요약

플라즈마는 스마트 컨트랙트의 인센티브 및 강제 실행을 위해 제안 된 프레임 워크로, 초당 상당한 양의 상태 업데이트 (잠재적으로 수십 억)까지 확장 가능하여 블록체인이 전 세계적으로 탈중앙화된 금융 애플리케이션으로 나타내는 것을 가능하게 한다. 이러한 스마트 컨트랙트는 거래의 상태 전환을 시행하기 위해서 네트워크 트랜잭션 수수료를 통해 자율적이고 지속적으로 운영되도록 인센티브를 제공하는데, 이 수수료는 궁극적으로 기초가 되는 블록체인(예: Ethereum)에 의존한다.

우리는 탈중앙화된 자율 애플리케이션을 확장하여 지불과 같은 금융활동을 처리할 뿐만 아니라, 중앙 집중화된 서버에 대한 대안으로 전 세계적으로 지속되는 데이터 서비스에 대한 경제적 인센티브를 구축하는 방법을 제안하고자 한다.

플라즈마의 설계는 두 가지 핵심 부분으로 구성되어 있다. : 모든 블록체인 계산을 MapReduce기능들로 재구성하는 것과 Nakamoto 컨센서스 인센티브가 block withholding을 막아준다는 것을 이해하여 기존 블록체인에 지분증명(Proof-of-Stake)토큰 결속시켜(bonding) 수행하는 선택적 방법이 있다.

이 구조는 부모 블록체인에서 상태 전환을 시행할 수 있는 위조증명을 사용하여 메인 블록체인의 스마트 컨트랙트를 작성함으로써 수행할 수 있다. 우리는 블록체인을 트리 구조로 구성하였으며, 각각을 분기된 블록체인으로 간주한다. 이 분기된 블록체인은 블록체인 히스토리와 Merkle 증명으로 커밋 된 MapReducible 계산으로 이루어져 있다. 원장(ledger entry)을 부모 체인에 의해 시행되는 자식 체인에 끼워 넣음으로써, 최소한의 신뢰로 굉장한 규모의 거래를 가능하게 할 수 있다. (루트 체인의 유효성과 정확성을 전제로 하였을 때).

비-글로벌 데이터를 글로벌하게 적용하는 과정에서 큰 어려움은 데이터 가용성과 block withholding attacks을 차단하는 것이다. 플라즈마는 결함이 있는 체인(faulty chain)을 나갈 수 있도록(exit) 하는 한편, 지속적으로 정확한 데이터 실행을 장려하고 강제하는 메커니즘을 구축함으로써 이 문제를 완화시켰다.

오직 결함이 없는 상태일 때만 merkleized된 약속(분기된 블록체인들)들은 주기적으로 루트체인(예: Ethereum)에 브로드캐스트 되며, 이는 확장성이 뛰어나고 비용이 저렴한 트랜잭션 및 계산을 가능하도록 한다. 플라즈마는 대량의 탈중앙화 응용 애플리케이션을 지속적으로 운용하는 것을 가능하게 한다.

확장성 높은 다중 연산

블록체인에서 정확성을 강화하기 위한 해결책은 일반적으로 모든 참가자가 체인의 유효성을 스스로 검증하도록 하는 것이다. 새 블록을 승인하려면 블록의 유효성을 검사하여 블록이 올바른지 확인해야한다. 주장된 데이터는 블록체인에 참가자들이 상태를 적용 할 수 있도록 반드시 분쟁 기간을 거쳐야하는데 블록체인 트랜잭션 용량을 확장하기 위한 많은 노력들은(예: LightningNetwork[1]) fidelity bond를 형성하기 위해 시간 약속을 사용해야 한다(an assert/challenge agreement). 이 assert/challenge 구조는 특정한 상태(state)가 옳다고 주장하는 것을 가능하게 한다. 값이 부정확한 경우, 다른 관찰자(observer)가 합의 된 시간 전에 이 주장에 도전하는 증거를 제공할 수 있는 분쟁 기간이 존재한다. 부정행위나 오류가 발생할 경우, 그 블록체인은 결함 있는 사용자(faulty actor)를 처벌할 수 있다. 이는 잘못된 상태가 주장된 경우 참가자들이 증거 제공을 시행하도록 장려하기 위한 메커니즘을 만들어 준다. 이러한 assert/challenge 증명 구조를 갖음으로서, 이해관계가 있는 참가자는 루트 블록체인(예: Ethereum)에 있는 이해관계가 없는 참가자들에게 진실에 기반하여 주장 할 수 있다.

이 구조는 지급을 위해서만 사용될 수 있는 것이 아니라, 계산 자체까지 확장하여 블록체인이 컨트렉트의 분쟁에 대해 판결을 내리는 레이어가 되도록 할 수 있다. 그러나 이것의 가정은 모든 당사자가 계산을 검증하는 데 참여하고 있다는 것이다. 예를 들어, 라이트닝 네트워크에서 이 구조는 컨트랙트 상태를 계산하기위한 약속을 설립할 수 있도록 한다. (예: 조건부 상태의 다중 서명 트랜잭션의 사전 서명 된 트리를 사용)

이러한 구조는 규모에 따라 매우 강력한 계산을 가능하게 하지만, 많은 외부 상태를 요약해야 하는 것과 같이 몇 가지 이슈가 존재한다(예: 전체 시스템/마켓의 합산, 다량의 나눠지고/불완전한 데이터 계산, 많은 수의 참여자). 다수의 오프체인 상태(state channels[4])에 대한 이러한 형태의 약속은 참가자들이 계산을 완전히 검증해야 하며, 그렇지 않은 경우 단일 라운드 게임에서도 계산 자체의 상당한 신뢰가 확립되어 있어야한다. 추가로, 대개 컨트랙트가 처음 시작되기 전에 실행 경

로를 완전히 해제되어야 하는 라운드의 가정(a presumption of "rounds") 같은 문제도 있다. 이는 참가자가 종료(exit) 및 온-체인의 비용이 많이 드는 계산을 강제로 수행하게 한다(어떤 당사자(party)가 정지하고 있는지 증명할 수 없으므로).

대신에, 우리는 오프체인에서 계산하지만 최소한의 온-체인 업데이트로 초당 수십억개의 연산으로 확장 가능한 시스템을 찾으려고 시도했다. 이러한 상태 업데이트는 위조 증명에 의해 시행되는 올바른 행동으로 보상을 얻는 자율적인 PoS 검증자들에 의해 이루어진다. 이것은 단일 참가자가 연산 서비스를 쉽게 정지하지 않고 연산을 수행할 수 있도록 해 준다. 이는 루트체인에서 비정상적 작업자(byzantine actors)에 의한 이벤트에서 risk-discounted 트랜잭션 수수료를 방지하기 위해 블록체인의 상태 업데이트 및 상태 변경을 강제하는 메커니즘을 최소함으로서 데이터 가용성 문제를 최소화할 수 있다.(예: block withholding)

라이트닝 네트워크와 마찬가지로 플라즈마는 기존의 블록체인에서 위에서 실행되는 집행을 보장하기 위한 일련의 컨트랙트로 어떤 사람이 나중에 지불과 인출(net settlement/ withdrawal)을 할 수 있도록 하며 컨트랙트 상태에서 자금을 보유할 수 있도록 한다.

플라즈마

플라즈마는 컨트랙트 생성자의 상태 전환 관리(state transition management) 없이 체인을 자동적이며 지속적으로 운영하는 경제적 인센티브를 창출하는 구조로 블록체인에서 확장 가능한 계산을 수행하는 방법입니다. 이는 노드 자체가 체인을 작동하도록 장려합니다.

추가적으로, 컨트랙트에서 지출된 금액을 비트맵에서 단일 비트로 최소화하여 하나의 트랜잭션과 서명이 다수의 참가자를 통합한 지불로 나타냄으로서 확장성을 갖습니다. 우리는 보증된 스마트 컨트랙트에 의해 확장 가능한 계산을 할 수 있도록 MapReduce 프레임 워크를 결합시켰습니다.

이 구성을 통해 표면화된 당사자(externalized parties)가 마이너와 마찬가지로 자금을 보유하고 컨트랙트를 계산할 수 있게 되지만, 플라즈마는 기존 블록체인의 상단에서 실행되므로 통합된 상태 업데이트를 위해 최소 데이터를 온-체인을 사용함으로서 모든 상태 업데이트(신규 사용자의 원장 항목 추가를 포함)에 대해 트랜잭션을 생성할 필요가 없습니다.

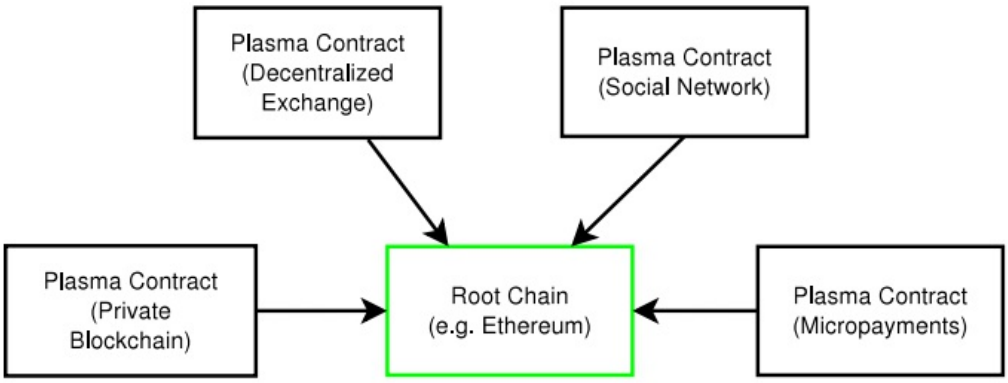

그림 1: 누구나 다양한 사용 사례에 스마트 컨트랙트 확장성을 이용할 수 있도록 사용자 정의 플라즈마 체인을 만들 수 있습니다. 플라즈마는 루트 체인 내에서 많은 블록체인을 허용하는 일련의 스마트 컨트랙트입니다. 루트 체인은 플라즈마 체인의 상태를 시행합니다. 루트 체인은 전 세계적으로 모든 계산을 시행하지만, 오직 사기의 증거가 있는 경우에만 계산되고 불이익을 받습니다. 많은 플라즈마 체인은 자체 비즈니스 로직 및 스마트 컨트랙트의 조건과 공존할 수 있습니다. 이더리움을 보면, 플라즈마는 이더리움에서 직접 실행되는 EVM 스마트 컨트랙트로 구성되지만, 비-비잔틴 사례에서는 엄청난 양의 계산 및 재무 원장 항목을 나타낼 수 있는 소소한 약정만 처리합니다.

Plasma는 5가지 주요 구성 요소로 구성됩니다. : 경제적으로 효율적인 방식으로 컨트랙트를 지속적으로 계산할 수 있는 인센티브 레이어, 거래 비용을 줄이고 거래의 정산을 극대화 할 수 있는 트리 구조로 하위 체인을 구성하는 구조, 이러한 중첩 체인 내에서 상태 트랜잭션의 사기 증거를 구성하여 트리 구조와 호환되도록 상태 트랜잭션을 재구성 해 높은 확장성을 갖게 하는 MapReduce 컴퓨팅 프레임 워크, Nakamoto 합의 인센티브의 결과를 재현하려는 루트 체인에 의존하는 합의

메커니즘, 대규모 출금 비용을 최소화하면서 루트 체인에서 정확한 상태 트랜잭션을 보장하기 위한 비트 맵-UTXO 약정 구조가 있습니다. 데이터 비가용성 또는 기타 비잔틴 행동의 이탈을 허용하는 것은 플라즈마 운영에서 중요한 설계 포인트 중 하나입니다.

플라즈마 블록체인 또는 표면화된 멀티파티 채널(Externalized Multiparty Channels)

우리는 다수의 off-chain 채널이 다른 사람들을 대신하여 상태를 유지할 수 있는 방법을 제안합니다. 이 프레임 워크를 플라즈마 블록체인 이라고 합니다. 플라즈마 체인에서 보유하고 있는 기금의 경우, 사기 증명에 의해 시행되는 상태 트랜잭션과 함께 플라즈마 체인에 자금을 예치하고 인출할 수 있습니다. 이것은 루트 체인에 보유된 자금과 일치하는 플라즈마 블록을 고려하여 입금 및 인출할 수 있기 때문에 집행 가능한 상태와 대체 가능성을 허용합니다. (플라즈마는 fractional reserve 금융 설계와 호환되지 않도록 설계되었다).

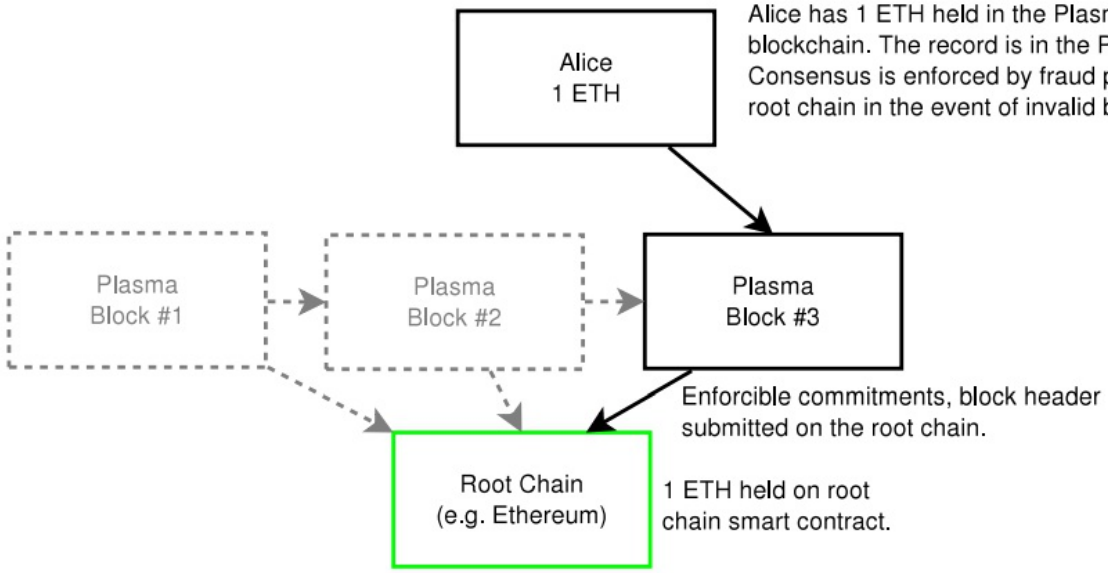

그림 2: 플라즈마 블록체인은 블록체인 내의 체인입니다. 이 시스템은 결합된 사기 증명들로 시행됩니다. 플라즈마 블록체인은 루트체인(예 : 이더리움)에 블록체인의 내용을 공개하지 않습니다. 대신, 루트 블록에 블록헤더 해시가 제출되고 루트 체인에 제출된 사기의 증거가 있는 경우 블록이 롤백 되고 블록 작성자에게 페널티를 줍니다. 많은 상태 업데이트가 단일 해시로 표시되므로 (일부 작은 관련 데이터 포함), 이는 매우 효율적입니다. 이 업데이트는 루트 체인에 표시되지 않은 잔액을 나타낼 수 있습니다. (앨리스의 원장 잔액을 루트 체인에 갖고 있지 않고 플라즈마 체인에 갖고 있으며, 루트 체인의 잔액은 플라즈마 체인 자체를 시행하는 스마트 컨트랙트를 나타냅니다). 회색 항목은 오래된 블록이고 검은색은 루트 체인에 전달되고 제출된 가장 최근의 블록입니다.

엄청나게 많은 양의 트랜잭션이 루트 블록체인에 게시되는 최소한의 데이터로 이 플라즈마 체인에 저장될 수 있습니다. 모든 구성원은 기존 구성원 집단이 아닌 모든 사람에게 자금을 이체할 수 있습니다. 이러한 이체는 루트 블록체인의 고유 코인 / 토큰으로 (얼마간의 시간 지연과 증명으로) 자금을 입금 및 인출할 수 있습니다.

플라즈마를 사용하면 루트 블록체인에 원장에 대한 전체 기록 없이, 제 3자 또는 구성원에게 신뢰를 위임하지 않고 블록체인을 관리할 수 있습니다 (또는 지분 증명(proof-of-stake) 네트워크의 참가자의 네트워크). 최악의 경우, 자금이 묶이고 시간-가치(time-value)는 블록체인의 대규모 출금(exit)과 함께 사라집니다.

우리는 사기 또는 비-비잔틴 행동에 대한 시도를 낮추기 위해 이 채널에서 상태를 시행하는 루트 블록체인에 스마트 컨트랙트[7]로 일련의 사기 증명을 구성합니다.

이러한 사기 증명은 자금 인출에 대해 상호작용하는 프로토콜을 시행합니다. 라이트닝 네트워크와 마찬가지로 자금을 인출할 때, 나가려면 종료 시간이 필요합니다. 우리는 기존 구성원이 참가자의 원장 아웃풋(outputs)의 비트맵을 증명하여 상호작용하는 게임을 구성합니다. 이 때, 참자가의 원장 아웃풋의 비트맵은 인출을 요청하는 UTXO 모델로 정리된 것입니다.

네트워크에 있는 누구나 이미 자금이 지출되었는지 여부를 증명하는 대체 *채권* 증명을 제출할 수 있습니다. 이것이 올바르지 않은 경우 네트워크의 모든 사람이 사기 행위를 입증하고 채권을 철저히 조사하여 증명을 되돌릴 수 있습니다. 충분한 시간이 지나면 두 번째 *채권* 라운드에서 철회가 발생할 수 있습니다. 이 상태는 저장된 타임스탬프 *이전* 상태에 있는 채권입니다. 이렇게 하면 일괄 철회 처리가 가능해지므로 잘못된 플라즈마 체인을 신속하게 종료할 수 있습니다. 조정된 대량 철회 이벤트에서, 참가자는 상위 블록체인에서 소비되는 2 비트 미만의 블록 공간으로 종료할 수 있습니다.

block withholding 공격의 경우, 참가자는 이전의 다른 오프 체인 제안과 비교하여 상당한 비용 절감으로 대규모 출금(exit)을 신속하고 저렴하게 수행할 수 있습니다. 또한 이는 유효성 검사 노드 연합(Sidechain Functionaries, Fishermen)에 대한 어떠한 신뢰도 필요 없습니다.

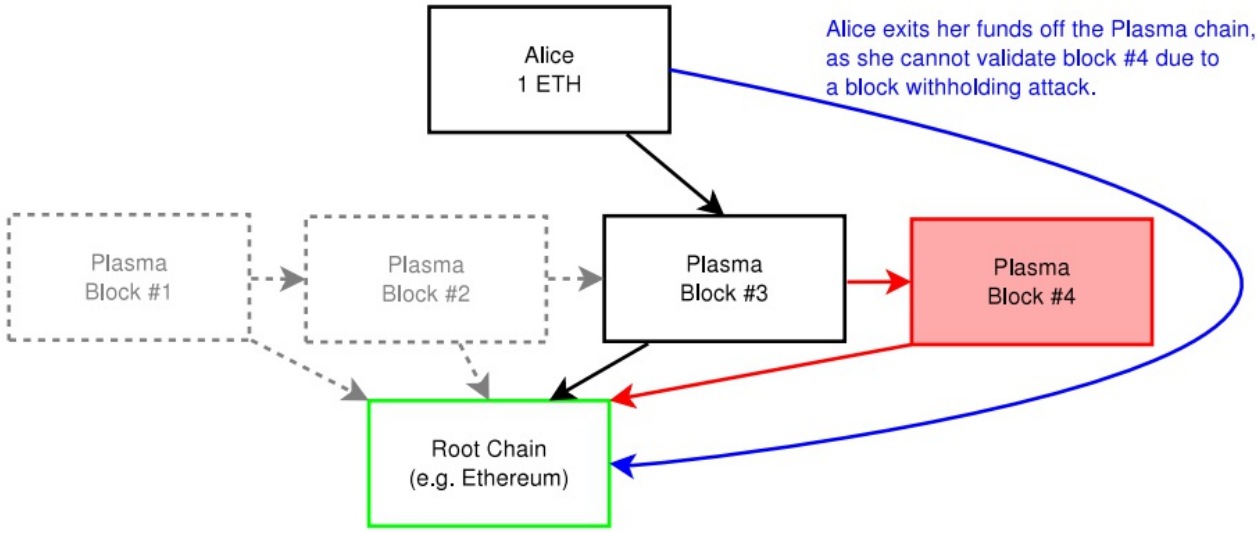

그림 3: block withholding시 자금 출금. 빨간색 블록(블록 #4)은 루트 체인에 withheld 및 커밋된 블록이지만, Alice는 플라즈마 블록 #4를 검색 할 수 없습니다. 그녀는 루트 체인에 자금의 증거를 브로드캐스팅함으로써 종료하고 그녀의 인출은 분쟁을 허용하기 위해 약간의 지연 후에 처리됩니다.

Lightning을 닫는 것이 두 참가자 간의 무한한 지불 시행을 가능하게 하는 상호 작용 메커니즘인 것처럼, 이것은 n참가자 간의 상호 작용 메커니즘을 허용합니다. 가장 큰 차이점은 모든 참가자가 상태를 업데이트하기 위해 온라인 상태일 필요는 없으며, 참여자는 자신의 참여를 가능하게하기 위해 루트 블록체인에 대한 기록을 필요로 하지 않는다는 것입니다. - 플라즈마 체인을 트리 형식으로 구성할 때 트랜잭션을 확인하기 위한 최소한의 테이터로 온-체인에 직접적인 상호 작용 없이 최소한의 비용으로 플라즈마에 자금을 배치할 수 있습니다.

블록체인의 집행 가능한 블록체인

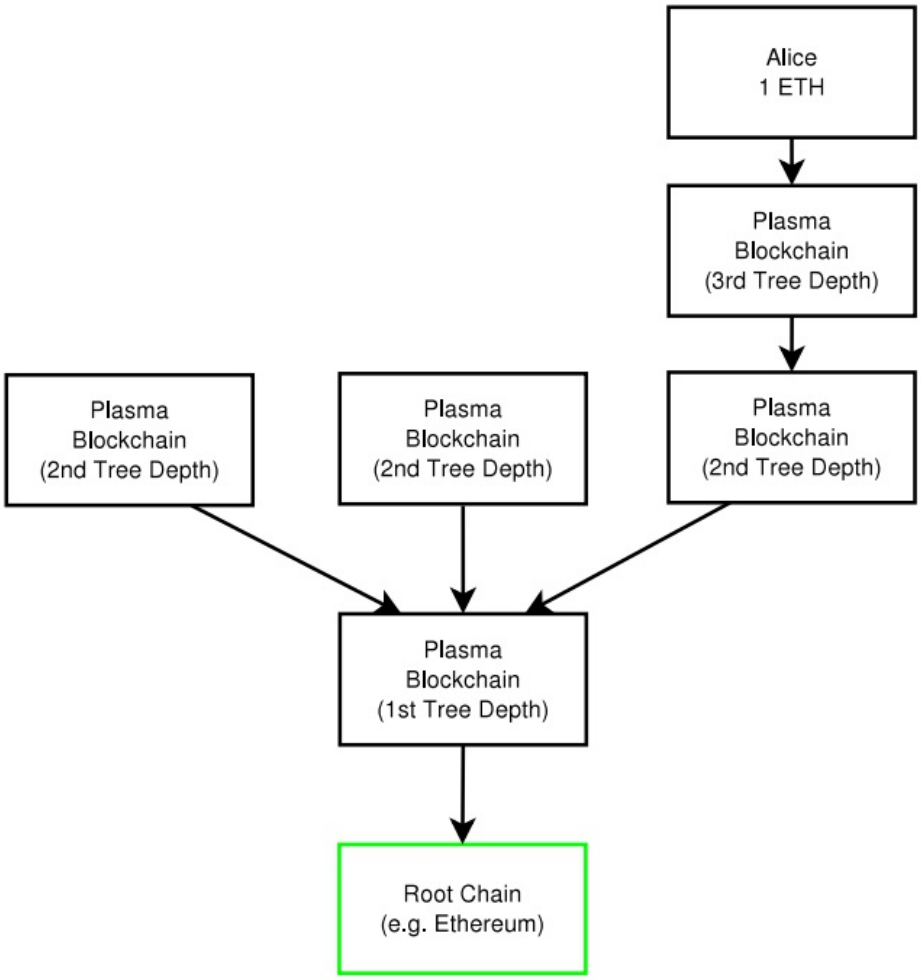

그림 4: 플라즈마는 트리 형식으로 블록체인을 구성합니다. 블록 커밋 흐름이 아래로 내려가고 출금(exit)은 모든 부모 체인에 제출될 수 있으며 궁극적으로 루트 블록체인에 커밋됩니다.

우린 법원 시스템과 유사한 메커니즘을 구축합니다. 라이트닝 네트워크가 궁극적으로 루트 블록체인에서 시행 할 수 있는 지불을 위해 판결 레이어를 사용한다면, 우리는 비-비잔틴 상태에서 가용성을 극대화하고 비용을 최소화하기 위해 상급 법원과 하급 법원을 만듭니다. 체인이 비잔틴인 경우, 상위 블록 (루트 블록체인 포함) 중 하나를 선택하여 작업을 계속하거나 현재 커밋된 상태로 종료할 수 있습니다. 증가하는 논스 상태의 시행 (폐지를 통한) 대신, 우리는 잔액 및 체인 계층 구조의 상태 변화를 시행하기 위한 사기 증명 시스템을 구축합니다.

실제로, 우리는 상위 체인에만 주기적으로 커밋되는 상태 변화를 만들 수 있습니다(그 후 루트 블록체인으로 이동). 비잔틴의 조건에서 상위 (또는 루트) 체인에만 가공되지 않은 데이터(raw data)를 전송할 수 있기 때문에, 이것은 굉장한 양의 계산 및 계정 상태(account state)를 허용합니다. 상위 플라즈마 체인을 사용하여 상태를 시행할 수 있기 때문에 부분적으로 비잔틴 상태를 복구하는 것은 비용이 최소화됩니다.

이 자녀 블록체인은 루트 블록체인 (예: Ethereum)의 최상위에서 실행되며 루트 블록체인의 관점에서 볼 때, 지분 증명 (proof-of-stake) 규칙 및 블록체인의 비즈니스 로직을 적용하기 위해 컨트랙트에 서명된 토큰만으로 주기적인 약속을 볼 수 있습니다.

이것은 블록 가용성을 극대화하고 누군가의 코인 유효성 확인을 위해 수고를 최소화하는데 커다란 이점이 있습니다. 그러나 모든 데이터가 모든 당사자 (특정 상태를 증명하고자 하는 사람)에게 전파되는 것은 아니기 때문에, 당사자는 주기적으로 특정 체인을 모니터링하여 사기를 처벌할 책임이 있을 뿐 아니라, block withholding 공격이 발생하면 개인적으로 신속히 체인을 나가야 합니다.

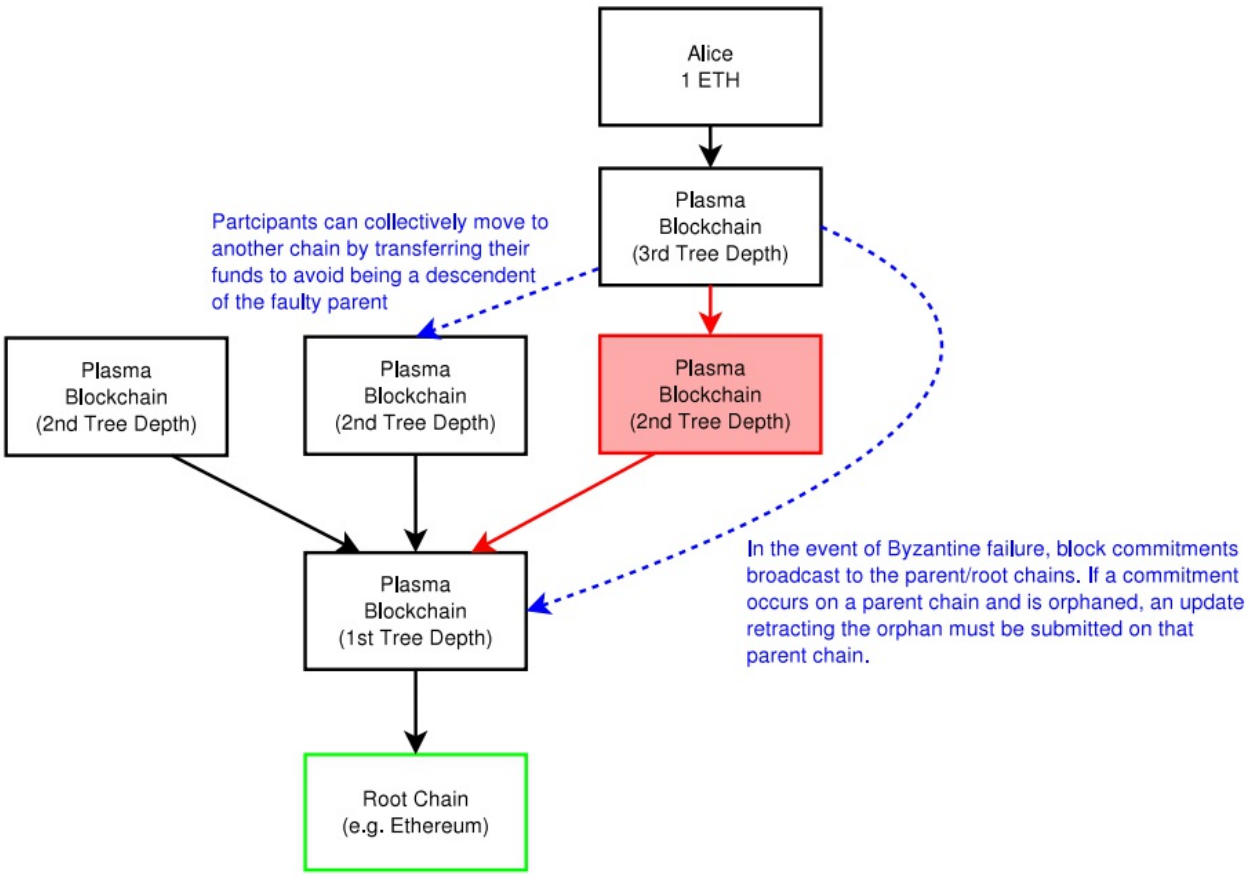

그림 5: 결함이 있는 블록체인 (빨간색으로 표시됨)은 상위 플라즈마/ 루트체인 (오른쪽 파란색 점선)에 약속을 브로드캐스팅하여 주위에 라우팅 됩니다. 3번째의 플라즈마체인에 참여한 사람들은 일정 시간이 지나면 다른 체인으로 다 같이 집단 이동(왼쪽 파란 점선)을 합니다.

비-비잔틴 환경에서 이 구조는 블록체인 상태의 트리를 통합하고 모든 하위 플라즈마 체인을 업데이트합니다. 모든 체인을 통한 전체 업데이트는 서명이 있는 32바이트 해시로 증명할 수 있습니다.

Plasma 지분 증명 (proof-of-stake)

단일 검증자를 사용하여 다른 사람을 대신하여 펀드를 보유 할 수 있는 것은 상당히 흥미롭지만, 우린 한 당사자가 ETH 본딩 또는 토큰으로 본딩해야 하는 지분 증명 (proof-of-stake) 프레임 워크를 사용하여 여러 검증자들로 상태를 시행할 수 있는 방법을 제안합니다.(예 : ERC-20)

이 지분 증명 (proof-of-stake) 시스템의 증거에 대한 합의 메커니즘은 다시 온-체인 스마트 컨트랙트에 적용됩니다.

나카모토 컨센서스 (Nakamoto Consensus)와 비슷한 인센티브를 재현하려고 노력했지만, 우리는 지분 증명(proof-of-stake) bonds를 사용합니다. 우린 나카모토 메커니즘의 결과로 만들어진 보다 유용한 인센티브 메커니즘 중 하나로서 block withholding 공격을 최소화하는 놀라운 인센티브 메커니즘이 있다고 믿습니다. 여기서는 리더는 확률적으로 선출됩니다. 리더는 시간이 지남에 따라 확률적으로 알려집니다. (원래 구현에서는 6-confirmations임). 블록을 발견하면 리더가 될 가능성이 높지만, 리더가 될지는 아직 확실하지 않습니다. 리더가 되도록 하기 위해서는 네트워크의 모든 참가자에게 자신의 블록을 퍼트려 자신의 배당률을 극대화합니다. 우리는 이것이 나카모토 메커니즘의 주요한 기여로 여기지 않고 이 인센티브를 재현하려 시도한다면 의미가 있다고 믿습니다.

since it’s possible if one does straight leader election, block withholding attacks by majority cartels (also generalized as the ”data availability problem”) become magnified 때문에 지분 증명 (proof-of-stake)은 문제에 직면해 있습니다.

이해 관계자가 새로운 블록의 커밋된 해시를 포함하는 루트 블록체인 또는 상위 플라즈마 체인에 (블록을) 게시할 수 있게 함으로서 우린 플라즈마 지분 증명 (proof-of-stake)에서 이를 완화할 수 있습니다. 검증자는 유효성을 완전히 검사한 블록만 연결 합니다. 그들은 (최대의 정보 공유를 장려하기 위해) 블록을 병렬로 구축 할 수 있습니다. 우리는 정확하게 나타내기 위해 더 많은 수수료를 보상함으로 현재의 staker 비율(예: 누군가 코인의 3%를 소유한다면, 그것들은 지난 100개의 블록 중 3 %가 되어야 함)과 일치하는 지난 100개의 블록을 나타내기 위해 검증자를 위한 인센티브를 창출합니다. (stakers에 의한 차선책으로 인해) 초과되는 수수료는 후에 수수료를 지불하기 위해 풀로 갑니다. 지난 100개의 블록의 데이터를 포함하는 모든 블록에는 약속이 존재합니다(논스와 함께). 올바른 체인 마지막은 가장 높은 수수료가 합산 된 체인입니다. 일정 기간이 지난 후에, 블록은 마무리(finalized)됩니다.

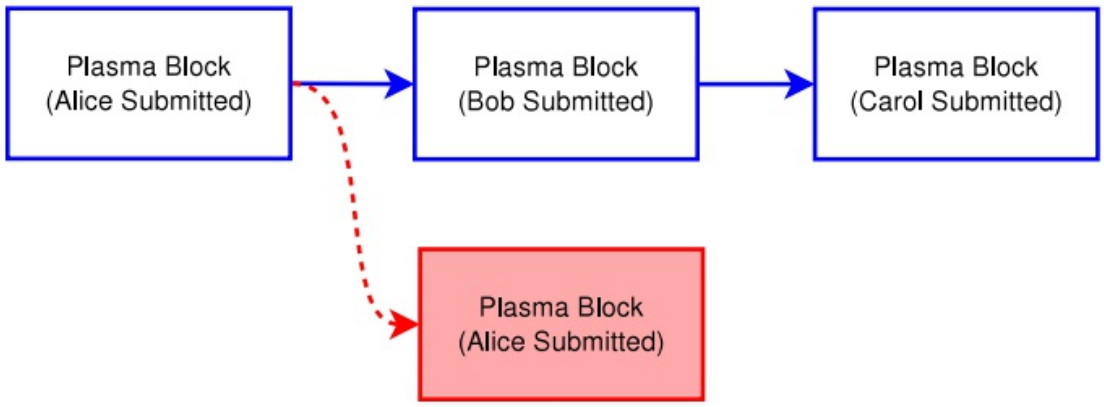

그림 6: 그림 6: Alice, Bob 및 Carol은 같은 무게의 양을 가진 3명의 검증자라고 가정합니다. 그들은 최대 이익을 위한 라운드 로빈 구조를 구축하기 위해 공동으로 인센티브를 제공합니다. 이러한 약속은 상위/루트 체인에 제출됩니다. 체인의 마지막은 n 개의 기간 동안 블록을 올바르게 분배하여 최대 가중치 점수에 부합하는 것입니다. (파란색은 현재 후보 체인의 끝, 빨간색은 고아(orphan)이다). 차선적인 체인 끝은 어떤 임계치 (예: 90%) 이상의 정확성을 지닌 미래 검증자를 위해 초과 비용을 풀에 넣습니다. n 개의 기간 후에 그것은 파란 체인의 끝이 완결(finalized) 되어지는 것으로 추정됩니다.

이것은 참여자들이 나카모토 컨센서스 (Nakamoto Consensus) 에서 51% 공격 가정에 참여하고 이를 복제하도록 권장합니다. block withholding 또는 기타 비잔틴 행동을 통해 체인이 공격받는 경우, 비-비잔틴 참가자는 상위/루트 체인에서 대량의 계약 철회를 간결하게 수행할 수 있습니다. 가장 상위의 플라즈마 체인에 대한 채권이 토큰 형태로 존재할 경우, 토큰의 가치는 대량 출금(exit)의 결과로 엄청나게 가치가 낮아질 수 있습니다.

MapReduce로서의 블록체인

blockchain : git :: Plasma : Hadoop (MapReduce)

MapReduce 형식으로 계산을 구성함으로, 계산 및 상태 트랜잭션을 계층적 트리에서 쉽게 디자인 할 수 있습니다.

MapReduce는 수천 개의 노드에서 대규모 계산을 위한 프레임 워크를 제공합니다. 블록체인은 계산 규모를 충족시키는 데 있어 비슷한 문제를 안고 있지만, 계산 증명을 생성하는 데 추가적인 요구 사항이 있습니다.

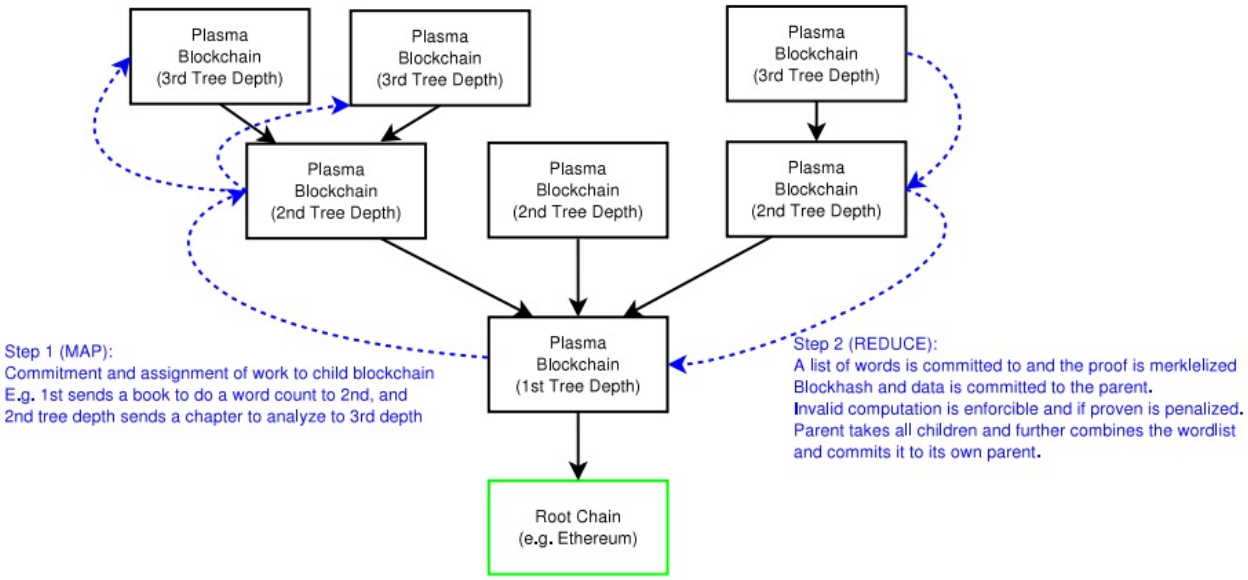

그림 7 : 파란색은 상위 블록에서 하위 블록에게 전달되는 메시지입니다. 하위블록들은 n 블록 이내의 상위 블록에 커밋해야 하며 그렇지 않으면 체인이 중단됩니다. 블록 데이터는 계산을 위탁한 하위 블록에게 작업을 분배합니다. 3레벨 자식체인은 계산을 수행하고 단어 목록을 반환합니다. (예: 계산하는 과정에서 , 단어 "Hello"가 3 번 발생하고 단어 "World"가 두 번 나타남) 단어 목록 데이터는 약속의 일부로 상위에게 반환되고, 단어 목록은 하위로부터 결합되어 상위로 제출되며, 궁극적으로 전체 단어 목록을 완성합니다. (예: 전체 자료에는 단어 "Hello" 100번과 “World” 150번이 포함됨). 이렇게 하면 매우 많은 양의 데이터와 작업을 처리하기 위해 루트 체인에서 커밋된 하나의 블록 헤더 / 해시만으로도, 경제적이며 실행 가능한 계산을 생성할 수 있습니다. 이의 제기가 된 결함이 있는 블록의 경우를 제외하고, 그 외에는 매우 적은 양의 데이터가 루트 체인에서 주기적으로 제출됩니다.

우리는 map 단계가 계산한 데이터에 대한 확약을 입력으로 포함하는 방법과, reduce 단계에서 결과를 리턴할 때 Merkleized 상태 변화 증거를 포함하는 방법을 제안합니다. Merkleized된 상태의 변화는 루트 블록체인에 구성된 위조 증명을 통해 시행됩니다. 또한 zk-SNARKs 상태 변화 증명을 구성하는 것도 가능합니다. 일부 계산 구조에서는 reduce 단계에서 상태 변화에 대한 비트맵이 필요할 수도 있습니다 (따라서 이러한 사용 사례를 위해 각 UTXO/계정은 한 비트 이상 이용 할 수 있다).

우리의 구성은 시간 또는 속도의 균형을 맞추어 엄청난 대규모의 계산을 가능하게 합니다. 이러한 균형은 노드가 계산을 하고 참여자가 이를 확인하는 네트워크를 생성합니다. 이것은 신뢰 없이 계산을 외부에서 완전히 아웃소싱 할 수 있는 시스템을 생성하는 것이 아니라, 보증된 증명으로 계산을 압축하는 기능을 가능하게 합니다. 이러한 보증된 증명은 참가자들이 정직하게 해당 사항을 증명하게 합니다. 이것은 다시 라이트닝 네트워크 이야기로 돌아가는데, 이건 마치 숲에서 나무가 떨어졌을 때 그 소리를 듣는 사람이 없어서 정작 소리가 났는지 안 났는지는 중요하지 않다고 추정할 수 있습니다. 마찬가지로 아무도 계산을 감시하고 있거나/수행하지 않으면 올바른 것으로 추정되는지 혹은 결과가 무엇인지는 중요하지 않다고 추정할 수 있습니다. 계산은 네트워크의 모든 참가자가 볼 수 있지만 잔액을 소유하고 있거나 정확한 계산이 필요한 참가자는 정기적으로 체인의 정확성을 확인할 것입니다. 스케일링의 이점은 경제적으로 영향을 받지 않는 체인을 지켜봐야 한다는 요구사항을 제거함으로서 올바르게 작동하길 바라는 체인만 주시하면 된다는 것입니다. 다른 플라즈마 체인에서의 작동은 최소 상태로 표현할 수 있는데 영향을 주는 계산을 위해 reduce 단계의 일부로 함께 엮여 있습니다. 예를 들어, 분산된 거래의 경우 어떤 거래 상대방이 어떤 주문을 하는지 상관하지 않고 하나의 통합 주문서만 볼 필요가 있으므로 다른 모든 체인을 단일 거래 상대방으로 관찰하면 됩니다. 반면에 누군가의 개인 체인은 트랜잭션의 시행과 (자신을 포함하여)정확한 사람에게 주문한 것이 완전히 검증되어 있을 것 입니다. 또 다른 예로는 플라즈마 체인 트리에서 BBS를 구성 할 수 있으며, 관심이 없는 주제에 대한 업데이트를 받을 필요가 없습니다.

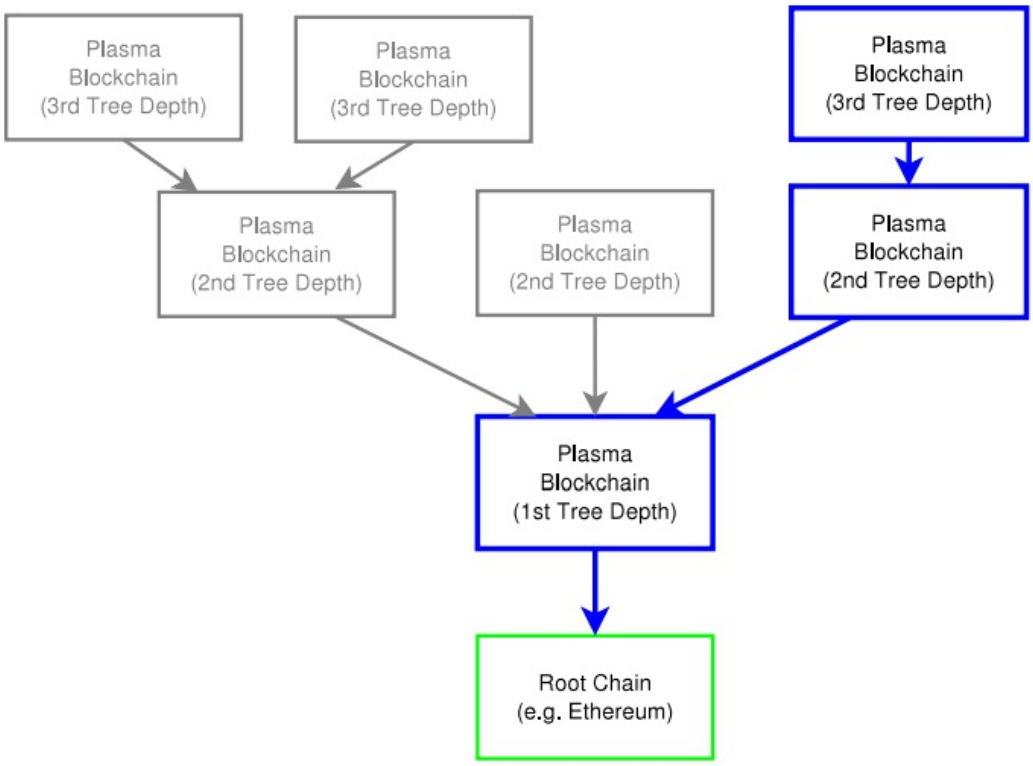

그림 8: 자신이 시행하고자 하는 데이터만 보아야 합니다. 경제적 활동이나 계산이 시행할 필요가 없는 다른 플라즈마 체인에서 발생하면 (회색) 다른 모든 체인을 단일 거래 상대방으로 여길 수 있습니다. 예: 플라즈마의 탈중앙화된 거래에서는 오직 자신의 약속에 영향을 미치는 체인을 봐도 됩니다(굵은 파란색).

영구적으로 탈중앙화 되어있고 자율적인 블록체인의 경제적 인센티브에 대한 설명

우리는 하위 블록체인을 지속적으로 운영하여 경제적인 인센티브를 창출 할 수 있는 구조를 제안합니다. 중대한 복잡성이나 상태 변화에 의존성을 필요로 하지 않는 상태의 경우, 네이티브 토큰(예: 이더리움의 경우 ETH)은 상태를 증명하는데 사용될 수 있습니다. 그러나 복잡한 컨트랙트의 경우에도, 활성 된 상태를 보장하는 것과 시스템의 공정성을 보장하는데 대한 인센티브 때문에 체인 운영을 지속할 수 있는 상당한 동기가 있습니다.

모든 플라즈마 체인은 일련의 계약으로 표현됩니다. 이러한 컨트랙트는 체인의 합의 규칙을 시행하고, 위조 증명이 제기되어 적용되면 사기에 대한 상당한 페널티를 부과합니다.

그러나 비잔틴 상태를 피하는 것을 장려하기 위해, 특히 정확성과 liveness에 대한 인센티브를 부여하기 위해서는 컨트랙트 당 토큰을 만드는 것이 이상적일 수 있습니다. 이 토큰은 컨트랙트 운영에서 네트워크 효과를 나타내며, 이 컨트랙트의 보안을 최대화하기 위한 인센티브를 제공합니다. 플라즈마 체인은 지분증명(Proof-of-Stake) 구조로 네트워크를 보호하기 위해 토큰을 요구하기 때문에, 보유자는 토큰의 가치를 잃을 수 있는 비잔틴의 행동이나 결함을 막도록 장려됩니다. 토큰의 역할은 토큰 가치의 감소로 인해 작동에 장애가 발생한 경우 검증자에게 현지화 된(localized) 비용이 있는지 확인하는 것입니다.

사용자를 대신해 자금을 보유하는 기본 컨트랙트와 같은 간단한 컨트랙트와 비즈니스 로직을 사용하여 이더리움 채권은 플라즈마 체인의 지분을 나타낼 수 있습니다.

채권(혹은 토큰이나 ETH)을 발행하는 지분은 네트워크 운영에 대한 거래 수수료를 받기 때문에 네트워크 운영을 지속하도록 장려한다. 이러한 거래 수수료는 비-비잔틴의 행동을 장려하는 네트워크의 유지자(stakers)들에게 지급되며, 토큰에 대한 장기적인 가치를 창출합니다.

유지자들(stakers)은 거래 수수료를 받기 위해 이 네트워크를 계속 운영하도록 장려되기 때문에 루트 블록체인의 계약에 정의된 위조 증명을 지키면서 지속적으로 체인을 운영할 것입니다.

디자인 스텍과 스마트 컨트렉트

역사적으로, 많은 사람들은 블록체인이 총액 결제 시스템(결산 시스템)과 같은 거래 결제 방식에 가장 잘 적용될 것이라고 믿었습니다. 그러나, 총액 결제 시스템(결산 시스템)에 블록체인을 적용하는 것은 확장성에 어려움이 있습니다. 결제 채널 네트워크인 Lightning Network와 같이 여러 결제를 묶어 확정하는 디자인(Net settled designs)은 참가자 간에 거의 무제한 지급을 허용하도록 구조를 변경 했습니다. 채널이 블록체인에 묶여서 있어(net-settled) 트랜잭션 용량이 크게 증가합니다. 이러한 채널 네트워크를 통해 지급은 라우팅 될 수 있습니다.

이 구조는 효과적이고 즉각적인 지불을 가능하게 합니다. 이것은 빠른 송금을 요하는 지불에 도움이 될 뿐만 아니라 컨트랙트에도 도움이 됩니다.

플라즈마는 자식 체인에 대한 트랜잭션이 신속하게 컨펌될지라도 최종 확정이 빠르게 되도록 설계되지 않았습니다. 최종 확정되기 위해서는 루트 블록체인에 대한 최종 승인이 필요합니다. 채널은 로컬 영역에서 빠른 지급 및 계약의 확정을 위해 필요합니다.

스마트 컨트랙트의 경우, "free option problem"이 있으며, 스마트 컨트랙트 제안의 수신자(두번째 또는 마지막 서명인)는 그것을 시행하기 위해 계약서에 서명하고 브로드캐스트 해야 합니다.- 그 기간 동안 컨트랙트의 수취인은 그것을 자유로운 옵션으로 간주할 수 있는데 만약 활동이 그들에게 흥미를 유발하지 않는다면 계약에 서명하기를 거부할 수 있습니다. 이는 신뢰할 수 없는 당사자를 다룰 때 스마트 컨트랙트가 가장 효과적이기 때문에 상황을 악화시킵니다. (상대방에 대한 위험을 감소시켜 그에 따른 정보비용의 최소화시키기 때문에).

플라즈마는 그 자체로 이 문제를 해결하는 것이 아닙니다. 왜냐하면 블록체인에 상호작용 프로토콜에 대한 첫 번째와 두 번째 서명 단계에 대한 계산의 보장이 없기 때문입니다.

라이트닝을(플라즈마 상단의 라이트닝을 포함하여) 사용하면, 합리적인 로컬 영역의 확정(finality)을 통해 상당히 빠른 속도로 업데이트할 수 있습니다. 마지막 당사자에게 선택권을 부여하는 단일 지불 대신에, 지불을 많은 작은 지불로 분할 할 수 있습니다. 이렇게 하면 free option을 분할된 양만큼 최소화 할 수 있습니다. 스마트 컨트랙트의 두 번째 당사자는 분할된 조각의 양에 대한 free option을 가지고 있기 때문에 그 값이 최소화됩니다.

위의 사례에서, 플라즈마는 최소한의 루트 체인 상태 확정으로 원장을 업데이트할 수 있으므로, 라이트닝은 신속한 금융 결제/계약을 위한 제1의 인터페이스 레이어가 될 수 있습니다.

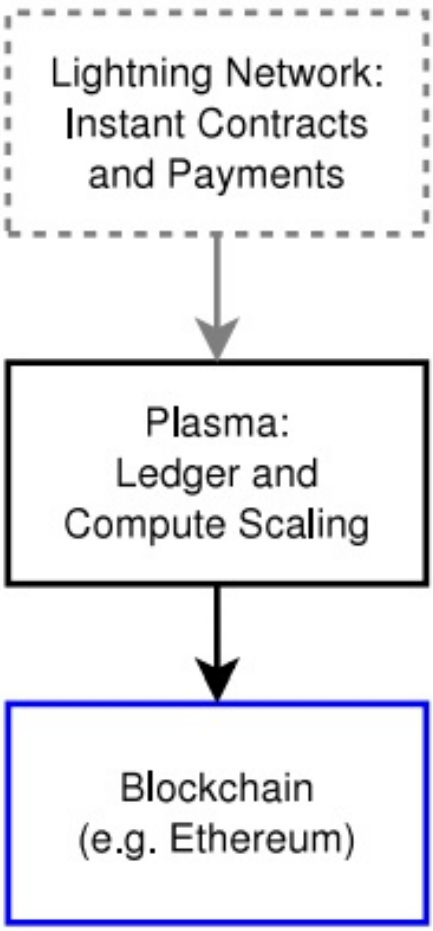

그림 9: 컨트랙트 및 지불에 대한 심판을 담당하는 계층인 루트 블록체인이 있습니다. 컨트랙트 자체는 루트 블록체인에 위치합니다. 플라즈마 체인에는 현재의 원장 상태가 저장되어 있으며, 이 상태는 루트 블록체인에 상환되고 다시 복구시킬 수 있습니다. 자금을 되찾기 위한 위조 증명이 존재합니다. 플라즈마는 중첩된 플라즈마체인 세트를 나타내어 최소한의 트랜잭션으로 자금을 인출할 수 있도록 해 줍니다. 상단의 라이트닝 네트워크는 플라즈마 및 블록체인에 대한 즉각적인 결제가 가능하게 합니다.

샤딩에서 가장 중요한 문제는 정보

분할된(sharded) 데이터 세트로 인해, 개별 파편(shard)이 정보 공개를 거부할 위험이 있습니다. 이는 위조 증명을 하는 것을 불가능하게 만들 것입니다.

우리는 다음 세가지 전략을 사용하여 이 문제를 해결하려고 합니다. :

1. 블록의 전파를 장려하는 새로운 PoS 매커니즘
   이 메커니즘은 인센티브의 올바른 작동에만 전적으로 의존하지 않습니다. 대신 이는 결함 있는 행동을 상당히 줄일 수 있습니다.

2. 정확한 인출 증명을 위해 상당히 인출 시간에 지연이 발생
   개인은 블록체인을 자주 지켜볼 필요가 없으며 상위 플라즈마 체인에 대한 위조는 루트제인에 같은 플라즈마 체인의 어떤 정직한 사용자에 의해 예방할 수 있습니다. block withholding 이벤트가 발생할 경우, 플라즈마 체인은 증거를 통해 즉시 자금을 차단할 수 있기 때문에 부정한 인출 증거를 제출하는 공격자를 막을 수 있습니다. 공격자가 한도를 초과하여 자금을 인출하려고 하여 더 많은 자금이 잠기(locked)는 경우에, 플라즈마 체인을 공격한 사람은 그들의 예치금을 잃게 됩니다.

3. 어떠한 부모 체인이든 트랜잭션을 전파할 수 있는 자식 체인을 생성 가능
   이런 이유로, 네트워크상의 참여자들은 자식 체인에 거래를 제출하기를 원할 것입니다. 이는 루트 블록체인에서 높은 거래 수수료를 지불할 필요 없이 작은 자금의 전송이 가능해지므로 경제적 효율을 창출합니다. 따라서 사람들은 상당한 가치의 자식 체인을 만들어 내도록 장려됩니다. 그러나 근본적인 블록체인 트랜잭션 수수료에 포함되지 않는 매우 적은 잔액을 가지는 개인에 대한 체인 선택과 관련하여 평판에 대한 약간의 가정이 있지만, 이는 깊이 중첩된 체인을 통해 완화됩니다. 이 보안 모델은 플라즈마 체인의 주요사항입니다.

관련연구

일부 관련 프로젝트에서는 계산의 증거를 계산하는 것을 축소하는 것으로 머클트리를 제안한다. 하지만, 이 제안은 주로 데이터 가용성에 관한 것이며, 경제적으로 인센티브를 받는 그룹을 통해 이를 관리하는 프로토콜이 있는 사기 입증에 대한 것이다. 다른 관련 프로젝트에서는 child blockchain 시스템을 제안하지만 접근 방식에 있어서는 상당한 차이가 있다. 플라즈마는 child chain을 증명하기 위해 merkleized proof를 사용한다.

트루빗(TrueBit)

플라즈마는 TrueBit와 마찬가지로 사기 증거에 의존하게 될 것이다. 사기 입증 구조는 TrueBit와 유사하며, TrueBit는 플라즈마에 직접적으로 적용될 수 있고, 특히 상태 전이(state transition)의 머클 증명은 더욱 그러하다. TrueBit설계는 플라즈마에 필요한 Ethereum 블록체인에 제출하기 위한 증명을 하게하므로 , TrueBit 문서 및 팀에 의해 이루어진 거의 모든 heavy lifting은 이 설계에 직접 적용 가능하다. merkized 증명을 생성하는 Verification Game의 사용은 계산 규모를 줄임으로써 증가 된 이점을 제공합니다. TrueBit과 유사한 가정과 같이, 계산 상태가 온라인으로 계산 가능하고 브로드캐스팅 가능해야한다. (대용량 데이터는 여러개로 분할되어야 함) 데이터 가용성 문제를 완화해야하며 실패를 공개해야 한다. 우리는 이러한 문제, 특히 후자의 문제를 완화하려고 시도한다. TrueBit에 플라즈마가 만드려고 시도하는 주요 특징은 서로 데이터를 공유하고 있는 상태(shared state)에서 계산해야 하는 복수 당사자의 개념이다. 예를 들어, 일련의 참여자들은 데이터 및 계산의 일부에 대해서만 관심이 있으며, 자신과 관련된 측면만 계산하면 된다. 또한 우리는 오프 체인을 통해 컴퓨터를 이용한 enforcement of computational rounds를 완화하려고 한다.

블록체인 샤딩

플라즈마는 TrueBit와 마찬가지로 사기 증거에 의존하게 될 것이다. 사기 입증 구조는 TrueBit와 유사하며, TrueBit는 플라즈마에 직접적으로 적용될 수 있고, 특히 상태 전이(state transition)의 머클 증명은 더욱 그러하다. TrueBit설계는 플라즈마에 필요한 Ethereum 블록체인에 제출하기 위한 증명을 하게하므로 , TrueBit 문서 및 팀에 의해 이루어진 거의 모든 heavy lifting은 이 설계에 직접 적용 가능하다. merkized 증명을 생성하는 Verification Game의 사용은 계산 규모를 줄임으로써 증가 된 이점을 제공합니다. TrueBit과 유사한 가정과 같이, 계산 상태가 온라인으로 계산 가능하고 브로드캐스팅 가능해야한다. (대용량 데이터는 여러개로 분할되어야 함) 데이터 가용성 문제를 완화해야하며 실패를 공개해야 한다. 우리는 이러한 문제, 특히 후자의 문제를 완화하려고 시도한다. TrueBit에 플라즈마가 만드려고 시도하는 주요 특징은 서로 데이터를 공유하고 있는 상태(shared state)에서 계산해야 하는 복수 당사자의 개념이다. 예를 들어, 일련의 참여자들은 데이터 및 계산의 일부에 대해서만 관심이 있으며, 자신과 관련된 측면만 계산하면 된다. 또한 우리는 오프 체인을 통해 컴퓨터를 이용한 enforcement of computational rounds를 완화하려고 한다.

연합 사이드체인

플라즈마는 연합된 사이드체인이 아니며 연합된 정당한 활동을 위해 의지하지 않고 또한 신뢰할 수 있는 행위자에게 체인 내부의 상태를 강화하도록 전적으로 의존하지 않는다. 플라즈마는 원장 상태를 다른 블록체인으로 구체화하여 동일한 코인/토큰을 사용할 수 있도록 허용하지만 사기 증명이 가능한지 여부를 검증하는 것은 가능하다. 플라즈마는 강력한 행위자 연합에 의존하지 않으며, 이러한 행위자의 정확성에 상당한 인수 위험이 따르므로, Federated-Pegged Sidechain이 아니다. Drivechains는 유효성 증명자(validatorP를 알 수없는 경우를 제외하고 연합된 sidechains와 유사하다.

결합마이닝된 블록체인(Merge-Mined Blockchain)

네임코인은 부모 블록체인과 동시적인 블록을 생성한다. 이는 블록체인의 전체 유효성 검사를 가정하므로 확장성 이점을 제공하지 않는다. 확장 블록은 기본 블록체인과 병합 채광 체인 사이에서 자금 이동을 허용하는 병합 채광 체인의 예시이다 (루트 체인에 대한 합의 규칙으로 채굴자 전체 집합의 집행 메커니즘 사용). 병합 채굴 체인은 새로운 합의 규칙을 허용하고 사용자 선거를 통해 자신이 염려하는 체인 만 유효성을 검사 할 수 있지만, 채굴자/ 유효성 검사자는 모든 항목의 유효성을 검사해야한다. 플라즈마의 목표는 사용자와 채굴자만이 관련 체인을 검증해야한다는 것이다.

트리체인

Treechains는 Proof of Work를 사용하여 자식 블록에서 유효성이 검증 된 트리 구조 블록체인을 제안한다. 루트 체인은 모든 하위 블록체인의 작업 증명을 합산 한 것이다. 스택을 낮추면 보안 수준은 높아지지만 스택을 따라 높을수록 유효성 검사 및 작업 수준에 따라 다를 수도 있다. 트리 체인의 토폴로지는 트리 구조에 있지만 그 구조는 분기를 통해 합산되는 채굴 보안에 따라 달라진다. 보안 모델은 작업 기록에 의해 보호되므로 가지의 보안이 낮다. 플라즈마는 루트에서 보안이 완벽하게 수행 된 채굴과는 반대로 루트에서 보안 및 증명이 함께 수행된다. 비슷한 작업은 나무 형성에서 보이는 블록의 증명을 만드는 데 있다.

영지식증명(zk-SNARK 및 zk-STARK)

비대화 형 (non-interactive) 계산 증명은 스케일 러블 컴퓨팅에서 상당한 이점을 가질 수 있도록 한다. zk-SNARKs/STARKs 및 기타 형식의 비대화 형 최소 증명은 Plasma에 최적이다. merklized 계산의 결과와 함께 증명을 제공 할 수 있다. 또한 어린이 혈장 체인에 작은 균형을 유지할 때 전신 공격을 줄이는 이점이 있다. MapReduce 기능에 대한 SNARKs에 대한 연구가 이미 있었으며, 이 연구가 도움이 되기를 바란다. Plasma는 블록체인 집합 내에서 주문을 하고 시행 할 수 있도록 해서 확장한다. 그 밖의 이점으로는 체인 자체의 빠른 동기화 및 확인을 허용하는 계산 증명이 있다. zk-SNARK는 데이터 가용성 문제를 해결하지 못하고 단지 데이터 요구량과 계산량을 줄여준다. 이는 특히 assert/challenge time-based mechanism을 대체하거나 보완하는데 유용하다. zk-SNARK는 심층적인 방어로 유용 할 수 있다. 마지막 방어선이 적합한 암호화 없이 블록체인을 사용하는 경우 두 번째 방어선은 zk-SNARK가 될 수 있으며 첫 번째 방어선은 신뢰할 수 있는 컴퓨팅 하드웨어이다. Withdrawals from Plasma chains는 아주 작은 균형을 위해 이동되는 비트맵을 선택적으로 필요로 하지 않는 이점을 제공하는 zk-SNARK에 의해 확보 될 수 있다.

코스모스와 텐더민트

Cosmos는 코스모스 "Hub"에 블록체인을 마련하고 스테이크 시스템의 증거를 통해 입증 된 "Zones(child blockchains)"을 가지고 있다. child blockchains 건설과 상당한 유사성이 있지만 Plasma는 child blockchains의 상태를 강요하기 위한 건설사기 증명에 의존하며, 많은 체인에 적용 할 수 있도록 일반화되어있다. Cosmos의 지분 건설 증명은 Cosmos Zones의 유효성 검사기를 포함하여 2/3의 정확한 유효성 검사기를 가정한다.

포카닷

Polkadot은 또한 블록체인의 계층 구조를 구성한다. 폴카 도트의 디자인과 약간의 유사성이 있다. 블록 정확성을 보장하는 " fishermen " 유효성 검사기를 포함함 구조 대신, Merkle 증명을 통해 상태를 시행하는 일련의 하위 블록체인을 구성한다. Polkadot 구조는 자식 블록 체인 상태와 fishermen에 의해 시행되는 정보 가용성에 의존한다.

루미노

Lumino는 블록 체인에서 압축 된 업데이트를 사용하는 EVM 계약을 위한 설계이다. 이를 통해 참가자는 최소한의 커밋 된 상태 만 업데이트 할 수 있다. Plasma의 출력 관리 설계는 특정 출력을 나타내는 단 하나의 비트만으로 작업을 수행한다. 이로 인해 자식 Plasma chain에 문제발생시 신속하고 저렴한 비용의 조정과 철수가 가능하다.

다중 오프체인 상태

플라즈마의 주 목적은 사용자들이 블록체인의 순수 코인/토큰 자금을 유효한 온-체인상태가 아니더라도 유지할 수 있는 방법을 만드는 것입니다. 플라즈마는 on-chain과 off-chain의 경계를 허물기 시작 했습니다 (예. On-chain이나 off-chain의 부분이 될 수 있다?).

Off-blockchain 다중(multiparty) 채널의 확립에는 두 가지 일반적인 문제가 있습니다. 첫 번째는 시스템에 업데이트가 필요할 경우 사용자 간에 동기화 상태의 업데이트 (또는 국제 규모의 거래 업데이트의 경우)가 필요하며 온라인 상태가 되어야 합니다. 두 번째는 추가되거나 제외되는 모든 참가자들을 나열할 수 있는 채널 내 참가자의 추가 여부를 업데이트 하는 거대한 온-체인을 필요로 한다는 것입니다.

많은 사용자들의 추가나 제외가 유효한 루트 체인 상태의 업데이트 없이 가능한 메커니즘의 개발이 바람직할 것이며, 이로 인해 모든 사용자들의 참여 없이도 내부 상태의 업데이트가 가능하고 그들은 오직 그들의 잔고가 조정되었을 때나 Byzantine 행동이 감지되었을 때에만 참가하면 됩니다.

일반적인 구성은 루트 체인(예: 이더리움)의 스마트 컨트랙트에 표시되고 잔고 유지가 허용되는 자식 블록체인입니다. 스마트 컨트랙에서 잔고는 하위 플라즈마 체인에서 마지막 블록의 잔고에 표시되고 할당됩니다. 이로 인하여 사용자는 잔고를 보여주는 루트 체인의 자식 체인에서 실제 화폐를 가질 수 있게 되고 이것은 조정 기간 후에 출금이 가능해집니다.

이를 가능하게하기 위하여, 거래 장부 용도의 목적으로 UTXO (사용되지 않은 트랜잭션 아웃풋) 모델을 만들었습니다. 이는 꼭 필요한 요구사항은 아니지만, 빠른 출금을 가능하게하기 위한 이유로 사용됩니다. UTXO 모델의 기본은 트랜잭션이 사용되었는지 아닌지와 같은 어떤 특정한 상황의 발생 여부를 간략하게 보여 주기 위함입니다. 이는 머클화된 증명을 위해 표현되며, 비트맵의 형태로 다른 사용자에 의해 간단한 분석을 가능하게 합니다. 즉 스마트 컨트랙트는 루트 체인에 계좌를 가지고 있지만, 플라즈마 체인은 루트 체인 계좌에 보관된 잔고의 배분을 위한 잔고의 UTXO 세트를 유지합니다. 어떤 상태 변화에 대하여 유효한 필요조건이 없는 자식 체인을 위하여, 이 시스템은 복잡하거나 빈번한 상태 변화가 있는 계좌 모델에 적용될 가능성을 가지고 있지만, 상위 주요 블록체인(들)에 블록 공간을 필요로 하게 됩니다.

현재는 하위 플라즈마 체인의 블록을 선택하는 단일 블록 리더를 생각해 볼 수 있습니다. 이러한 개념은 지분증명(Proof of Stake) 세트 또는 미리 정해진 n-of-m 검사자(n-of-m validators)라고 이름 지어진 시스템으로 구현 가능합니다. 하지만, 이 시스템들로는 간결함을 위하여 단일 검사자를 사용했습니다. 검사자의 기능은 트랜잭션을 정렬하는 역할을 하여 블록을 만드는 것입니다. 검사자/제안자는 주 블록체인 계약에 생성되어 있는 위조 증명 기능에 의하여 제한됩니다. 만약 유효하지 않은 상태의 블록을 생성하면, 이 블록을 받는 다른 사용자는 상위 블록체인에서 merkleized 위조 증명 방식을 이용할 수 있으며, 유효하지 않은 블록은 벌칙과 함께 되돌려집니다.

블록들은 잔고를 가지고 있거나 각자의 플라즈마 체인에서 계산/시행을 원하는 사용자를 포함하여 블록 관찰을 원하는 사용자들에게 배포됩니다.

오프 체인 상태에서 잔고를 유지하는 데에는 복잡함이 최소화되지만, 상태 변화나 출금의 경우 굉장히 복잡한 현상이 생기게 됩니다.

위조증명

이 자식 블록체인 안에 있는 모든 상태들은 위조 증명 방식을 통하여 시행되는데, 이는 누구나 블록 데이터 유효성을 근거로 유효하지 않은 블록들에 대한 위조 증명을 할 수 있게 합니다.

하지만, 이 구조 방식에서 가장 큰 어려움은 데이터/블록 유효성에 관하여 확실한 증명 방식이 없다는 것입니다.

루트 블록체인(예. 이더리움)에는, 블록 데이터가 유효할 때 모든 상태 변화가 유효함을 입증하는 위조 증명 시스템들이 있습니다. 복잡한 계산 과정을 위해, 상태 변화는 효과적인 검증을 위해 반드시 merkleized 방식을 이용해야 합니다.

추가적으로, 상태 변화는 부당한 방법으로 종료하는 것을 방지하는 zk-SNARKs/STARKs을 통하여도 시행됩니다. Zk-SNARKs 구조는 효과의 극대화를 위하여 SNARKs 반복적으로 필요할 수도 있으며, 그 가능성을 위해 조금 더 심도 있는 연구가 필요할 것입니다. 하지만, 현재 시스템은 SNARKs 없이 작동할 수 있도록 설계되어 있습니다.

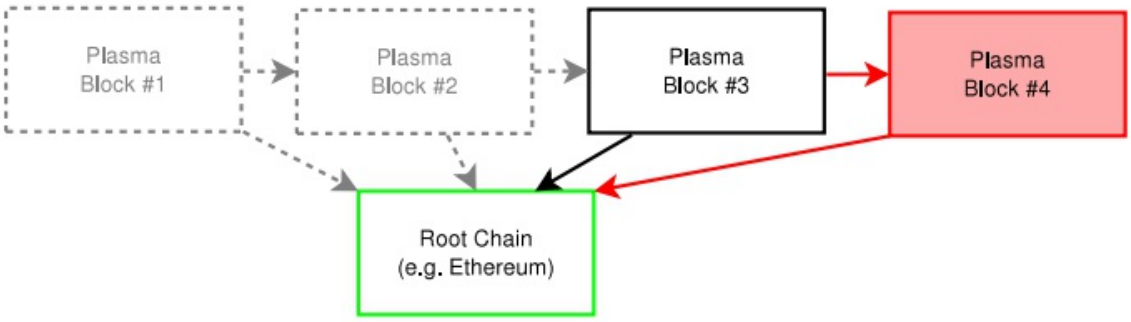

그림 10: 모든 사람은 1-4개의 블록들에 블록 데이터를 가지고 있습니다. 블록 4에 커밋된 상태변화는 블록 4에 할당된 merkleized 방식이나 이전 블록의 데이터를 통하여 부정행위를 입증할 수 있습니다.

위조 증명은 모든 상태 변화이 유효하다는 것을 보장합니다. 위조 증명 방식들의 예는 지출 거래의 증명 (현재UTXO에 가능한 잔고), 상태 변화의 증명 (사용 가능한 잔고를 위한 서명 확인 포함), 블록들 간의 포함/제외 증명, 그리고 입금/출금에 관한 증명 들이 있습니다. 일부 조금 더 복잡한 증명 방식은 상호작용을 필요로 합니다. 일반적인 구조는 블록 검증에 기능적인 접근 방식을 취합니다. 이 합의 메커니즘이 솔리티디로 견고하게 프로그램 되었다면, 블록의 머클 증명 기능 당 추가적인 입력 방식이 검증되어야 할 것이며, 결과 값은 검증 값의 유효여부를 리턴하게 됩니다. 그 후 일치하는 합의 검증 코드를 간결한 merkleized 증명 양식에서 처리 가능하도록 간단하게 복제합니다 (위조 증명을 전체 블록에서 처리할 필요가 없게 하도록).

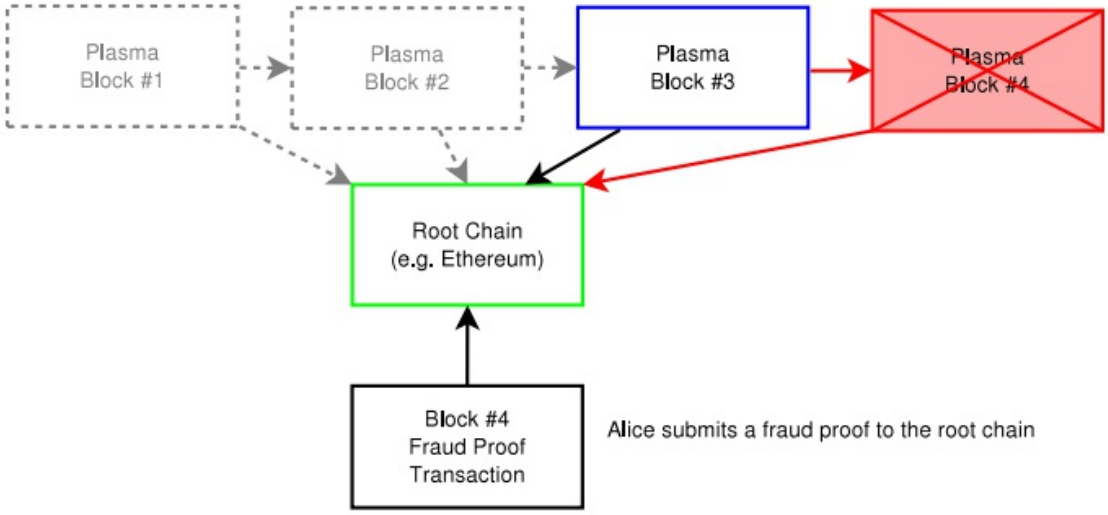

그림 11: 앨리스는 위조 증명을 루트 체인에 제출하기 위하여, 모든 블록의 데이터를 복사합니다. 블록 4가 유효하지 않다고 판단되어 롤백 됩니다. 블록 4의 제출자는 스마트 컨트랙트의 채권을 상실하였으므로 패널티를 받게 됩니다. 현재 블록은 3 (파랑색)이 됩니다. 일정 시간 경과 후, 블록은 확정되며 위조 증명은 제출할 필요가 없게 됩니다. 부정행위가 증명되지 않은 완벽하게 검증된 블록으로만 블록 구조를 만들어야 합니다.

최소한의 증명만 갖는 이러한 구조를 위하여, 모든 블록들은 현재 상태의 merkleized 트리, 지출된 아웃풋의 트리, 거래의 머클 트리, 그리고 바로 전 상태의 변경에 관한 내용 증명을 제공해야 합니다.

위조 증명은 일종의 연합한 사용자들이 패널티없이 부정적인 블록을 만들지 못하도록 보장해준다. 부정적 블록이 감지되고 루트 블록체인 (또는 부모 플라즈마 체인)에서 검증이 될 경우에는, 그 유효하지 않은 블록은 롤백됩니다. 이는 federated-peg 비트코인 사이드체인에 상태 변화의 취약점을 해결하는 비잔틴 행동에 대항하는 각각의 참가자들에게 보상을 줌으로서 이러한 행동을 장려합니다.

그 결과로는 블록 데이터에 접근이 가능한 관측자들이 무효한 상태 변화를 증명할 수 있는 기회를 제공함과 동시에 높은 확장 가능 상태 변화가 플라즈마 블록체인에서 가능해 진다는 것이다. 즉, 주 루트 체인에서 정기적인 약속만으로 하위 체인에서도 입출금이 가능해 진다는 것이다.

입금(deposit)

루트 체인으로부터의 입금은 마스터 컨트랙트로 직접 보내어집니다. 계약(들)은 현재 상태에 대한 의무, 위조 증명으로 인한 무효화에 관한 패널티, 그리고 출금 절차에 관한 추적을 할 의무가 있습니다. 자식 플라즈마 체인은 루트 블록체인의 완벽한 검증자 이므로, 입금 절차는 반드시 이중 잠금 장치를 이용하여 처리되어야 합니다.

입금 절차는 목적지인 자식 체인을 명확하게 하기 위하여 목적지 체인의 블록해시 정보를 반드시 포함하여야 하며, 코인이 복구 불가능하도록 다중 처리 시스템을 이용하여 수행하여야 합니다.

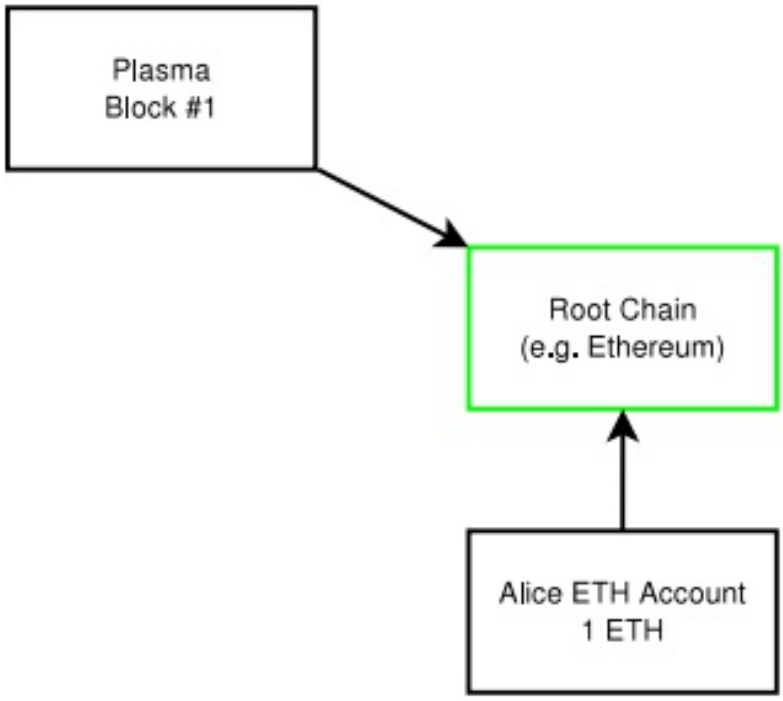

그림 12: 앨리스는 ETH 계좌에 1 ETH를 가지고 있습니다다. 그녀는 1 ETH를 플라즈마 블록체인에 보내기를 원합니다. 그녀는 플라즈마 컨트랙트로 그것을 보냅니다.

1. 코인/토큰 (예, ETH or ERC-20 토큰) 들은 루트 블록체인의 플라즈마 컨트랙트로 보내어집니다. 코인은 일정 시간 동안에는 challenge/response를 위하여 복구가 가능합니다.

2. 플라즈마 블록체인은 입금 거래의 증명 정보를 포함합니다. 이 때, 플라즈마 블록체인은 트랜잭션이 입력되었으며 lock-in 트랜잭션 또는 입금자로부터 처음 사용 이벤트가 일어난 후에 코인이 사용 가능하다는 사실을 인식하게 됩니다. 이 절차가 수행 될 때에, 블록체인은 인출 절차를 허가되었다는 사실을 확인하게 됩니다. 하지만, 이 때는 예금자가 위조 증명을 만들어 낼 수 있는 충분한 정보를 가지고 있다는 확신이 없으며, 그러므로 아직 예금자는 책임이 없습니다. 이 블록은 상태 트리 구조, 비트맵, 트랜잭션 트리 구조에 추가적인 요소를 포함하고 있으므로, 간략한 수정 증명 방식이 포함되어 있습니다.

3. 예금자는 2단계에 체인의 약속을 봤다는 내용을 포함하는 트랜잭션을 활성화시키며, 자식 플라스마 블록체인의 트랜잭션에 사인을 합니다. 이 단계에서의 의무는 예금자가 잔고를 인출할 수 있는 충분한 정보를 가지고 있다고 증명하는 것입니다.

이 절차 후, 체인은 거래자들이 이 코인들을 취급하며 인출이 간단하게 증명될 수 있도록 할당해 준다는 내용으로 약속하게 됩니다. 제 3단계에서는 사용자가 인출할 수 있다는 정보를 증명하게 됩니다.

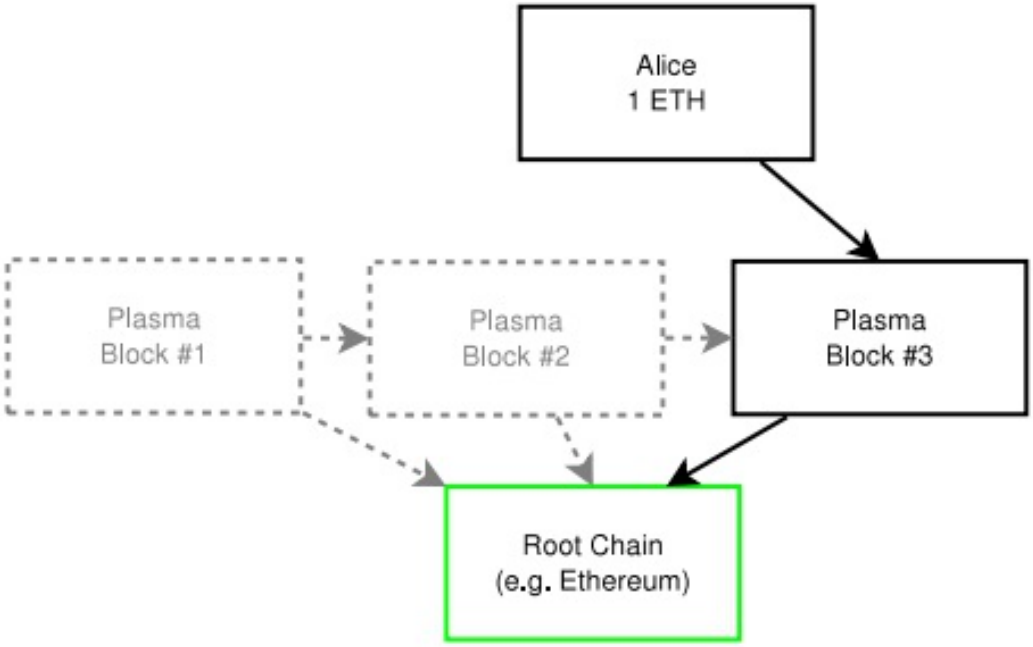

그림 13: 앨리스는 이제 플라즈마 블록에 1ETH를 가지게 되었습니다. 그녀는 자금을 확인하였고 블록이 locked-in 되었음을 확인한 것입니다. 자금이 루트 체인의 스마트 컨트랙트에 유지되고 있으나, 이 특정 플라즈마 블록체인(상태 변화, 예 : 다른 사용자나 스마트 컨트랙트로 이체하는 것)에서 장부 기록은 루트 블록체인의 비용을 들이지 않고 생성될 수 있습니다.

예금자가 제 3단계를 거치지 않을 경우에도, 예금자가 루트 블록체인에서 인출을 시도할 수 있습니다. 예금자는 확인되지 않은 인출을 요구하게 되는 것이며, 플라즈마 블록체인의 잔고가 잠겨 있으며 예금자가 승인을 했다는 위조 증명을 네트워크상의 다른 사람이 확인 할 수 있을 때까지 긴 시간동안 기다려야 합니다. 특별한 부정행위의 증거가 발견되지 않는다면 예금자는 미확인 된 잔고를 인출할 수 있게 됩니다. 이 인출 방식은 비-비잔틴 행동을 위하여 어마어마한 양의 루트 체인 연결을 필요로 하게 됩니다.

거액 인출과 비트맵 방식의 상태

이 시스템의 주요 쟁점은 상태의 검증이 불가능하다는 것입니다.

상태 트랙잭션의 간결화를 최대화 할 수 있도록 하기 위하여, 아웃풋은 선택적으로 비트맵 방식으로 표현될 수도 있습니다. 이는 루트 체인에서 막대한 비용이 발생 할 수 있는 인출 증명을 위하여 필요한 절차입니다. 이 구조의 목적은 플라즈마 체인에서 소액의 잔고를 유지할 수 있게 해줍니다. 이러한 소액 잔고들은 루트 블록체인의 계약에 예약되어 유지되지만, 완벽한 거래 장부는 블록체인에 저장되지는 않습니다. 완화되어야 할 주요 공격은 타당하지 않은 블록(루트 체인에 연결된)에 보유됩니다. 시스템이 타당하지 않은 상태 변화를 감지할 경우에는 사용자들이 대량으로 종료(exit)하게 됩니다.

비트맵 구조에서 인출은 종료 하고자하는 서명된 거래의 비트맵을 포함합니다. 정보의 정확성을 위하여 스마트 컨트랙트에 의하여 수행되는 게임/프로토콜 구조가 만들어졌습니다. 비트맵 방식은 사용자들이 어떤 아웃풋이 사용 될지 추론할 수 있도록 보장해줍니다.

이 방식은 비트맵을 사용하므로, 소규모 잔액의 효능을 최대화하기 위하여 사용되지 않은 거래 결과 데이터 구조 (UTXO)에 상태가 표시 되는 것을 필요로 하게 됩니다. 사용된 상태는 간결하게 증명될 수 있으며, 대량의 상태 변화 세트는 명확하게 실행됩니다. 미리 정해진 합의 기간 후에 비트들은 재사용 될 수 있습니다.

높은 보장은 비용이 비싸고 낮은 보장은 저렴한 차이가 있습니다. :

1. 루트 블록체인의 장부 상태
2. 플라즈마의 장부 상태, 온-체인 단일 거래 실행으로 경제적으로 실행 할 수 있음

3. 플라즈마의 장부 상태, 비트맵을 이용하여(1-2 비트 비용으로) 경제적으로 실행 할 수 있음
4. 플라즈마의 장부 상태, 루트 블록체인의 비트맵을 이용한 경제적으로 실행 불가능함. 1-2 비트 대량 인출의 비용이 너무 높은 경우.

루트 체인에서 실행할 수 있는 잔고를 가지고 있는 사용자들은 UTXO 비트맵 방식의 포맷을 반드시 실행할 필요가 없습니다. 하지만 루트 블록체인에서 1-2 비트 트랜잭션 비용이 충분히 낮을 경우에만 실행이 가능합니다.

4번째 타입의 경우에도 (대량 인출을 위한 1-2비트 온 체인 비용이 너무 높은 경우), 시스템은 회복할 수 있게 디자인 되었다 (알려진 엔터티가 안정적일 것이라는 가정 하에). 이 문서의 후반부에는 대량 인출을 경제적으로 실행할 수 있는 많은 공간을 만들 수 있는 블록체인의 계층 구조를 설명할 것이다. 추가적으로, 4번째 타입에서 거래의 총 가치가 현저하게 토큰의 가치보다 작을 경우 잔고를 공격 하는 데에 너무 큰 비용이 이론적으로 발생하게 되어 토큰 소지자들은 명성에 피해를 입게 될 것이다.

상태변화

기본적으로, 플라즈마 체인의 상태 변화는 입금절차와 같이 비슷한 다단계 절차로 운영됩니다. 이는 사용자가 상태 변화를 제공할 수 있도록 정보를 얻을 수 있게 합니다. 그러나 입금 구조와는 달리 거래가 승인되고 블록에 포함이 되면, 참가를 해야만 한다는 약속을 하게 됩니다. 이러한 이유 때문에, 상태 변화는 서명, 상태 업데이트 (예, 목적지, 수량, 토큰, 그리고 다른 관련된 상태 데이터), 그리고 만료를 위한 일종의 TTL과 특정 블록에 약속 등을 포함하여야 합니다. 이 TTL은 절대적으로 필요한 것은 아니지만, 역방향 종료 조건을 알 수 있는 종료 증명(exit proofs) 구조 시스템을 만들기 위하여 시간과 연계되어야 합니다. 물론, 이미 증명된 거래는 TTL을 포함할 필요가 없습니다. 재배치와 관련된 인출에 관한 liveness 추정은 이미 있었으며, 약한 liveness 가정은 이 구조와 함께 가정됩니다. 블록의 계약은 플라즈마 체인에서의 거래가 그 시점에서 관찰되며, 증명과정이 실행되며, 최종 결과물의 사용이 이루어지는 블록 다음에 위치되는 것이 알려진 소비자에 의하여 연계됩니다.

빠른 최종 승인을 위한 multi-phase 계약은 다음과 같이 이루어집니다:

1. 앨리스는 플라즈마 체인에 있는 그녀의 아웃풋에서 같은 플라즈마 체인의 밥에게로 보내고자 합니다.(블록체인에 자세한 트랜잭션 기록의 제출 없이) 그녀는 플라즈마 체인에 그녀의 아웃풋 중 하나를 사용하고자 하는 거래내용을 생성하고, 승인하며, 그리고 거래를 브로드캐스트합니다.

2. 플라즈마 체인의 검증자에 의하여 이 거래는 블록에 포함됩니다. 데이터의 헤더는 루트 블록체인이나 부모 플라즈마 체인에 블록의 형태로 포함되며, 최종적으로 루트 블록체인에 연계되고 보증됩니다.

3. 앨리스와 밥은 밥이 거래내용과 블록을 확인했다는 승인과 거래내용을 확인합니다. 이 확인 사실은 서명되며 다른 플라즈마 블록에 포합 됩니다.

느린 최종 승인 절차에서는 첫번째 과정만 발생합니다.

승인이 일어난 후, 그 거래는 최종승인(finalized) 된 것으로 간주된다. 3번째 과정이 존재하는 이유는 사용자들(앨리스와 밥)이 유효한 블록을 확인하는 것을 보장하기 위해서입니다. 이 3번째 과정은 필요한 절차는 아니지만, 최종 승인까지 엄청난 지체 현상이 발생합니다. 트랜잭션과 관련된 모든 사용자들에 의하여 블록의 검증과 정보의 유효성이 최종 승인이 날 때까지 트랜잭션은 보여져서는 안 된다는 근거를 따릅니다.

첫 번째 과정 후 블록이 보류되는 경우 앨리스는 그녀의 트랜잭션 사용여부를 확인하기 어렵습니다. 거래가 블록에 포함되고 (거래가 보류되던 아니던), 3단계가 완료되지 않았을 경우 미확인(unconfirmed)되었다고 간주됩니다. 그러므로 앨리스는 블록의 최종승인(finalized) 전에 루트/블록체인에 제공된 그녀의 인출 메세지를 승인하지 않았다면, 잔고의 인출이 가능합니다. 블록의 최종 승인 후에는 앨리스는 잔고의 인출이 불가능해지며, 블록은 밥에게 전송되었다고 가정 됩니다. 블록이 최종 승인 전에 (첫번째와 두번째 과정 사이) 보류된다면, 앨리스와 밥은 이 상황을 확인할 수 있으며 앨리스는 미 승인된 잔고를 인출할 수 있습니다. 블록들이 2번째 과정 후와 3번째 과정 전 단계에서 보류가 된다면, 밥은 잔고의 인출에 관한 충분한 정보를 가지고 있다고 추정할 수 있습니다. 하지만, 앨리스와 밥 모두 지급에 관한 관계가 없기 때문에, 이론적으로 두 사용자들이 자금을 주장 할 수 있는 정보의 유효성에 따라서 완료되지 않은 상태로 취급됩니다. 두 사용자가 3번째 단계를 승인할 경우에는 최종 승인이 이루어 진 것으로 여겨집니다. 특히 서명이 온-체인에서 입증할 수 있게 관찰될 때에

는 이 단계가 완료된 후에 Pay-to-contract-hash의 시행이 일어납니다. 만약 한 사용자가 승인을 거절하거나 블록이 보류가 되면, 상환 증명을 위한 조건부 상태가 됩니다. 모든 상태들은 결국 머클 증명방식을 통하여 체인에 연계되므로, 최종 승인 후 지급 관련 실행이 입증되고 이행 되는 것과 같이 pay-to-contract-hash에 관한 의존도가 약해집니다.

제 3단계 절차에서는 두 사용자의 서명 대신에 스마트 컨트랙트에 따라 조건부 상태가 되는 것을 인지하여야 합니다. 예 : HTLC 원상 공개에 따른 조건부 상태. 이는 멀티-체인이나 멀티-트랜잭션 축소를 가능하게 합니다. 이러한 기능을 사용하기 원한다면, 컨트랙트를 만드는 과정이 복잡해질 수 있으며, 높은 수준의 프로그래밍 과정이 필요할 수 있습니다.

루트 체인에 주기적인 이행

플라즈마 체인은 블록체인의 정렬을 할 수 있어야 합니다. 플라즈마 체인에는 블록 안에 정렬 절차가 있기는 하지만 그 블록들은 검증되지 않았고 자체적으로 정렬이 불가능합니다. 그래서 루트 블록체인에서의 약속이 필요한 것입니다. 플라즈마 체인은 그 블록 헤더를 루트 체인에 공개하고 그 헤더는 위조 증명 방식에 의하여 시행 됩니다. 만약 부정한 헤더가 유효한 데이터와 함께 공개가 되면, 다른 사용자가 위조 증명과 약정을 공개할 수 있으며 그 블록은 공개자에게 패널티를 부여하고 블록을 롤백 시킵니다.

이 약속은 후에 실제 주문에 애매한 절차가 없게 만들어 줍니다. 애매한 절차가 생기게 되면, 충분한 위조 증명 정보가 공개되며 패널티가 주어집니다. 일정 시간 후 블록이 최종 승인되며, 그 결과 루트 블록체인에서 제공하던 재-주문이 불가능해지며, 마무리 되게 됩니다.

인출

플라즈마 시스템은 순수 코인이나 토큰(예, ETH와 ERC-20 토큰)의 입금을 블록체인을 이용하지 않고도 가능하게 해준다. 그리고 루트 블록체인에 의하여 실행되는 플라즈마 블록체인 내의 상태 변화는 유효한 정보를 제공하게 된다. 유효한 정보의 제공이 불가능 할 경우에는 플라즈마 체인에서 대거 퇴장을 필요로 하게 된다. 마지막으로, 플라즈마 체인에서 간단하게 자산의 인출을 가능하게 해준다. 하지만, 보통 절차에서 주로 간단한 인출절차가 이용된다.

단순 인출

간단한 인출 절차는 사용자가 루트 블록체인에 연계된 자산을 인출만 할 수 있게 해 주며 최종적으로는 플라즈마 체인에서 승인된다.

이 문서에서 입금 시스템, 장부 표현 방식, 그리고 상태 변화 디자인은 서술 되었다. 지금까지의 단계에서, 부정행위 증명을 제외하고, 현재 플라즈마 체인의 장부 상태를 루트 체인에 공개한 경우는 없었다. 그럼에도 불구하고 인출 절차에서는 자금이 플라즈마 체인에 유지되고 있으며 출금 가능한 것을 증명할 특별한 검증 절차가 필요하다.

인출 절차는 코인을 루트 체인과 하위 플라즈마 체인에서 대체할 수 있는 절차를 보장해야 하는 가장 중요한 프로세스다. 사용자가 플라즈마 체인에 입금을 할 수 있다면, 상태 변화 (예, 코인의 다른 사용자에게 이전)가 이루어지며, 다른 사용자들은 그 자산을 인출할 수 있게 되며, 코인의 가치는 루트 체인에서 정해진다. 어떤 경우에는, 보안이 루트 체인에 속해 있고, 많은 거래 능력을 가지고 있는 플라즈마 내의 자금이 조금 더 유용할 수 있다.

간단한 인출절차에서는 모든 자산들이 대규모로 연결되어 있어야 하며, 모든 인출 요청은 부정행위 증명 방식과 연결되어야 한다. 현재의 블록 데이터가 유효하다면 제 3자가 플라즈마 블록체인이 사용 가능하며 인출 정보가 검증되었다는 정보를 적은 비용으로 제공할 수 있다.

플라즈마 체인의 모든 사용자들은 특정 계좌에 인출 절차가 진행되고 있지 않음을 업데이트를 통하여 모든 상위 플라즈마 체인들과 루트 블록체인을 검증해야만 한다. 인출이 진행 중인 경우, 그 다음의 블록의 코인/토큰은 사용 불가능 하며, byzantine 행동은 합의를 위반하는 것이며, 부정행위 증명이 되며, 벌칙이 주어지고, 루트 블록체인에서 플라즈마 계약당 블록의 전환이 이루어진다.

인출은 다음과 같은 단계로 이루어진다;

1. 인증된 인출 거래는 루트 블록체인이나 상위 플라즈마 체인에 제출된다. 인출 금액은 전체 결과물과 같아야 한다 (일부 인출 불가). 여러 개의 결과물을 인출할 수 있지만, 모든 인출은 같은 플라즈마 체인에 속해 있어야 한다. 인출의 한 과정으로서 결과물의 비트맵은 공개되어야 한다. 인출 과정의 한 부분으로서 추가적인 연결이 부정적인 인출 요청에 대한 벌칙을 위하여 수립되어야 한다.

2. 거래의 항의를 이하여 미리 정해진 일정 기간의 시간이 존재한다. 이는 Lightning Network 의 거래 항의 시스템과 유사하다. 이 경우, 사용자가 체인의 결과물이 인출을 목적으로 이미 사용되었다면 (많은 경우, 루트 블록체인에서), 인출은 취소되고, 인출 요청에 관한 연계는 무효화된다. 사용자가 인지한 이 과정은 항의 할 수 있다. 만약 결과물의 부정 행위 증명을 제공한다면, 연계는 무효화 되고 인출은 취소된다.

3. 낮은 레벨의 블록 인증시스템에서는 다른 인출 요청이 일정시간 보류되는 두 번째의 시간 지체가 있을 수 있다. 이는 특정 플라즈마나 루트 체인에 접수된 인출 요청을 실행하기 위해서다.

4. 플라즈마 스마트 계약에 합의된 항의 조정 기간이 루트 또는 상위 체인에서 부정행위 증명 없이 일정 시간 지나게 되면, 인출은 정확하다고 인정되며, 인출자는 자산을 루트/상위 체인에 인출할 수 있다. 인출 절차는 UTXO/계좌 기간에 의거하여 먼저 요청된 순서대로 처리된다.

플라즈마 체인에서, 경제적으로 실행 가능한 범위에서, 보류된 블록에 인출을 요구하는 경우가 있을 수 있다는 것을 알아야 한다.

부정행위 증명은 사용자가 동일한 결과물에 대하여 네트워크 상에 비교적 쉽게 발견할 수 있는 이중으로 인증된 요청을 증명하였을 경우에만 필요로 하게 된다. Lightning과 다른 채널의 경우, 추가적인 절차가 높은 레벨의 임시적인 절차와 함께 증명되어야 한다. 일반 채널의 경우, 낮은 레벨의 임시적인 인출이 시도되면, 자금은 플라즈마 체인에 유지되며, 정확한 서명과 함께 인출이 가능해진다. 다른 구조적 방식도 가능하지만, 디자인은 플라즈마 체인의 스마트 계약 부정행위 증명 방식을 포함하여야 한다.

일반적인 인출 방식은 느리고 비용이 발생하는 절차이기 때문에, 사용자들은 단일 인출로 합치려고 하거나, Lighting이나 atomic swap을 이용하여 코인을 다른 체인으로 교환하려고 하는 경향이 있다.

빠른 인출

빠른 인출 시스템은 간단한 인출 시스템과 동일한 구조를 가지고 있다. 하지만 자산이 atomic swap으로 운영되는 계약으로 보내어 진다. 교환되는 자산은, 약한 시간적 보류와 플라즈마 체인에 존재하는 높은 시간적 보류와 함께, 루트/상위 체인에 저장되는 자산이다.

빠른 인출을 즉각적으로 실행되는 절차가 아니다. 그러나, 플라즈마 체인이 Byzantine (블록의 보류 포함) 이 아닐 때 거래가 완료되는 시간만큼 인출에 걸리는 시간을 대폭 줄여준다. 이러한 이유때문에, 빠른 인출은 블록이 보류되었을 때에는 이용이 불가능하며, 대신에 느린 대량 인출 요청이 필요하게 된다.

빠른 인출은 다음과 같은 단계로 진행된다:

1. 앨리스는 자금을 인출하여 루트 블록체인으로 시간의 지체 없이 이체 하고자 한다. 그녀는 편한함의 대가로 시간적 가치를 지불하고자 한다. 래리 (유동성 공급자)는 이 같은 서비스를 제공하고자 한다. 앨리스와 래리는 인출을 하고 루트 블록체인에 이체하기 위하여 서로 협동하기로 하였다.

2. 자금은 플라즈마 체인의 특정 결과물 계약에 잠겨 있는 상태이다. 이는 전형적인 이체 과정과 비슷한 형태이며, 두 사용자가 거래를 공표하고, 나중에 플라즈마 블록에서 자신들이 거래내용을 확인했다는 계약을 하게 된다. 이 계약의 조건은 계약이 루트 블록체인에 공개되고 승인이 나게 되면, 지급은 플라즈마 체인으로 이행된다는 내용이다. 거래 내용 증명이 제공되지 않을 경우에는, 앨리스는 자금을 회수할 수 있다. 또한 이러한 절차를 HTLC와 같은 구조적 시스템으로 만들 수 있으며, 앨리스는 원상을 생성하고, 그녀가 자금이 이체되고 유효하다고 판단한 후 공개된다.

3. 위의 플라즈마 블록이 승인되고 래리가 자신이 계약의 조건에 맞게 자금을 회수 할 수 있다고 판단되면, 래리는 특정 금액 (그가 받을 금액은 이 서비스 비용보다 작다)을 앨리스가 지급할 수 있는 온체인 계약을 생성한다.

이 예시에서, 유동성 공급자 래리는 교환 과정을 수락하기 전에 반드시 실제 존재하여야 하며 플라즈마 블록체인을 검증해야만 한다. 래리가 플라즈마 체인을 완벽하게 검증 할 수 없을 경우 (또는 루트 체인에 명시된 스마트 계약의 부정행위 검증 방식에 익숙하지 않을 때), 그는 인출을 실행하면 안된다. 만약 래리가 이 체인에 소속되는 자금을 원하지 않고 대신에 루트 블록체인에 자금을 소속되기를 원한다면, 래리는 선행 인출 절차 완료 후 다른 인출 절차를 실행하던지, 인출 자체를 atomic swap을 이용하여 실행할 수 있다.

많은 경우, 자금이 안정화된 플라즈마 블록체인과 유동성 공급자 간 이체를 할 때에 더 비용적인 효과가 크다. 빠른 완료과정이 가능한 Lightning이나 atomic swap 을 통하여 플라즈마 체인간에 이체가 이루어진다.

이것은 atomic 교차-체인 교환 방식이므로, 앨리스와 래리는 상호간의 자금에 대한 사소한 신뢰를 줄 필요가 없다. 앨리스는 루트/상위 체인에 자금을 소유하고 있으며, 래리는 후에 루트/상위 체인에 모든 접근 권한을 가지게 될 것이다. 루트 블록체인의 non-Byzantine 행동을 마무리하고 적은 비용의 유효한 블록을 제공하게 됨으로써, 래리는 플라즈마 블록체인 자체를 신뢰하지 않더라도 그는 자신의 자금을 받을 수 있다는 확신을 가지게 된다.

적대적 대량 인출

플라즈마 시스템 내에서 적대적 대량 인출 거래가 있을 때, 프로토콜이 필요하지 않으며, 블록이 보류된 상태에서 그 디자인 자체는 비용적으로 안정화 되게 되어 있다. 한 사용자가 플라즈마 체인 내의 계좌 상태를 이용하기 원한다면, 지급 계층구조와 같은 다른 디자인에 의존할 수 있다. 그리고, UTXO 모델이 이 곳에서 사용되지만 이 시스템은 루트체인이 계좌 모델을 이용중일 때에만 작동을 하게 된다는 것을 알아야 한다. 게다가 대량 인출이 필요 없거나 원하지 않을 때, 플라즈마 체인에 자금을 유지할 수 있도록 계좌 모델을 쓰는 것이 가능해지며 단순 인출만 가능해진다 (순차번호 증가와 함께).

플라즈마 디자인의 주요 관심이 부정행위 증명 방지를 위한 사항과 관련되어 있으므로 (데이터 유효성 부족의 다른 영향), 감지된 데이터의 비유효성을 위한 완화 절차가 필요하다. 플라즈마 체인에서 사용자가 블록의 비유효성을 발견하면, 특정 시간 안에 그 블록에서 긴급히 퇴장해야 한다. 만약 정해진 시간 안에 체인에서 퇴장하지 않을 경우에는 Lighting 에서 부정확한 인출을 항의 하지 않는 결과와 같은 것으로 취급된다. 이 메커니즘은 플라즈마 블록체인의 운영을 수정하는 주요 기능이다. 플라즈마는 사용자가 Byzantine 행동을 블록의 보류를 통하여 인지하였을 때, 사용자가 플라즈마 블록체인에서 퇴장해야 한다는 사실에 의존한다. 이것의 주 원리는 블록이 보류되었는지 아닌지를 루트 블록체인에서 감지가 불가능 하다는 것이다 (사용자가 블록을 할당 받지 못한 것을 주장하거나, 플라즈마 체인이 사용자가 블록이 유효한지 거짓인지 확인 과정을 거부하였음을 주장하거나). 그 결과, 비유효한 블록의 주장에 관한 비용은 일반적으로 현재 상태의 온체인을 공개하는 것으로 가정한다 (Lighting 이 하는 것처럼). 하지만 대량의 블록들이나 상태 변화에서는 이 시스템은 엄청나게 큰 비용이 발생하며, 플라즈마는 누가 이 비용을 지불할지에 대한 불확실성 때문에 이 구조 시스템을 사용하지 않는다. 그 대신에, 플라즈마는 사용자가 플라즈마 블록체인이 블록을 적대적으로 보류하고 나중에 상태 변화 실행에 영향이 있을 것이라고 믿고 이 플라즈마 체인에서 다른 곳으로 퇴장을 서두른다고 가정한다.

그러므로, 블록이 유효하지 않을 때에 한하여, 적대적 대량 인출로 정의하고 플라즈마 체인이 적대적이거나 Byzantine되었다고 가정하는 것이다. 대량 퇴장은 플라즈마 체인의 Byzantine 행동이 많은 시간 경과 후에도 개인의 자산에 영향을 주지 않으며 체인을 손상시키지 않는 것을 보장한다.

SNARKs 를 이용한 추가적인 보안 완화시스템이 후에 쓰일 것을 예상할 수 있으나, 구체적인 디자인은 여전히 해결해야 할 문제로 남아 있다. 이 구조 시스템은 인출 절차에 관하여 SNARKs에 의존하지 않으며 루트 블록체인에 관측자의 정기적인 활성화가 있게 된다. 하지만, 플라즈마 체인 내에서 상태 변화가 이루어지게 됨에 따라서, 플라즈마 체인의 정기적인 관측이 없는 곳에서 자금을 횡령하기 위한 적대적인 블록의 보류를 가능하게 하는 공격이나 Byzantine을 최소화 하고 SNARKs 순환 속성으로 보완을 강화하게 된다. 이러한 경우, 상태 변화를 위하여 SNARKs 증명과 인출을 위한 높은 신뢰도의 SNARKs 증거가 필요하게 된다. 그러나 플라즈마의 주요 목적은 사용자가 체인을 관측하는 상태 변화의 행동을 수정하는 SNARKs에 의존하지 않으며, 스마트 계약은 이 메커니즘을 수정하여 암호화하며, 루트 블록체인에서 인출이 가능하게 함에 있다. 이와 유사한 이점들은 Lightning 네트워크에도 존재하는데, 이는 스마트 계약을 지원하는 제 3의 체인에 의하여 반복적인 SNARKs 증거가 제공될 때에만 오프체인 상태를 수정할 수 있다는 것을 확인 시켜준다.

플라즈마 체인은 강한 보안 시스템으로 보호되는데, 첫 단계의 보안으로 요소들/하드웨어를 보호하게 되며, 두번째 단계로 SNARKs/STARKs가 사용되며, 마지막 단계로 온체인에서 상호작용 게임 방식이 사용 된다. 첫 단계의 보안이 실패하면, 두번째 단계의 보안 시스템이 혁신적인 암호시스템으로 보호하고, 마지막 단계의 상호작용 게임방식이 투명하게 공개된다. 이 마지막 보안 시스템이 적용된 플라즈마를 앞부분에서 제안하였다.

대량 인출은 다음과 같은 방식으로 퇴장이 발생하는 상호작용 게임의 작용과 함께 수행된다.

1. 앨리스는 플라즈마 체인에서 대량 인출을 위하여 다른 사용자와 협업하고 있다. 다방면의 대량 퇴장이 한 번에 발생 할 수 있지만, 그들이 인출 기능을 중복 사용할 수는 없다. 만약 그들이 중복 인출을 하였다면, 대량 퇴장은 그들의 잔고를 업데이트 하고 중복 인출을 시도한 사용자에게는 벌칙이 주어진다. 모든 사용자들은 다른 플라즈마 체인에 자금을 보내기 위하여 서로 협업해야 한다.

2. 퇴장 관리자, 패트는 퇴장을 구조화 하고자 한다. 패트는 최종 목적 플라즈마 체인과 협업하여 자금을 보내고, 대량 퇴장이 마무리 되면 새로운 체인에서 유용 가능한 자금이 자동적으로 인지되는 것으로 계약하였다.

3. 패트는 플라즈마 체인을 정보가 가능한 지점 까지 검증하였다. 이 지점은 거래 항의를 수락할 수 있거나 플라즈마가 최종 승인 (루트 블록체인의 최종 승인과는 다름) 날 때까지의 범위 안에 있어야 하고, 스마트 계약의 조건에 부합되어야 한다. 패트는 새 플라즈마 체인에 미결된 장부 내용을 사용자에게 보여주게 된다. 패트는 퇴장을 원하는 모든 사용자들로부터 서명을 받는다. (위의 앨리스의 예시 포함). 패트는 데이터의 유효성이 최고점에 다다를 때까지 모든 사용자가 퇴장할 수 있는 권한을 가지고 있는 블록체인을 검증한다. 패트는 막대한 연계가 있는 퇴장 거래를 만들게 된다 (스마트 계약의 루트 블록체인에 정의). 패트는 퇴장하는 사용자들에게 비용을 청구할 것이다.

4. 사용자들은 모든 서명들을 다운로드한 후 대량 인출을 다시 승인한다. 이는 패트에게 벌칙이 부과되지 않는 다는 것을 사용자들이 알게 해 주며, 잠기게 된다. 두번째 서명을 제출하지 않은 사용자들은 그들의 비트를 받을 수 없게 된다.

5. 패트는 그 후 다른 퇴장 거래가 있는지 확인하고 필요할 경우, 중복 거래는 삭제하게 되며, 퇴장 거래에 대하여 서명하고 루트 블록체인이나 상위 플라즈마 체인에 공표하게 된다. 중복 퇴장 거래가 발견될 경우, 상위 체인은 그 선행 체인을 받아들인다 (최고 선행된 체인으로 루트 블록체인 까지만). 선행된 거래는 높은 레벨의 선행 체인을 받아들인다. 대량 퇴장 거래 공표 때에, 패트는 다음과 같은 정보가 정확하다고 연계된 검증을 해야 한다: 블록의 검증, 블록 높이에 따른 UTXO 세트, 비 최종승인, UTXO를 위한 비트맵의 merkleized 매핑방식, 인증된 금액 (빠른 증명을 위하여 merkleized 종합 트리 이용), 앨리스와 다른 사용자들의 서명 확인. MEIT의 한 부분으로서, 패트는 퇴장된 상태의 전체 비트맵을 공개한다. 이는 다른 사용자들이 루트/상위 체인이 퇴장되었고 실행되었음을 검증할 수 있게 해 준다. MEIT의 마무리는 굉장히 오랜 시간을 필요로 하며, 몇 주가 걸릴 수도 있기 때문에, MEIT는 마지막 수단의 거래가 되어야 한다 (SNARKs를 이용하여 후에 시간이 단축될 수도 있음).

6. 만약 중복된 인출이 있으면, 패트는 비트맵을 업데이트하고 짧은 유예 기간안에 잔고를 인출할 수 있는 선택이 주어진다.

7. 네트워크 상의 모든 사용자는 대량 퇴장 거래 항의 (DMET)와 함께 MEIT의 확인된 데이터에 접근할 수 있다. 그러나, 패트는 다음의 블록이 결과물을 대체하는지를 알 수가 없기 때문에 패트는 다음 블록에서 거래가 사용되어도 벌칙을 받지 않게 된다. (하지만 사용자는 벌칙을 받을 수 있다). 데이터의 접근 도전이 허용되면, 자금은 접근 도전 게임이 완료될 때까지 잠기게 된다. 이 도전은 유예기간 초에 수행되어야 하며, 도전이 검증되지 않으면, 패트는 인출할 수 있는 잔고를 업데이트 하여야만 한다.

8. 어떠한 접근 도전도 없는 경우에는, MEIT의 마무리 완료 기간이 지난 후에 사용자들은 자금을 수령할 수 있게 된다.

플라즈마 체인의 마무리 윈도우 시간은 적어도 한 사용자가 정기적으로 체인을 확인하는 시간이다. 윈도우 시간 마무리 후, 모든 사용자는 플라즈마 블록체인 블록의 데이터 유효성을 획득한다고 가정한다.

사실상, MEIT 가 패트에 의하여 생성되어질 때, 패트는 특정 플라즈마 블록 높이까지 기록을 수정할 것을 확인하며, 각 개별 결과물의 인출에 대하여 서명을 가지고 있음을 확인한다. 확인 기간 후, 결과값의 중복 사용이 있어도 패트는 벌칙을 받지 않게 된다 (블록 보류에 관한것은 패트에게 벌칙을 줄 수 없는 것처럼).

대량 인출 항의: 부정확한 인출 시도

앨리스와 같은 사용자가 패트가 그녀의 동의 없이 대량 인출을 시도한다는 것을 알았을 때에는 도전과제를 만들어 무효화 시킬 수 있다.

1. 앨리스는 하나의 비트맵 방식의 필드가 가능함에 따라 패트가 플라즈마 블록체인에서 그녀의 결과물 중 한 곳에서 대량 인출을 시도한다는 것을 알아 차렸다. 앨리스는 대량의 채권과 함께 시도 도전을 공표하였다. 이 채권은 시도 도전은 가능하지 않는다는 내용을 증명하는 것이다. 그녀는 이런 사항을 블록체인에도 공표한다.

2. 시도 도전이 일정 시간 경과후에도 항의 되지 않는다면, 앨리스는 그녀의 채권을 회수 받게 되며 전체 MEIT 는 취소 된다. 패트 또는 다른 사용자들이 그녀의 부정확한 인출 시도의 부정행위 증명을 만들어내면, 시도 도전의 항의가 성립이 되고, MEIT는 유효한 상태가 되고 그녀의 채권은 깎이게 된다.

사용자들은 MEIT의 두번째 단계에 있다는 것을 (네번째 스텝) 증명할 서명이 유효하다는 것을 확신하게 되며, 시도 도전이 부정행위라면 그들은 그 도전을 항의 할 충분한 정보를 가지게 되는 것이다. 제공된 블록의 유효성과 루트 체인의 비검열에 의하여 그들은 벌칙을 받게 됨에 따라, 그에 대한 보상은 도전의 부정행위에 관하여 이루어진다.

대량 인출 거래에 관한 승인된 항의

다음 블록에서 대량 퇴장 시작 거래로부터 발생한 결과물의 부적절한 사용이 있을 경우, 패트는 이 사실을 모를 수 있고, 누구도 블록이 보류된 것을 증명할 방법이 없는 것과 같이, 그에게는 벌칙이 부과되지 않는다.

유사한 비트맵 방식 세트의 항의와 같이 다수의 항의가 있을 수 있으나, 그들 모두 대규모 채권과 연결되어야 한다.

어느 사용자라도 대규모 채권과 함께 비트맵/사용범위를 지정할 수 있다. 대규모 채권은 블록 헤더와 연계된 다음 블록에서 코인이 사용될 수 있다는 증명을 하기 위함이다.

하지만, 이러한 항의 절차는 간단하게 승인되지는 않기 때문에 대량 퇴장 거래에 관한 승인된 항의의 도전을 (CEMET) 발행하기 위하여 다른 반복적인 시도 도전이 가능하다.

이 항의에 관한 시도 도전은 다음과 같다:

1. 앨리스는 그녀가 참가하고 있는 곳에서 누군가가 (예. 체인 운영자가 블록 보류를 할 경우) 그녀의 대량 인출에 관한 항의를 시도하고 있다는 것을 알아차렸다. 그녀는 항의제출자가 유효한 사용을 하고 있지 않는 사실을 증명하기 위하여 대규모 채권과 함께 시도도전을 제시하게 된다.

2. 항의 제출자는 이 시도도전에 대하여 일정 시간 안에 응답을 하여야 한다. 항의 제출자가 사용 증명에 관한 내용을 제시하지 못하게 되면, 마지막 서명자 앨리스는 정당하게 되는 것이며, 제출된 항의 내용은 취소된다 (이것이 이중 항의가 받아들여지는 이유다). 항의 제출자가 코인이 사용되었음을 입증하게 되면, 앨리스는 그녀의 채권을 잃게 되며, 그 항의는 계속 유지된다.

UTXOs의 재활용

결과물의 사용이 마무리 된 후에는 간략함을 위하여 UTXO 비트맵을 재사용할 수 있다.

요약

이와 같은 대량 인출 게임의 결과로, 많은 사용자들의 인출의 경우 가장 최적화된 상태인 한 인출 당 1–2 비트의 정보를 소비하는 것이 가능하다.

대량 인출은 블록의 보류가 발생할 경우 필요한 절차이다. 하지만, 이는 많은 비용 발생을 초래할 수도 있다. 이러한 이유로, 루트 체인의 과부하에 의존하지 않는 차선의 전략이 필요하다.

이 구조는 많은 사용자들이 그들의 자산을 하위 블록체인에 유지할 수 있게 해주며, 블록의 정보가 유효하거나, 상태 변화가 일어나거나 (예, 지급), 인출이 가능하거나, 그리고 블록이 보류가 되었을 때 대량 퇴장 (약간의 지체가 있더라도)이 가능할 때, 부정행위 증명을 통하여 상태의 무효화를 시킬 수 있다.

블록체인의 블록체인

앞서 설명한 바와 같이 Plasma는 확장 가능한 컴퓨팅을 수행하는 핵심 구성 요소이지만 사기 방지를 생성하기 위한 블록 원천 징수(around block withholding) 문제와 블록 공간 가용성 이슈를 해결해야 한다. 플라즈마에서 원천 징수(block withholding)를 해결하기 위한 솔루션은 체인이 멈추거나 플라즈마에서 블록 원천 징수(block withholding)가 나타날 경우 대량의 출금 혹은 종료(exit)가 가능하게 구축하는 것이다.

그러나 UTXO 세트가 크고 비트맵을 게시해야하는 경우에는 블록체인에서 대량의 출금(mass exit) 트랜잭션은 매우 비싸다. 따라서 이 경우, 단일 출금(single exit)를 게시하는 것이 바람직 할 수 있다. 대량 출금 거래에는 많은 참가자가 참여하는 복잡한 양방향 게임이 필요하기 때문에 최후의 수단으로만 사용해야합니다.

대신, 우리는 상태(state) 증명을 할 수 있는 상위와 하위 법원 시스템(higher and lower courts)을 구축하여 상태(state)를 증명한다. 루트 블록체인을 모든 대법원(Supreme Court)의 권한으로 파생시키는 대법원으로 볼 수 있다. 모든 하급 법원이 사법권을 확보 할 수 있게 하는 것은 루트 블록체인의 법이다. 이는 확장성을 허용하며, 더 낮은 재판소의 상태가 논쟁을 당하거나 중단되어보다 대표적인 장소의 상급 법원으로 옮겨 가야 할 때만 가능하다. 상위 법원에서의 방송 증명은 항상 가능하지만 더 비쌀 수 있다.

모든 상태가 merkleized되어 루트 블록체인에 기록된다. 가장 이상적인 경우는 , 블록 헤더는 직접 부모체인에 게시되고, 부모체인은 그것의 부모체인에 게시하여 루트 체인에 도달 할 때까지 이 과정을 계속하는 것이다. 헤더 안에는 부모가 본 블록에 대한 merkleized된 기록이 있다.

거래는 플라즈마 체인과 모든 플라즈마 체인의 부모체인, 그리고 루트 블록체인에 제출할 수 있습니다. 이것의 목적은 대체성 및 검열에 대한 저항을 보장하는 것이다. 특히, 블록 이동이 중지되고 비공개 된 경우에도 자금을 인출 할 수 있다.

블록 커밋이 제출되면 승인 전에 루트 블록체인에 반영된 확인 금액을 기다려야 한다. 이 기간 동안 사기 증명은 루트 블록체인이나 중간 플라즈마 체인에 제출 될 수 있다.

각각의 개별 Plasma 체인은 Plasma 블록에 약속된 내용을 결합하는 상태 시스템을 실행한다. 개별 Plasma 체인은 하위 Plasma 체인의 세부 사항을 조사 할 수도 있고 하지 않을 수도 있다. 대신, 그들은 Plasma 체인의 가치에 의해 확인 된 균형을 유지하고 있다. 자식 Plasma 체인이 상태를 업데이트하면 부모는 플라즈마 블록체인의 헤더의 해시를 부모 플라즈마 체인 또는 루트 블록체인에 제출한다.

즉, 특정 블록 상태를 여러 상위 체인에 제출할 수 있다. 중복이 발생해도 문제가 되지 않으나 신청에 따라 특정 합의 규칙에 따라 벌칙이 부과 될 수 있다. 반면에 상태가 불투명하다면 (e.g. Parent1에게 제출된 상태가 Parent2와 다르다면) 플라즈마 체인의 본더(bonders)가 그들의 예금을 삭감 할 수 있다.

새로운 자식 상태 업데이트는 상태 업데이트 메시지의 다음 필드를 사용하여 업데이트 할 수 있다.
(massage : 지불되는 수수료, 루트 블록체인 해시 커밋, 이전 블록 해시, 부모 블록 해시 커밋, 예치금 증빙, 철회 증거.)

부모 블록체인이 무엇을 하던간에, 자식 체인에서 그 위 모든 부모 체인을 재귀적으로 포함하여, 그 점까지 모든 것을 보았다고 가정한다. 이것은 거래를 모호하게 하고 이중 지출하지 않을 것이라는 증명을 약속하는 것이다.

모호한 상황이 발생하면 부모 체인 상태가 항상 우선순위를 갖는다. 인센티브는 해당 당사자가 알고 있는 당사자에 의해 해당 사실을 공개하기 위해 만들어진다.

입금과 인출은 루트 체인뿐만 아니라 부모 체인 모두에서 가능하다.

충분한 유동성이 있고 다른 당사자가 기금을 다른 곳에서 기꺼이 부담 할 경우 플라스마 체인간에 인출이 가능하다. 이는 크로스체인 원자 교환(crosschain atomic swap)을 통해 수행 할 수 있다.

메인 블록체인을 사용하여 클리어링을 원할 경우, 체인간에 온-체인 Lightning payments처럼 보이는 HTLC를 구성 할 수 있다.

모든 사기 증명은 체인 약속에 대한 합법적인 증거를 제공해야 한다. 거짓으로 증명하는 것은 사기 블록을 담당하는 특정 플라즈마 체인에 불이익을 준다.

주요 디자인 복잡성은 검열에 대한 저항을 위해 다수의 부모 체인에 걸쳐 이루어지는 거래 상태를 브로드캐스트를 표현하는 것에 초점을 두었다. 초기 반복 작업에서는 상태 변환 / transactions는 개별 플라즈마 체인에서만 수행될 수 있으며, 부모/자식체인 간의 상호작용 및 임금/출금과 같은 다른 체인과의 상호 작용만 메시지로 간주된다. 그런 식으로, 1 차적인 복잡성은 예금과 인출에만 관련된 증거이다.

체인 내부에서 펀드 받기

블록체인에 있는 블록체인의 계층 적 프레임 워크에서, 사용자가 다른 사용자로부터 자금을 받을 때, Alice가 Plasma chain의 3 단계 레벨에서 Bob에게 자금을 보내기를 원하면 프로세스가 다음과 같다.

1. 앨리스는 밥과 조정하여 밥에게 돈을 보내고 싶어한다. Alice는 Bob에게 자금을 수령 할 Plasma 사슬을 Bob에게 공개한다. Bob은 지불을 수락할지 여부를 결정한다. 구체적으로 Bob은 루트 블록체인의 스마트 계약에 지불을 수락 할 것인지 확인해야한다 (스마트 계약 코드/메커니즘, 수용 가능한 합의 종료 지연 등)

2. 이것이 어떤 상품에 대한 지불이라면, 지불 조건을 정의하는 진술서에 미리 서명한다. 많은 경우, 충분한 성숙도를 가진 블록체인에 블록을 포함시켜 지불하는 증거가 될 수 있지만, 일부 상황에서는 계약 해시를 제출해야 할 수도 있다(pay-to-contract-hash). 이것은 온-체인에 있지 않지만 다른 사람들에게 입증하기 위해 합의 조건을 첨부하는 것이다.

3. Alice는 Plasma 체인의 내부에서 지불한다. 블록은 유효성 검사자들에 의해 서명되고, 블록 헤더에 대한 커밋이 부모 블록에 게시됩니다. 하위 플라즈마 체인에 대한 Merkleized 약정 Plasma chain은 모든 부모 블록에 포함되며 궁극적으로는 루트 블록체인에 포함됩니다.

4. Bob은 루트 블록체인과 완벽하게 동기화 된 다음 자금이 수신되는 사슬과 그 부모를 검증한다. Bob은 그의 자금이 일부가 아닌 다른 Plasma 체인의 유효성을 확인할 필요가 없다. Bob은 Alice가 충분하게 Plasma 체인에서 지불을 완료했음을 완전히 검증 할 수 있다. 그러나 신속한 최종성(finality)이 필요한 경우 Alice는 새 블록에서 지불이 완료되면 서명 할 수 있다 (이전의 성명서에서 Plasma chain 내부 지불에 대한 내용 참조). Alice가 지불에 대해 기꺼이 서명하고 Bob이 이를 수령하면 (철회를 증명할 수 있는 것처럼), 최종성에 도달했다고 가정한다. Bob은이 Plasma 체인에서 자금을 인출 할 수 있다.

이 디자인의 핵심은 자식 블록체인의 유효성을 전적으로 책임지는 것이다. Bob은 Plasma chain과 모든 부모체인을 검증하지 않는다면, (궁극적으로 루트 체인에 대한 정기적인 커밋이 게시 된 경우) 그것은 조건을 충족했다고 해서는 안 된다. Lightning 네트워크의 구성과 마찬가지로 Bob은 다른 Plasma 블록체인에서 어떤 일이 일어나는지 신경 쓰지 않아도 된다. 그는 그에게 중요한 사슬의 정확성만을 관찰한다. 그는 코인을 사용할 수 있는 권리(ability)를 가지고 있을 때, 그것을 쓸 수 있다고 확신할 수 있다.

부모 체인에서 펀드 받기

상위 체인에서 자금을 받는 것은 루트 블록체인의 입금과 유사하다. 받는 사람은 모든 상위 Plasma 체인을 검증해야 한다 (단, Plasma 체인 자체가 아닌). 하위 Plasma 체인에게 예치금을 넣는 것은 빠르게 처리된다.

트리에서 웹으로

위의 설명은 단일 상위 체인에 대한 내용이지만 플라즈마 체인은 여러 개의 루트 블록체인을 갖을 수 있다. 이를 통해 자식 체인과 함께 잔액을 업데이트 할 수 있다. 한 상위 체인의 실패는 모든 참여자들에 의해 동시에 인식되지 않을 수 있기 때문에 주의를 기울여야 하며, 계단식 시스템 실패는 시간 지연을 통해 완화하고 교차 사슬 유동성의 가정(assumptions of cross-chain liquidity)을 최소화해야한다. 이에 대한 올바른 구성에 대한 문제는 열려있다.

Mitigating the Block Withholding Problem

출금 거래를 브로드캐스팅 할 수 있는 많은 장소를 선정함으로써, 중단되거나 보류 된 블록이 있는 많은 장소에서 출금(exit) 할 수 있다. 자식 체인이 실패하면, 부모 체인에서 단순히 개별 종료를 처리 할 수 있으며, 트랜잭션이 비싸지만 루트 체인에서 종료 할 수도 있다.

이를 통해 상위 Plasma 체인 중 하나가 올바르게 작동하고 있다는 확신이 있는 경우 Plasma 체인에서 소액 결제 결과를 보유 할 때 어느 정도 확신을 가질 수 있다. 이러한 목표는 이 목표의 주요 원인이자 계단식 오류(cascading failures)의 영향을 완화하는 것이다.

보유하고 있는 출력 잔액이 충분히 큰 경우 중요한 시간 가치가 없으면 상당한 인수(significant underwriting) 작업을 수행 할 필요가 없다. 단 하나의 낮은(low-value) 출력(수수료로 더 비싼 비용을 지불하는 경우)이 있는 경우에는 상위 Plasma 체인 중 하나에 가용성이 있는지에 대한 확신이 있어야한다. 더 큰 확신을 원하면 각 레벨에서 각 Plasma 체인을 실행하는 많은 독립 당사자와 함께 중첩(nested) 된 체인을 실행할 수 있다. 이런 식으로 일부 트레이드-오프가 존재하지만 특정 플라스마 체인이 비잔틴이 되기 시작한 것처럼 모든 사람들이 새로운 체인에 대량 철수해야 한다. 비잔틴이 아닌 부모가 있는 경우 부모가 비잔틴 체인의 약정을 거절하면 다른 체인으로 신속한 전환 및 운영을 지속할 수 있다.

하위 체인이 실패 할 경우 프로세스 트랜잭션 이외의 작업을 수행하지 않는 서비스가 발생할 수 있다. 이 서비스의 운영자는 자식 체인이 실패하지 않는 한 아무 것도 할 필요가 없다. (장애가 발생하여 가상 서버가 서버를 끌 수 있을 정도로 수동적(passive) 일 수 있는 지점까지, 블록 헤더는 패시브 운영자보다 높은 수준의 체인에서 브로드 캐스트 되도록 자동으로 건너뛴다).

상위 체인의 많은 인출은 대량 인출 대신 간단한 인출이 될 것으로 예상된다. 상위 체인은 엄청난 거래량 (블록 크기 / 가스 한도)을 가질 수 있기 때문이다.

출금하기

대량 출금(exits)은 상위 체인 또는 루트 체인에서 가능하다. 하위 체인이 Byzantine을 시작하면, 중첩 된 상위 체인이 없는 Plasma 체인과 마찬가지로 모든 상태가 유효하지 않을 수 있다고 추정된다. 마찬가지로 대량 출금(exits)은 비잔틴 부모 체인에서 빠르게 출금(exits)하는 방법이다. 상위 체인(또는 하위 체인 자체)을 그것의 상위 체인 또는 루트 체인으로 건너 뛸 수 있다.

디자인에 약간의 복잡성이 있는 것처럼 보일 수 있지만, 어떤 체인이 비잔틴인 경우, 그것의 모든 하위체인은 동작(act)해야 한다는 가정이 있다. 가능한 최적화가 가능하므로 heartbeat를 통한 조정 없이 종료(exit)가 가능하다. (종료(exit)는 사용자 측면에서 서명을 철회하고 Plasma 체인 자체가 서명을 받았음을 약속하지만 아직 최적화 되어있지는 않다).

구성은 기본적으로 단순 종료(exit) 또는 대량 종료(exit)과 동일하지만 중첩 된 체인을 지원하기 위해 디자인에 약간의 변경이 있다. 종료(exit)는 중복 될 수 있지만 상위 체인의 종료(exit)가 항상 우선순위를 갖는다. 상위 체인이 Byzantine을 시작하면 루트 체인에서도 종료를 커밋 할 수 있다. 부모/루트 체인 중복 종료의 상태를 반영 및 업데이트하고 자체 체인에서 중복 된 종료를 취소한다. 이렇게 하지 않으면 사용자의 자금이 루트 체인에서 사용 가능 하게 된다.

부모 체인이 비잔틴이지만 자금을 보유하고 있는 자녀 체인이 올바르게 운영되고 있다면 복잡한 대량 출금(exit) 거래를 피할 수 있다. 참가자는 자신의 자금을 송금하고 간단한 출금(exit)을 제공하는 새로운 체인을 발견하여 유동성을 제공해주는 자(liquidity provider)가 이 자녀 체인에서 자금을 받고 다른 사용자가 새로운 체인(비잔틴 부모체인이 아닌)에게 자금을 제공한다. 하위 체인 블록의 약정은 루트 체인 또는 상위 수준의 부모(비잔틴 노드가 아닌)에 게시된다. 사용자는 새로운 체인에 신속하게 자금을 보유하고 있으며, 유동성 공급자(liquidity provider)는 루트체인이나 상위 체인에서 나중에 자금을 출금한다. 이것의 목적은 새로운 자금을 새로운 체인에 신속하게 할당 할 수 있고 출금을 빠르게 하는 것에 있다.

확장성

이것은 UTXO 비트 맵 확장성을 허용한다. 비트맵이 너무 커지면 비트맵을 여러 하위 체인으로 분할하면 된다. 하위 체인의 경우 출력(output) 대신 블록 높이 nonces (및 후보 체인 팁)로 계정 잔액을 표시한다고 가정한다. 마찬가지로, UTXO 대신 계정을 사용하는 것을 선호하는 상태(state)에서는, 단순 인출만을 지원한다는 절충안을 제공한다면 가능하다.

최종 결과로 이것은 사용자에게 많은 확장성을 제공한다. 그들은 그들의 자금이 있는 플라즈마 체인을 관찰해야합니다(그것의 부모뿐만 아니라). 이렇게 하면 데이터 세트가 자신에게 영향을 미치는 유효성 검사에 효과적으로 분할된다.

플라즈마 지분증명

우리는 단순한 지분증명 증명 구조를 제안합니다. 이것이 최적의 지분증명 구조가 아닐지라도, 플라즈마 체인에서 가능한 방식을 설명하고 있습니다.

지금까지 플라즈마 체인의 운영자가 블록에서 서명을 담당하는 단일 개체라고 가정했습니다. 잘못된 블록을 만들면 블록 데이터가 있는 다른 모든 사람이 사기 증명 증거를 생성하고 운영자에게 패널티와 함께 블록을 롤백할 수 있습니다. 이 증거는 운영자가 서명으로 블록에서 서명했기 때문에 가능합니다. 루트 체인에 Merkleized된 플라즈마 블록의 커밋이 게시되므로(가장 상위의 플라즈마 블록은 하위 체인의 상태 업데이트를 포함하므로), 상태 업데이트가 올바르게 작동하도록 정렬되고 결합됩니다.

그러나 대부분의 경우 단일 개체가 증명하는 체인보다 지분증명 체인을 구성하는 것이 좋습니다. 이렇게 하면 block withholding문제와 관련된 위험을 최소화 할 수 있습니다(단일 개체가 증명하는 체인과 다수의 지분증명 체인을 결합함으로서 두 방식의 최대 장점을 활용 하는것도 가능합니다.) 토큰화 된 지분증명 체인은 악의적 행위(Byzantine behavior)에 따라 토큰의 가치가 감소하므로 토큰 제조자가 올바르게 작동할 수 있는 동기를 부여합니다. 토큰화의 잠재적 가치에 대한 자세한 내용은 이후 섹션에서 설명합니다.

이는 루트 체인의 견고성에 의존하기 때문에, 지분증명 구조는 플라즈마를 구성하기에 용이합니다. withholding 문제, 최종성(finality) 및 기타 요인과 관련된 문제는 루트 체인의 신뢰성으로부터 영향을 받습니다. 플라즈마는 루트 체인만큼 안전 할 수 있습니다. 루트 체인이 작업증명(Proof of Work)을 방식인 경우, 작업 증명에 대한 지분증명 방식이 될 것입니다(루트 블록체인에 대한 각각의 플라즈마). 루트 체인이 지분증명(Proof of Stake)인 경우, 지분 증명에 대한 지분증명 방식이 될 것입니다. 그러나 지분증명 메커니즘은 루트 체인에서 실행되는 것보다 간단하거나 다를 수 있습니다.

나카모토 합의 인센티브

우리는 Nakamoto 합의(Proof of Work 마이닝)의 주요 인센티브를 재현하려고 시도합니다. 재현하고자하는 가장 중요한 인센티브 중 하나는 다른 마이너에게 블록 전파를 장려하는 것입니다.

기존에 제안된 많은 지분증명 메커니즘은 리더를 선거하는 것에 달려 있는데, 시간 t0에서 리더가 선출되면 시간 t1에 리더는 블록을 생산할 권리가 있습니다. 이것은 블록 전파와 관련하여 Nakamoto 합의 인센티브를 재현하는 것이 아닙니다. Nakamoto 합의는 리더를 선출하기는 하지만 확률적으로 리더를 선출합니다. 블록을 발견한 사람이 리더가 될 가능성이 높지만 완전히 확신 할 수 없습니다. 다른 누군가가 정확히 같은 순간에 블록을 채굴 할 수 있기 때문입니다. 리더가 되기 위한 확률을 최대화하는 가장 좋은 방법은 블록을 가능한 한 멀리 넓게 브로드캐스팅하여 다른 사람들이 그 위에 블록을 쌓을 수 있도록 하는 것입니다. 이 경우 정보 가용성으로 인해 인센티브가 창출됩니다.

플라즈마의 지분증명 구조는 위 방식과 비슷해야 할 필요가 있습니다.

우리는 모든 사람이 가능한 한 광범위하게 블록을 전파하도록 권장한다는 점에서 타협점을 만들었습니다. 그러나 이것 외에 다른 구조도 있을 수 있습니다(특히 무작위 점수를 특정 branches에 할당하고, 무작위 점수가 가장 높은 branch로 체인의 마지막을 결정함으로써 무작위 선택과 확률론적 지도자 선거에 대한 의존도를 높이는 것).

간단한 지분증명 모델의 예시

이것은 지분증명 모델을 만드는 간단한 제안이지만, 어디서나 최적화되지는 않습니다. 목표는 플라즈마가 사용할 수 있는 간단한 예시를 만드는 것입니다.

강제되는 메커니즘을 만드는 대신 적절한 조정과 올바른 행동(블록 전파)에 대한 인센티브를 만드는 것입니다.

수수료는 루트체인의 컨트랙트에 의해 할당되고 분배되며 원할 경우 주기적으로 지불되지만 요금 계산(accounting)은 체인 자체 내에서 이루어집니다.

staking 컨트랙트의 일환으로, 지분 보유자들의 기금을 위임 된 사람(staker)에게 할당됩니다. 위임 된 사람(staker)은 사용자를 대신해서 행동할 책임이 있으며 만약 위임 된 사람(staker)이 잘못을 한다면 사용자는 불이익을 받습니다. Staking은 특정 시간(e.g. 3개월) 동안 수행됩니다. 각 보유자(staker)별 최소 금액은 모든 토큰의 1 %이며 최대 한도는 5 %입니다. 5 % 이상 할당하려는 경우, 여러 개의 staking 신원을 사용해야합니다 (목적은 데이터 분배를 최대화하고 51% cartels 이하의 효과를 최소화하는 것입니다).

자금은 지난 100개의 플라즈마 블록이 모든 참가자를 대표하는지 여부에 따라 할당됩니다. 예를 들어, 누군가가 stakers의 3%에 자금을 건 경우, 그들은 이전의 100 블록의 3 %이어야합니다. 이 금액을 초과하는 경우, 개별 보유자(staker)는 여분의 블록 약정 게시에 대한 추가 보상을 받지 못합니다. 지난 100 개의 블록이 3 개 미만이면 현재 블록 작성자는 더 적은 보상을 받습니다. 루트 체인에서 블록 당 하나의 블록만 할당 할 수 있습니다.

이렇게 하면 모든 참가자가 모두의 블록을 동일하게 조정하고 포함시킬 수 있습니다. 참가자들은 최대한의 보상을 보장하기 위해 일종의 조직(scheme)(e.g. 라운드 로빈)을 조정하고 보장합니다.

부적절한 금액으로 인해 거래 수수료가 최대치를 받지 못하면, 미래의 블록을 위해 자금이 풀에 할당됩니다.

그 결과 모두가 참여하도록 경제적으로 격려합니다.

그러나, 우리는 보유자들(stakers)로부터 정확한 참여를 장려할 뿐이기 때문에 아직 완성된 것은 아닙니다. 모든 블록은 지난 100 개의 블록에서 무작위 부분에 대한 데이터를 merkleized한 약정입니다. 이렇게 하면 보유자(staker)가 전체 블록 데이터를 갖게 되고 결과적으로 블록 생성자가 모든 보유자들(stakers)에게 전파해야합니다.

병렬적인 branches가 있는 경우, 체인의 마지막은 최대 보상에 의해 결정됩니다. 즉, 최대로 조정한 것에서 최대의 수수료 보상이 있는 것이 이기게 되어있습니다.

이 구조는 51% 공격을 막기 위해 설계된 것이 아니라 블록 전파를 권장하도록 설계 되었습니다(블록을 보류하도록 설정하면 위협이 동일하므로). 또한, 이 구성은 루트 체인에 정보 가용성 및 공평성에 의존합니다. ; 데이터 가용성 및 검열 인센티브에 대한 가정 때문에 루트 체인에 이러한 유형의 지분증명을 구축하는 것은 불가능합니다.

경제적 인센티브

지분증명 유효성 모델에서, 컨트랙트 조건의 올바른 작동과 일치하는 것에 인센티브를 주도록 구성할 수 있습니다. fidelity bonds는 체인에 대한 정확성을 보장하지만, 데이터 가용성에 대한 인센티브를 창출하고 중단(halting)되는 것을 방지해야합니다. 플라스마 체인에 특정한 토큰을 사용하고 보유하는 것을 허용함으로써 운영을 계속할 동기가 있음을 보장 할 수 있습니다. as the value of the token is derived from the net present discounted value of all future returns from staking. 결과적으로 네트워크의 실패는 보유 중인 토큰의 가치를 감소시키며, 개별 행위자들은 네트워크의 지속적 운용에 가장 큰 이익이 되도록 작용할 동기를 부여 받습니다.

플라스마 체인 운영자는 온-체인에 브로드캐스팅하는 수수료를 받습니다. 서로 다른 작업에 대해 서로 다른 수수료를 부과할 수 있으며, 특히 복잡한 작업에 대해서는 수수료가 급격히 낮아질 수 있습니다. 더 낮은 수준의 자식 체인에서 더 많은 트랜잭션이 수행 될 수 있도록 하는 인센티브가 있지만, 일반적인 자식 체인에서 자금 송금 및 계산에 대한 약정을 체결하는 것도 가능합니다. 이것은 부모 체인이 자식체인에 대한 비용을 부과하도록 하며, 올바르지 않은 확약(commitments)이 있는 경우, 블록 데이터가 유효하지 않으며 시행 할 수 없습니다. 이것은 필수적인 것은 아니며 많은 경우 부모 체인까지 수수료를 분배 할 필요성이 적기 때문에 자식 체인에서의 계산이 더 선호됩니다.

시스템 업그레이드의 경우, 동일한 토큰을 허용하고 전환 기간을 알리는 또 다른 컨트랙트를 생성하여 시스템을 업그레이드 할 수 있습니다 (또는 커뮤니티가 탈중앙화 시스템에서 공동으로 결정).

이를 통해 스스로 실행되는 시스템을 만들 수 있습니다. 데이터 저장 및 계산을 수행하는 사이트를 호스트하기 위해 클라우드 컴퓨팅 서비스에 돈을 지불하고 운영해야하는 반면, 이제는 스마트 컨트랙트(사기 증명 포함하는), 토큰 및 수수료를 지불하는 충분한 수의 참가자로 구성 할 수 있습니다. 이 시스템은 네트워크 및 컴퓨팅 인프라 스트럭처를 계속 올바르게 운영

하여 비정형 클라우드(amorphous cloud)에서 컴퓨팅을 실현하는 보유자들(stakers)의 집단을 통해 자체적으로 작동할 수 있습니다.

토큰 vs 코인과 경제적 보안(Economic Security)

루트 체인에서 궁극적으로 개최되는 이러한 사기 증거 및 채권은 기본 토큰(e.g Ethereum의 Ether(ETH))이 될 수 있으며. 혹은 기본 블록체인의 합의 규칙을 유지하는 별도의 토큰이 될 수 있습니다.

루트 체인의 기본 토큰 (e.g ETH)을 사용하는 것이 표면적으로 가장 간단하지만 흥미로운 경제적 보안 의미를 포함하고 있습니다.

블록체인 적용에 따라 체인 중단 및 오류 동작을 방지하는 것이 목표 인 경우, ETH만 사용 된다면 오류 동작을 방지하기 위한 인센티브가 충분하지 않을 수 있습니다. 체인이 정지되거나 비잔틴 오류인 경우 토큰의 가치가 감소합니다. 또한, 토큰의 가치는 토큰을 가치 있게 만드는 미래 거래 수수료의 현재 가치(NPV)입니다. ETH를 걸었으면, 얻게 되는 수수료의 양에 비례하여 시간 가치에서 파생 된 가치를 책정합니다. 이 값은 토큰의 현재 할인 값보다 훨씬 낮을 것으로 예상됩니다. 또한 체인의 중단과 block withholding은 증명하기가 어렵고, ETH를 담보로 한 기간 후에 돈을 되돌려 받는다면, 비-비잔틴 식으로 행동하는 데는 인센티브가 충분하지 못하며 토큰의 가치는 비잔틴 행동이 널리 퍼지며 감소합니다.

블록체인을 위한 맵리듀스

MapReduce에서 계산할 수 있는 거의 모든 것이 체인에서도 계산 가능해야합니다. 이를 위해서는 블록체인에서 계산과 프로그래밍에 관해 생각하는 방식을 철저히 재구성해야합니다. 이것은 MapReduce이지만 사기 증명을 할 수 있습니다. 각 노드는 블록체인을 나타냅니다. 이는 이전 섹션에서 설명한 플라즈마 블록체인 트리 구조와 호환됩니다.

E.g. 표준 단어 수의 카운트를 원하는 경우, reduce 함수를 사용하는 체인의 머클트리를 만들 수 있습니다. 사기의 증거가 있는 경우 사기를 일으킨 노드는 불이익을 받습니다. 합계에 대해 reduce 함수를 생성 할 수 있으면 평균도 생성 할 수 있습니다. (E.g.평균 가격 등) Map 함수는 계산을 개별 체인에 전송 한 다음 결과를 커밋하는 것입니다. 분명히, 데이터 처리량에 대한 제약이 있기 때문에 이는 사기 증명을 줄이는 것이 왜 필요한지를 보여줍니다. 이는 모든 유형의 임의 계산은 불가능하지만 많은 유형의 문제를 해결할 수 있습니다 ; 일반적으로 메모리제약문제는 우선적으로 sorting 알고리즘을 실행하여 해결할 수 있으며, 이로 인해 플라즈마 체인 간 트래픽의 균형을 유지시킵니다.

노드가 계산을 증명하기 위해 실제 블록을 생성 할 수 없으면 결과를 버리고 롤백 해야합니다. 이것은 MapReduce가 수행하는 계산의 확장성을 보장하지는 않지만(컨센서스를 유지하기 위해 체인을 관찰해야하므로), 액티비티를 시행하고 액터에 맞게 확장 할 수 있는 기능을 제공합니다. 그 결과, 주요한 제한사항은 특정 계산에 영향을 받는 당사자가 해당 계산 집합을 관찰해야한다는 사실에 있습니다. 만약 하나의 작은 부분을 관찰 할 필요가 있다면 괜찮을 것입니다. 그러나 모든 계산을 관찰 할 필요가 있다면 그것은 확장성의 이점을 제공하지 않습니다.(오직 확장성을 가능하게 해주는 것만 보장한다는 이점만 있음) 즉, 많은 문제가 이러한 방식으로 해결 될 수 있습니다. e.g. 탈중앙화 된 환전(exchange) (매핑 된 집합(set)은 자신의 거래는 신경 쓰지만, 다른 모든 사람들이 실행을 통제 할 수 있다면 세부 사항에 신경 쓰지 않아도 됩니다.)

블록 포맷은 TrueBit 구조에서 계산할 수 있는 데이터와 호환 가능해야합니다. 상태에 대한 약속 (포함되었는지 제외시 상태 전환의 증거를 허용하는 UTXO / 상태 트라이를 구성 할 수 있음), 계정 트라이 (하위 체인 및 복잡한 상태 전이), 요금 약정 (상태를 확약하는 트리) 부모 / 자식 블록에서 전달 된 데이터에 대한 약속, 부모 / 자식 블록 (재주문 방지) 및 비즈니스 로직 (예 : 단어 수 계산의 예는 단어에 대한 merkleized sorted commitment를가집니다. 그리고 그것을 보았던 곳). Merkle 약정을 구성함으로써 루트 또는 상위 체인에서 입증 할 수있는 현명한 계약을 만들 수 있습니다.이 계약은 잘못된 상태 전이를 증명할 수 있습니다. 이 형식과 호환되지 않는 문제 세트가 있지만 중요한 메모리 요구 사항이없는 일반적인 계산이 가능합니다. 이를위한 정신적 인 틀은 계산을위한 최대 메모리 크기를 사기 증거에 허용 된 최대 데이터와 동일하게 취급하는 것입니다.

일련의 map 및 reduce 함수는 블록체인이 데이터를 처리 할 의무가 있는 방식으로 작동 하도록 합니다. 이는 부모 체인과 자식 체인이 데이터 처리 의무를 지도록 합니다. 자식 체인은 부모 체인에 데이터를 전달하는 것을 포함해야 하며 그렇지 않으면 자식 체인은 중단될 것입니다. 부모 체인은 자식 체인들에게 계산을 실행하도록 할 수 있으며, 만약 자식 체인들이 멈추면 부모 체인에 있는 데이터를 브로드 캐스팅하고 그 증거를 증명함으로써 계산을 시행 할 수 있습니다. TrueBit 구조

의 주된 위협은 정지 관련 문제와 관련이 있기 때문에, 시간이 지남에 따라 복잡해지더라도 만약 자식 체인이 중단 되어도 계속해서 작동 할 수 있도록 주의를 기울여야합니다 (데이터 셋이 변경될 수 있고 시간 일관성을 갖는 것이 일부 문제에 대해 추론하기가 더 어렵습니다.)

map and reduce 프레임 워크를 이용하는 자식 체인에서 블록체인 계산을 하게함으로써. 기존의 컴퓨터 과학 연구를 수행하고 블록체인에 존재하는 탈중앙화 시스템에 대한 문제들에 직접 적용할 수 있습니다. 확장 가능한 방식으로 많은 유용한 비즈니스 애플리케이션을 생성하는 Solidity 컨트랙트를 구성 할 수 있습니다. 여기서는 자신과 관련된 활동만 계산하고 확인하면 됩니다.

어플리케이션 예시

탈중앙화된 애플리케이션은 MapReduce 문제로 재구성되어 토큰으로 결합 된 올바른 활동에 대해 경제적 인센티브를 제공합니다.

블록체인 레딧

이것은 주로 데이터 저장(CRUD)에 관한 것입니다. 주로 계산 및 증명은 액세스 제어, 신원 (투표 및 게시물 등록) 및 조정과 관련되어 있습니다. 많은 웹 응용 프로그램은 실제로 백엔드에서 CRUD를 수행하고 있습니다.

루트 체인에는 스마트 컨트랙트 합의 규칙 및 사기 증명이 포함되어 있습니다. 최상위의 부모 체인은 하위 reddit 체인 (subreddits)의 계정을 포함합니다. 각 subreddit은 최상위 부모의 플라즈마 체인의 자식체인 입니다. 각 subreddit 안에는 플라즈마 체인의 게시물이 있습니다. 그 자식 체인의 게시물에는 코멘츠도 포함됩니다. 합의 메커니즘은 접근 제어를 시행합니다. 이전 블록 데이터에 대한 무작위 약속(상위 체인에서 제공하는 임의의 넌스를 사용)은 모든 블록 헤더에 커밋됩니다. reduce 함수는 상위 게시물 및 기타 통계에 대해 주기적으로 계산합니다.

개별 사용자의 컴퓨터는 로컬에 있는 데이터와 소프트웨어를 다운로드하여 데이터를 포맷합니다. 데이터를 제출하려면 데이터 포함에 대한 인센티브를 위해 거래 수수료를 지불해야하며, 가용성에 따라 이전 블록 데이터를 다운로드하는 데 요금이 부과 될 수 있습니다.

특정 게시물을 보려면 사용자는 루트 체인에서 약정을 확인한 다음 맨 위에 있는 부모 (마지막 n 블록은 최종 기간으로 되돌아 가야합니다. 일주일 정도 소요될 수 있음)의 체인 설명으로 이동하여 해당 게시물에 대한 주 계정 트라이를 찾습니다. 관련 subreddit. DHT 네트워크에 연결하여 서브 레딧에서 노드를 발견하고, 서브 레딧 및 게시물 목록보기에 대한 chaintip (확인을 위해 n 개의 블록을 더한 것)을 다운로드하고 의견이있는 관련 게시물의 원시 데이터 및 라이트 클라이언트로 상태 trie를 다운로드합니다. 사용자는 자신과 관련된 Plasma chain의 부분 만 관찰하면됩니다 (자신과 관련된 게시물과 하위 참조 번호 만 다운로드).

이것은 블록체인에 대한 일부 계산과 함께 데이터를 저장하는 간단한 예시입니다. 유효성 검사기가 모든 노드의 유효성을 완전히 검사 할 수는 있지만 나눠서 수행할 수도 있습니다. 샤딩이 너무 길어지게 되면 정보 가용성 문제가 있습니다. 이를 완화하기 위한 한 가지 방법은 subreddit 소유자에게 하위 체인에 대한 완전한 통제권을 주는 것입니다.

탈중앙화된 환전

Blockchain의 reddit 복제본은 CRUD 웹 애플리케이션에 대한 함축적인 의미를 나타내지만 사이트 통계를 제외하고 MapReduce의 이점을 크게 활용하지는 않습니다.

탈중앙화된 환전은 높은 계산 작업에 대해 지연 시간을 최소화하여 교환 할 수 있음을 보여줍니다. 많은 상태들이 있기 때문에, 가능한 출력은 UTXO 대신 계정에 정의되거나, or for each step in the state machine that a larger bitmap is used to represent each state instead of a single boolean value representing spentness in the bitmap.

subreddit과 마찬가지로, 각각 거래 쌍을 나타내는 하위 체인 트리가 있습니다. 각각의 내부에는 확장성을 최대화하기 위한 체인 트리가 있습니다 (활동이 별로 없는 쌍의 경우 하나의 플라스마 체인 일 수 있지만, 활동이 많은 체인의 경우 더 많은 자식 체인을 가질 수 있음). 이 체인들 각각은 결합된 활동들을 가지고 있으며 각 라운드 당 처리 할 수 있는 양은 결합된 양에 의해 제한됩니다.

첫 번째 단계는 하위 체인에 잔액이 있어야하므로 페이먼트 플라즈마 체인을 기본으로 삼아야 합니다.

다음으로, 명령서는 하위 체인으로 직접 발행됩니다. 부모 체인에 대한 약속의 일환으로, 모든 명령서는 체인 자체에 의해 단일 주문으로 표현된 단일 order book의 Merkleized된 약정으로 통합됩니다. 이 단계는 가장 상위 플라즈마 부모 체인에 도달할 때까지, 모든 자식 체인의 order book들을 해당 체인이 나타내는 단일 order book으로 재귀적으로 반복하여 줄입니다. 주문이 접수되면 주문 창이 닫히고 거래가 일괄적으로 실행됩니다.

이 reduce 단계가 완료되고 루트 체인에 커밋 된 후에는, map 단계를 통해 개별 체인에 할당량이 통보됩니다. 부모는 자녀에게 그들의 주문의 할당이 어떤 결정론적 방식으로 결정되었는지 알려줍니다. 자녀가 다른 주문을 볼 수 있었다면(이 단계에서 상위 체인을 관찰 할 수 있음을 의미 함), map 단계에서 올바르게 할당 되었다는 것을 증명할 수 있습니다. 할당을 받은 후에, map 단계는 그 체인의 자식 체인들에게 이것을 재귀적으로 반복합니다.

이 작업이 완료되면, 모든 자금을 블록으로 업데이트하는 것을 커밋하고 블록 헤더를 부모에게 제출함으로서 최종 reduce 단계가 수행됩니다.

가격 변동이 심한 경우 다중의 MapReduce 라운드를 허용함으로써 더 많은 최적화가 이루어 지지만(가격 책정의 정확도를 높일 수 있음), 이 일반적인 구성으로도 엄청나게 많은 양을 처리하는 것을 가능하게 합니다. 이론적으로는 이 프레임 워크에서 전세계의 거래 활동을 수행 할 수 있으며, 루트 체인에 완전히 묶이고 결합 된 일괄 처리 환전으로 속도를 일부 상쇄할 수 있습니다.

이 유형의 구성은 다양한 유형의 금융 활동 및 계산에 유용합니다.

탈중앙화된 메일

D-Mail을 만들려면, 플라즈마 체인에 자신의 계정을 나타내고 메일 수신을 위해 결제하는 것이 가능합니다(체인에 메시지 삽입). 제출은 공개키로 암호화됩니다. 알려지지 않은 엔티티가 지불해야하는 것을 보장하기 위해 시행하는 것도 가능하며, zk-SNARK를 사용하여 추가 최적화가 가능합니다. 상위 체인은 체인의 디렉토리를 포함하고 결제하는 것을 시행합니다. 심플한 디자인.

탈중앙화된 CDN

Ethereum sharding proposal과 비슷한 구조로 탈중앙화 된 CDN을 가질 수 있습니다. 각 어린이 블록체인을 조각(Shards)으로 취급하십시오. 무작위 비컨 (root blockhash 또는 다른 것일 수 있음)을 가지고 있습니다. Shards 사이의 데이터를 n 블록마다 임의로 섞습니다. 부모 체인은 셔플에 대한 책임을집니다. 다른 사람들은 아카이브를 지연 보관할 수 있습니다. 데이터 손실이 발표되고 아카이브 보관 담당자에게 보상이 제공됩니다. 다른 샤드에 데이터가있는 경우에만 보상을 받기 때문에 인센티브가 전파됩니다. 견고성은 흐름의 길이에 대한 요구 사항에 달려 있습니다. 더 견고할수록 파편이 많을수록 언제든지 복사본을 가져야합니다. 여기서 핵심적인 통찰력은 스토리지가 대역폭의 함수라는 것입니다. 데이터는 디스크의 고정 데이터로 취급되지 않습니다. 모든 데이터는 실제로 다음 목적지로 흐르고 동작합니다.

데이터를 다운로드하기 위해 부모 체인의 조각(shard)과 랜덤 비컨을 확인하여 어떤 샤드에 데이터가 있는지 확인한 다음 DHT를 통해 피어를 식별하고 데이터를 다운로드합니다.

프라이빗 체인

참가자는 체인의 데이터를 다른 사람에게 공개 할 의무가 없습니다(비록 모두에게 공개되는 것을 막을 수는 없지만). 그래서 만약 체인의 참가자가 루트 체인에 의해 시행되는 프라이빗 블록체인 네트워크를 원할 경우 그렇게 할 수 있습니다. 이것은 인트라넷 / 인터넷 분리와 유사합니다. 트랜잭션은 로컬 프라이빗 체인에서 일어나지만, 퍼블릭 체인에 의해 커뮤니케이션되고 경제 활동이 확정됩니다.

공격과 리스크 그리고 대비책

스마트 컨트렉트 코드

좋은 스마트 컨트랙트 코드를 작성하는 것은 어렵습니다. 보안성은 사기 증명의 올바른 실행에 전적으로 의존합니다. 일부 사기 증명은 포함되지 않을 수 있으며 유효하지 않은 상태 전이가 루트 체인에서 유효 할 수 있습니다.

메인 체인에서의 Closing Transaction이 너무 비용이 많이 발생

트랜잭션이 메인 체인에서 닫힐 수 있는 위험이 있지만, 사실 이는 경제적으로 불가능합니다. 이 경우 작은 값들로 이루어진 많은 트랙잭션을 큰 값에 추가하여 조정하는 것에 의해 특정 유형의 출금(exit) 사기를 만들 수 있습니다.

이는 출금(exit) 조항에 따라 모든 거래를 분류하고 특정 분쟁 조정 기간 후에 한 번에 전체 체인의 출금(exit)을 허용함으로써 이를 완화 할 수 있습니다. 또한 제 3자인 감시자가 자신을 대신하여 감시할 수 있게 할 수 있습니다. 그러나 이 구성은 복잡성을 상당히 증가시킵니다. 이러한 미리 서명(pre-signed) 된 병합 트랜잭션은 체인의 특정 부분의 실패에 따라 상위 네트워크 궁극적으로는 루트 네트워크에 전파 될 수 있습니다. 그러나 이 과정은 정확하게 행동하는 지명 된 당사자들에 의존합니다. 이는 개인이 사용되지 않은 모든 지불금을 단일 outputs 또는 outputs 집합으로 통합하여 출금 트랜잭션이 경제적으로 실현 가능하도록 합니다.

추가로 매우 가치 있는 토큰에 의해 결합 된 체인에 소액의 지불(micropayments)을 남기고 그 값에 대해 간접 적용할 수 있습니다. (플라즈마 체인을 완전히 죽이는(killing) 데에 충분한 불이익이 있기 때문에).

일반적인 재귀 SNARK / STARK가 실현가능 해지면, withheld 블록조차도, 철회하는 개체가 허가되지 않은 종료(exit)를 할 수 있는 권한을 보유하지 못하게 하는 것이 이론적으로 가능할 것이다.

최종성(Finality)

종료(exit)을 위한 분쟁에서는 본질적으로 최종 가정을 만듭니다. 밑에 놓인 체인이 최종성을 결정 짓기 위해 상당한 결합 비용을 갖는다면, 체인 간 싱크(synchronicity)를 맞추는 것에 문제를 야기하는 체인 재구성에 대한 위험을 크게 줄일 수 있습니다. 완화하는 방법의 예로는 'Ethereum CASPER finality gadget'가 있습니다.

루트 체인의 용량 부족 또는 비용 증가

이러한 완화하는 방법이 없으면, 요금이나 가스가 너무 비싸서 일정 기간 내에 거래를 종료 (exit)할 수 없습니다. E.g. 거래 수수료 / 가스 비용이 50배 증가하거나 종료(exit) 트랜잭션을 수행하기에 충분한 공간이 없고 마이너가 용량이나 가스 한도를 늘리지 않는다면

순서대로 종료(exit)를 허용하는 종료(exit) 카운팅 메커니즘을 일시 중지하여 종료(exit) 지연 시간을 연장함으로써 몇 가지 완화 방법이 있습니다. 과거 x 블록에서 발생한 종료(exit) 트랜잭션이 있는 한 종료(exit)를 일시 중지하여 이 작업을 수행 할 수 있습니다. 최근에 적어도 하나 이상의 종료(exit) 트랜잭션이 있는 경우 모든 사용자가 퇴출당할 수 있습니다. 누군가 종료하기 전에 종료가 발생하면, 카운터가 재설정됩니다. 그 결과, 자금을 수령하기 전에 얼마 동안 기다려야하는지 결정되지 않아 유동성 공급자의 비율에 대한 비용을 증가시킬 것 입니다.단순한 메커니즘은 평균 블록체인 가스 / 수수료 비용이 매우 높은 금액을 넘는 경우 인출 시간에 일시 중지하는 것입니다.(일시 중지 된 상태가 지속될 수 있는 합리적인 상한 시간에 의해 종료 됨).

자금을 보유한 사용자는 최소한 하나의 상위 플라즈마 체인에 대해 정보 가용성과 함께 높은 신뢰성을 지니고 있는지 확인해야 합니다.(이상적으로는 여러 명의 독립적인 부모들에 의해서).

루트 체인 검열 (Censorship)

이 설계에서는 루트 체인의 51 % 이상이 정직하다고 가정합니다. 루트 체인에 있는 참가자가 검열 블록을 사용하여 네트워크를 공격하는 경우, 종료(exit) 트랜잭션 또는 상태 업데이트에 상당한 어려움이 발생할 수 있으며 잠재적으로 자금 손실과 관련하여 중대한 문제가 발생할 수 있습니다. 검열은 보안의 핵심 요소이며 가치 기반 위험(value-at-risk)뿐만 아니라 최종성을 속이는 것(finality tricks) (e.g. CASPER finality gadget)은 향후 체인에서 제한되어야 할 수 있습니다.

이것은 zk-SNARKs / zk-SNARKs 자금 증명을 추가함으로써 완화 될 수 있지만, 새로운 엔지니어링 및 연구가 필요합니다.

모든 종료(exit) 트랜잭션의 한 부분으로 매우 큰 채권을 사용하면 마이너가 사기 증명의 상당 부분을 보상 받기 때문에 사기 증명에 동기를 부여할 것이며, 검열은 매우 어려울 것입니다.

이 네트워크에 제공되는 보안은 상위 플라즈마 체인과 루트체인 및 잔액(balance) 사이즈의 정직성과 정확성 함수를 제공하는 것입니다.

전 세계적으로 전달되는 양에 대한 구조적 제한(블록 당 종료(exit) 속도 제한)과 finality gadget보다 낮은 것을 보장하는 것은 이 문제를 완화시키는 가능한 경로가 될 수 있습니다.

체인 중단(halt)

체인이 멈추면 설정된 시간 후에 사전-커밋(pre-committed) 된 상태 전환을 제안을 할 수 있습니다. 그러면 거래를 처리하는 소비(consuming) 체인은 이를 수용하고 전체 체인 움직임을 브로드 캐스트 할 수 있습니다. 이것은 체인(부모 체인에서 브로드 캐스트되는 트랜잭션들은 무시)이 설정된 시간 동안 활동하지 않은 경우에만 허용됩니다. 사기 증명은 체인의 마지막에 대해 논란을 만들 수 있습니다.

그곳에는 복잡한 상태 전환을 포함하는 금융 활동을 중단시킬 수 있는 더 나은 인센티브가 있을 수 있습니다.

합의 규칙 변경 불가

설계가 미리 설정(front-loaded)되어 있기 때문에 사전에 프로그래밍하지 않고 합의 규칙을 변경할 수는 없습니다. 이는 업그레이드 경로를 시스템의 일부로 생성하여 완화 할 수 있습니다 (e.g. 특정 날짜 이후에 강제 중지). 이러한 합의 규칙 변경이 불가능한 것은 토큰 홀더가 시스템을 계속 운영하도록 하는 경제적 인센티브가 있기 때문에 사슬을 정지시킬 수없는 상황에 사회적 영향을 미칠 수 있습니다. 이는 플라즈마 체인이 시작된 후에는 플라즈마 체인을 정지시키는 것이 어려워지도록 만듭니다.

향후 연구

이러한 체인의 보안과 관련된 이익을 주는 것을 포함하여 향후에 추가로 연구되어야 할 영역이 있습니다. 현재 연구 분야는 일반적인 재귀 SNARK / STARK로 종료(exit) 트랜잭션의 보안을 크게 향상시킵니다. 심층적으로 보안하는 것이 바람직하므로 최전선의 보안은 새로운 암호와 안전한 하드웨어 요소이고 최후의 보안은 분쟁의 증거를 허용하는 직관적인 탈중앙화된 종료(exit) 메커니즘이 될 것입니다. 페어링 암호화 나 다른 유사 형태의 암호화에 대한 새로운 용도의 개발이 또한 도움이 될 수 있습니다.

싱크를 유지하면서 동시에 여러 루트 체인을 볼 수 있는 능력은 더 특별한 것이 필요합니다.(단순히 hard synchronicity를 시행하는 것을 넘어서)

블록체인 종료(exit) 위험의 최소화(SNARK / STARK가 여기에서 도움이 될 수 있음)뿐만 아니라 최종 체인 및 여러 체인 전반의 상호 작용에 대한 추가 연구가 필요합니다.

결론 및 요약

플라즈마는 데이터 압축으로 정보 가용성(특히 block withholding attacks 차단)을 보장하는 데 주안점을 두고 설계되었습니다.

우리는 루트 체인에 의해 시행되며 블록체인에서 자금을 보유 할 수 있게 하는 강력한 약속을 제출하는 메커니즘을 제안합니다.

이는 컴퓨터의 광범위한 amorphous 네트워크에서 중요한 계산 및 저장이 가능도록 합니다. 활동들은 모든 상위 체인을 통해 궁극적으로 시행 할 수 있는 경제적 활동자에 의해 결속되며 스마트 컨트랙트를 보유하고 있는 루트 체인까지 적용됩니다. 이 구성을 사용하면 루트 체인에서 비용대비 효율적으로 상태 전환을 수행 할 수 있습니다.

블록체인에 대한이 구성은 전 세계적으로 거의 모든 재무 계산에서 처리 약속이 될 수 있습니다 (한 번에 너무 많은 작업 메모리가 필요하지 않는 한). 만약 타당하지 않은 계산이 있는 경우에만 증명이 제출되고 해당 약정이 롤백됩니다. 체인 운영자에게 관리적인 신뢰를 제공 할 필요가 없습니다.

체인 정지 및 기타 비잔틴 행위에 대한 인센티브를 줄이기 위해. 수수료는 체인이 잘 운영되도록 인센티브를 창출합니다. 플라스마 체인이 이 체인과 관련된 토큰의 활동으로 묶여있다면 중지하지 않는 것이 좋습니다. 지속적인 운영에 상당한 경제적 인센티브가 생기는 반면에 체인이 멈추면 가치가 떨어질 것입니다.

이러한 인센티브와 구조로 인해 거래 수수료로 지속적으로 운영되는 탈중앙화되어 있으며 자율적으로 동작하는 프로그램을 만들 수 있습니다. 이러한 탈중앙화된 자율 응용 프로그램은 데이터가 처리 및 검증되지만 멤버가 변경 가능한 진정한 클라우드 컴퓨팅을 생성할 수 있습니다. 플라즈마를 사용하면 많은 수의 사용자가 많은 제한 없이 일반화 된 응용 프로그램을 제공 할 수 있도록 블록체인을 확장 할 수 있습니다. 응용 프로그램 작성자는 스마트 컨트랙트 코드를 작성한 다음 블록체인에 코드를 제출할 수 있으며 사람들이 Plasma 체인을 사용하여 수수료를 지불하는 한 이러한 컨트랙트는 계속 운영 될 수 있습니다.

알리는글

Chrstian Reitwießner를 포함하여 Merkleized 증명의 설계 및 구현을 위해 TrueBit 제작자에게 많은 감사의 말을 전합니다. 여러 분야에서 영감을 주고 이러한 아이디어를 형식화하는 데 도움이 되는 아이디어를 준 Vlad Zamfir에게 감사드립니다. 피드백 및 공헌을 한 Thomas Greco, Piotr Dobaczewski 및 Pawe l Peregud에게 감사드립니다.

참고문선

[1] Joseph Poon and Tadge Dryja. Lightning Network. https://lightning.network/lightning-network-paper.pdf, Mar 2015.

[2] Ethereum. Ethereum. https://ethereum.org.

[3] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. http://gavwood.com/paper.pdf, Feb 2015.

[4] Raiden. Raiden Network. https://raiden.network/.

[5] Jeffrey Dean and Sanjay Ghemawat. Mapreduce: Simplified data processing on large clusters. In OSDI, pages 137–150. USENIX Association, 2004.

[6] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, Oct 2008.

[7] Nick Szabo. Formalizing and Securing Relationships on Public Networks. http://szabo.best.vwh.net/formalize.html, Sep 1997.

[8] Fred Erhsam. Blockchain Tokens and the dawn of the Decentralized Business Model. https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.

[9] Naval Ravikant. The Bitcoin Model for Crowdfunding. https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/.

[10] Jason Teutsch and Christian Reitwiessner. A scalable verification solution for blockchains. https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf, Mar 2017.
46

[11] Vitalik Buterin. Ethereum Sharding FAQ. https://github.com/ethereum/wiki/wiki/Sharding-FAQ.

[12] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timn, and Pieter Wuille. Enabling Blockchain Innovations with Pegged Sidechains. https://blockstream.com/sidechains.pdf, Oct

2014.

[13] Paul Sztorc. Drivechain - The Simple Two Way Peg. http://www.truthcoin.info/blog/drivechain/.

[14] Bitcoin Wiki. Merged mining specification. https://en.bitcoin.it/wiki/Merged_mining_specification.

[15] Peter Todd. Tree Chains. https://github.com/petertodd/tree-chains-paper.

[16] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Mardas Virza. Succinct NonInteractive Zero Knowledge for a von Neumann Architecture. https://eprint.iacr.org/2013/879.pdf, May 2015.

[17] Alessandro Chiesa, Eran Tromer, and Madars Virza. Cluster Computing in Zero Knowledge. https://eprint.iacr.org/2015/377.pdf, Apr 2015.

[18] Jae Kwon. Cosmos: A Network of Distributed Ledgers. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md, Sep 2016.

[19] Gavin Wood. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. https://github.com/w3f/polkadot-white-paper/raw/master/PolkaDotPaper.pdf, Nov 2016.

[20] Sergio Demian Lerner. lumino transaction compression protocol (ltcp). https://uploads.strikinglycdn.com/files/9dcb08c5-f5a9-430e-b7ba-6c35550a4e67/LuminoTransactionCompressionProtocolLTCP.pdf, Feb 2017.

[21] Ilja Gerhardt and Timo Hanke. Homomorphic Payment Addresses and the Pay-toContract Protocol. http://arxiv.org/abs/1212.3257, Dec 2012.

[22] Tier Nolan. Re: Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949.