전환을 검증한다. 이는 전체 상태 저장 없이 거래 유효성을 증명하는 이더리움 생태계의 블록 증인과 유사하다. 이러한 설계는 상태 유지 관리를 롤업에 위임하는 동시에 암호화 증명을 통한 안전한 검증을 가능하게 하여 확장성을 보장한다.

Polkadot 롤업은 낙관적 롤업과 비교하여 다음과 같은 주요 차이점이 있다.

- 폴카닷은 네이티브 레벨(즉, L2 확장 솔루션을 사용하지 않음)에서 롤업 기능을 구현하여 파라체인 프로토콜을 통해 각 롤업에 대한 보안 및 확장성을 공유한다. 폴카닷은 파라체인에서 L2 롤업과 유사한 집계된 대표 상태로 데이터 조정을 처리한다.
- 낙관적 롤업이 모든 거래가 유효하다는 가정에 기반하는 반면, 폴카닷 롤업은 "냉소적"이며 항상 밸리데이터 하위 집합을 사용하여 거래의 유효성을 확인한다. 분쟁 발생 시, 더 많은 밸리데이터가 참여하는 에스컬레이션 효과가 발생하고, 분쟁 해결은 악의적인 행위자가 삭감 되는 것으로 끝난다.
- 폴카닷은 파라체인 프로토콜(Parachain Protocol) 덕분에 실행 샤딩(execution sharding)이 가능한 여러 개의 가상 코어를 가지고 있다. 롤업은 코어타임(coretime)을 통해 해당 코어의 시간을 예약하여 폴카닷에 접근한다.
폴카닷 롤업과 낙관적 롤업, zk 롤업을 더 자세히 비교한 내용은 아래 비교 표에서 확인할 수 있다.

롤업 비교표

아래는 Polkadot, ZK, Optimistic 롤업의 주요 차이점을 요약한 비교표이다. 다양한 유형의 Optimistic 롤업과 ZK 롤업에 대한 심층적인 비교는 l2beat에서 확인하실 수 있다.

특징	ZK 롤업	낙관적 롤업	폴카닷 파라체인/롤업
최종성	증명이 즉시 제공되므로 최종성은 L1의 최종성에 의해서만 제한된다(예: 이더리움의 경우 약 13분).	사기 방지 메커니즘으로 인해 최종확정이 지연됐다(1주일).	릴레이 체인 합의를 통한 빠른 확정(1분 이내).
보안 모델	암호화 유효성 증명을 사용하여 높은 보안을 보장하고 게임 이론적 가정에 의존하지 않는다.	경제적 인센티브와 사기 적발을 위한 도전 기간에 의존한다. 낙관적인 가정으로 인해 ZK 롤업보다 보안성이 떨어진다.	모든 거래가 밸리데이터 하위 집합에 의해 확인되고, 분쟁이 발생할 경우 단계적으로 확대 및 삭제되는 “방송적” 모델이다.
확장성	단일 상태 머신이기 때문에 확장성이 제한적이며, 검증 머신과 연산 요구 사항에 따라 확장성이 결정된다. 많은 zk-rollup은 엄청난 연산 요구 사항으로 인해 메인넷에서 암호화 사전 컴파일을 비활성화한다.	높은 병렬화가 가능하지만, 이더리움과 같은 L1 체인의 가스 비용으로 제한된다.	네이티브 실행 샤딩과 병렬로 작동하는 파라체인을 통해 본질적으로 확장 가능하다. 파이프라이닝과 코어 스케줄링은 단일 롤업의 처리량과 확장성을 향상시킨다. 실행 샤드는 코어타임을 사용하여 여러 가상 코어를 통해 활성화된다.
상호운용성	제한된 상호 운용성, 종종 호환되는 L1에 국한됨.	상호운용성이 제한적이며 종종 상위 블록체인의 생태계에 국한된다. 제한된 L2 상호운용성	XCM을 통한 네이티브 상호운용성을 통해 서로 다른 목적을 가진 파라체인 간의 원활한 통신이 가능하다. 신뢰할 수 없는 브릿지를 통해 폴카닷과 다른 블록체인과 연결할 수 있다.

용성 비교를 참조
하십시오.

상태 전환 논리	일반 용도이지만 zk-회로 구현의 복잡성에 제약을 받는다.	EVM 환경 내의 다른 가상머신(VM) 논리를 해석하여 EVM 호환성을 넘어서 상태 전환을 지원할 수 있다.	각 파라체인은 Wasm으로 컴파일되고 파라체인 프로토콜 규칙에 따라 검증되는 고유한 상태 전환 함수(STF)를 정의할 수 있다.
개발 복잡성	영지식 증명의 수학으로 인해 복잡하다.	중간 정도의 복잡성으로 사기 방지 구현이 필요하다.	중간에서 높은 수준의 복잡성을 지닌다. 파라체인 런타임은 Wasm 호환 언어로 작성되어야 하지만, 사용자의 로직과 거버넌스를 정의할 수 있다. 파라체인 유지 관리의 오버헤드가 클 수 있다.
데이터 가용성	낙관적 롤업과 ZK 롤업에서 게시된 데이터 가용성 요구 사항은 동일하다.	낙관적 롤업과 ZK 롤업에 게시된 데이터 가용성 요구 사항은 동일하다.	분쟁 발생 시 분산된 상태 저장 및 재구성을 보장하는 검증기를 통해 내장된 데이터 가용성을 제공한다.
비용 효율성	효율성은 높지만 비용이 많이 드는 증명자 계산.	비용 효율성은 높지만 사용량이 많을 때 혼잡해질 수 있다.	파라체인은 독립적으로 확장 가능하며 L1 가스 요금에 구속되지 않음으로 비용 효율적이다.
거버넌스 업그레이드	모회사 체인의 거버넌스에 따른다.	부모 L1 네트워크 거버넌스에 의해 관리된다.	포크리스 업그레이드는 Polkadot의 기본 거버넌스 메커니즘을 통해 지원된다.
사기/유효성 증명	비대화형 유효성 증명을 통해 체인 밖에서도 정확성을 보장한다.	분쟁 기간 동안 적극적인 이의 제기가 필요한 사기 증거.	밸리데이터가 지속적으로 유효성을 검사하여 분쟁을 확대하는 효과를 낳고 악의적인 행위자를 제거하는 방식이다.

응 용 프 로 그 램	금융 거래나 개인정보 보호 애플리케이션 등 보안성이 높은 사용 사례에 이상적이다.	중간 수준의 보안 요구 사항이 있는 일반 용도 dApp에 적합하다.	다양한 블록체인 앱에 적합한 거버넌스, 로직, 사용자 정의 런타임 환경을 정의할 수 있는 본격적인 상태 머신이다.
탈 출 구	탈출구가 내장되어 있지 않다. zk 회로가 제대로 작동해야 한다.	시퀀서가 고장날 경우 자금을 인출할 수 있는 탈출구를 포함할 수 있다.	기본적인 탈출 메커니즘이 없으므로, 파라체인 수집기가 실패하면 자금이 갇힐 수 있다.
허 가	일반적으로 허가된 시퀀서를 사용한다.	시퀀서는 허가를 받거나 부분적으로 허가 없이 사용할 수 있다.	파라체인은 허가형 및 허가 없는 클레임 세트를 지원하여 개인 또는 공공 사용 사례에 대한 유연성을 제공한다.
공 유 보 안	부모 체인의 보안 보장에 의존하여 zk-proofs를 활용한다.	사기 방지 메커니즘을 통해 L1과 보안이 공유된다.	보안은 Parachain Protocol을 통해 Relay Chain과 공유된다.
샤 딩	데이터 샤딩만 가능하다. 실행 샤딩은 이더리움 ZK 롤업에는 적용되지 않음.	데이터 샤딩만 가능하다. 실행 샤딩은 Ethereum Optimistic 롤업에는 적용되지 않는다.	Parachain Protocol을 통해 데이터 분할 및 실행 분할이 가능하며, 여러 개의 가상 코어를 활용하고 폴크 작업을 위해 코어 타임을 예약한다.

1. 롤업 허브 내에서 기본 상호 운용성을 허용하려는 노력이 있다. 예를 들어, OP 스택 생태계 내에서는 독립적인 L2보다 "더 나은" 상호 운용성이 제공된다.
2. 낙관적 롤업은 사기 방지 메커니즘과 분쟁 해결을 위해 이더리움의 EVM(이더리움 가상 머신)에 의존한다. 하지만 EVM은 L2 명령어를 기본적으로 실행하는 대신 롤업 가상 머신의 로직을 해석한다. 낙관적 롤업은 이더리움 및 생태계와의 원활한 통합을 위해 EVM 호환 상태 전환을 지원하는 경우가 많지만, 본질적으로 EVM 로직에만 국한되지는 않는다. 개발자는 Wasm이나 사용자 지정 환경과 같은 다른 가상 머신에 대한 해석 로직을 구현하여 낙관적 롤업이 다양한 연산 프레임워크를 지원할 수 있도록 할 수 있다. 이러한 유연성은 낙관적 롤업의 잠재력을 기존 EVM 기반 경계를 넘어 확장하며, 이더리움의 연산 모델에 엄격하게 종속되어 있다는 인식과는 대조적이다.
3. 탈출구는 롤업 사용자가 운영자(시퀀서)가 오프라인일 때 롤업에서 디지털 자산이나 프로그램 상태를 복구할 수 있는 방법이다.

상호 운용성 비교

이 섹션에서는 Polkadot, Optimism Superchain Ecosystem, Chainlink CCIP(Cross-chain Interoperability Protocol) 간의 상호 운용성의 주요 차이점을 살펴보겠다.

특징	폴카닷 XCM	낙관주의 슈퍼체인 상호 운용성	체인링크 CCIP
아키텍처	통합된 릴레이 체인을 사용하여 Polkadot 생태계 내의 파라체인 간 직접 통신을 구현한다.	이더리움을 기반으로 구축된 코스모롤업 상호 운용성으로 롤업의 호환성이 확장됐다.	모든 블록체인 네트워크에서 크로스체인 통신을 가능하게 하는 범용 표준이다.
범위	폴카닷/쿠사마 생태계의 파라체인과 릴레이 체인으로 제한된다.	Ethereum Layer 2(예: Optimism, Base)의 롤업에 중점을 둔다.	블록체인에 구매받지 않고 공공 및 사설 체인을 지원한다.
합의종속성	Polkadot의 공유 릴레이 체인 합의에 의존한다.	Superchain 롤업 내에서 보안 및 시퀀서 신뢰를 위해 Ethereum Layer 1에 의존한다.	특정 체인의 합의와 관계없이 안전한 메시징을 위해 오라클 네트워크를 사용한다.
상호운용성 모델	메시지는 XCMP 및 HRMP 채널을 사용하여 파라체인 간에 신뢰할 수 없이 전달된다.	롤업은 슈퍼체인의 시퀀서 인프라를 통해 통신한다.	체인링크 분산 오라클을 사용하여 체인 전반에 걸쳐 데이터를 안전하게 전송한다.
확장성	생태계 내에서 확장성이 높지만 릴레이 체인 용량에 의해 제한된다.	이더리움 처리량과 슈퍼체인 아키텍처에 의해 제한됨.	확장 가능, 크로스체인 메시징을 오라클 네트워크로 오프로드한다.
보안 모델	폴카닷의 릴레이 밸리데이터와 스테이크로 보호된다.	이더리움의 기본 계층과 롤업별 사기 방지 또는 유효성 증명으로 보호된다.	Chainlink 오라클과 암호화 증명을 통해 보안이 보장된다.
통합의 용이	기반 기반 파라체인과 폴카닷 프로토콜 준수가 필요하다.	롤업은 Optimism의 OP 스택 아키텍처에 맞춰야 한다.	블록체인에 구매받지 않으며 CCIP 라이브러리를 사용하여 모든 체인과 통합된

성			다.
상호 운용성 속도	Polkadot의 공유 릴레이 체인이 상호작용을 검증하므로 거의 즉각적이다.	레이어 1 이더리움 최종성과 롤업 지연에 따라 종속성으로 인해 상대적으로 느리다.	빠른 속도, 데이터 전송을 위해 Chainlink 오라클 노드를 사용한다.
사용 사례	네이티브 토큰 전송, 계약 실행(Polkadot은 XCM을 통해 스마트 계약 실행을 허용하지만, 암기 접근 없이 간단한 호출만 전달할 수 있으므로 실제로는 신뢰 없이 사용하는 것은 거의 불가능하다.) 및 공유 스테이킹 풀.	롤업 간의 자산과 상태를 연결한다.	크로스체인 DeFi, 게임, 기업 블록체인 커뮤니케이션.
중앙 집중화 경향이 있음	낮음. 폴카닷의 디자인은 분산화를 강제하지만, 수집기 노드 분산화를 허용하지 않더라도 모든 수집기를 운영하는 팀이 있는 체인이 있기 때문에 이를 의무화하지는 않는다.	낙관론은 현재 선택권을 주지 않는다. 시퀀서는 중앙 집중화되어야 한다.	Chainlink 오라클 네트워크의 분산화 수준에 따라 달라진다.
현재 배치	Polkadot과 Kusama 생태계에 적극적으로 배포됐다.	초기 단계이다. 기본 요소가 활성화되어 있으며 OP 스택 롤업과 함께 확장 중이다.	테스트넷과 메인넷 모두에서 여러 체인에 널리 채택됐다.
주요 강점	생태계 내에서 원활하고 지연 시간이 짧은 통신이 가능하다.	상호 운용성은 이더리움 확장성과 레이어 2 도입에 중점을 두었다.	유연한 사용 사례를 갖춘 보편적이고 체인에 구애받지 않는 표준이다.
제한 사항	Polkadot과 호환되는 파라체인으로 제한된다.	OP 스택을 사용하는 Ethereum 및 롤업으로 제한된다.	이는 오라클 네트워크 보안 및 도입률에 따라 달라진다.

쿠사마와의 비교

Polkadot과 Kusama는 사촌처럼 코드의 많은 부분을 공유하지만, 서로 다른 우선순위를 가진 독립적인 네트워크이다. Kusama는 자유롭고 빠르며, 과감한 실험과 초기 단계 배포에 적합하다. Polkadot은 안정성과 신뢰성을 우선시하는 보수적인 네트워크이다. 결국 사촌끼리도 차이점이 있다.

비용과 속도

파라체인을 운영하려는 팀은 토큰을 담보로 예치해야 한다. 쿠사마의 예치 요건은 폴카닷보다 낮아 개발 환경이 더 저렴한다.

폴카닷과 쿠사마의 또 다른 주요 기술적 차이점은 쿠사마가 더 빠른 업그레이드를 가능하게 하는 거버넌스 매개변수를 수정했다는 것이다. 쿠사마는 폴카닷보다 최대 4배 빠르다. 이는 쿠사마 블록체인 자체가 더 빠르다는 것을 의미하지 않는다. 즉, 블록 생성 시간이나 트랜잭션 처리량(두 네트워크 모두 동일)이 더 빠르다는 의미이다. 하지만 새로운 국민투표 제안, 투표, 승인된 업그레이드 시행과 같은 거버넌스 이벤트 간의 간격이 더 짧다는 것을 의미한다. 이러한 차이로 쿠사마는 폴카닷보다 더 빠르게 적응하고 발전할 수 있다.

카나리아 네트워크

Kusama의 초기 사용 사례는 사전 프로덕션 환경, 즉 "카나리아 네트워크"였다.

카나리아는 새의 일종이다. 옛날 석탄 광부들은 터널 내 유독 가스의 양을 측정하기 위해 카나리아를 탄광에 넣었다. 마찬가지로, 카나리아 테스트는 광범위한 사용자에게 피해를 주지 않으면서 제한된 수의 사용자 또는 격리된 환경에 소프트웨어를 배포하여 소프트웨어의 유효성을 검증하는 방법이다.

쿠사마(Kusama)에 배포되는 릴리스는 카나리아 릴리스(Canary Release) 라고 할 수 있다. 이러한 릴리스는 일반적으로 단계적으로 진행된다. 쿠사마 초창기에는 네트워크가 단순히 파라체인 후보들의 혁신과 변화 테스트에만 사용되는 것이 아니라, 폴카닷(Polkadot)의 샤딩 모델에 대한 개념 증명(PoC)에도 사용될 것이다.

쿠사마는 단순한 테스트넷이 아니다. 블록체인은 경제적 가치와 자체 거버넌스를 갖추고 완벽하게 작동한다. 쿠사마의 미래는 참여자들의 손에 달려 있다. 일반적인 블록체인 개발 파이프라인에서 쿠사마는 "테스트넷"과 "메인넷" 사이에 위치한다.

!!!info 테스트넷 → Kusama → Polkadot

상상할 수 있듯이 Kusama를 기반으로 구축하면 팀은 Polkadot보다 문제나 버그가 발생할 경우 위험이 적고 실제 조건과 완전히 분산되고 커뮤니티가 제어하는 라이브 네트워크에서 테스트를 진행할 수 있다.

많은 프로젝트가 두 네트워크 모두에서 파라체인을 유지하며, 새로운 기술과 기능을 쿠사마에서 실험하고 테스트한 후 폴카닷에 배포할 것이다. 일부 팀은 쿠사마에만 머무르기로 결정할 것이며, 쿠사마는 앞으로 새로운 기술을 활용한 흥미로운 실험이 진행될 가능성이 높다. 게임, 소셜 네트워킹, 콘텐츠 배포 애플리케이션처럼 높은 처리량을 요구하지만 은행 수준의 보안은 필요하지 않은 프로젝트가 이러한 사용 사례에 특히 적합하다.

쿠사마는 거버넌스, 인센티브, 통화 정책, DAO(탈중앙화 자율 조직)와 같은 분야에서 새로운 아이디어와 혁신을 야심차게 실험하기에 완벽한 환경이 될 수 있다. 폴카닷 런타임에 대한 향후 업그레이드 또한 폴카닷 메인넷보다 먼저 쿠사마에 배포될 가능성이 높다. 이를 통해 새로운 기술과 기능들이 폴카닷에 적용되기 전에 실제 환경에서 어떻게 작동하는지 확인할 수 있을 뿐만 아니라, 두 네트워크에 모두 배포한 팀도 업그레이드 후 자사 기술이 어떻게 작동하는지 미리 살펴볼 수 있다.

앞으로 나아가기

궁극적으로 쿠사마와 폴카닷은 자체 커뮤니티, 자체 거버넌스, 그리고 상호 보완적인 사용 사례를 갖춘 독립적인 네트워크이다. 하지만 앞으로도 긴밀한 관계를 유지할 것이며, 많은 팀이 두 네트워크 모두에 애플리케이션을 배포할 가능성이 높다. Web3 Foundation은 앞으로도 두 네트워크에 전념하며 생태계 구축을 위한 팀들에게 중요한 지원과 지침을 제공할 것이다.

이더리움과의 비교

두 프로토콜 모두 핵심적으로 블록체인이지만 활용 방식에 있어서 근본적으로 다른 역할을 수행한다.

이더리움은 스마트 컨트랙트 실행 환경인 이더리움 가상 머신을 호스팅하는 범용 블록체인이다. 이더리움은 동질적이지만 롤업 및 레이어 2 솔루션을 활용하여 사용 범위를 확장할 수 있다.

폴카닷은 여러 개의 레이어 1 블록체인을 호스팅하고 공유 보안에 참여할 수 있도록 하는 이기종 멀티체인 프로토콜("레이어 0" 또는 메타프로토콜)이다. 폴카닷은 여러 프로토콜이 공존하고 함께 작동할 수 있도록 하는 메타 프로토콜 역할을 한다.

샤딩

블록체인의 맥락에서 "샤딩" 또는 "샤딩 프로토콜"이라는 용어는 일반적으로 하위 프로토콜을 지칭하는 데 사용되거나 수평적 확장의 한 형태를 지칭하는 일반 용어로 사용된다.

상위 수준 비교

두 프로토콜은 근본적으로 다른 목표를 가지고 있다.

이더리움은 이더리움 가상 머신(EVM)을 기반으로 하는 범용 블록체인이다. 이더리움은 특정 애플리케이션에 특화되거나 최적화되지 않았다. 대신, 스마트 계약을 실행하기 위한 이더리움 가상 머신에 주력한다. 이더리움은 이더리움을 결제 계층으로 활용하는 보조 프로토콜인 롤업을 통해 확장성을 확보한다.

폴카닷은 각 파라체인에 공유 보안과 안전한 상호운용성을 제공하는 멀티체인 프로토콜이다. 각 파라체인(여기서는 "앱체인"이라고도 함)은 특정 목표에 특화되어 있으며, 해당 목표에 맞춰 최적화되어 있다. 파라체인은 파라체인 프로토콜을 준수해야 한다.

폴카닷의 주요 목적은 프로토콜의 유효성을 검사하는 것이지만, 스마트 컨트랙트 배포도 지원한다. 또한, 여러 파라체인(parachain)이 스마트 컨트랙트 기능을 제공한다. 폴카닷의 파라체인은 서브스트레이트의 이더리움 호환 계층인 Frontier를 사용하여 솔리디티로 작성된 스마트 컨트랙트를 실행하는 EVM을 실행할 수도 있다.

간단히 요약하자면, 폴카닷은 파라체인 프로토콜 (낙관적 롤업과 유사) 을 따르는 하위 프로토콜들을 조정 하고 검증한다고 할 수 있다. 반면, 이더리움은 EVM의 입력과 출력을 조정한다. 폴카닷에서는 모든 하위 프로토콜이 웹어셈블리로 컴파일되는 한 자체 로직을 가질 수 있다.

확장성 접근 방식

이더리움은 트랜잭션 처리량 확장을 위해 롤업 중심 접근 방식을 선호한다. Danksharding 은 롤업을 위한 더 나은 유틸리티(예: 프로토- Danksharding을 통한 데이터 가용성)를 제공하여 롤업이 이더리움에 상태를 기록할 수 있도록 함으로써 롤업 활동을 더 잘 수용하고 촉진하는 방식이다.

Danksharding(Danksharding)은 이더리움에서 블록당 훨씬 더 많은 공간을 활용할 수 있게 해 주며, 네트워크에서 삭제되기 전에 일정 시간 동안 데이터 블록을 검증할 수 있게 된다. 이러한 접근 방식은 1계층에서의 데이터 가용성을 높이고, 이더리움에서 2계층 프로토콜의 활성화를 더욱 촉진할 것이다.

반면, 릴레이 체인은 파라 체인 프로토콜(Parachains Protocol)에 따라 파라체인(parachain)이 스스로 등록해야 한다. 등록이 완료되면 릴레이 체인은 파라체인 검증 함수(PVF)에 따라 각 파라체인의 상태 변화를 검증한다. 데이터 가용성은 파라체인 상태 검증에 필수적인 요소이다. 이러한 접근 방식은 파라체인 간의 병렬화된 상호작용을 가능하게 한다. 폴카닷(Polkadot)이 공동으로 검증했기 때문에 각 하위 프로토콜의 상태가 유효함을 신뢰할 수 있다.

롤업 vs. 파라체인 생성

이더리움은 주로 롤업을 최적화하는 데 중점을 두고 있다. 폴카닷의 파라체인 프로토콜을 사용하면 2계층 솔루션이 필요 없이 프로토콜 수준에서 검증이 가능하다.

각 파라체인은 런타임 (상태 전이 함수 라고도 함) 이라는 자체 핵심 로직을 호스팅한다. 폴카닷은 웹어셈블리(Wasm)를 "메타 프로토콜"로 사용한다.

파라체인은 크로스 합의 메시징(XCM)을 사용하여 서로 통신하고 체인 간 반응을 촉진할 수 있다. XCM은 특정 네트워크의 상태 전환을 설명하는 단순한 형식이므로 이더리움에서도 XCM을 활용할 수 있다.

아키텍처 차이점: 폴카닷과 이더리움

앞서 언급했듯이, 이더리움은 솔리디티로 작성된 샌드박스 프로그램을 실행할 수 있는 범용 가상 머신인 반면, 폴카닷은 다른 파라체인이 서로 연결하고 상호작용할 수 있는 메타 프로토콜이다.

이더리움은 단일의 동질 체인으로 작동한다. 각 이더리움 노드는 합의 계층과 실행 계층이라는 두 개의 계층으로 나뉜다. 각 계층은 이더리움 클라이언트의 블록 검증 정보, 피어 검색, 그리고 지분증명(PoS)을 처리한다.

폴카닷의 주요 구성 요소는 다양한 파라체인(parachain)을 호스팅하는 릴레이 체인(relay chain)이다. 릴레이 체인은 각 파라체인에서 정보를 수집하며, 밸리데이터들은 이를 통해 합의와 완결성에 동의한다. 폴카닷은 파라체인과 폴카닷 자체를 설명하는 데 사용되는 상태 전이 함수인 일련의 런타임 으로 볼 수 있다.

포크, 업그레이드 및 거버넌스

이더리움의 거버넌스는 오프체인 방식으로 이루어지며, 다양한 이해관계자들이 프로토콜 자체가 아닌 다른 매체를 통해 합의에 도달한다. 이더리움의 업그레이드는 표준 하드포크 절차를 따르며, 커뮤니티와 검증인들이 프로토콜 변경 사항을 구현하기 위해 노드를 업그레이드하도록 조율한다.

폴카닷은 런타임 업그레이드를 용이하게 하기 위해 오픈거브(OpenGov)라는 온체인 거버넌스를 사용한다. 폴카닷 이해관계자들은 이러한 업그레이드에 투표하며, 성공하면 업그레이드가 이후 블록에 자동으로 적용된다. 폴카닷 밸리데이터 운영자는 클라이언트 자체가 업데이트될 때만 노드를 업그레이드한다.

이 메커니즘 덕분에 릴레이 체인은 하드 포크 없이 Wasm 메타 프로토콜을 사용하여 업그레이드를 실행할 수 있다. Polkadot(및 모든 후속 파라체인)의 WebAssembly 런타임은 온체인에 저장되므로, 거버넌스에서 업그레이드 실행을 허용하면 런타임을 새로운 WebAssembly 블록으로 간단히 교체하면 된다.

상태 전환 함수, 트랜잭션 대기열 또는 오프체인 워커 내의 모든 항목은 체인을 포크하지 않고도 업그레이드할 수 있다. 이러한 항목은 모두 WebAssembly 런타임의 일부이기 때문이다.

블록 생산 및 마무리

이더리움과 폴카닷은 모두 블록 생성과 최종성이 분리된 하이브리드 합의 모델을 사용한다.

마무리를 위해 이더리움은 Casper FFG를 활용하는데, 이는 마무리를 위한 포크 선택 규칙으로 LMD-GHOST와 함께 작동한다.

폴카닷은 GRANDPA를 최종 확정에 활용한다. GRANDPA는 블록 단위로 결정하는 대신, 블록 체인을 최종 확정할 수 있다. 두 최종 확정 메커니즘 모두 GHOST 기반이며, 한 라운드에서 여러 블록을 최종 확정할 수 있다.

블록 생성을 위해 두 프로토콜 모두 슬롯 기반 프로토콜을 사용하여 밸리데이터를 슬롯에 무작위로 할당하고, 미완료 블록에 대한 포크 선택 규칙을 제공한다. 폴카닷은 블록 생성에 BABE를 사용한다. BABE는 블록 생성자를 선택하는 두 가지 메커니즘을 포함하는데, 그중 하나는 첫 번째 블록 생성자가 실패할 경우를 대비한 대체 메커니즘으로, 체인의 활성 상태를 유지한다. BABE는 GRANDPA가 이미 완료한 체인 위에 미완료 블록을 생성한다.

이더리움과 폴카닷 컨센서스 사이에는 두 가지 주요 차이점이 있다.

1. 폴카닷(Polkadot)의 최종성 프로토콜인 GRANDPA는 제안된 체인이 성장함에 따라 발생하는 가용성 및 유효성 검사를 기반으로 블록 배치를 최종적으로 확정한다. 최종성 확보에 걸리는 시간은 수행해야 하는 검사 횟수(및 추가 검사를 유발하는 무효성 보고서)에 따라 달라진다. 최종성 확보에 걸리는 예상 시간은 30초이다.
2. 이더리움은 일반적으로 라운드당(이더리움에서는 에포크라고 함) 여러 밸리데이터를 통해 강력한 유효성 보장을 제공하는 반면, 폴카닷은 라운드당 밸리데이터 수가 적으면서도 더 강력한 유효성 보장을 제공한다. 폴카닷은 밸리데이터가 시스템의 모든 밸리데이터에게 이 레이저 코딩을 배포하도록 하여, 라운드의 밸리데이터뿐만 아니라 누구나 파라체인 블록을 재구성하고 유효성을 검증할 수 있도록 한다. 이러한 데이터 가용성은 폴카닷의 핵심 요소로, 상태 전환 시 상태의 유효성을 보장한다. 무작위 파라체인 밸리데이터 할당 및 2차 검사는 무작위로 선택된 밸리데이터에 의해 수행되므로 각 파라체인에

속한 소수의 밸리데이터가 공모할 가능성이 줄어든다.

스테이킹 메커니즘: 이더리움 PoS vs. 폴카닷 NPoS

폴카닷은 지명 지분 증명(NPoS) 방식을 사용하여 소규모 검증인 그룹에서 검증인을 선정한다. 이를 통해 소규모 보유자는 노드를 운영하지 않고도 시스템 보상을 획득하면서 네트워크를 운영할 검증인을 지명할 수 있다. 폴카닷은 네트워크의 각 파라체인마다 약 5명의 검증인이 필요하다. 자세한 내용은 스테이킹 페이지를 참조하세요.

이더리움은 지분증명(PoS) 네트워크로, 각 밸리데이터 인스턴스에 32 ETH를 스테이킹해야 한다. 밸리데이터는 기본 비콘 체인 노드와 여러 밸리데이터 클라이언트(각 32 ETH당 하나씩)를 운영한다. 이러한 밸리데이터는 네트워크의 블록을 검증하기 위해 무작위로 선정된 그룹인 "위원회"에 배정된다.

상호 운용성 및 메시지 전달

폴카닷은 파라체인 간 임의의 메시지를 전송하기 위해 크로스 컨센서스 메시징(XCM)을 사용한다. 파라체인은 서로 연결을 맺고 설정된 채널을 통해 메시지를 전송할 수 있다. 콜레이터(collator)가 릴레이 체인과 직접 통신하기 때문에, 콜레이터는 서로 연결되고 필요한 경우 이러한 메시지 전달 채널을 통해 파라체인 A에서 파라체인 B로 메시지를 전달할 수 있다(HRMP, VMP 및 XCM을 위한 기타 메시지 전달 메커니즘 참조).

메시지는 릴레이 체인을 통과하지 않는다. 유효성 증명과 채널 연산(열기, 닫기 등)만 릴레이 체인을 통과한다. 이는 데이터를 시스템 경계에 유지함으로써 확장성을 향상시킨다.

현재 이더리움 롤업은 공유 시퀀서를 사용하여 통신할 수 있으며, 이를 통해 2계층 솔루션 간의 공통된 상호 운용성 기반을 제공한다.

폴카닷은 협정(Accord)이라는 개념을 다양한 프로토콜이 참여할 수 있는 옵트인(opt-in) 조약으로 도입할 계획이다. 협정은 상호운용성에 대한 논리가 일관되게 유지되고 참여 프로토콜에 의해 변경되거나 훼손될 수 없도록 보장한다. 이를 통해 모든 XCM 메시지가 완전히 신뢰할 수 없는 환경에서 대상 프로토콜에서 필요에 따라 올바르게 해석되고 실행될 수 있도록 보장한다.

SPREE(Shared Protected Runtime Execution Enclaves)는 교차 합의 메시지에 대한 공유 논리를 제공하는 메커니즘이며, Accord를 구성하는 데 사용된다.

DApp 지원 및 개발

이더리움은 솔리디티를 활용한 스마트 컨트랙트 개발을 지원한다. 이러한 컨트랙트는 변경 불가능하며, 온체인에 게시된 후에는 변경할 수 없다.

폴카닷은 패러체인(parachain)을 통해 스마트 컨트랙트를 지원하며, 일반적으로 ink! 스마트 컨트랙트 언어를 사용한다. 또한, 프론티어 기반 패러체인을 통해 솔리디티를 지원한다. 이더리움에서는 스마트 컨트랙트가 서로를 호출할 수 있지만, 이더리움 도메인에 온체인으로 고정되어 있다. 폴카닷에서는 스마트 컨트랙트가 동일한 패러체인과 여러 패러체인에서 서로를 호출할 수 있다.

폴카닷에서 개발자는 스마트 컨트랙트를 사용하거나, 팔레트에서 특정 방식으로 체인 상태를 수정하는 외부 함수를 호출하거나, 폴카닷의 RPC를 사용하여 체인 내 정보를 직접 검색하고 처리할 수 있다. 폴카닷의 DApp은 종종 이러한 여러 구성 요소로 구성되어 상태 변경 사항을 실시간으로 수정, 검색하고 모니터링한다.

Polkadot에서 빌드하는 방법에 대한 보다 포괄적인 목록을 보려면 메인 웹사이트의 빌드 섹션을 확인하세요.

결론

이더리움과 폴카닷은 모두 샤딩 모델을 사용한다. Danksharding은 데이터 가용성에 중점을 둔 롤업 중심 접근 방식을 활용할 계획이다. 폴카닷 생태계는 "릴레이 체인"이라는 메인 체인으로 보호된다. 릴레이 체인은 코어를 관리하고, 파라체인과 같은 작업이 코어 위에서 실행되고 코어 간에 메시지가 전송될 수 있도록 한다.

두 프로토콜의 주요 차이점은 다음과 같다.

- 이더리움은 롤업이나 메인넷 자체를 통해 EVM 호환 상태 전환을 처리하는 반면, 폴카닷은 파라체인에서 추상적인 상태 전환 함수 구현을 허용한다.
- 이더리움의 거버넌스 프로세스는 오프체인으로 계획되어 있으므로 하드포크를 통해 거버넌스 결정을 내리기 위한 조정이 필요하다. 반면, 폴카닷의 거버넌스 결정은 온체인으로 진행되며 포크리스 업그레이드를 통해 자율적으로 실행된다.
- 밸리데이터 선택 메커니즘은 Polkadot이 프로토콜당 밸리데이터가 적더라도 강력한 가용성과 유효성 보장을 제공할 수 있기 때문에 다르다.

코스모스와의 비교

폴카닷과 코스모스는 서로 다른 상태 머신이 서로 통신할 수 있는 인터페이스를 제공하는 프로토콜이다. 두 프로토콜 모두 미래에는 개별 블록체인이 고립되어 존재하는 것이 아니라, 서로 상호 운용되어야 하는 여러 블록체인이 존재할 것이라는 가정에 기반한다.

모델

폴카닷은 프로토콜의 각 샤드가 추상적인 상태 전이 함수(STF)를 갖는 샤드 모델을 사용한다. 폴카닷은 웹어셈블리(Wasm)를 "메타 프로토콜"로 사용한다. 폴카닷의 밸리데이터가 Wasm 환경에서 실행할 수 있는 한, 샤드의 STF는 추상적일 수 있다.

폴카닷의 샤드는 "파라체인"이라고 한다. 파라체인은 상태 전환을 수행할 때마다 폴카닷 밸리데이터가 독립적으로 검증할 수 있는 상태 증명과 함께 블록(상태 전환 배치)을 제출한다. 이러한 블록은 시스템의 메인체인인 폴카닷 릴레이 체인에 의해 최종 확정될 때 파라체인에 대해 최종 확정된다. 따라서 모든 파라체인은 전체 시스템과 상태를 공유한다. 즉, 단일 파라체인의 체인 재구성은 모든 파라체인과 릴레이 체인의 재구성을 필요로 한다.

코스모스는 앱 체인을 사용하여 수평적 확장성을 구현한다. 코스모스 네트워크는 코스모스 허브, 오스모시스, 셀레스티아, dYdX v4 체인, 인젝티브 등을 포함하여 100개 이상의 IBC 연결 체인으로 구성된다. 각 체인은 충분히 스테이킹되고 탈중앙화된 검증인 세트를 통해 체인 보안을 담당한다. 또한, 체인은 코스모스 허브의 공유 보안을 활용할 수도 있다. 코스모스 체인은 블록체인 간 통신(IBC) 프로토콜을 사용하여 크로스체인 메시지를 전송한다. 체인은 상태를 공유하지 않으므로, 한 체인을 재구성하더라도 다른 체인은 재구성되지 않는다. 즉, 각 메시지는 수신자가 발신자의 보안에 대한 신뢰에 따라 신뢰 바인딩된다.

아키텍처

폴카닷

폴카닷은 시스템의 메인 체인 역할을 하는 릴레이 체인을 가지고 있다. 폴카닷의 모든 밸리데이터는 릴레이 체인에 속한다. 파라체인에는 밸리데이터에게 파라체인 블록을 생성하고 제안하는 콜레이터(collator)가 있다. 콜레이터는 보안 책임이 없으므로 강력한 인센티브 시스템이 필요하지 않다. 콜레이터는 6초마다 모든 릴레이 체인 블록에 대해 하나의 파라체인 블록을 제출할 수 있다. 파라체인이 블록을 제출하면, 밸리데이터는 최종 체인에 블록을 커밋하기 전에 일련의 가용성 및 유효성 검사를 수행한다.

파라체인은 코어를 통해 릴레이 체인에 접근할 수 있다. 릴레이 체인 코어는 제한되어 있지만, 파라체인은 코어타임을 대량 구매(전체 코어 예약)하거나, 필요에 따라 구매(코어를 다른 체인과 연동)하여 필요할 때만 블록을 실행하는 데 비용을 지불하는 방식으로 사용할 수 있다.

Polkadot은 최종화 프로세스(예: 비트코인)를 사용하려는 체인과 상호 작용하기 위해 양방향 호환성을 제공하는 브릿지를 갖추고 있다.

코스모스

코스모스는 CometBFT를 합의 엔진으로, Cosmos SDK를 VM으로, 그리고 체인 간의 상호 운용을 가능하게 하는 IBC를 사용하여 구축된 블록체인 네트워크이다.

IBC는 상대방 체인의 합의를 추적할 수 있는 라이트 클라이언트를 활용한다. 예를 들어, 체인 A와 B가 서로 통신하려고 할 때, 체인 A는 체인 B의 라이트 클라이언트를 사용하여 체인 B에서 전송된 메시지를 검증하고, 그 반대의 경우도 마찬가지이다.

컨센서스

폴카닷은 BABE와 GRANDPA라는 두 가지 하위 프로토콜을 사용하는 하이브리드 합의 프로토콜을 사용한다. BABE (Blind Assignment for Blockchain Extension)는 검증 가능 난수 함수(VRF)를 사용하여 밸리데이터에게 슬롯을 할당하고, 대체 라운드 로빈 패턴을 사용하여 각 슬롯에 작성자가 있는지 확인한다. GRANDPA (GHOST 기반 재귀 조상 도출 접두사 합의)는 개별 블록이 아닌 체인에 대해 투표한다. BABE는 최종 체인을 확장하기 위한 후보 블록을 작성하고, GRANDPA는 이를 일괄적으로(한 번에 최대 수백만 개의 블록까지) 최종화할 수 있다.

이러한 작업 분리는 여러 가지 이점을 제공한다. 첫째, 블록 생성 및 완료 시 전송 복잡도가 감소한다. BABE는 선형 복잡도를 가지므로 낮은 네트워킹 오버헤드로 수천 개의 블록 생성자로 쉽게 확장할 수 있다. GRANDPA는 이차 복잡도를 가지지만 지연 시간 측면에서 유리하다. 한 번에 여러 블록을 완료할 수 있다.

둘째, 최종화되지 않은 블록으로 체인을 확장할 수 있는 기능을 갖추면 네트워크의 활성 상태를 유지하고 밸리데이터가 광범위한 가용성 및 유효성 검사를 수행하여 잘못된 상태 전환이 최종 체인에 유입되지 않도록 보장할 수 있다.

코스모스 체인은 즉각적인 완결성을 제공하는 라운드 로빈 프로토콜인 텐더민트 합의 알고리즘을 사용한다. 블록 생성과 완결은 알고리즘의 동일한 경로에 있으므로, 한 번에 한 블록씩 생성하고 완결한다. GRANDPA와 같은 PBFT 기반 알고리즘이기 때문에 이차 복잡도를 가지며, 한 번에 한 블록씩 완결하도록 설계됐다.

스테이킹 메커니즘

폴카닷은 순차적 Phragmén 알고리즘을 사용하여 지명 지분 증명(NPoS)을 통해 밸리데이터를 선정한다. 밸리데이터 그룹 규모는 거버넌스에 의해 결정되며(1,000명의 밸리데이터 예정), 밸리데이터 인프라 운영을 원하지 않는 스테이커는 최대 16명의 밸리데이터를 지명할 수 있다. Phragmén 알고리즘은 최적의 지분 배분을 선택하며, 최적의 지분 배분은 가장 균등하게 지분을 보유한 그룹을 기준으로 한다.

폴카닷의 모든 밸리데이터는 합의 프로토콜에서 동일한 가중치를 갖는다. 즉, 특정 체인에 대한 지지율 $\frac{2}{3}$ 이상을 달성하려면 지분 $\frac{2}{3}$ 가 아닌, 검증자의 $\frac{2}{3}$ 이상이 참여해야 한다. 마찬가지로, 밸리데이터 보상은 지분량이 아닌 활동량, 주로 블록 생성 및 완결성 검증에 따라 결정된다. 이는 지분이 낮은 밸리데이터를 추천하는 유인을 제공하는데, 이는 스테이킹된 토큰에 대해 더 높은 수익을 얻을 수 있기 때문이다.

코스모스 허브는 위임 지분 증명(Delegated PoS)의 변형인 담보 지분 증명(Bonded Proof of Stake)을 사용하여 검증인을 선출한다. 스테이커는 자금을 담보로 제공하고, 위임하려는 각 검증인에 대해 위임할 토큰 수와 함께 위임 트랜잭션을 제출해야 한다. 코스모스 허브는 최대 300명의 검증인을 지원할 계획이다.

코스모스에서는 합의 투표와 보상 모두 지분 기반으로 진행된다. 합의 투표의 경우, 검증자의 $\frac{2}{3}$ 가 아닌 지분의 $\frac{2}{3}$ 이상이 참여해야 한다. 마찬가지로, 총 지분의 10%를 보유한 밸리데이터는 보상의 10%를 받게 된다.

마지막으로, 코스모스에서는 스테이커가 거버넌스 투표에 참여하지 않으면 밸리데이터가 투표권을 행사한다. 이로 인해 코스모스의 많은 밸리데이터는 프로토콜에 대한 통제력을 강화하기 위해 수수료를 받지 않는다. 폴카닷에서는 거버넌스와 스테이킹이 완전히 분리되어 있다. 밸리데이터를 지명하더라도 밸리데이터에게 거버넌스 투표권이 부여되지 않는다.

메시지 전달

폴카닷은 파라체인(parachain) 간 임의의 메시지를 전송하기 위해 교차 합의 메시지 전달 형식(XCM)을 사용한다. 파라체인은 서로 연결을 맺고 설정된 채널을 통해 메시지를 전송할 수 있다. 콜레이터(collator)는 파라체인의 전체 노드이자 릴레이 체인의 전체 노드이므로, 콜레이터 노드는 메시지 전달의 핵심 구성 요소이다. 메시지는 릴레이 체인을 통과하지 않으며, 게시 및 채널 작업(열기, 닫기 등)에 대한 증명만 릴레이 체인으로 전달된다. 이는 데이터를 시스템 경계에 유지함으로써 확장성을 향상시킨다.

체인 재구성의 경우, 릴레이 체인의 게시물 증명을 기반으로 메시지를 재구성 시점으로 롤백할 수 있다. 파라체인 간의 공유 상태는 메시지가 신뢰 한계로부터 자유롭다는 것을 의미하며, 모든 메시지는 동일한 맥락에서 작동한다.

폴카닷에는 크로스 체인 메시지에 대한 공유 로직을 제공하는 SPREE 라는 추가 프로토콜이 있다. SPREE 를 통해 전송된 메시지는 수신 체인의 출처 및 해석에 대한 추가적인 보장을 제공한다.

코스모스는 임의 메시지 전달을 위해 블록체인 간 통신(IBC) 이라는 가벼운 클라이언트 기반 크로스 체인 프로토콜을 사용한다. 현재 설계에서 IBC 체인은 서로 1:1 연결을 생성하며, 이를 통해 채널을 설정할 수 있다. IBC 데이터 패킷은 이러한 채널을 통해 서로 다른 체인에 있는 애플리케이션 모듈 간에 전송된다. IBC의 경우, 체인 간에 상태를 공유하지 않으므로 수신 체인은 메시지 출처의 보안을 신뢰해야 한다.

거버넌스

폴카닷은 여러 경로를 통해 제안을 공개 국민투표로 통과시키는 OpenGov 프레임워크를 보유하고 있으며, 대부분의 토큰이 항상 결과를 통제할 수 있다. 국민투표에는 온체인 재무부 의 자금 배분을 포함한 다양한 제안이 포함될 수 있다. 결정은 온체인에서 실행되며 구속력과 자율성을 갖는다.

코스모스는 코인 투표 신호를 사용하여 국민투표를 통과시킨다. 거버넌스 결정의 실제 시행은 다른 블록체인과 마찬가지로 프로토콜 포크를 통해 이루어진다. 모든 토큰 보유자는 투표할 수 있지만, 위임자가 투표에서 기권하면 위임받은 밸리데이터가 투표권을 행사하게 된다. 폴카닷의 밸리데이터는 노미네이터에 따라 투표권을 부여받지 않는다.

업그레이드

Polkadot은 Wasm 메타 프로토콜을 사용하여 하드 포크 없이 체인 업그레이드 및 성공적인 제안을 실행할 수 있다. STF, 트랜잭션 큐 또는 오프체인 워커 내에 있는 모든 것은 체인을 포크하지 않고도 업그레이드할 수 있다.

코스모스는 메타 프로토콜을 기반으로 하지 않기 때문에 일반적인 포킹 메커니즘을 통해 업그레이드와 제안을 시행해야 한다.

개발 프레임워크

코스모스와 폴카닷은 각 체인이 자체 STF를 가지도록 설계되었으며, Wasm과 이더리움 가상 머신(EVM) 모두에서 스마트 계약을 지원한다. 폴카닷은 사전 Wasm 컴파일러와 실행을 위한 인터프리터(Wasmi)를 제공하는 반면, 코스모스는 인터프리터에서만 스마트 계약을 실행한다.

코스모스 체인은 Go 언어로 작성된 코스모스 SDK를 사용하여 개발할 수 있다. 코스모스 SDK에는 체인의 STF(스테이킹, 거버넌스 등)에 포함될 수 있는 약 10개의 모듈이 포함되어 있다. 이 SDK는 텐더민트(Tendermint)를 기반으로 구축된다.

파라체인의 주요 개발 프레임워크는 Rust로 작성된 서브스트레이트이다. 서브스트레이트에는 체인의 STF(Simple Functional Framework)에서 사용할 수 있는 약 40개의 모듈("팔레트")로 구성된 FRAME이 포함되어 있다. 서브스트레이트는 단순히 팔레트를 사용하는 것 외에도, 개발자가 사용자 지정 모듈을 추가하고 체인의 매개변수와 초기 저장 값을 구성하여 FRAME의 팔레트를 구성할 수 있도록 하는 추가적인 추상화 계층을 제공한다.

결론

폴카닷은 확장성과 상호운용성을 위해 신뢰 없는 환경을 조성하기 위해 공유 검증 로직이 필요하다는 원칙에 따라 설계됐다. 더 많은 블록체인이 개발됨에 따라, 보안은 경쟁적인 것이 아니라 협력적인 것이 되어야 한다. 따라서 폴카닷은 여러 체인에서 공유 검증 로직과 보안 프로세스를 제공하여, 상호 작용 시 상대방이 동일한 보안 컨텍스트 내에서 실행된다는 것을 인지하고 상호 작용할 수 있도록 한다.

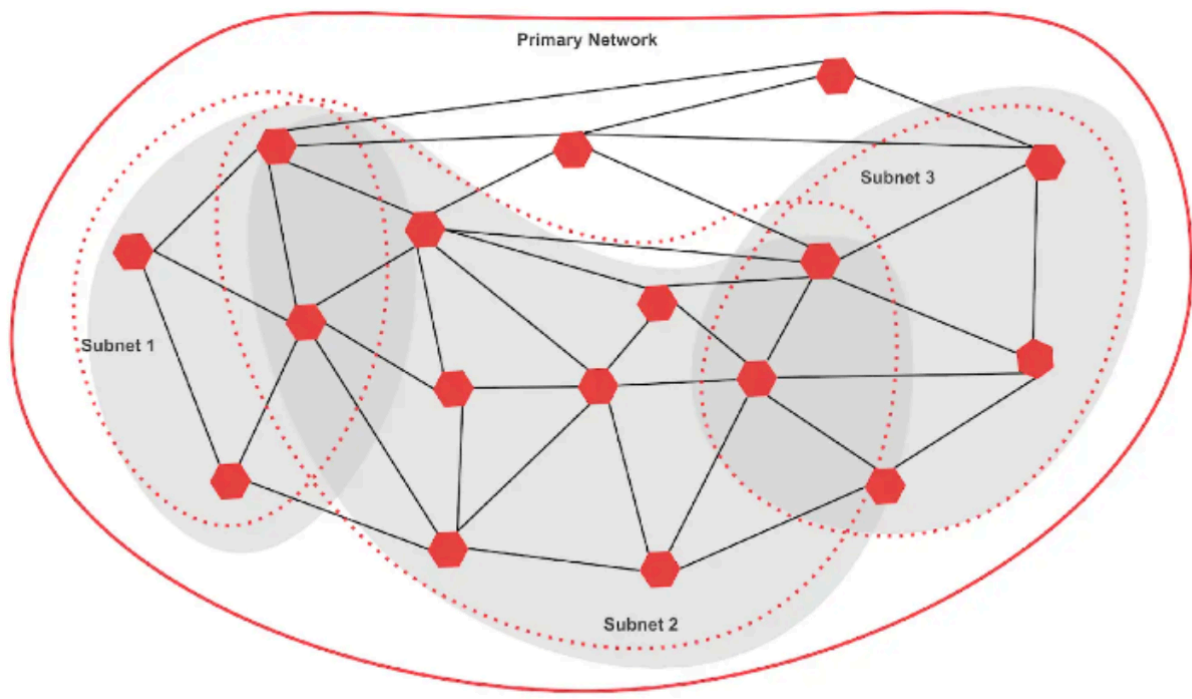
코스모스 네트워크는 IBC를 사용하여 독립적인 보안 보장을 통해 체인을 연결하는 인터넷과 유사한 비정형 네트워크를 사용한다. 즉, 데이터가 한 체인에서 다른 체인으로 전송될 때 수신 체인은 송신 체인을 신뢰해야 한다. 따라서 코스모스 네트워크의 각 블록체인은 독립적인 보안 메커니즘을 갖는다. 또한 체인은 코스모스 허브와 보안을 공유하여 경제적 보안을 활용할 수 있다.

아발란체와의 비교

폴카닷과 아발란체 모두 애플리케이션별 블록체인이 공개적으로 사용 가능한 상태 검증을 위해 기본 네트워크에 연결할 수 있도록 하는 아키텍처를 가지고 있다. 폴카닷의 기본 네트워크는 릴레이 체인인 반면, 아발란체는 P-체인, X-체인, C-체인이라는 세 개의 메인 체인을 사용하며, 이를 통칭하여 "기본 체인"이라고 한다. 폴카닷의 파라체인 및 롤업과 유사하게, 아발란체는 서브넷을 사용한다. 두 네트워크 모두 밸리데이터가 네트워크 보안을 위해 토큰을 스테이킹하는 PoS 메커니즘을 채택하고 있다.

아키텍처

Avalanche의 아키텍처는 각 체인의 역할을 세 가지 체인으로 분리하여 밸리데이터, 거래, 스마트 컨트랙트 실행에 대한 고유한 역할을 부여한다. X-체인은 비선형 DAG(Directed Acyclic Graph) 구조를 사용하는 반면, Polkadot은 비트코인 및 이더리움과 유사한 선형 체인 구조를 사용한다.



이미지 출처: Avalanche docs.

폴카닷의 스마트 계약은 파라체인에서 구현된다. 아발란체의 기본 네트워크는 세 개의 블록체인으로 나뉜다.

P-체인(플랫폼)

- 밸리데이터 세트를 유지 관리하고 네트워크를 보호한다.
- 스테이킹 작업과 Avalanche L1을 지원한다.
- 위임 지분 증명(DPoS)을 사용하여 토큰 보유자가 밸리데이터에게 지분을 위임할 수 있다.

X-체인(거래소)

- UTXO 모델(비트코인과 유사)을 사용하여 거래 계층을 처리한다.
- 빠른 거래 처리를 위해 DAG 구조를 구현한다.
- 스마트 계약 실행을 지원하지 않는다.

C-체인(계약)

- EVM 호환 스마트 계약을 지원한다.
- Avalanche에 특화된 네트워킹과 컨센서스를 갖춘 go-ethereum의 포크인 Coreth VM을 실행한다.
- 스마트 계약 실행을 위한 높은 활동에 중점을 둔다.

서브넷

Avalanche는 서브넷을 블록체인 집합에서 합의를 이루는 동적 밸리데이터 집합으로 정의한다. Polkadot 용어로, 서브넷은 Polkadot 릴레이 체인에서 사용 가능한 컴퓨팅 자원을 활용하는 파라체인(롤업)과 유사하다. 서브넷을 통해 밸리데이터는 특정 런타임을 검증할 수 있으며, 이를 통해 거래 수수료 모델, 토큰 경제학 및 사용자 지정 규칙에 유연성을 제공한다. 밸리데이터는 하나 이상의 서브넷을 검증하여 전체 밸리데이터 집합의 하위 집합을 형성할 수 있다.

가상 머신

Avalanche는 상태 전환, 트랜잭션 규칙, API 인터페이스 등 블록체인 동작을 정의하기 위한 청사진으로 가상 머신(VM)을 사용한다. 개발자는 동일한 VM을 사용하여 동일한 규칙을 가진 여러 개의 독립적인 블록체인을 생성할 수 있다.

Avalanche를 사용하면 개발자가 고급 사용 사례에 맞는 맞춤형 VM을 구축할 수 있다. 이러한 VM은 모든 프로그래밍 언어로 구현할 수 있으며, 언어에 구애받지 않는 RPC 프로토콜을 사용하여 Avalanche와 통신한다. 또한, 개발자는 Subnet-EVM과 같은 미리 빌드된 런타임을 사용하여 솔리디티 기반 블록체인을 빠르게 배포할 수도 있다.

반면, 폴카닷 개발자들은 폴카닷 SDK를 사용하여 맞춤형 블록체인 런타임을 구축한다. 폴카닷 SDK는 런타임을 Wasm으로 컴파일하며, 릴레이 체인은 이를 사용하여 파라체인이나 롤업의 상태 변경을 검증한다. 폴카닷에는 기본 스마트 컨트랙트 계층이 없다. 대신 EVM과 Wasm 스마트 컨트랙트 기능이 파라체인에 구현되어 있다.

이러한 구분은 Avalanche가 VM 기반 블록체인 사용자 정의에 중점을 두고 있고 Polkadot이 공유 보안 및 모듈식 런타임 개발에 중점을 두고 있다는 점을 강조한다.

합의 프로토콜

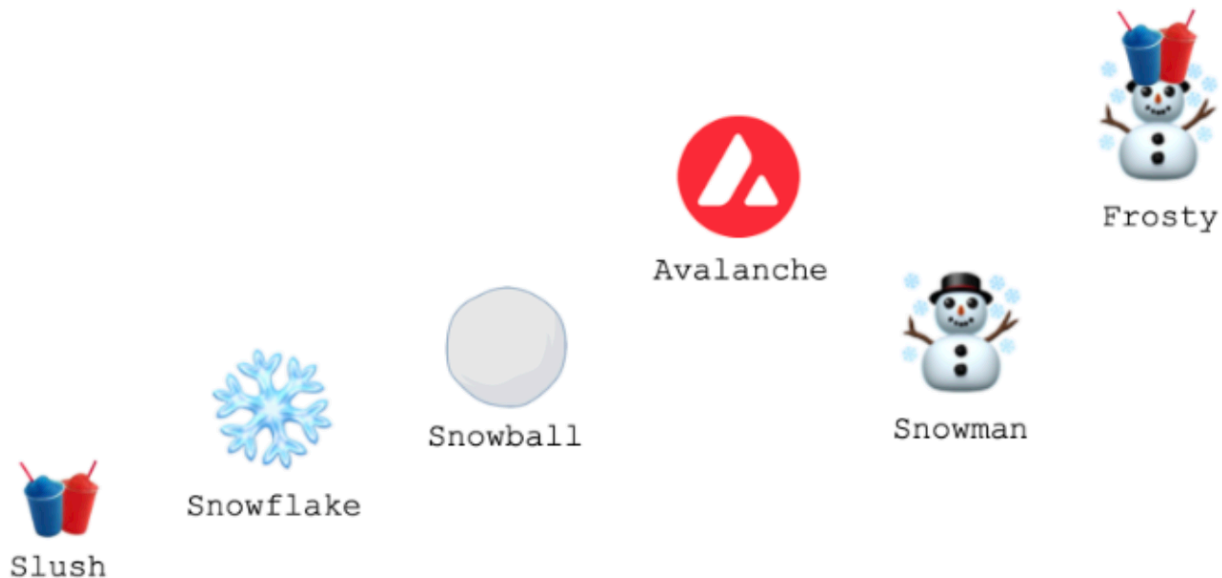


Figure 1. Snow is a family of binary BFT protocols based on a non-BFT protocol *Slush*, which incrementally builds up to *Snowflake* and *Snowball* BFT protocols in the Snow family.

이미지 출처: gyuho.dev.

아발란체 컨센서스는 기존 컨센서스와 나카모토 컨센서스의 특징을 결합하여 처리량, 완결성, 그리고 에너지 효율성을 달성한다. 또한, 반복적인 하위 샘플링 투표를 통해 확장성과 견고성을 보장한다.

폴카닷은 릴레이 체인을 통해 결정론적 완결성과 공유 보안을 구현한다. 폴카닷은 블록 생성을 위한 BABE와 결정론적 완결성을 위한 GRANDPA를 사용하는 동기식 하이브리드 모델을 사용한다. 폴카닷 밸리데이터는 개별 블록이 아닌 전체 체인에 동의하여 견고한 완결성을 보장한다. 이 두 가지 메커니즘은 네트워크의 견고성과 활성성을 유지한다.

스노우볼 알고리즘

스노우볼 알고리즘은 Avalanche Consensus의 핵심 구성 요소이다. 반복적인 샘플링과 선호도 업데이트를 통해 합의를 보장한다.

- 매개변수:
 - k : 샘플 크기(예: 밸리데이터 20개).
 - α : 정족수(예: 밸리데이터 14명).
 - β : 결정 임계값(예: 20라운드 연속).
- 프로세스:
 - 노드는 k 개의 검증자를 조회하고, 정족수 크기 α 를 충족할 경우 다수 선호를 채택한다.
 - 이 과정은 β 회 연속 라운드 동안 동일한 선호가 확인될 때까지 반복된다.

이 알고리즘은 네트워크가 성장하더라도 합의 메시지의 수가 일정하게 유지되므로 확장성이 보장된다.

DAG(유형 비순환 그래프)

Avalanche는 트랜잭션의 부분 정렬을 위해 DAG 구조를 사용한다. 각 트랜잭션은 정점으로 표현되며, 간선은 부모 트랜잭션을 가리킨다. 이 구조는 Snowball 알고리즘을 사용하여 높은 처리량과 효율적인 충돌 해결을 가능하게 한다.

스테이킹 메커니즘

Avalanche는 슬래싱 없는 위임 지분 증명(DPoS) 메커니즘을 사용한다. 주요 스테이킹 세부 정보는 다음과 같다.

- 밸리데이터 요구 사항: 밸리데이터가 되려면 최소 2,500 AVAX가 필요하다.
- 위임자 요구 사항: 지분을 위임하려면 최소 25 AVAX가 필요하다.
- 스테이킹 기간: 검증인과 위임자는 최소 2주에서 최대 1년까지 스테이킹할 수 있다. 이 기간이 지나면 재스테이킹이 필요하다.
- 보상: 밸리데이터는 가동 시간과 정확성에 따라 보상을 받는다. 위임자는 선택한 밸리데이터에게 보상을 공유한다.

폴카닷에서 스테이킹 요건은 동적이며 네트워크 상황에 따라 달라진다. 검증인과 노미네이터의 최소 스테이킹은 네트워크의 총 스테이킹 금액에 따라 달라진다. 폴카닷은 또한 부정행위를 처벌하기 위해 슬래싱을 사용한다. 자세한 내용은 스테이킹 페이지를 참조하세요.

메시지 전달

Avalanche는 안전하고 신뢰할 수 있는 크로스체인 통신을 위한 네이티브 프로토콜인 Avalanche 인터체인 메시징(ICM)을 출시했다. 주요 기능은 다음과 같다.

- 상호 운용성: 암호화 증명을 사용하여 서브넷 간에 메시지를 교환할 수 있도록 한다.
- 제한 사항: ICM은 Avalanche 생태계 내의 서브넷으로 제한되며 외부 블록체일까지 확장되지 않는다.
반면, 폴카닷은 XCM과 XCMP를 사용하여 네이티브하고 신뢰할 수 없는 크로스체인 통신을 구현한다. XCM은 파라체인 간 결합성을 지원하고 폴카닷 생태계를 넘어 확장되어 더 광범위한 상호 운용성을 구현한다.

거버넌스

백서에 따르면, Avalanche는 온체인 거버넌스 메커니즘을 구축할 계획이다. 현재 Avalanche는 온체인 또는 오프체인 시스템을 운영하지 않고 있다. Avalanche의 거버넌스 시스템은 다음을 포함한 몇 가지 주요 프로토콜 매개변수만 업데이트하는 데 국한될 것이다.

- 스테이킹 금액: 이 값은 시스템에 참여하기 전에 보증금으로 배치해야 하는 최소 스테이킹 금액을 정의한다.

- 노드의 최소 스테이킹 시간: 노드가 시스템에 스테이킹하는 데 필요한 최소 시간이다.
- 노드의 최대 스테이킹 시간: 노드가 스테이킹할 수 있는 최대 시간이다.
- 채굴 비율: 보상 비율 함수는 채굴 비율이라고도 하며, 참여자가 소유한 x 개의 공개 노드 수에 따라 t 개의 연속된 최소 스테이킹 시간 프레임 기간 동안 스테이킹 금액의 함수로 청구할 수 있는 보상을 결정한다. 여기서 $t_{\text{최소 스테이킹 시간}} \leq \text{최대 스테이킹 시간}$ 이다.
- 거래 수수료 금액: 수수료 구조는 다양한 거래에 대한 비용을 지정하는 일련의 규제 가능한 수수료 매개변수이다.
거버넌스 기능을 제한하는 것은 예측 가능성과 안전성을 높이기 위한 설계 선택이다.

폴카닷의 거버넌스(OpenGov) 메커니즘은 초기 단계부터 개발되어 왔으며, 기능을 점진적으로 출시하고 초기 네트워크를 탈중앙화하는 데 사용됐다. 폴카닷 거버넌스는 다양한 네트워크 매개변수에 대한 매개변수를 설정할 수 있을 뿐만 아니라, 이해관계자들이 국민투표에 투표할 수 있도록 거버넌스를 통해 자체적으로 업그레이드할 수도 있다.

프로토콜을 통한 런타임 업그레이드 개념으로 인해 Polkadot은 메타 프로토콜이 된다.

업그레이드

Avalanche 업그레이드는 Ava Labs에서 관리하며, 구현을 위해서는 밸리데이터 간의 협력이 필요하다. 서브넷 내 각 밸리데이터는 동일한 업그레이드를 적용해야 하므로, 프로세스가 수동적이고 협업적으로 진행된다.

폴카닷은 온체인 거버넌스를 통해 포크리스(forkless) 런타임 업그레이드를 사용한다. 파라체인 업그레이드는 자동화되어 밸리데이터의 조정이 필요하지 않아 프로세스가 간소화된다.

결론

Avalanche는 블록체인 개발자에게 맞춤형 환경을 제공하는 데 중점을 두고 서브넷을 통해 독립적인 블록체인을 구축할 수 있도록 지원한다. 그러나 서브넷은 Avalanche의 기본 네트워크와 같은 보안을 제공하지 않는다. Polkadot은 릴레이 체인, 파라체인 등을 통해 공유 보안과 상호 운용성을 강조한다.

폴카닷의 기능 중 신뢰 없는 메시징 및 포크리스 업그레이드를 위한 XCM은 이미 개발 단계에 있으며, 아발란체(Avalanche)는 아직 유사한 기능을 개발 중이다. 폴카닷의 거버넌스 메커니즘인 오픈거브(OpenGov)는 폴카닷 릴레이 체인의 방향 및 기술적 측면과 관련하여 탈중앙화된 의사 결정을 가능하게 한다.

DOT 토큰

DOT는 폴카닷의 기본 토큰으로, 비트코인의 BTC나 이더리움의 ETH와 유사하다. DOT는 세 가지 주요 기능을 가지고 있다.

- 거버넌스 : DOT 보유자는 네트워크 거버넌스에 투표하고 수수료, 토큰 인플레이션, 코드 업그레이드 등 프로토콜 변경 사항을 제안할 수 있다. 거버넌스 페이지에서 자세히 알아보세요.
- 스테이킹 : DOT 보유자는 토큰을 잠가 네트워크를 보호하고 스테이킹에 대한 보상을 받을 수 있다. 스테이킹 페이지에서 자세한 내용을 확인하세요.
- 보안 계산에 접근 : DOT는 Coretime을 구매 하고 보안 계산과 상호 운용성에 접근하며 롤업을 위해 파라체인 식별자를 예약하는 데 사용된다.

DOT 인플레이션 의 일부는 재무부 로 전환되며, 재무부는 OpenGov 국민투표를 통해 Polkadot 관련 프로젝트에 자금을 지원할 수 있다.

DOT 총 발행량, 활성 및 비활성 발행량, 예금 등에 대한 자세한 내용은 체인 상태 값 페이지를 참조하세요.

플랑크 단위

폴카닷 SDK 기반 블록체인 의 최소 계좌 잔액 단위는 플랑크(Planck)로, 플랑크 길이(Planck Length)에서 이름을 따왔다. DOT는 10^{10} 플랑크이고, 쿠사마의 KSM은 10^{12} 플랑크이다.

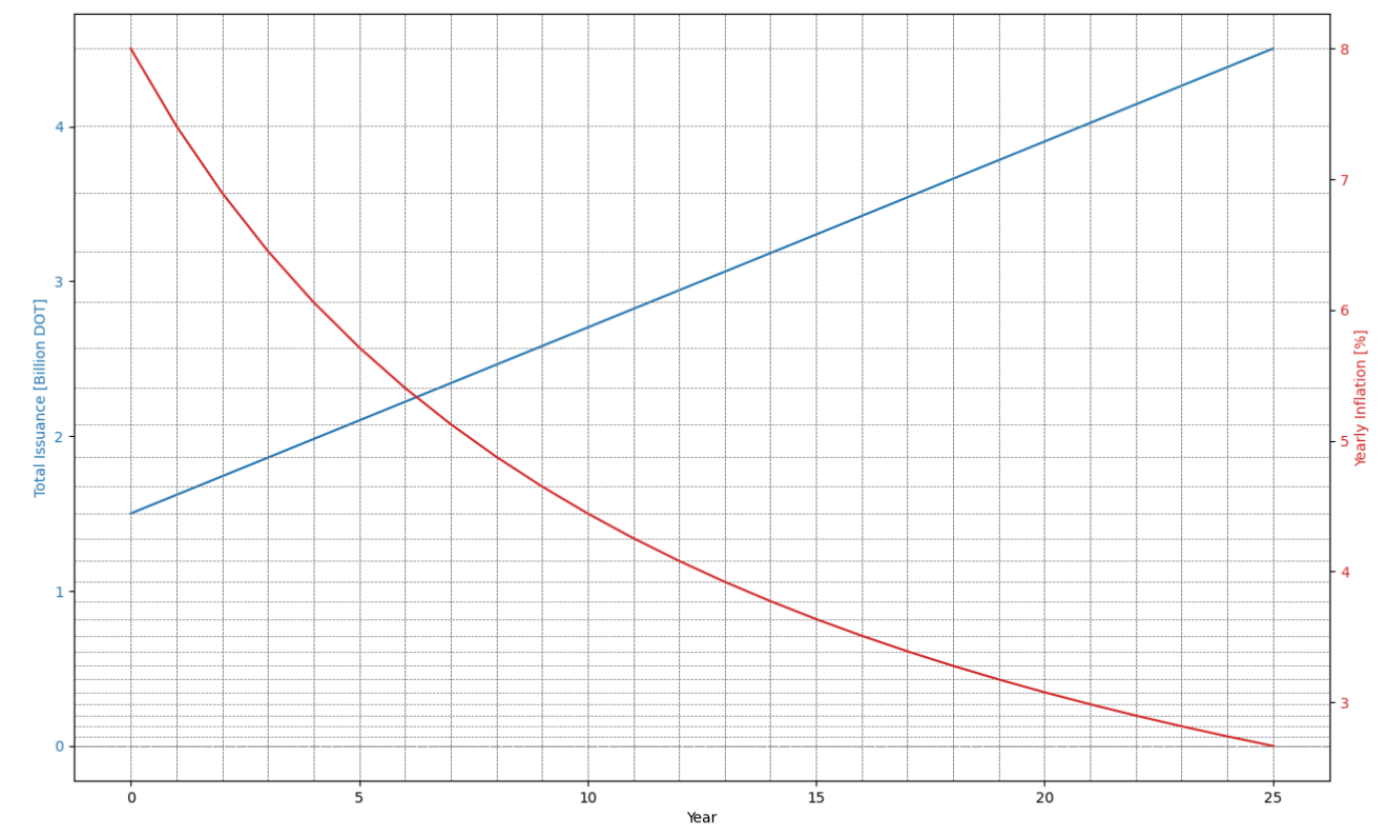
단위	소수점 이하 자릿수	플랑크로의 변환	DOT로의 전환
플랑크	0	1 플랑크	0.0000000001 도트
마이크로닷(uDOT)	4	10^4 플랑크	0.000010000 도트
밀리도트(mDOT)	7	10^7 플랑크	0.001000000 도트
도트(DOT)	10	10^{10} 플랑크	1.000000000 도트
백만(MDOT)	16	10^{16} 플랑크	1,000,000.00 DOT

DOT 인플레이션

DOT는 인플레이션 토큰으로, 토큰 공급량은 매년 1억 2천만 DOT로 고정적으로 늘어나며, 그 중 15%는 재무부에, 85%는 스테이커에게 지급된다.

인플레이션의 주요 목적은 지명 지분 증명(NPoS)을 통해 네트워크 참여자들에게 인센티브를 제공하고, 온체인 재무에 자금을 지원하여 네트워크를 성장시키는 것이라는 점을 이해하는 것이 중요하다. 토큰 인플레이션율은 철저한 토큰 이코노미 연구를 기반으로 한 온체인 거버넌스를 통해 업데이트될 수 있다.

아래는 현재 고정 인플레이션율을 가정한 25년간의 DOT 총 연간 인플레이션(빨간색 선)과 DOT 총 발행량(파란색 선)에 대한 예측이다.



총 발행량에는 총 DOT 인플레이션이 고려되므로 소각된 토큰은 고려되지 않는다.

순 DOT 인플레이션은 재무부 소각과 핵심 시간 매출에 따라 달라지며, 이는 변수이므로 예측이 불가능하다. 순 인플레이션은 다음과 같이 정의할 수 있다.

$$\text{Net Inflation} = \text{Gross fixed inflation} - \text{burned supply (treasury + coretime sales)}$$

총 고정 인플레이션은 연간 1억 2천만 DOT의 인플레이션을 의미하며, 소각 공급량은 재무부 소각 및 코어타임 판매 소각으로 인한 연간 소각 공급량을 의미한다.