Positioning Paper
NervosNetwork

Kor ver.

1. 이 문서의 목적

Nervos Network는 다양한 프로토콜과 혁신으로 이루어져 있습니다. 핵심 프로토콜 디자인 및 구현에 대한 명확한 문서 및 기술 사양이 필요하기 때문에, 우리는 RFC (request for comment, 의견 요청) 프로세스를 활용합니다. 그러나 우리는 우리의 커뮤니티가 우리가 시도하는 것을 이해하고, 우리가 한 제안의 대가들, 그리고 우리가 현재 디자인 결정에 이르기까지 어떻게 도달했는지를 이해할 수 있도록 하는 것이 동등하게 중요하다고 생각합니다.

이 문서에서는 현재 퍼미션리스 블록체인이 직면한 문제와 이를 해결하려는 기존 솔루션에 대해 자세히 살펴봅니다. 우리는 이를 통해 독자들이 이러한 도전 과제에 최선의 방법으로 접근하고, 우리의 근본적인 디자인 결정을 이해할 수 있도록 하는 데 필요한 맥락을 제공할 것을 기대합니다. 그런 다음 Nervos Network의 모든 부분에 대한 높은 수준의 탐색을 제공하며, 이들이 어떻게 함께 작동하여 네트워크의 전반적인 비전을 지원하는지에 중점을 둡니다.

2. 배경

확장성, 지속 가능성 및 상호 운용성은 현재 공개 퍼미션리스 블록체인이 직면한 가장 큰 문제 중 일부입니다. 이러한 문제에 대한 해결책을 많은 프로젝트들이 주장하지만, 이러한 문제의 원인과 가능한 대가를 고려하여 문제에 대한 해결책을 이해하는 것이 중요합니다.

2.1 확장성

비트코인[1]은 최초의 공개 퍼미션리스 블록체인으로, P2P 전자 화폐로 사용하기 위해 설계되었습니다. 이더리움[2]은 보다 다양한 활용을 가능하게 하고 일반적인 탈중앙화 컴퓨팅 플랫폼을 만들었습니다. 그러나 두 플랫폼 모두 거래 가능성에 제한을 두고 있습니다. 비트코인은 블록 크기를 제한하고 이더리움은 가스의 한도를 제한합니다. 이는 장기적인 탈중앙화를 보장하기 위한 필수적인 단계이지만, 두 플랫폼의 기능을 제한하기도 합니다.

블록체인 커뮤니티는 최근 몇 년간 많은 확장성 솔루션을 제안해왔습니다. 일반적으로 이러한 솔루션은 온체인 확장과 오프체인 확장, 두 가지 범주로 나눌 수 있습니다.

온체인 확장 솔루션은 합의 프로세스의 처리량을 확장하고 중앙집중 시스템과 경쟁 가능한 기본 처리량을 갖는 블록체인을 만드는 것을 목표로 하며, 오프체인 확장 솔루션은 거의 모든 거래를 상위 레이어로 이동하면서 블록체인을 안전한 자산 및 정산 플랫폼으로만 사용하는 차이를 갖고 있습니다.

2.1.1 단일 블록체인을 사용한 온체인 스케일링

블록체인의 처리량을 증가시키는 가장 간단한 방법은 블록 공간을 늘리는 것입니다. 블록 공간이 추가되면 더 많은 거래가 네트워크를 통해 흐르고 처리될 수 있습니다. 증가하는 거래

수요에 대응하여 블록 공간을 늘리는 것은 수수료를 낮게 유지하는 데 필수적입니다.

비트코인 캐시(BCH)는 이 방법을 채택하여 P2P 결제 네트워크를 확장했습니다. 비트코인 캐시 프로토콜은 처음에 최대 블록 크기를 8MB로 설정하였으며, 나중에 32MB로 늘리기도 하였고, 거래 수요가 증가함에 따라 블록 크기는 계속해서 증가할 예정입니다. 참고로, 2017년 8월 세그윗(Segregated Witness)을 구현한 비트코인(BTC)은 평균 블록 크기가 약 2MB가 되도록 변경되었습니다.

데이터센터의 범위 내에서는 수학적으로 문제가 없습니다만, 만약 75억 명이 하루에 각각 2개의 온체인 거래를 생성한다면, 10분마다 26GB의 블록을 생산해야 하며, 블록체인 성장률은 하루에 3.75TB 또는 1.37PB가 됩니다[3]. 이러한 저장 및 대역폭 요구 사항은 현재 클라우드 서비스에서도 적합합니다.

그러나 노드 운영을 데이터센터 환경으로 제한하면 하나의 유효한 네트워크 토폴로지(topology)만 존재하게 되며, 보안 측면에서 타협을 강요하고 (블록체인의 포크 비율이 네트워크 간 데이터 전송 요구 사항이 증가함에 따라 증가함) 중앙 집중화도 증가시킵니다 (전체 노드 수가 합의 참여 비용이 증가함에 따라 감소됨).

경제적인 측면에서, 블록 크기를 계속 늘리면 사용자가 느끼는 수수료 압박을 완화할 수 있습니다. 비트코인 네트워크의 분석 결과, 수수료는 블록이 약 80% 정도 차지하면 평평하게 유지되다가 급격히 증가한다는 것을 보여줍니다[4].

그러나 성장하는 네트워크의 비용 부담을 운영자에게 떠넘기는 것은 합리적인 결정처럼 보일 수 있지만, 이는 두 가지 이유로 인해 장기적으로는 현명하지 못한 선택일 수 있습니다.

- 트랜잭션 수수료의 억제는 채굴자들이 새로운 코인 발행(블록 보상)에서 대부분의 보상을 받게 합니다. 그러나 인플레이션이 프로토콜의 영구적인 부분이 아닌 경우, 전체 코인 하드캡이 달성되면 새로운 코인 발행은 결국 멈추게 되며, 채굴자들은 블록 보상이나 상당한 거래 수수료를 받지 못하게 됩니다. 이로 인해 경제적 영향이 발생하며, 이는 네트워크의 보안 모델을 심각하게 저해시킵니다.
- 전체 노드를 운영하는 데 드는 비용이 급증하게 됩니다. 이는 보통 사용자들이 블록체인의 이력과 거래 내역을 독립적으로 검증하는 능력을 제거하며, 거래의 진실성을 보장하기 위해 거래소나 결제 처리 업체와 같은 서비스 제공 업체에 의존하게 합니다. 이러한 신뢰 요구사항은, 퍼미션리스 블록체인의 핵심 가치 제안인 동등한 P2P, 신뢰 없는 분산 시스템을 무효화시킵니다.

거래 비용을 최적화한 비트코인 캐시와 같은 플랫폼은 기타 블록체인(퍼미션, 퍼미션리스) 및 전통적인 결제 시스템과의 중요한 경쟁을 직면하고 있습니다. 보안 또는 검열 저항력을 향상시키는 설계 결정은 관련 비용을 발생시키고, 이에 따라 플랫폼 사용 비용이 증가합니다. 경쟁 환경과 네트워크 명시적 목표를 고려할 때, 낮은 비용이 모든 고려 사항을 희생시키는 것보다 우선시되는 목표가 될 것입니다.

이 목표는 거래 네트워크 사용의 관찰 결과와 일관됩니다. 이러한 시스템을 사용하는 사용자들은 네트워크를 짧은 시간 동안만 사용하기 때문에 중요한 장기적인 트레이드 오프에 무관심합니다. 상품이나 서비스를 받고 결제를 마친 후에는 이러한 사용자들은 더 이상 네트워크의 효율적인 운영에 대해 관심이 없습니다. 중앙 집중형 암호 자산 거래소 및 더 중앙 집중형 블록체인의 광범위한 사용에서 이러한 트레이드 오프의 수용이 분명하게 나타납니다. 이러한 시스템은 주로 편의성과 거래 효율성 때문에 인기가 있습니다.

일부 스마트 컨트랙트 플랫폼은 블록체인 처리량 확장에 대해 유사한 접근 방식을 취하고, 제한된 집합의 "슈퍼 컴퓨터" 검증자들만이 합의 프로세스에 참여하고 블록체인을 독립적으로 검증할 수 있습니다.

탈중앙화와 네트워크 보안 측면에서 양보를 하면 더 싼 거래 비용과 일부 사용자들에게는 편리함을 제공할 수 있지만, 장기적인 보안 모델의 양보, 거래 독립적 검증의 비용 장벽, 그리고 노드 운영자의 집중과 고착화 가능성으로 인해, 이는 공개 블록체인 확장을 위한 적절한 방식이 아니라는 결론에 이르게 했습니다.

2.1.2 다중 체인을 통한 온체인 확장

다중 체인을 통한 온체인 확장은 이더리움 2.0에서 보인 샤딩 또는 폴카닷(Polkadot)에서 볼 수 있는 어플리케이션 체인을 통해 구현될 수 있습니다. 이러한 설계는 전역 상태와 거래를 여러 체인으로 분할하여 각 체인이 빠르게 지역 합의에 도달하고, 나중에는 "비콘 체인" 또는 "릴레이 체인"의 합의를 통해 전체 네트워크가 전역 합의에 도달할 수 있도록 허용합니다.

이러한 설계는 다중 체인이 공유 보안 모델을 활용하면서, 샤드(이더리움) 또는 파라 체인(폴카닷) 내에서 높은 처리량과 빠른 거래를 가능하게 합니다. 이러한 시스템은 상호 연결된 블록체인 네트워크이지만, 각 체인에서 실행되는 프로토콜에 대해 차이가 있습니다. 이더리움 2.0에서는 각 샤드가 동일한 프로토콜을 실행하지만, 폴카닷에서는 각 패러 체인이 Substrate 프레임워크를 통해 생성된 사용자 정의 프로토콜을 실행할 수 있습니다.

이러한 다중 체인 아키텍처에서 각 dApp(또는 dApp의 인스턴스)은 하나의 체인에만 상주합니다. 블록체인에서 어떤 다른 dApp과도 원활하게 상호작용할 수 있는 능력에 익숙한 개발자들이 오늘날은 있지만, 설계 패턴은 새로운 다중 체인 아키텍처에 적응해야 할 필요가 있습니다. 만약 dApp이 다른 샤드에 걸쳐 분할되면, 해당 dApp 인스턴스가 다른 샤드에 상주하더라도 상태를 동기화하는 메커니즘이 필요합니다. 또한, 교차 샤드 거래는 전역 합의를 필요로 하며, 확인 지연시간을 도입할 수 있습니다.

이 비동기적인 트랜잭션들로, 악명 높은 "기차와 호텔" 문제가 발생합니다. 예를 들어 두 개의 트랜잭션이 원자적이어야 하는 경우 (예를 들어 서로 다른 샤드에서 기차표와 호텔 예약을 하는 경우) 새로운 솔루션이 필요합니다. 이 문제를 해결하기 위해 이더리움은 종속적인 컨트랙트를 삭제하고 다른 종속적인 컨트랙트가 포함된 두 번째 샤드에 생성한 후, 두 트랜잭션 모

두 두 번째 샤드에서 실행하는 "컨트랙트 이관"(contract yanking)을 도입합니다. 그러나 이관된 컨트랙트는 원래의 샤드에서 사용할 수 없게 되므로 이용성 문제를 발생시키고 다시 새로운 디자인 패턴이 필요하게 됩니다.

샤딩에는 그 자체로 이점과 도전 과제를 가지고 있습니다. 샤드가 실제로 독립적이고 샤드 간 필요성이 최소한이면 블록체인은 샤드 수를 증가시켜 처리량을 선형적으로 확장할 수 있습니다. 이것은 외부 상태나 다른 애플리케이션과의 협력이 필요하지 않은 독립된 애플리케이션에 가장 적합합니다.

하지만 블록체인 애플리케이션을 구성하는 "빌딩 블록" 애플리케이션들을 결합하여 개발하는 경우 (이를 "composability problem"이라고 합니다) 샤드 아키텍처는 문제가 발생할 수 있습니다. 특히, 이는 탈중앙화 금융(DeFi) 분야에서 빌딩 블록 제품 위에 더 복잡한 제품을 만드는 경우에 더욱 중요합니다.

기술적인 측면에서 샤딩은 보통 "1 + N" 토폴로지가 필요합니다. 이는 N 개의 체인이 메타체인에 연결되는 구조를 의미하며, 메타체인이 스케일링 문제에 직면하지 않으면서 지원 가능한 샤드 수에 상한선이 도입됩니다.

우리는 통합된 전역 상태에 상당한 가치를 인식하며, 종속적인 애플리케이션 생태계와 개발자가 엣지에서 혁신할 수 있도록 웹 개발자의 하위 수준 문제에 대해 라이브러리를 사용하고 서비스 통합을 위해 오픈 API를 사용하는 것과 유사한 방식으로 개발자가 개발을 진행할 수 있도록 합니다. 블록체인 상호작용의 구조적 고민에 대한 일관성으로 인해 동기화(샤드간 자산 전송이나 메시지 전달)를 고려할 필요가 없어지므로 훨씬 간단한 개발 경험을 제공하며 사용자 경험도 우수해집니다.

우리는 샤딩이 유망한 확장성 해결책이라고 인식하지만, 상호의존성이 적은 애플리케이션에 특히 적합한 것으로 판단되며, 가장 가치 있는 상태를 단일 블록체인에 집중시키는 디자인을 가지는 것이 유용하다고 믿습니다. 이 디자인에서는 오프체인 스케일링 접근 방식을 활용하여 더 높은 처리량을 제공할 수 있습니다.

2.1.3 레이어 2를 통한 오프체인 스케일링

레이어 2 프로토콜에서 기본 블록체인은 결제(또는 커밋) 레이어로 작동하며, 두 번째 레이어 네트워크는 암호학적 증명을 경유하여 참가자가 암호화폐를 "인수"할 수 있도록 라우팅 됩니다. 두 번째 레이어의 모든 활동은 기본 블록체인과 암호학적으로 보호되며, 기본 레이어는 두 번째 레이어 네트워크로 진입/이탈하는 금액을 결제하고 분쟁 해결에만 사용됩니다. 이러한 설계는 자금의 보관 권한(또는 손실 위험)의 위임 없이 작동하며 즉각적이고 거의 무료인 거래를 가능하게 합니다.

이러한 기술들은 비트코인과 같은 가치 저장망이 일상 결제에 사용될 수 있는 방법을 보여줍

니다. 실제 레이어 2 솔루션의 가장 일반적인 예는 고객과 커피숍 사이의 결제 채널입니다. 예를 들어 앨리스 씨가 매일 아침 비트코인 커피숍을 방문한다고 가정해 봅시다. 그녀는 매월 커피숍과 열어 둔 라이트닝 결제 채널에 자금을 예치합니다. 그녀가 매일 방문할 때마다, 그녀는 커피를 받기 위해 일부 자금을 채널에서 가져가도록 커피숍에 대한 권리를 암호학적으로 서명합니다. 이러한 거래는 즉각적으로 이루어지며 완전히 P2P "오프체인"이므로 원활한 고객 경험을 가능하게 합니다. 라이트닝 채널은 신뢰성이 있으며 앨리스 씨나 커피숍은 언제든지 채널을 종료하여 그 때까지 받을 자금을 가져갈 수 있습니다.

라이트닝과 같은 결제 채널 기술은 오프 체인 확장 기술의 한 예일 뿐이며, 이 방법으로 블록체인 처리량을 안전하게 확장할 수 있는 많은 성장 기술이 있습니다. 결제 채널은 두 당사자 간에 잔액을 채널링하는 오프 체인 계약을 포함하고, 상태 채널은 채널 참가자 간에 임의의 상태를 오프 체인 계약으로 포함합니다. 이러한 일반화는 확장 가능하고, 신뢰 없이 분산된 애플리케이션의 기초가 될 수 있습니다. 단일 상태 채널은 여러 애플리케이션에서도 사용할 수 있으므로 효율성을 더욱 높일 수 있으며, 채널에서 한 당사자가 채널을 종료할 준비가 되면, 암호화된 증명을 블록체인에 제출하여 합의된 상태 전이를 실행할 수 있습니다.

사이드체인은 신뢰할 수 있는 제3자 블록체인 운영자를 통해 처리량을 늘리는 다른 구성입니다. 신뢰할 수 있는 블록체인과 양방향 핀을 이용하여 자금을 주 체인과 사이드체인 간에 이동할 수 있습니다. 이를 통해 사이드체인에서 신뢰할 수 있는 거래량을 처리하고, 나중에 주 체인에서 최종 정산이 가능합니다. 사이드체인 거래는 수수료가 적고, 빠른 확인과 높은 처리량을 갖습니다. 그러나, 보안에 관해서는 어느 정도 타협해야 합니다. 하지만 보안을 저해하지 않으면서도 같은 성능 향상을 제공할 수 있는 무신뢰 사이드체인에 대한 많은 연구가 진행 중입니다.

Plasma는 신뢰할 수 있는 사이드체인 기술의 한 예로 (5.3절에서 다룸), 전체적으로 글로벌 합의를 얻은 블록체인에 대한 신뢰 루트(trust root)를 활용하는 사이드체인 아키텍처입니다. Plasma 체인은 중앙 집중형 사이드체인과 동일한 성능 향상을 제공하지만 보안 보장 역시 제공합니다. 만약 Plasma 체인 운영자가 악의적이거나 제대로 작동하지 않는다면, 사용자들은 사이드체인 자산을 메인체인으로 안전하게 인출할 수 있는 메커니즘을 제공받습니다. 이는 Plasma 체인 운영자의 협조 없이 이루어지며, 사용자들은 사이드체인 거래의 편리성과 레이어 1 블록체인의 보안성 모두를 누릴 수 있습니다.

오프 체인 스케일링은 탈중앙화, 보안 및 확장성을 제공합니다. 결제 및 분쟁 해결 외의 모든 것을 오프 체인으로 이동함으로써 공개 블록 체인의 제한된 글로벌 합의가 효율적으로 활용됩니다. 응용 프로그램 요구 사항에 따라 다양한 레이어 2 프로토콜을 구현할 수 있으며, 개발자와 사용자에게 유연성을 제공합니다. 네트워크에 더 많은 참여자가 추가되면 성능이 영향을 받지 않으며, 모든 참가자는 레이어 1 합의에서 제공되는 보안 보장을 공유할 수 있습니다.

2.2 지속 가능성

자율적이고 소유하지 않은 공개 블록체인의 장기적인 운영을 유지하는 것은 상당한 도전입니다. 다양한 이해관계자들 사이에 균형잡힌 인센티브가 필요하며, 시스템은 전체 노드 운영과 공개 검증이 가능한 방식으로 설계되어야 합니다. 하드웨어 요구 사항은 합리적으로 유지되어야 하며, 동시에 개방적이고 글로벌한 네트워크를 지원해야 합니다.

블록체인의 네이티브 자산의 인센티브와 제어는 장기 보유자들의 가치 상승 요구와 네트워크를 보호하는 채굴자 또는 검증자들의 보상 요구를 균형 있게 조절할 수 있어야 합니다.

또한, 공개 블록체인이 운영되고 나면, 프로토콜을 지배하는 규칙을 변경하는 것이 매우 어렵습니다. 따라서 시스템은 지속 가능하게 설계되어야 합니다. 이에 대한 관심으로, 우리는 지속 가능한 퍼미션리스 블록체인을 구축하는 과제들을 철저히 조사해 보았습니다.

2.2.1 탈중앙화

공개 블록체인이 장기적으로 직면하는 가장 큰 위협 중 하나는 전체 노드 운영 비용에 반영된 독립적 참여와 거래 검증의 장벽이 점점 높아지는 것입니다. 전체 노드는 블록체인 참가자가 온체인 상태,기록을 독립적으로 확인하고, 잘못된 블록을 전달하지 않아 채굴자나 검증자를 책임질 수 있게 해줍니다. 전체 노드의 비용이 증가하고 그 수가 감소함에 따라, 블록체인 참가자들은 현재 상태와 기록을 제공하는 전문 서비스 운영자에 의존해야 하므로, 공개 퍼미션리스 블록체인의 근본적인 신뢰 모델이 침해됩니다.

전체 노드가 블록체인 진행에 따라 가지고 있어야 할 적절한 컴퓨팅 처리량, 트랜잭션 수신 대역폭, 전역 상태를 저장하기 위한 저장 용량이 필요합니다. 전체 노드의 운영 비용을 제어하기 위해 프로토콜은 모든 이러한 자원의 처리량 또는 용량 성장을 제한하는 조치를 해야 합니다. 대부분의 블록체인 프로토콜은 컴퓨팅 처리량이나 대역폭 처리량을 제한하지만, 전역 상태의 성장을 제한하는 프로토콜은 거의 없습니다. 이러한 체인이 크기와 운영 기간이 길어질수록, 전체 노드 운영 비용은 불가피하게 증가할 것입니다.

2.2.2 경제 모델

최근 몇 년간 합의 프로토콜에 대한 많은 연구가 이루어졌지만, 우리는 암호 경제학이 미완성된 분야라고 믿습니다. 일반적으로, 레이어 1 프로토콜의 현재 암호 경제 모델은 네트워크 합의를 보장하기 위한 인센티브와 처벌에 중점을 둔 것이며, 네이티브 토큰은 대부분 거래 수수료를 지불하거나 스테이킹 요구 사항을 충족시키기 위해 사용됩니다.

우리는 잘 설계된 경제 모델이 합의 과정을 넘어 프로토콜의 장기적인 지속 가능성을 보장해야 한다고 믿습니다. 특히, 경제 모델은 다음 목표를 가지고 설계되어야 합니다.

- 네트워크는 서비스 제공자(보통 채굴자 또는 검증자)를 보상하기 위한 지속 가능한 수익 모델을 가져야 하며, 이를 통해 네트워크가 지속적으로 안전하게 유지될 수 있어야 합니다.

- 네트워크 참여 장벽이 낮아지도록 지속 가능한 방법을 가져야 하며, 이를 통해 네트워크가 시간이 지나도 탈중앙화된 상태로 유지될 수 있어야 합니다.
- 공개 네트워크의 자원은 효율적이고 공정하게 할당되어야 합니다.
- 블록체인의 네이티브 토큰은 타당한 내재 가치가 있어야 합니다.

2.2.3 비트코인의 경제 모델 분석

비트코인 프로토콜은 블록의 크기를 제한하고 고정된 블록 시간을 시행합니다. 이로 인해 네트워크의 대역폭 처리량은 사용자가 거래 수수료를 통해 경쟁해야 하는 희귀한 자원입니다. 비트코인 스크립트는 루프를 허용하지 않으므로, 스크립트의 길이는 그것의 계산 복잡성의 좋은 근사치가 됩니다. 일반적으로, 블록 공간에 대한 수요가 높아질수록 사용자들에게 더 높은 거래 수수료가 부과됩니다. 또한, 거래에 참여하는 데 필요한 입력, 출력 또는 계산 단계가 많을수록 사용자가 지불해야 하는 거래 수수료도 더 많아집니다.

비트코인의 내재적 가치는 대부분 금융 프리미엄(사회가 이를 화폐로 취급하는 의지)에서 비롯되며, 특히 가치 저장 수단으로 사용하기 위한 의지에서 비롯됩니다. 채굴 수익은 BTC로 책정되기 때문에 이러한 인식은 비트코인의 경제 모델이 지속 가능하도록 유지되어야 합니다. 다시 말해, 비트코인의 보안 모델은 순환적이며, 네트워크가 지속 가능하게 보안되고 화폐 저장 수단으로 사용될 수 있다는 집단적인 믿음에 따라 결정됩니다.

비트코인의 블록 크기 제한은 사실상 네트워크 참여 장벽을 설정합니다. 블록 크기 제한이 낮을수록 비전문가들도 전체 노드를 운영하기 쉬워집니다. 비트코인의 전역 상태는 UTXO(미사용 트랜잭션 출력, Unspent Transaction Outputs) 집합입니다. 이 집합의 성장률은 블록 크기 제한을 사용해 효과적으로 제한됩니다. 사용자들은 효율적으로 UTXO를 생성하고 활용하도록 인센티브가 주어지며, UTXO가 더 많이 생성될수록 트랜잭션 수수료도 높아집니다. 그러나 UTXO를 결합하고 전체 상태의 크기를 줄이기 위한 인센티브는 제공되지 않기때문에, UTXO가 생성되면 사용될 때까지는 무료로 전체 상태를 차지합니다.

비트코인의 거래 수수료 기반 경제 모델은 프로토콜에서 부과된 희소 자원인 대역폭 처리량을 할당하는데 공정한 모델입니다. 이것은 P2P 결제 시스템에 적합한 경제 모델이지만, 진정한 가치 보관 플랫폼으로는 부적합합니다. 가치를 저장하기 위해 블록체인을 이용하는 비트코인 사용자는 한 번의 거래 수수료만을 지불하고 계속해서 채굴자에 의해 제공되는 지속적인 보안을 누릴 수 있습니다. 이 보안은 채굴자가 계속 자원을 투자해야 하므로 비트코인의 상태가 계속 유지되어야 한다는 전체적인 신뢰에 따라 결정됩니다.

비트코인은 총 발행량 상한선을 가지며, 새로운 발행은 블록 보상을 통해 이루어지고, 언젠가는 0이 될 것인데, 이는 두 가지 문제를 일으킬 수 있습니다.

첫째, 비트코인이 가치 저장 수단으로 계속 성공할 경우 BTC의 단위 가치는 계속 증가하고,

네트워크가 보호하는 총 가치도 증가할 것입니다(즉, 더 많은 금전적 가치가 네트워크로 이동함). 가치 저장 수단 플랫폼은 시간이 지남에 따라 보호하는 가치가 증가함에 따라 보안 예산을 늘릴 수 있어야 합니다. 그렇지 않으면 공격자가 이중 지불을 하고 네트워크 자산을 도난당할 수 있습니다.

프로토콜 보안을 깨는 비용이 성실하게 행동할 때 얻을 수 있는 이익보다 적으면 공격자는 언제나 공격을 합니다. 이것은 도시가 부유해짐에 따라 군사 지출을 늘려야 하는 것과 유사합니다. 이 투자가 없으면 일찍이 도시는 공격받아 약탈당할 것입니다.

블록 보상의 존재로 인해, 비트코인은 저장하는 총 가치에 따라 보안을 확장할 수 있습니다. 비트코인 가격이 두 배가 되면, 채굴자가 블록 보상에서 받는 수입도 두 배가 되기 때문에, 그들은 두 배의 해시율을 생산할 여력이 있습니다. 이로 인해 네트워크를 공격하는 데 두 배의 비용이 들게 됩니다.

그러나 이는 예측 가능한 블록 보상이 제로에 도달할 때 변경됩니다. 채굴자들은 전적으로 거래 수수료에 의존해야 하며, 그들의 수입은 더 이상 비트코인 자산 가치에 비례하지 않을 것입니다. 대신 네트워크의 거래 수요에 의해 결정될 것이기때문에, 거래 수요가 충분하지 않으면 이용 가능한 블록 공간이 채워지지 않으므로 총 거래 수수료는 미약해질 것입니다. 거래 수수료는 엄격하게 블록 공간 수요의 함수이며 비트코인 가격과는 독립적입니다. 이는 비트코인의 보안 모델에 깊은 영향을 미칠 것이며, 비트코인이 안전하게 유지되기 위해서는 일관되고 초과 용량의 거래 수요가 있어야 하고, 이것은 비트코인 가격에 비례해서 확장되어야 합니다. 이는 매우 강력한 가정입니다.

둘째로, 예측 가능한 블록 보상이 제로가 되면 채굴자의 블록당 수입의 분산이 증가하며 블록체인을 진행하는 대신 포크하는 동기를 제공합니다. 극단적인 경우 채굴자의 메모리 풀이 비어있고 수수료가 많이 들어있는 블록을 받으면, 그들의 동기는 수익이 없을 가능성이 있는 블록을 생성하고 진행하는 대신 체인을 포크하고 수수료를 가로채는 것입니다[5]. 이는 비트코인 커뮤니티에서 "수수료 도둑질(fee sniping)" 챌린지로 알려져 있으며, 비트코인의 하드캡을 제거하지 않으면 아직도 만족스러운 해결책이 없습니다.

2.2.4 스마트 컨트랙트 플랫폼의 경제 모델 분석

스마트 컨트랙트 플랫폼의 전형적인 경제 모델은 더 많은 도전 과제를 직면하고 있습니다. 예를 들어 이더리움을 살펴보면, 이더리움의 스크립트는 루프를 허용하기 때문에 스크립트의 길이는 해당 스크립트의 계산 복잡성을 반영하지 않습니다. 이것이 이더리움이 블록 크기나 대역폭 처리량을 제한하지 않고, 대신 블록 가스 한도로 표현되는 계산 처리량을 제한하는 이유입니다.

이더리움 블록체인에 자신의 거래를 기록하려면 사용자들은 거래 수수료로 지불할 준비가 있는 계산 비용을 입찰해야 합니다. 이더리움은 ETH로 가격이 책정된 계산 비용의 측정 단위인

"가스" 개념을 사용하며, "가스 가격" 비율 제어를 통해, 기본 토큰의 가격 변동과 무관하게 계산의 각 단계 비용이 독립적으로 책정됩니다. ETH 토큰의 본질적 가치는 분산 계산 플랫폼의 지불 토큰으로서의 위치에서 비롯되며, 이더리움에서의 계산 비용 지불 수단으로만 사용할 수 있는 유일한 화폐입니다.

이더리움의 전역 상태는 EVM(Ethereum Virtual Machine, 이더리움 가상머신)의 상태 트라이로 나타내며, 모든 계정의 잔액과 내부 상태를 포함하는 데이터 구조입니다. 새 계정이나 계약 값이 생성될 때 전역 상태의 크기가 확장됩니다. 이더리움은 상태 저장소에 새 값이 삽입되는 데 고정된 양의 가스를 청구하며, 값이 제거될 때 거래의 가스 비용을 상쇄하는 고정된 "가스 스티펜드(gas stipend)"를 제공합니다.

"한번 지불하면 영구적으로 점유"하는 저장소 모델은 채굴자와 전체 노드의 지속적인 비용 구조와 일치하지 않으며, 사용자가 상태를 자발적으로 제거하거나 더 빨리 제거할 동기를 제공하지 않기 때문에 결과적으로, 이더리움은 상태 크기가 급격히 증가하였습니다. 더 큰 상태 크기는 거래 처리 속도를 늦추고 전체 노드의 운영 비용을 높입니다. 상태를 청산할 강력한 동기가 없으면, 이러한 경향은 계속될 것입니다.

비트코인과 유사하게, 이더리움의 수요 중심 가스 가격 책정은 플랫폼의 희귀 자원인 계산 처리량을 할당하는 공정한 모델입니다. 이 모델은 또한 이더리움이 탈중앙화 계산 시스템으로서의 목적에 부합하지만, 이더리움의 상태 저장료 모델은 탈중앙화 상태나 자산 저장 플랫폼의 가능성과 맞지 않습니다. 장기적인 상태 저장에 대한 비용이 없으면 항상 사용자의 이익에 맞게 무료로 상태를 영원히 점유할 것입니다. 상태 저장 용량의 희소성이 없으면 시장도 형성되지 않고 공급과 수요 역학도 확립될 수 없습니다.

비트코인이 코어 프로토콜에서 블록 크기 제한을 지정하는 반면, 이더리움은 채굴자가 블록을 생산할 때 블록 가스 한도를 동적으로 조정할 수 있도록 허용합니다. 고급 하드웨어와 상당한 대역폭을 가진 채굴자는 더 많은 블록을 생산할 수 있으며, 이 투표 과정을 지배하게 됩니다. 그들의 이익은 블록 가스 한도를 상승시켜 참여 장벽을 높이고 작은 채굴자들을 경쟁에서 제외시키는 것이기 때문에, 이것은 전체 노드 운영 비용이 급격히 상승하는 또 다른 요인이라고 볼 수 있습니다.

이더리움과 같은 스마트 컨트랙트 플랫폼은 다양한 자산을 지원하는 멀티 자산 플랫폼입니다. 이러한 자산은 "토큰"으로 표현되며 발행 및 거래가 가능합니다. 이러한 플랫폼은 자체 네이티브 토큰 뿐만 아니라 모든 암호화폐 자산의 가치를 보호하기 위한 보안 기능을 제공하며, 멀티 자산 컨텍스트에서의 "가치 저장"은 이에 따라 플랫폼의 네이티브 토큰과 플랫폼에 저장된 모든 암호화 자산의 가치 보존 속성에 혜택을 제공한다는 의미입니다.

비트코인은 블록 보상을 통해 우수한 "가치 저장" 경제 모델을 가지고 있습니다. 채굴자는 BTC로 지불되는 고정 블록 보상을 받으므로 BTC 가격이 오르면 수익도 증가합니다. 이에 따라 플랫폼은 채굴자에게 수익을 높이도록 블록 보상을 지급함으로써 보안성을 유지하면서 수익을 증대시킬 수 있습니다.

멀티 자산 플랫폼에서는 "가치"가 네이티브 토큰 이상의 암호화 자산으로 표현될 수 있기 때문에 이 요구 사항을 충족시키는 것이 더욱 어려워집니다. 플랫폼이 보호하는 암호화 자산의 가치가 증가하더라도 네이티브 토큰의 가치가 증가하지 않으면, 네트워크 보안은 증가하지 않으며 플랫폼의 합의 과정을 공격하여 플랫폼에 보관된 암호화 자산을 이중으로 지불하는 것이 더욱 유리해집니다.

다중 자산 스마트 컨트랙트 플랫폼이 가치 저장소로 기능하기 위해서는, 블록체인 상의 자산을 소유하는 수요가 해당 네이티브 토큰 소유의 수요를 분명히 만들 수 있어야 합니다. 다시 말해, 플랫폼의 네이티브 토큰은 플랫폼의 총 자산 가치를 잘 반영할 수 있어야 합니다. 플랫폼의 네이티브 토큰의 내재적 가치가 거래 수수료 지불에 제한된 경우, 그 가치는 단지 거래 수요에만 결정됩니다. 네이티브 토큰의 가격은 플랫폼에 저장된 암호 자산 소유의 수요에 반응하지 않을 것입니다.

가치 저장소로 기능하도록 설계되지 않은 스마트 컨트랙트 플랫폼은, 네이티브 토큰의 화폐적 프리미엄(사람들이 내재 가치 이상으로 토큰을 보유할 의향)에 의존하여 계속해서 보안을 유지할 수 있습니다. 이는 어떤 플랫폼이 독특한 기능을 가지고 있거나 다른 플랫폼보다 최소 거래 비용을 제공하여 경쟁에서 우위를 점할 수 있는 경우에만 실현 가능합니다.

현재 이더리움은 그런 지배력을 가지고 있어서 자체의 통화 프리미엄을 유지할 수 있습니다. 그러나 경쟁 플랫폼들이 떠오르면서 더 높은 TPS를 지원하고 비슷한 기능을 제공하는 플랫폼들이 등장하면서, 자체 토큰의 통화 프리미엄만으로 블록체인 플랫폼의 보안을 유지할 수 있는지는 논란이 되고 있습니다. 특히, 해당 토큰들이 돈으로 설계되지 않거나 돈으로 여겨지지 않는 경우에는 더욱 그렇습니다. 게다가, 플랫폼이 고유한 기능을 제공한다고 하더라도, 대규모의 블록체인 채택이 이루어지면 효율적인 스왑으로 토큰의 통화 프리미엄이 추상화될 수 있습니다. 사용자들은 가장 익숙한 자산인 비트코인이나 스테이블 코인 등을 보유하면서 거래 수수료를 지불하기 위해 필요한 순간에만 플랫폼 토큰을 획득하게 될 것이고, 그렇다면 어느 경우에도, 플랫폼의 암호경제의 기반이 붕괴될 것입니다.

레이어 1 멀티 자산 플랫폼들은 그들이 보호하는 모든 암호 자산들에 대한 지속 가능한 보안을 제공해야하며, 즉, 그들은 가치 저장을 위해 설계된 경제 모델을 가지고 있어야 합니다.

2.2.5 핵심 프로토콜 개발 자금 조달

공개 퍼미션리스 블록체인은 공공 인프라입니다. 이러한 시스템의 초기 개발은 많은 자금을 필요로 하며 운영 후에도 지속적인 유지보수와 업그레이드가 필요합니다. 시스템을 유지 보수하지 않으면 치명적인 버그와 최적화되지 않은 운영의 위험에 노출됩니다. 비트코인과 이더리움 프로토콜은 지속적인 개발 자금 조달을 보장하는 내부 메커니즘이 없기 때문에, 이러한 시스템은 관련 이해관계를 가진 비즈니스의 지속적인 참여와 이타적인 오픈소스 커뮤니티의 지원에 의존합니다.

Dash는 자금 조달을 위해 트레저리를 최초로 활용한 프로젝트입니다. 이러한 디자인은 프로토콜 개발을 지속적으로 지원하면서도, 암호화폐 가치의 지속 가능성에 대한 타협이 필요합니다. 대부분의 블록체인 트레저리와 마찬가지로 이 모델은 인플레이션 기반 자금 조달에 의존하며, 장기 보유자들의 가치가 침식됩니다.

Nervos Network는 핵심 개발에 대한 지속 가능 자금 조달을 제공하는 트레저리 모델을 사용합니다. 트레저리 자금은 단기 토큰 홀더의 목표 인플레이션으로부터 유입되며, 이 인플레이션의 영향은 장기 보유자에게 완화됩니다. 이러한 메커니즘에 대한 자세한 정보는 (4.5)에서 설명하겠습니다.

2.3 상호 운용성

블록체인 간 상호 운용성은 종종 논의되는 주제로, 이 도전 과제를 해결하기 위해 많은 프로젝트가 제안되어 왔습니다. 신뢰성 있는 블록체인 거래를 통해 탈중앙화된 경제에서 실제 네트워크 효과를 실현할 수 있습니다.

블록체인 상호 운용성의 첫 번째 예는 비트코인과 라이트코인 간의 아토믹 스왑(Atomic Swap)입니다. 비트코인과 라이트코인 간의 신뢰성 있는 거래는 프로토콜 내 기능이 아닌, 공유 암호화 표준(특히 SHA2-256 해시 함수 사용)을 통해 가능합니다.

마찬가지로, 이더리움 2.0의 디자인은 많은 샤드 체인 간의 상호 연결성을 가능하게 합니다. 이러한 체인들은 모두 같은 프로토콜을 실행하고 동일한 암호화 기본 요소를 활용합니다. 이러한 일관성은 샤드 간 통신을 위한 프로토콜을 맞춤화하는 데 유용할 것이지만 이더리움 2.0은 같은 암호화 기본 요소를 사용하지 않는 다른 블록체인과는 상호 운용이 불가능합니다.

폴카닷이나 코스모스와 같은 블록체인 네트워크는 동일한 프레임워크(코스모스의 SDK와 폴카닷의 Substrate)로 구축된 블록체인이 서로 통신하고 상호작용할 수 있도록 한 단계 더 나아가고 있습니다. 이러한 프레임워크는 개발자들이 자신만의 프로토콜을 구축하는 데 유연성을 제공하며, 동일한 암호화 기본 구성 요소의 가용성을 보장하여 각 체인이 다른 체인의 블록을 구문 분석하고 교차 확인할 수 있도록 하지만, 두 프로토콜 모두 자체 프레임워크로 구축되지 않은 블록체인과 연결하기 위해 브릿지나 "페깅 존"에 의존하고 있기 때문에 추가적인 신뢰 계층을 도입하고 있습니다. 즉, 코스모스와 폴카닷은 "블록체인 네트워크"를 가능하게 하지만, 코스모스와 폴카닷 네트워크는 서로 상호 운용할 수 있도록 설계되지 않았다는 것을 보여줍니다.

크로스체인 네트워크의 암호경제학적인 측면에 대해서는 추가적인 연구가 필요할 수 있습니다. 코스모스와 폴카닷 모두 스테이킹, 거버넌스, 그리고 거래 수수료에 대한 네이티브 토큰을 사용하고 있습니다. 스테이킹에 의해 도입되는 암호경제학적인 역학을 제외하면, 네이티브 토큰의 내재적 가치를 스테이킹만으로 부여할 수는 없습니다(4.2.4에서 자세히). 생태계 가치를 포착하기 위해 크로스체인 거래에 의존하는 것은 약한 모델일 수 있습니다. 특히, 크로스체인 거래는 멀티체인 네트워크의 장점이 아닌 약점입니다. 샤드 데이터베이스의 크로스-샤드 거래

와 마찬가지로, 이러한 거래는 지연 및 원자성 및 구성성 손실을 야기하고, 상호작용이 필요한 애플리케이션이 서로 상호작용하기 위해서는 크로스체인 오버헤드를 줄이기 위해 같은 블록체인에 상주하는 경향이 있으며, 이는 크로스체인 거래 수요와 따라서 네이티브 토큰 수요를 줄일 수 있습니다.

다른 블록체인과 연결된 체인은 네트워크 효과를 누리게 됩니다. 즉, 연결된 블록체인의 수가 많을수록 가치가 높아지고 새로운 참여자들이 이를 더욱 매력적으로 느끼게 됩니다. 이 가치는 네이티브 토큰에 누적되어 네트워크 성장을 더욱 장려할 것이지만, 폴카닷과 같은 공동 보안 네트워크에서는 토큰 가격이 높아지면 참여 비용이 높아지기 때문에, 네트워크가 추가 가치를 축적하기 어려워집니다. 코스모스와 같이 느슨하게 연결된 네트워크에서는 토큰 가격이 높아지면 교차체인 거래 수수료를 벌기 위해 필요한 자본 비용이 증가하기 때문에 참여자들의 예상 수익률이 감소하게 됩니다.

Nervos Network는 계층적 접근 방식을 사용하는 다중 체인 네트워크입니다. 아키텍처적으로 Nervos 셀 모델은 저수준 가상 머신을 사용하여 사용자 정의 및 사용자가 생성한 암호 원시자를 지원하여 이종 블록체인 간 상호 운용성을 제공합니다(4.4.1에서 설명). 암호 경제적으로, Nervos Network는 가치를 루트 체인으로 집중시키며 (메시지 전달 대신), 가치 획득을 통해 Nervos Network의 네이티브 토큰 가치가 상승함에 따라 네트워크의 보안 예산이 증가합니다. 마지막으로, 네이티브 토큰 가격이 상승하면 네트워크의 핵심 가치 제안이 강화됩니다. 이에 대한 자세한 내용은 (4.4)에서 다루고 있습니다.

3. Nervos Network의 핵심 원칙

Nervos는 분산 경제의 요구사항을 지원하기 위해 구축된 계층형 네트워크입니다. 블록체인 시스템을 구축할 때 분산성 vs 확장성, 중립성 vs 준수성, 개인정보 보호 vs 개방성, 가치 저장 vs 거래 비용, 암호학적 안전성 vs 사용자 경험과 같은 상충하는 요소들이 잘 알려져 있습니다. 우리는 이러한 모든 충돌이 단일 블록체인으로 완전히 반대되는 문제를 해결하려는 시도 때문에 발생한다고 믿습니다.

우리는 시스템을 구성하는 가장 좋은 방법이 모든 것을 포함하는 단일 레이어를 구축하는 것이 아니라, 다른 레이어에서 문제를 분리하고 해결하는 것이라고 믿습니다. 이렇게 함으로써, 레이어 1 블록체인은 안전하고 중립적이며 분산적이고 개방적인 공공 인프라에 초점을 맞출 수 있으며, 더 작은 레이어 2 네트워크는 사용 컨텍스트에 가장 적합하도록 특별히 설계될 수 있습니다.

Nervos Network에서 레이어 1 프로토콜(공통 지식 기반)은 전체 네트워크의 가치 보존 레이어입니다. 이는 철학적으로 비트코인에서 영감을 받아 만들어졌으며, 최대한 안전하고 검열에 강한 분산 저장소 및 암호화 자산의 탈중앙화 보호자로서 기능하기 위해 공개적이고, 공공적이며, 작업 증명 기반 블록체인으로 설계되었습니다. 레이어 2 프로토콜은 레이어 1 블록체인의 보안성을 활용하여 제한 없는 확장성 및 최소 거래 수수료를 제공하며, 신뢰 모델, 개인정보 보호 및 최종성에 관한 애플리케이션별 트레이드오프를 가능하게 합니다.

이건 Nervos Network 디자인의 핵심 원칙입니다.

- 지속 가능한, 다중 자산의 레이어 1 블록체인은 가치 보존을 위해 암호 경제적으로 설계되어야 합니다.
- 레이어 2는 거의 무한한 확장성, 저렴한 수수료 및 개선된 사용자 경험을 제공하는 최상의 스케일링 옵션을 제공합니다. 레이어 1 블록체인은 레이어 2 솔루션과 경쟁하는 것이 아니라 보완되도록 설계되어야 합니다.
- 레이어 1 블록체인에서 시빌(Sybil Attack)에 저항하는 방법으로 작업 증명이 필수적입니다.
- 레이어 1 블록체인은 상호 작용 프로토콜 및 블록체인 상호 운용성을 위한 일반 프로그래밍 모델을 제공하고 프로토콜을 최대한 사용자 정의 가능하고 업그레이드가 쉽도록 해야 합니다.
- 자원을 최적으로 할당하고 "공유지의 비극(tragedy of the commons)"을 피하기 위해 상태 저장소에는 명확하고 세분화된 소유권 모델이 있어야 합니다. 거래 수요와 관계없이 일관된 장기 보상을 채굴자에게 제공하기 위해 상태 점유에는 지속적인 비용이 들어가야 합니다.

4. Nervos 공유 지식 베이스(CKB)

4.1 개요

"공유 지식"은 대개 해당 용어를 사용하는 커뮤니티 내에서 모두 또는 대부분이 알고 있는 지식으로 정의됩니다. 일반적으로 이 용어는 해당 지역의 커뮤니티를 참조할 때 사용됩니다. 블록체인 전반과 특히 Nervos Network에서 "공유지식"은 글로벌 합의로 검증된 상태이며, 모든 네트워크 참가자가 인정하는 상태를 의미합니다.

공유지식의 특성은 우리가 공개 블록체인에 저장된 암호화폐를 돈으로 인식할 수 있게 합니다. 예를 들어, 비트코인의 모든 주소의 잔액과 히스토리는 비트코인 사용자들에게 공유지식입니다. 이는 사용자들이 공유원장을 독립적으로 복제하고, 제네시스 블록 이후의 글로벌 상태를 검증하며, 다른 사람도 동일하게 할 수 있다는 것을 알고 있기 때문입니다. 이러한 공유지식은 제3자를 신뢰할 필요 없이 완전하게 P2P로 거래할 수 있게 합니다.

Nervos 공유 지식 베이스(CKB)는 돈에 국한되지 않고 모든 종류의 공유 지식을 저장하도록 설계되었습니다. 예를 들어, CKB는 대체 가능한 및 비대체 가능한 토큰과 같은 사용자 정의 암호 자산, 지불 채널(5.2) 및 Plasma 체인(5.4)과 같은 상위 계층 프로토콜의 보안을 제공하는 가치있는 암호학적 증명을 저장할 수 있습니다.

비트코인과 Nervos CKB 모두 공유 지식 저장 및 검증 시스템입니다. 비트코인은 전역 상태를 UTXO 세트로 저장하며, 거래에 내장된 하드 코딩 규칙 및 스크립트를 통해 상태 전이를

검증합니다. Nervos CKB는 비트코인의 데이터 구조와 스크립팅 기능을 일반화하고, 전역 상태를 활성 프로그래머블 셀의 집합으로 저장하며, 가상 머신에서 실행되는 사용자 정의 튜링 완전 스크립트를 통해 상태 전이를 검증합니다.

Nervos CKB는 이더리움 및 기타 플랫폼과 같은 전체적인 스마트 컨트랙트 기능을 갖추고 있지만, 분산 계산을 위한 지불 대신 공유 지식 보존을 위해 경제 모델이 설계되었습니다.

4.2 합의(Consensus)

비트코인의 나카모토 합의(Nakamoto Consensus, NC)는 간단하고 통신 오버헤드가 적은 구조 때문에 널리 사용되고 있습니다. 그러나 NC는 두 가지 단점이 있습니다.1) 거래 처리량이 만족스럽지 않고, 2) 공격자가 규약에서 권장하는 동작에서 벗어나 추가적인 블록 보상을 얻을 수 있는 이기적인 채굴(selfish mining) 공격에 취약합니다.

CKB 합의 프로토콜은 NC의 장점을 유지하면서 성능 한계와 이기적인 채굴 저항성을 높이는 변형입니다. NC의 블록 전파 지연 병목 현상을 식별하고 제거하여, 프로토콜 보안을 희생하지 않으면서 매우 짧은 블록 간격을 지원합니다. 줄어든 블록 간격은 처리량을 높이는데만이 아니라 거래 확인 지연 시간을 줄입니다. 모든 유효한 블록을 난이도 조절 계산에 통합하여, 이기적인 채굴이 더 이상 수익성이 없습니다.

4.2.1 증가하는 처리량

Nervos CKB는 나카모토 합의(Nakamoto Consensus)에서 파생된 합의 알고리즘을 사용하여 PoW(Proof of Work,작업 증명) 합의의 처리량을 증가시킵니다. 이 알고리즘은 블록체인의 고아(Orphan) 비율(카노니컬 체인의 일부가 아닌 유효한 블록의 백분율)을 네트워크 전체의 연결성을 측정하는 기준으로 사용합니다.

이 프로토콜은 고정된 고아 비율을 대상으로 합니다. 고아 비율 대상이 낮은 경우, 대상 난이도는 낮아지고(블록 생성 속도 증가), 정의된 임계값을 넘어 고아 비율이 높아지면 대상 난이도가 증가합니다(블록 생성 속도 감소).

이를 통해 네트워크의 전체 대역폭 용량을 활용할 수 있습니다. 낮은 고아 블록의 비율은 네트워크가 잘 연결되어 있고 더 큰 데이터 전송을 처리할 수 있는 것을 나타내므로, 이러한 조건에서 프로토콜은 처리량을 증가시킵니다.

4.2.2 블록 전파 병목현상 제거하기

어떤 블록체인 네트워크에서 병목현상은 블록 전파입니다. Nervos CKB 합의 프로토콜은 트랜잭션 확인을 두 단계 프로세스인 제안과 커밋으로 수정함으로써 블록 전파 병목현상을 제거합니다.

트랜잭션은 먼저 블록의 "제안 영역" (또는 그 블록의 어떤 삼촌 블록)에서 제안되어야 합니다. 그러고 나면 트랜잭션이 "커밋 영역"에 정의된 시간 내에 블록에 나타나면 커밋됩니다. 이러한 설계는 새로운 블록의 커밋된 트랜잭션은 제안될 때 모든 노드에서 이미 수신되어 검증되었기 때문에 블록 전파 병목현상을 제거합니다.

4.2.3 이기적인 채굴 공격 완화

나카모토 합의(Nakamoto Consensus)에서 가장 기본적인 공격 중 하나는 이기적 채굴(selfish mining)입니다. 이 공격에서는 악의적인 채굴자들이 다른 채굴자가 채굴한 블록을 의도적으로 유실시키면서 부당한 블록 보상을 얻습니다.

연구원들은 불공정한 보상이 나카모토 합의의 난이도 조정 메커니즘에 기인한다고 관찰합니다. 이는 버려진 블록을 계산능력 산정에서 제외하기 때문에 마이닝 난이도가 낮아지고 시간 평균 블록 보상이 높아지는 현상을 초래합니다.

Nervos CKB 합의 프로토콜은 삼촌 블록을 난이도 조정 계산에 포함시켜, 이기적인 채굴이 이제 더 이상 수익성이 없게 만듭니다. 어떤 공격 전략이나 기간에 대해서도 채굴자는 정직한 채굴과 이기적인 채굴의 어떤 조합으로도 불공정한 보상을 얻을 수 없습니다.

우리의 분석에 따르면, 두 단계 트랜잭션 확인 프로세스를 사용함으로써, 사실상 이기적인 채굴도 제한된 공격 시간 창에서 제거됩니다.

우리의 합의 프로토콜에 대한 자세한 이해를 위해서는 여기를 읽어주세요.

4.2.4 Proof of Work vs Proof of Stake

작업 증명 (PoW) 및 지분 증명 (PoS) 시스템은 모두 권력 집중에 취약하지만 시스템의 특성은 권력을 가진 자에게 매우 다른 운영 현실을 제공합니다.

PoW 채굴은 실제 비용이 발생할 수 있으며, 비용을 세심하게 관리하지 않으면 채굴 수익을 초과할 수도 있습니다. 권력을 가진 사람들은 혁신적인 방법을 모색하고 건전한 비즈니스 전략을 추구하며, 계속해서 인프라에 투자하여 우위를 유지해야 합니다. 채굴 장비, 채굴 풀 운영 및 저렴한 에너지에 대한 접근은 모두 기술적 혁신의 영향을 받으며, 이러한 세 가지를 오랜 기간 동안 독점적으로 유지하는 것은 어렵습니다.

반면, PoS 시스템의 블록 생성자들은 투자한 금액에 따라 결정론적으로 보상을 받으며 운영 자본에 대한 요구 사항이 매우 낮습니다. 시스템이 성장함에 따라, 초기에 이동한 기업과 개인에게 제공되는 자연적 이점의 영향이 커질 것입니다. PoS 시스템에서는 소수의 스테이커들에게 권력이 집중될 수 있습니다. PoW 시스템은 채굴 집중 문제와 비슷한 문제가 있지만, PoS 시스템에서 권력을 유지하기 위한 비용은 상당히 낮습니다.

게다가, PoS 검증자들은 검증자 집합을 통제하는 특별한 권력을 가지고 있습니다. 유효성 검사기가 합의 그룹에 참여할 수 있도록 허용하는 거래의 수용은 기존 검증자들의 손에 달려 있습니다. 거래 검열과 순서 조작을 통해 검증자 집합에 영향을 끼치기 위한 결집 노력은 감지하기 어렵고 처벌하기도 어렵습니다. 반면, PoW 시스템에서는 합의 참여가 실제로 열려 있으며 현재의 권력 구조에 영향을 받지 않으며, 시스템 초기 참여자들에게 혜택이 주어지지 않습니다.

토큰 경제학에 관해서는, 스테이킹이 수익을 얻기 위해 자본을 유치하는 것으로 알려졌지만, 이것만으로는 충분하지 않습니다. 모든 PoS 프로젝트는 결국 스테이킹 비율이 안정화되며, 자본이 스테이킹 풀에 들어오고 나가는 것은 대략 같을 것입니다. 스테이킹 메커니즘 자체만으로는 네이티브 토큰에 대한 수요를 증가시키지 않습니다. 즉, 스테이킹은 프로젝트의 초기 단계에서 네이티브 토큰에 대한 수요를 제공하긴 하지만, 스테이킹 자체로는 장기적인 네이티브 토큰에 대한 수요를 제공할 수 없으며, 따라서 네이티브 토큰의 유일한 내재 가치가 될 수 없습니다.

PoS 시스템에서 장기 토큰 홀더는 세 가지 선택지가 있습니다. 1) 자체 인프라를 관리하고 검증 노드를 운영하여 새 발행을 받을 수 있습니다. 2) 토큰을 제 3자에게 위임하고 그들의 진실성과 인프라를 신뢰하는 것입니다. 3) 또는 지속적인 발행으로 토큰 가치가 희석될 수 있습니다. 이러한 선택지 중 어느 하나도 장기적으로 가치 저장에 중점을 둔 토큰 홀더들에게 특별히 매력적인 옵션은 아닙니다.

우리는 PoW의 허가 없는 참여가 글로벌 경제 활동의 기초에 필수적이라고 믿습니다. 레이어 1의 가장 중요한 목표는 블록체인이 가능한 한 분산, 안전하고 중립적이도록 보장하는 것입니다. PoS 시스템은 분산 경제에 기여할 수 있지만, 우리의 의견으로는 정말로 열린 탈중앙형 레이어 1의 요구 사항을 충족하지 못합니다.

4.2.5 작업 증명 기능

Nervos CKB 블록은 유효한 경우 어느 노드에서든 제안할 수 있습니다. 단, 제안자는 작업 증명이라는 계산적으로 어려운 퍼즐을 해결해야 합니다. 작업 증명 퍼즐은 제안 중인 블록을 기반으로 정의되며, 이로 인해 퍼즐의 해결책이 블록을 고유하게 식별합니다.

비트코인의 작업 증명은 블록 해더에 해시 함수를 적용하여 일정 수준의 난이도를 충족시키는 유효한 nonce를 찾는 것을 요구합니다. 비트코인에서 사용되는 해시 함수는 SHA2-256의 이중 반복입니다. SHA2는 비트코인에 적합한 선택이었지만, 이후 나온 암호화폐에는 적합하지 않습니다. 비트코인을 채굴하기 위해 많은 전용 하드웨어가 개발되었지만, 이러한 하드웨어 대부분은 효율성 개선으로 더 이상 사용되지 않고 방치되어 있습니다.

같은 작업 증명 퍼즐을 사용하는 새로운 암호화폐는 이 오래되고 사용되지 않는 하드웨어를 다시 유용하게 만들 것입니다. 최신 하드웨어도 임대해서 새로운 코인 채굴을 위해 재활용할 수 있습니다. SHA2 기반 코인의 채굴 파워 분포는 예측하기 매우 어렵고 갑작스러운 대규모

변화에 취약합니다. 이러한 논점은 소프트웨어 계산 비용을 줄이기 위해 개발된 SHA2에 맞춘 알고리즘 최적화에도 적용됩니다.

새로운 암호화폐의 경우, 다른 암호화폐에서 사용되지 않은 함수를 기반으로 작업 증명 퍼즐을 정의하는 것이 합리적입니다. Nervos CKB에서는 더 나아가서, 이것을 이전의 암호화폐에서 선행 최적화의 대상이 되지 않았을 새로운 작업 증명 함수로 정의하기로 결정했습니다.

하지만, 채굴 하드웨어의 의도된 이용 불가능성은 초기에만 해당합니다. 장기적으로는 전용 채굴 하드웨어의 배치는 네트워크 공격의 어려움을 크게 증가시키므로 이점이 있습니다. 따라서, 새로운 암호화폐를 위한 이상적인 작업증명 함수는 새롭고, 더불어 하드웨어 개발의 진입 장벽을 크게 낮출 정도로 간단해야 합니다.

보안은 명백한 세번째 설계 목표입니다. 알려진 취약점은 모든 채굴자들에게 동등하게 악용될 수 있고, 단지 난이도를 높일 뿐입니다. 반면, 알려지지 않은 취약점은 발견자들에게 그들이 기여한 채굴 능력보다 더 많은 이점을 제공하는 채굴 최적화로 이어질 수 있습니다. 이러한 상황을 피하기 위한 가장 좋은 방법은 취약점이 없다는 주장을 강력하게 내세우는 것입니다.

4.2.6 Eaglesong

Eaglesong은 Nervos CKB 작업 증명을 위해 특별히 개발된 새로운 해시 함수이며, 안전한 해시 함수가 필요한 다른 사용 사례에도 적합합니다. 설계 기준은 위에서 언급한 대로 새로움, 간단함, 안전성이었습니다. 우리는 과학적으로 약간의 발전을 이루는 충분히 새로운 디자인과 강력한 보안 주장을 만들기 위해 기존 디자인에 가까운 디자인을 동시에 원했습니다.

이를 위해, 우리는 ARX 연산 (덧셈(addition), 회전(rotation) 및 배타적 논리합(xor))에서 만들어진 순열로 스펀지 구성을 인스턴스화 하도록 선택했습니다(Keccak/SHA3에서 사용됨). 그것의 보안 주장은 AES를 기반으로 하는 넓은 트레일 전략에 기반 합니다.

우리의 지식으로 Eaglesong은 모든 세 가지 디자인 원칙을 성공적으로 결합한 첫 번째 해시 함수(또는 함수)입니다.

여기에서 Eaglesong에 대한 자세한 내용을 읽을 수 있습니다.

4.3 셀 모델

Nervos CKB는 계정 모델(이더리움에서 사용)의 많은 이점을 제공하면서도 UTXO 모델(비트코인에서 사용)의 자산 소유권 및 증명 기반 검증 특성을 유지할 수 있는 새로운 구조인 셀 모델을 사용합니다.

셀 모델은 상태에 중점을 둡니다. 셀에는 토큰 금액과 소유자와 같은 단순한 데이터뿐만 아니라 토큰 전송의 검증 조건을 지정하는 코드와 같은 더 복잡한 데이터도 포함될 수 있습니다.

CKB의 상태 머신은 셀과 관련된 스크립트를 실행하여 상태 전이의 무결성을 보장합니다.

셀은 자신의 데이터를 저장하는 것 외에도 다른 셀의 데이터를 참조할 수 있습니다. 이를 통해 사용자 소유 자산과 그에 대한 논리를 분리할 수 있습니다. 이는 상태(state)가 스마트 컨트랙트의 내부 속성이 되어 스마트 컨트랙트 인터페이스를 통해 액세스해야 하는 계정 기반 스마트 컨트랙트 플랫폼과 대조적입니다. Nervos CKB에서 셀은 독립적인 상태 객체이며, 직접 소유하고 참조 및 전달할 수 있습니다. 셀은 소유자에게 속하는 진정한 "안전 자산(bearable assets)"으로 나타낼 수 있으며 (비트코인 소유자에게 UTXO가 안전 자산이 되는 것과 마찬가지로), 상태 전환의 무결성을 보장하는 로직이 담긴 셀을 참조합니다.

셀 모델 트랜잭션은 또한 상태 전이 증명입니다. 트랜잭션의 입력 셀은 활성 셀 집합에서 제거되고 출력 셀은 집합에 추가됩니다. 활성 셀은 Nervos CKB의 전역 상태를 구성하며 변경할 수 없습니다. 셀이 생성되면 변경할 수 없습니다.

셀 모델은 적응성, 지속 가능성, 유연성을 갖도록 설계되었습니다. 이는 일반화된 UTXO 모델로서 사용자 정의 토큰, 스마트 컨트랙트 및 다양한 레이어 2 프로토콜을 지원할 수 있도록 설계된 것입니다.

셀 모델에 대한 자세한 이해를 위해서는 여기를 참조하세요.

4.4 가상 머신

다음 세대 블록체인 프로젝트들이 블록체인 가상 머신의 기초로 WebAssembly를 사용하는 것과 달리, Nervos CKB는 RISC-V 명령어 집합을 기반으로 한 가상 머신 (CKB-VM)을 독특한 디자인 선택으로 포함하고 있습니다.

RISC-V는 2010년에 새로운 하드웨어와 소프트웨어 개발을 용이하게 하기 위해 만들어진 오픈 소스 RISC 명령어 집합 구조로, 로열티가 없으며, 널리 이용되며 검증된 명령어 집합입니다.

블록체인 컨텍스트에서 RISC-V를 사용하는 것에는 많은 장점이 있다고 발견되었습니다.

- 안정성: RISC-V 코어 명령어 집합은 최종적으로 결정되고 동결되었으며, 널리 구현되어 테스트 되었습니다. RISC-V 코어 명령어 집합은 고정되어 있으며 업데이트가 필요하지 않습니다.
- 오픈 소스와 지원: RISC-V는 BSD 라이선스로 제공되며 GCC와 LLVM과 같은 컴파일러에서 지원되며, Rust와 Go 언어의 구현도 개발 중입니다. RISC-V 재단은 235개 이상의 회원 기관으로 구성되어 있으며 명령어 집합의 개발과 지원을 진행하고 있습니다.
- 단순성과 확장성: RISC-V 명령어 집합은 단순합니다. 64비트 정수를 지원하며 102개의 명령어만을 포함합니다. RISC-V는 고성능 암호 알고리즘을 위한 256비트 정수나 벡터 컴퓨팅을 위한 확장 명령어 집합을 모듈식으로 제공합니다.

- 정확한 자원 가격 책정: RISC-V 명령어 집합은 물리적 CPU에서 실행될 수 있으므로 각 명령어를 실행하는 데 필요한 기계 사이클의 정확한 예측을 제공하여 가상 머신 자원 가격 책정을 지원합니다.

4.4.1 CKB-VM 및 셀 모델

이미 배포된 공개 블록체인은 기본적으로 더 이상 변경할 수 없거나, 암호학적 원시 기능과 같은 핵심 요소를 업그레이드하려면 몇 년의 노력이 필요합니다.

CKB-VM은 이러한 문제를 해결하기 위해 이전에 사용되었던 사용자 정의 VM에 내장된 원시 기능을 가상머신 위에 있는 셀로 이전시킵니다. 이러한 방법으로 CKB 스크립트는 이더리움의 스마트 컨트랙트보다는 더 낮은 수준으로 구현되지만, 적극적인 플랫폼과 진행중인 탈중앙화 경제를 위한 유연성과 효율성을 제공합니다.

셀은 실행 가능한 코드를 저장하고 다른 셀을 종속성으로 참조할 수 있습니다. 거의 모든 알고리즘과 데이터 구조는 셀 내부에 저장된 CKB 스크립트로 구현됩니다. VM을 가능한 한 간단하게 유지하고 프로그램 저장소를 셀로 옮기는 것으로, 핵심 알고리즘을 업데이트하는 것은 새로운 셀에 알고리즘을 로드하고 기존 참조를 업데이트하는 것만으로 간단히 수행됩니다.

4.4.2 CKB-VM에서 다른 가상 머신 실행하기

CKB-VM의 저수준 특성과 RISC-V 커뮤니티의 도구들의 가용성 덕분에 이더리움의 EVM과 같은 다른 VM을 CKB-VM에 직접 컴파일하는 것이 쉽고, 이렇게 하면 여러 이점이 있습니다.

다른 가상 머신에서 작성된 전문 언어의 스마트 컨트랙트는 쉽게 CKB-VM에서 실행될 수 있습니다. (엄밀히 말하면 CKB-VM 내에서 실행되도록 컴파일된 자체 VM에서 실행됩니다.)

CKB는 레이어 2 트랜잭션의 분쟁 해결 상태 전이를 검증할 수 있습니다. 이는 CKB-VM 이외의 가상 머신에서 작성된 상태 전이 규칙을 실행하는 것이 요구되는 신뢰성 있는 레이어 2 범용 사이드 체인을 지원하는 데 필수적인 요구 사항 중 하나입니다.

CKB-VM에 대한 기술적인 설명서는 여기를 참고해주세요.

4.5 경제 모델

CKB의 기본 토큰은 "Common Knowledge Byte" 또는 CKByte라고 합니다. CKByte 소유자는 블록체인의 총 상태 저장 공간의 일부를 점유할 수 있습니다. 예를 들어, 1000 CKByte를 보유하고 있다면, 사용자는 1000 바이트 용량의 셀 하나를 생성하거나 1000 바이트 용량을 추가로 가진 여러 셀을 만들 수 있습니다.

CKByte를 사용하여 CKB에 데이터를 저장하는 것은 CKByte 소유자에게 기회 비용을 발생시

킵니다. 즉, 누군가 CKByte를 NervosDAO에 예치하여 보조 발행량의 일부를 받을 수 없게 됩니다. CKByte는 시장 가격이 존재하므로 사용자가 확장되는 상태의 높은 수요를 충족하기 위해 상태 저장 공간을 자발적으로 해제하도록 경제적 인센티브를 제공합니다. 사용자가 상태 저장 공간을 해제하면, 그들의 데이터가 점유하고 있던 크기에 해당하는 CKByte 금액을 받게 됩니다.

CKB의 경제 모델은 기본 발행과 보조 발행으로 구성되어 있으며, 상태 성장을 제한하여 참여 장벽을 낮추고 분산화를 보장합니다. CKByte가 부족 자원이 되면 가장 효율적으로 가격을 책정하고 할당할 수 있습니다.

Nervos Network의 제네시스 블록에는 336억 개의 CKByte가 포함되어 있으며, 이 중 84억 개가 즉시 소각됩니다. CKByte의 신규 발행은 기본 발행과 보조 발행 두 부분으로 나뉩니다. 기본 발행은 유한 총 공급 (336억 CKByte)으로 제한되며, 비트코인과 유사한 발행 일정을 갖고 있습니다. 블록 보상은 약 4년마다 반으로 줄어들고, 신규 발행이 0에 도달할 때까지 지속됩니다. 모든 기본 발행은 네트워크 보호를 위한 인센티브로 채굴자에게 수여됩니다. 보조 발행은 매년 13.44억 CKByte의 일정 발행률을 갖고 있으며, 상태 저장 공간 점유에 대한 기회 비용을 부과하기 위해 설계되었으며, 기본 발행이 중단되면 보조 발행만 남게 됩니다.

Nervos CKB에는 NervosDAO라는 특별한 스마트 컨트랙트가 포함되어 있으며, 이는 보조 발행의 인플레이션 효과에 대한 "인플레이션 쉘터"로 작동합니다. CKByte 소유자는 자신의 토큰을 NervosDAO에 예치하고, 그 예치금액에 해당하는 일정 비율의 보조 발행을 받을 수 있습니다. 이를 통해 보조 발행의 인플레이션 효과를 완전히 상쇄할 수 있습니다. 장기적으로 토큰을 보유하는 사용자는 자신의 토큰을 NervosDAO에 잠그는 한, 보조 발행의 인플레이션 효과가 거의 없습니다. 이러한 사용자는 보조 발행의 효과가 완화된 채로 비트코인과 같은 하드캡 토큰을 보유하고 있는 것입니다.

CKByte가 상태를 저장하는 데 사용될 때, NervosDAO를 통해 보조 발행 보상을 얻을 수 없습니다. 이로 인해 보조 발행은 일종의 "상태 임대료"로 작용하며, 상태 저장 공간과 저장 시간에 비례하는 상태 저장 수수료를 부과합니다. 이 경제 모델은 다른 플랫폼에서 사용되는 "한 번 지불하고 영구히 점유하는" 모델보다 더 지속 가능하며, 명시적인 지불이 필요한 다른 상태 임대료 솔루션보다 더 실행 가능하고 사용자 친화적입니다.

채굴자들은 블록 리워드와 거래 수수료를 받습니다. 블록 리워드의 경우, 채굴자가 블록을 채굴하면 블록의 전체 기본 발행 보상과 일부 이차 발행 보상을 받으며, 이 부분은 상태 점유에 기반합니다. 예를 들어, 모든 원래 토큰 중 절반 이상이 상태 저장을 위해 사용된다면, 채굴자는 블록의 이차 발행 보상의 절반을 받게 됩니다. (이차 발행 분배에 대한 추가 정보는 다음 섹션(4.6)에 포함되어 있습니다.) 기본 발행이 중지되면, 장기적으로 마이너는 거래와 관련없이 Nervos Common Knowledge Base의 채택에 따라 독립적인 "상태 임대료" 수입을 받게 됩니다.

유사성을 비유하면, CKByte는 땅과 같고, CKB에 저장된 암호 자산은 집과 같습니다. 집을 짓

기 위해서는 땅이 필요하듯이, CKB에 자산을 저장하려면 CKByte가 필요합니다. CKB에 자산을 저장하는 수요가 증가함에 따라 CKByte 수요도 증가하게되고, 저장된 자산의 가치가 상승하면, CKByte의 가치도 상승합니다.

이 디자인을 사용하면 다양한 자산에 대한 수요가 단일 자산에 대한 수요로 전환되며, 비트코인의 보안을 보장하는 동일한 인센티브 시스템을 적용할 수 있습니다. 채굴자들은 CKByte로 블록 보상을 받으며, 수요 증가로 인해 가치가 오르면 Nervos Network의 보안 예산이 증가합니다.

경제 모델에 대한 자세한 설명은 여기를 참조해주세요.

4.6 Treasury

보조 발행량 중에서 1) 채굴자에게 주어지지 않은 부분과 2) NervosDAO에 토큰을 잠금으로 보유하고 있는 장기 보유자들에게 주어지지 않은 부분은 Treasury fund로 사용됩니다. 예를 들어, 발행된 CKBytes의 60%가 상태 저장에 사용되고 30%가 NervosDAO에 예금되면, 마이너는 보조 발행량의 60%를 받으며, NervosDAO (장기 보유자)는 보조 발행량의 30%를 받으며, 나머지 10%는 Treasury로 사용됩니다.

Treasury fund는 프로토콜의 지속적인 연구 및 개발, Nervos Network 생태계 구축에 사용됩니다. Treasury fund의 사용은 모든 사람들이 개방적이고, 투명하게 블록체인 상에서 확인할 수 있습니다. 인플레이션 기반의 Treasury fund 모델과 비교하여, 이 모델은 장기 토큰 보유자들의 가치를 희석시키지 않으며 (NervosDAO에 토큰을 예금한 경우), 프로토콜 개발 자금 조달은 단기 토큰 보유자들의 기회 비용에서 엄격히 유도됩니다.

Nervos Common Knowledge Base의 본격적인 런칭 시점에서 treasury는 즉시 활성화되지 않습니다. 이것은 Nervos Foundation이 제네시스 블록에 포함된 생태계 기금을 소진한 후에만 하드포크를 통해 활성화하며, 토지를 활성화하기 전에는 이 보조 발행 부분이 소각됩니다.

4.7 거버넌스

거버넌스는 사회 또는 그 내부 집단이 의사결정을 내리기 위해 조직화하는 방식을 말합니다. 시스템에 관심이 있는 모든 관련 당사자들이 이 과정에 참여해야 합니다. 블록체인에 대해서는 사용자, 보유자, 채굴자, 연구자, 개발자뿐만 아니라 지갑, 거래소 및 채굴 풀과 같은 서비스 제공자도 포함되어야 합니다. 다양한 이해관계자 그룹은 각기 다른 이익을 가지고 있으며 모든 이해관계자들의 인센티브를 일치시키는 것은 거의 불가능하기때문에, 블록체인 거버넌스가 복잡하고 논란이 많은 주제인 이유입니다. 블록체인을 대규모 사회 실험이라고 생각한다면, 거버넌스는 시스템의 다른 어떤 부분보다도 더 정교한 디자인이 필요합니다. 10년간의 진화를 거치면서 블록체인 거버넌스를 위한 일반적인 최선의 방법이나 지속 가능한 프로세스를 발견하지 못했습니다.

일부 프로젝트는 "자비로운 종신독재자"를 통해 거버넌스를 진행합니다(예: Linux의 Linus Torvalds). 이 방법은 프로젝트를 높은 효율성과 일관성을 갖게 만들어주며 매력적이기도 합니다. 그러나 이것은 블록체인의 핵심 가치인 탈중앙화와 모순됩니다.

일부 프로젝트는 EOS의 ECAF(EOSIO Core Arbitration Forum)와 같이 권위있는 오프체인 위원회에 폭넓은 결정권을 위임합니다. 그러나 이러한 위원회는 참가자가 그들의 결정에 따를 것을 보장할 권한이 없으며, 이는 올해 ECAF를 폐쇄 결정에 이끈 원인 중 하나가 될 수 있습니다.

일부 프로젝트들은, Tezos와 같이, 참여자들이 투표한 결정을 준수하도록 온체인 거버넌스를 구현하여 더 나아갑니다. 이는 개발자와 채굴자(또는 풀 노드 사용자) 간의 불일치로 인한 영향을 피할 수도 있습니다. 온체인 거버넌스는 단순한 온체인 투표와 다릅니다. 만약 제안된 기능이나 패치가 온체인 거버넌스를 통해 충분한 투표를 받는다면, 체인 코드가 자동으로 업데이트되며, 채굴자나 풀 노드는 이 변경을 제어할 방법이 없습니다. 폴카닷은 더욱 복잡한 온체인 거버넌스 방식을 채택하며, 선출된 의회, 지분 가중 투표를 위한 국민투표 절차, 투표자 투표 참여도에 따른 긍정, 부정적 편향 기구를 활용합니다.

그러나 실제로는 온체인 거버넌스가 제시된 것만큼 우아하지 않습니다. 첫째, 투표는 토큰 홀더의 이해관계만을 반영하고, 모든 다른 당사자들을 무시합니다. 둘째, 낮은 투표율은 블록체인 세계와 실제 세계 모두의 오래된 문제입니다. 소수의 사람들만 투표하면 대다수의 이해관계에 부합하는 결과를 어떻게 도출할 수 있을까요? 마지막으로, 하드포크는 모든 이해관계자들에게 최후의 수단으로 고려되어야 합니다. 무제한 블록체인의 넓은 복제가 제공하는 우수한 데이터 가용성을 고려하면, 기존 체인에서 데이터를 완전히 보존하고 중단없이 포크하는 것이 항상 가능한 선택 사항이어야 합니다. 하드포크는 온체인 거버넌스를 통해 실행될 수 없습니다.

아직까지 운영 문제에 대한 충분한 대답은 없으므로, Nervos Network에서는 점진적인 방법을 채택할 것입니다. 초기에는 Nervos Foundation이 프로젝트의 운영 기관 역할을 맡게 될 것입니다. Nervos Foundation은 독립된 이사회로 구성된 파나마 재단입니다. 이 재단은 Nervos Network의 발전과 생태계 및 채택을 촉진하는 역할을 맡고 있습니다.

시간이 지남에 따라 토큰이 더 채굴되고 채굴이 더 분산되며 더 많은 개발자가 참여함에 따라, 지배 책임은 점차 커뮤니티로 이동할 것입니다. 장기적으로는 커뮤니티 기반 지배가 프로토콜 업그레이드 프로세스와 자금 배분을 관리할 것입니다.

Nervos CKB는 수백 년간 지속될 수 있는 탈중앙화된 자율 인프라로 설계되어 있으며, 이는 이 네트워크가 어떻게 발전하든 상관없이 우리 커뮤니티가 지켜야 할 몇 가지 중요한 사항이 있다는 것을 의미합니다. 이러한 핵심 불변식은 다음과 같습니다.

- 발행 일정은 완전히 고정되어 있으므로 결코 변경되지 않습니다.
- 셀에 저장된 상태, 데이터는 변경되지 않아야 합니다.

- 기존 스크립트의 의미는 변경되지 않습니다.

블록체인 기반 커뮤니티 기반 지배는 매우 새로운 분야이며 많은 가치 있는 실험이 진행 중입니다. 우리는 이것이 단순한 주제가 아니며, 최적의 접근 방식에 도달하기 위해 완전히 연구, 관찰 및 반복하는 데 시간이 필요하다는 것을 인식합니다. 우리는 단기적으로 커뮤니티 기반 지배에 대해 보수적인 접근을 취하면서도 장기적으로 이 방향성에 완전히 헌신할 것입니다.

5. 레이어 2 솔루션 개요

5.1 레이어 2란 무엇인가?

블록체인 네트워크의 레이어 1은 제약 조건에 의해 정의됩니다. 이상적인 레이어 1 블록체인은 보안, 탈중앙화 및 지속 가능성에 대한 어떠한 타협도 없이 구현되어야 하지만, 이는 확장성과 거래 비용과 관련된 문제를 야기합니다. 레이어 2 솔루션은 레이어 1 프로토콜 위에 구축되며, 계산을 오프 체인으로 이동시켜 레이어 1 블록체인으로 안전하게 처리하는 메커니즘을 제공합니다.

이는 오늘날 은행 시스템의 순자산 결제 또는 SEC 규제 제출과 유사합니다. 글로벌 합의가 필요한 데이터 양을 줄이면서, 네트워크는 더 많은 참가자를 수용하고 더 많은 경제 활동을 가능케 할 수 있으며, 여전히 분산성의 특성을 유지할 수 있습니다.

레이어 2 사용자들은 레이어 1 블록체인에서 제공되는 보안에 의존하며, 자산을 레이어 간 이동하거나 분쟁을 해결할 때 이 보안을 활용하는 기능이 법원 체계와 유사합니다. 중재 체계는 모든 거래를 모니터링하고 유효성을 검증할 필요가 없으며, 핵심 증거를 기록하고 분쟁을 해결하기 위한 장소로서 기능합니다. 마찬가지로 블록체인에서 레이어 1 블록체인은 참가자가 오프 체인으로 거래할 수 있게 하며, 분쟁이 발생할 경우 암호화된 증거를 블록체인에 제출하고 부정행위자에게 처벌할 수 있는 능력을 가지게 됩니다.

5.2 지불 및 상태 채널

지불 채널은 자주 거래하는 두 당사자 간에 생성됩니다. 이는 글로벌 블록체인 상에서 직접적으로 거래하는 것이 제공하지 못하는 저지연 시간과 즉각적인 결제 경험을 제공합니다. 지불 채널은 바에서 메뉴판을 열어 음료를 주문하면서 주문한 금액을 모아둔 후 나가기 전에 한꺼번에 정산하는 것과 비슷한 방식으로 작동합니다. 지불 채널을 운영하면 참가자들은 상호간에 계좌 잔액에 대한 암호학적 증명을 포함한 메시지를 교환하고 이러한 계좌 잔액을 오프 체인에서 무제한으로 업데이트 할 수 있습니다. 그들이 채널을 닫고 잔액을 블록체인으로 정산할 준비가 될 때까지입니다.

지불 채널은 단방향 또는 양방향일 수 있습니다. 단방향 지불 채널은 위에서 예시로 든 바 메뉴판과 비슷하게 A 그룹에서 B 그룹으로 흐릅니다. A 그룹은 B 그룹과 거래할 가능성이 있는 최대 금액을 예치한 후 상품 또는 서비스를 받으면서 천천히 자금을 전달합니다.

양방향 결제 채널은 더 복잡하지만 레이어 2 에대한 가능성을 보여줍니다. 이러한 결제 채널에서 자금은 양쪽으로 이동하며, 이로 인해 결제 채널을 "재조정"할 수 있으며 공유 대리인을 통해 결제 채널 간 결제가 가능해집니다. 이를 통해 비트코인의 Lightning Network와 같은 결제 채널 네트워크가 가능해집니다. 자금은 A가 두 당사자 간에 직접적인 채널이 없어도, A가 양 당사자에게 연결된 중개인을 통해 경로를 찾을 수 있는 경우, A에서 B로 이체될 수 있습니다.

결제 채널이 온체인 결제를 확장할 수 있는 것처럼, 상태 채널은 온체인 거래를 확장할 수 있습니다. 결제 채널은 두 당사자 간의 잔액 관리에 한계가 있지만, 상태 채널은 임의의 상태에 대한 동의로, 신뢰 없는 체스부터 확장 가능한 탈중앙화 애플리케이션까지 모든 것이 가능합니다.

이것은 지불 채널과 유사하게, 당사자들이 채널을 열고 시간이 지남에 따라 암호 서명을 교환하며 최종 상태(또는 결과)를 온체인 스마트 컨트랙트에 제출합니다. 스마트 컨트랙트는 이 입력을 기반으로 실행되어 계약에 인코딩된 규칙에 따라 거래를 결제합니다.

"일반화된 상태 채널"은 강력한 상태 채널 구조로, 단일 상태 채널이 여러 스마트 컨트랙트 간의 상태 전환을 지원할 수 있도록합니다. 이것은 "하나의 애플리케이션당 하나의 채널" 아키텍처에서 고유한 상태 증가를 감소시키고 이미 열린 상태 채널을 활용할 수 있는 쉬운 온보딩을 가능하게합니다.

5.3 사이드 체인

사이드 체인은 이중 보증 블록체인 (메인 체인)과 연결된 별개의 블록체인입니다. 사이드 체인을 이용하려면, 사용자는 메인 체인의 지정된 주소로 자금을 보내어 사이드 체인 운영자의 통제 아래에 자금을 잠급니다. 이 거래가 확인되고 안전 기간이 지나면, 자금 입금 내용을 상세히 설명하는 증명서를 사이드 체인 운영자에게 전달할 수 있습니다. 운영자는 사이드 체인에서 적절한 자금을 분배하는 거래를 생성하며, 이러한 자금은 낮은 수수료, 빠른 확인 속도 및 높은 처리량을 가진 사이드 체인에서 사용될 수 있습니다.

사이드 체인의 주요 단점은 추가적인 보안 메커니즘과 보안 가정이 필요하다는 점입니다. 가장 간단한 사이드 체인 구조인 연합 사이드 체인은 멀티 시그니처 그룹의 운영자에 대한 신뢰를 기반으로 합니다. 스마트 컨트랙트 플랫폼에서는 토큰 인센티브 또는 bonding, challenging, slashing economic game을 이용하여 보안 모델을 세밀하게 조정할 수 있습니다.

다른 오프 체인 일반적인 스케일링 솔루션과 비교하여 사이드체인은 이해하고 구현하기가 더 쉽습니다. 사용자들이 수용할 수 있는 신뢰 모델을 구축할 수 있는 유형의 애플리케이션에 대해서는 사이드체인이 실용적인 해결책이 될 수 있습니다.

5.4 커밋 체인

커밋 체인(Commit-chains)은 Plasma와 같은 것들을 말하며, 이는 레이어 1 블록체인(root-chain)에서 광범위한 글로벌 컨센서스를 활용하는 레이어 2 체인이 구축됩니다. 이러한 커밋 체인은 안전하며, 체인 운영자가 악질이거나 기능이 제대로 작동하지 않을 경우, 사용자들은 항상 루트 체인 상의 메커니즘을 통해 자산을 인출할 수 있습니다.

커밋 체인 운영자는 거래를 올바르게 실행하고 루트 체인에 주기적으로 업데이트를 게시하는 것을 신뢰합니다. 루트 체인에 대한 긴급한 검열 공격을 제외한 모든 조건에서 커밋 체인 상의 자산은 안전하게 유지됩니다. 연합 사이드 체인(federated side-chains)과 유사하게, 커밋 체인 디자인은 믿을 수 있는 블록체인보다 더 우수한 사용자 경험을 제공합니다. 그러나 보다 강력한 보안 보장을 유지하면서 이를 수행합니다.

커밋 체인은 루트 체인 상에서 실행되는 스마트 컨트랙트에 의해 보호됩니다. 사용자는 자산을 이 계약에 예치하고, 커밋 체인 운영자는 커밋 체인 상에서 이를 대체할 자산을 제공합니다. 운영자는 주기적으로 루트 체인에 커밋을 발행하며, 이를 이용해 사용자는 머클 증명을 통해 자산 소유권을 증명하고, "이탈(exit)" 기능을 통해 커밋 체인 상의 자산을 루트 체인으로 인출할 수 있습니다.

이것은 Plasma를 비롯한 새로운 프로토콜 군을 기반으로 하는 커밋 체인 디자인의 일반적인 개념을 설명합니다. 2017년 Vitalik Buterin과 Joseph Poon이 발표한 Plasma 백서[7]는 야심찬 비전을 제시했습니다. 현재 모든 Plasma 체인은 자산 기반으로 동작하며, 대체 가능 및 대체 불가능 토큰(NFT) 소유권만 저장할 수 있습니다. 그러나 신뢰 없는 코드 실행(또는 스마트 컨트랙트)은 활발한 연구 분야입니다.

5.5 검증 가능한 오프체인 계산

암호학은 비싼 온 체인 검증 및 저렴한 오프 체인 계산의 동적에 적합한 도구를 제공합니다. 대화형 증명 시스템은 이러한 도구 중 하나입니다. 대화형 증명 시스템은 증명과 검증 두 참가자로 이루어진 프로토콜입니다. 증명자는 메시지를 주고 받음으로써 검증자를 설득할 정보를 제공하고, 검증자는 제공된 정보를 검토하고 거짓 주장을 거부하며, 검증자가 거부할 수 없는 주장은 참으로 인정됩니다.

검증자가 단순히 스스로 주장을 검증하지 않는 이유는 효율성 때문입니다. 증명자와 상호작용함으로써, 검증자는 이로인해 엄청난 비용이 드는 주장을 검증할 수 있습니다. 이 복잡성 격차는 다양한 원인으로 인해 발생할 수 있습니다: 1) 검증자가 가벼운 하드웨어를 사용하고 있어 공간 제한이나 시간 제한(또는 둘 다)이 필요한 계산만 지원할 수 있는 경우, 2) 단순한 검증에는 많은 수의 비결정적 선택에 대한 액세스가 필요한 경우, 3) 단순한 검증이 불가능한 경우, 검증자가 특정 비밀 정보를 소유하지 않기 때문입니다.

중요한 정보의 비밀성은 암호화폐 분야에서 분명히 관련된 제약요인이지만, 확장성 관점에서

더 중요한 제약요인은 상대적으로 저렴한 오프 체인 계산과 대조하여 높은 비용으로 이어지는 체인 상 검증 비용입니다.

암호화폐 분야에서는 중요한 관심사가 zk-SNARKs(Zero-Knowledge, Succinct Non-Interactive Argument of Knowledge)로 집중되고 있습니다. 이 비대화형 증명 시스템 패밀리는, 유한체 상의 덧셈과 곱셈으로 이루어진 회로로 임의의 계산을 인코딩합니다. 예를 들어, 산술 회로는 "이 Merkle tree에서 leaf값을 얼마나 알고 있는지"를 인코딩할 수 있습니다.

zk-SNARK 증명은 일정한 크기(수백 바이트)이며 일정한 시간 내에 검증할 수 있지만, 이 검증자 효율성은 신뢰 설정과 구조화된 참조 문자열이 필요하며, 페어링 기반 산술(구체적인 암호학적 난해성은 여전히 우려의 대상입니다.)도 필요합니다.

대안적인 증명 시스템은 서로 다른 트레이드 오프를 제공합니다. 예를 들어, Bulletproofs는 신뢰할 수 있는 설정이 없으며 더 일반적인 이산로그 가정에 의존하지만 로그 크기의 증명(그러나 여전히 상당히 작은)과 선형 시간 검증기를 갖습니다. zk-STARKs는 신뢰할 수 있는 설정이 필요하지 않으며 매우 견고한 암호학적 가정만을 사용하여 확장성 측면에서 zk-SNARKs에 대한 대안을 제공하지만 생산된 증명의 크기가 로그형태입니다.(그리고 수백 킬로바이트 정도로 상당히 큽니다.)

Nervos Network와 같은 다중 레이어 암호화폐 생태계에서는, 상호작용 증명은 증명자 측의 비용이 많이 드는 계산을 레이어 2로 오프로드하면서, 레이어 1에서는 수용 가능한 검증자 측의 작업만 필요로 합니다. 이러한 직관은 예를 들어 Vitalik Buterin의 ZK Rollup 프로토콜[8]에서 포착됩니다. 퍼미션리스 리레이어(relayer)가 체인 외부에서 트랜잭션을 수집하고 주기적으로 체인 상에 저장된 Merkle root를 업데이트합니다. 모든 이러한 루트 업데이트는 새로운 Merkle 트리에 유효한 트랜잭션만이 누적되었음을 보여주는 zk-SNARK와 함께 수행됩니다. 스마트 컨트랙트가 증명을 검증하고 증명이 유효한 경우에만 Merkle root를 업데이트할 수 있습니다.

위에서 개요한 구성은 단순한 트랜잭션 이외에도 DEX, 여러 토큰 및 프라이버시 보존 계산과 같은 더 복잡한 상태 전이를 지원할 수 있어야 합니다.

5.6 레이어 2 솔루션의 경제 모델

레이어 2 솔루션은 놀라운 확장성을 제공하지만, 이러한 시스템의 토큰 경제는 디자인적인 과제를 제기할 수 있습니다.

레이어 2 토큰 경제는 중요 인프라 (검증자 및 감시체계 같은)에 대한 보상, 그리고 응용 프로그램 특정 인센티브 디자인을 포함할 수 있습니다. 중요한 레이어 2 인프라는 기간 기반의 구독 모델로 더 잘 작동하는 경향이 있습니다. Nervos 네트워크에서는, CKB의 기회 비용 기반 지불 방법을 통해 이러한 가격 구조를 쉽게 구현할 수 있습니다. 서비스 제공자는

NervosDAO를 통해 자신의 사용자의 "보증금"에 대한 이자를 수집할 수 있습니다. 레이어 2 개발자는 그들의 응용 프로그램에 특화된 인센티브에 대한 토큰 경제 모델에 집중할 수 있습니다.

어떤 면에서는 이러한 가격 책정 모델은 사용자가 CKB 상에 상태 저장소에 대한 비용을 지불하는 방식과 정확히 동일합니다. 사용자들은 NervosDAO에서 발행된 인플레이션 보상을 지급함으로써 채굴자들에게 구독료를 지불하게 됩니다.

6. Nervos Network

6.1 레이어 1을 자산 저장소 플랫폼으로 구축

우리는 레이어 1 블록체인이 자산 저장소로서 구축되어야 한다고 믿습니다. 장기적인 탈중앙화를 극대화하기 위해, 트랜잭션 수수료 대신 상태 저장 공간 점유를 중심으로 한 경제 모델을 갖춘 작업 증명 합의 기반으로 구축되어야 합니다. 공유 지식 베이스(Common Knowledge Base, CKB)는 상태(state)를 기반으로 프로그래밍과 경제 모델이 설계된, 여러 자산을 보관할 수 있는 가치 저장소로, 작업 증명을 기반으로 합니다.

CKB는 Nervos Network의 기초적인 레이어로, 최고의 보안성과 최고의 탈중앙화를 제공합니다. CKB에서 자산을 소유하고 거래하는 것은 가장 높은 비용이 발생하지만, 네트워크에서 가장 안전하고 접근 가능한 자산 저장소를 제공하며 최대한의 결합성을 가능하게 합니다. CKB는 고가의 자산과 장기적인 자산 보존에 가장 적합합니다.

공유 지식 베이스(Common Knowledge Base)는 레이어 2 프로토콜을 지원하기 위해 특별히 구축된 첫 번째 레이어 1 블록체인입니다.

- CKB는 확장성과 같은 레이어 2 우선 순위와 겹치지 않고 보안과 탈중앙화에 초점을 맞춘 레이어 2 프로토콜을 보완하는 데 설계되었습니다.
- CKB는 계정이 아닌 상태(state)를 중심으로 자신을 모델링합니다. 셀(cell)은 기본적으로 거래에 의해 참조되고 레이어 간에 전달될 수 있는 독립적인 상태 객체입니다. 계정(account) 대신 상태(state)의 작은 조각이 레이어 간에 참조되고 전달되는 레이어식 구조에서 이상적입니다.
- CKB는 계산 엔진 대신 일반화된 검증 머신으로 설계되었습니다. 이를 통해 CKB는 오프체인 상태 전이를 검증하는 암호학적인 법원으로 작동할 수 있습니다.
- CKB는 개발자가 쉽게 사용자 지정 암호 프리미티브를 추가할 수 있도록 설계되었습니다. 이를 통해 다양한 레이어 2 솔루션에서 생성된 증명을 검증할 수 있어 CKB를 미래에 대비할 수 있습니다.

공유 지식 베이스는 최고의 레이어 2 생태계를 제공하여 뛰어난 확장성과 효율적인 블록체인 거래를 제공하며, 세상에서 가장 가치 있는 공유 지식을 저장하는 인프라를 지향합니다.

6.2 레이어 2 솔루션으로 확장하기

레이어화 아키텍처로 인해, Nervos Network는 탈중앙화와 자산 보존의 중요한 속성을 유지하면서 레이어 2에서 참가자 수를 어떤 수에도 확장할 수 있습니다. 레이어 2 프로토콜은 레이어 1 커밋먼트나 암호 프리미티브 자원을 사용할 수 있으므로, 레이어 2 사용자 베이스를 지원하는 거래 시스템을 설계하는 데 큰 유연성과 창의성을 제공합니다. 레이어 2 개발자는 자신의 애플리케이션과 사용자 컨텍스트에서 가장 잘 작동하는 처리량, 최종성, 개인 정보 보호 및 신뢰 모델에 대한 교환이 가능합니다.

Nervos Network에서 레이어 1 (CKB)은 상태 검증을 위해 사용되며, 레이어 2는 상태 생성을 담당합니다. 상태 채널과 사이드 체인은 상태 생성의 예시입니다. 그러나 제로 지식 증명 생성 클러스터와 같은 상태 생성-검증 패턴을 사용할 수 있습니다. 지갑 또한 레이어 2에서 운영되며 임의의 논리를 실행하고 새로운 상태를 생성한 다음 CKB에 상태 전환을 제출하여 검증합니다. Nervos Network의 지갑은 상태 생성자이므로 상태 전환을 완전히 제어할 수 있어 굉장히 강력합니다.

사이드체인은 개발자 친화적이며 좋은 사용자 경험을 제공하지만, 그들의 검증자의 정직성에 의존합니다. 검증자들이 악의적으로 행동하면 사용자들은 자산을 잃을 위험이 있습니다. Nervos Network는 "Muta"라는 지분증명 (Proof of Stake) 블록체인 프레임워크와 그 위에 기반한 사이드체인 솔루션 "Axon"으로 구성된 CKB 상에서 사이드체인을 출시하기 위한 오픈 소스이고 쉽게 사용할수있는 사이드체인 스택을 제공합니다.

Muta는 매우 유연하며 높은 성능의 블록체인 프레임워크로서 지분 증명, BFT 합의 및 스마트 계약을 지원하도록 설계되었습니다. 높은 처리량 및 낮은 지연 시간의 BFT 합의 "Overlord"가 특징이며, CKB-VM, EVM 및 WASM을 비롯한 다양한 가상 머신을 지원합니다. 여러 가상 머신을 동시에 사용하여 상호 운용성을 지원합니다. Muta는 개발자들이 고성능 블록체인을 구축하는 데 필요한 장벽을 크게 낮추면서도 프로토콜을 사용자 정의하는 최대한의 유연성을 제공합니다.

Axon은 Muta를 기반으로 한 완전한 솔루션으로, Nervos CKB 상의 턴키 사이드 체인을 개발자들에게 제공하여 실용적인 보안 및 토큰 경제 모델을 제공합니다. Axon 솔루션은 안전한 자산 보호를 위해 CKB를 사용하며, 토큰 기반의 거버넌스 메커니즘을 사용하여 사이드 체인 검증자를 관리합니다. Axon 사이드 체인과 CKB 간, 그리고 Axon 사이드 체인 간 상호 작용을 위한 크로스 체인 프로토콜도 내장됩니다. Axon을 사용하면 개발자는 인프라 및 크로스 체인 프로토콜을 구축하는 대신 응용 프로그램을 구축하는 데 집중할 수 있습니다.

Muta와 Axon 모두 현재 활발한 개발 단계에 있습니다. 우리는 곧 프레임 워크를 오픈 소스로 공개할 예정이며, Muta와 Axon 모두를 위한 RFC도 곧 출시될 예정입니다.

레이어 2 프로토콜은 연구 및 개발 분야에서 번성하고 있으며, 우리는 모든 레이어 2 프로토

콜이 표준화되고 매끄럽게 상호 운용될 미래를 예상합니다. 그러나 레이어 2 솔루션이 아직 완전하게 성숙하지 않으며, 그들이 할 수 있는 것의 한계를 자주 넘어서는 것을 알고 있습니다. 또한 그들의 허용 가능한 트레이드오프를 찾아야 합니다. 초기 전도유망한 솔루션을 볼 수 있었지만, 상호 운용성, 보안 및 레이어 2 설계에서의 경제 모델과 같은 주제에 대한 연구가 여전히 충분히 이루어지지 않은 상황입니다. 메인넷 런칭 이후, 우리는 레이어 2 프로토콜에 대한 연구 노력의 대부분을 집중하고 투자할 것입니다.

6.3 지속 가능성

장기적인 지속 가능성을 고려하여, Nervos CKB는 상태를 제한하고 온체인 스토리지에 비용을 부과하며 사용자가 상태 저장소를 청소할 수 있는 인센티브를 제공합니다. 제한된 상태는 전체 노드 참여 요구 사항을 낮추어 노드를 저렴한 하드웨어에서 실행할 수 있도록 보장합니다. 강력한 전체 노드 참여는 탈중앙화 및 보안을 증가시킵니다.

Nervos CKB는 상태 저장소에 대한 시간 비례 "상태 임대료" 비용을 부과함으로써, "한 번 지불하고 영원히 저장" 패러다임에서 많은 블록체인이 직면하는 공유 지역의 비균형성 문제를 완화합니다. 이 상태 임대 기능은 "타겟 인플레이션"을 통해 구현되며, 부과된 비용은 사용자 경험을 원활하게 유지하면서 상태 저장소에 대한 비용을 부과합니다.

사용자가 자신의 데이터가 차지하는 컨센서스 공간을 소유하기 때문에 이러한 인플레이션 비용은 대상 지정이 가능합니다. 이 모델은 또한 사용자가 상태를 컨센서스 공간에서 제거할 수 있는 기본적인 메커니즘도 포함하고 있습니다. 상태 대여의 경제적 인센티브과 결합하여 상태 크기가 항상 네트워크 참여자가 필요로 하는 최소한의 데이터 양으로 이동함을 보장합니다.

개별적으로 소유된 상태는 개발자의 비용을 크게 줄입니다. 사용자의 상태 요구 사항에 대해 CKByte를 구입해야 하는 대신, 개발자는 응용 프로그램에서 필요한 검증 코드를 저장하는 데 충분한 CKByte만 구입하면 됩니다. 각 사용자는 자신의 셀을 사용하여 토큰을 저장하고 자산에 대한 완전한 책임을 집니다.

마지막으로, 상태 대여는 채굴자에게 새로운 토큰 발행을 통한 지속적인 보상을 제공합니다. 이 예측 가능한 수익은 채굴자가 수수료를 받기 위해 이윤 창출 블록을 포킹하는 대신 블록체인을 진전시키는 데 인센티브를 제공합니다.

6.4 일치된 인센티브

CKB의 경제 모델은 생태계의 모든 참여자들의 인센티브를 일치시킵니다. 특히, 상승하는 토큰 가격은 모든 참여자들의 목표를 지원합니다.

- 채굴자 : 상승하는 토큰 가격은 채굴 수익을 증가시킵니다.
- 사용자 : 상승하는 토큰 가격은 더 많은 채굴 참여를 유도하며 더 높은 자산 보안을 제공합니다.

- 개발자 : 상승하는 토큰 가격은 사용자에게 더 높은 보안을 제공하면서 개발자 비용을 크게 올리지 않습니다.
- 토큰 홀더 : 상승하는 토큰 가격은 그들의 토큰 가치를 증가시킵니다.

Nervos CKB는 안전한 자산 보존을 목적으로 구축되었으며, 저렴한 거래 수수료를 위해 만들어진 것이 아닙니다. 이러한 중요 입장은 중앙집중화를 추구하는 거래 매개체 사용자 대신 비트코인 사용자 커뮤니티와 유사한 자산 보존 사용자를 유치할 것입니다.

거래 매개체 사용 사례는 항상 효율성과 낮은 수수료를 추구하여 블록체인 네트워크를 중앙집중화로 밀어붙이는 경향이 있습니다. 네트워크를 보호하는 인프라 운영자(마이너 또는 검증자)들이 네트워크를 보호하는 데 중요한 수입원이 부족한 경우, 보안은 통화적 인플레이션을 통해 지원되거나 무시당할 수 있습니다. 통화적 인플레이션은 장기 보유자에게 해로울 뿐만 아니라 보안 자금 부족은 네트워크의 모든 이해 관계자에게 해로울 수 있습니다.

반면, 자산 보존 사용자는 검열 저항성과 자산 보안에 대한 강력한 요구사항이 있습니다. 그들은 채굴자가 이를 제공하고, 그 역할을 보상합니다. 자산 보존 네트워크에서 이러한 당사자는 서로 이해 관계가 있습니다.

여타 다른 블록체인에서는 장기 보유자들이 "투기꾼"으로 여겨질 수 있지만, Nervos Network의 토큰 홀더들은 전체 네트워크 가치의 직접적인 공헌자입니다. 이들 사용자는 네이티브 토큰에 대한 수요를 만들어, 네트워크의 증가한 보안 예산에 기여합니다.

모든 참가자들의 인센티브를 일치시킴으로써, 단결된 Nervos 커뮤니티가 성장할 수 있으며, 네트워크의 일치된 경제 시스템은 하드포크에 대한 저항력을 갖게 됩니다.

6.5 가치 획득과 생성

어떤 블록체인 플랫폼이 보안을 유지하면서 플랫폼에 의해 보호되는 자산의 가치가 증가함에 따라 가치를 포착할 수 있는 메커니즘이 필요합니다. CKB는 상태를 제한하여 공유 공간을 희소하게 만들어 시장 가격을 부여합니다. 네트워크에서 자산 저장 수요가 증가하면 상태 저장 공간 (및 CKB의 네이티브 토큰)의 가치도 상승할 것입니다. CKB는 네이티브 토큰에 가치를 직접적으로 누적시키는 최초의 멀티 애셋 플랫폼입니다.

CKB는 가치 보존 플랫폼으로, 보호하는 자산의 보안 수준에 따라 CKB의 본질적 가치가 결정됩니다. 보호하는 자산의 가치가 증가함에 따라, CKB의 경제 모델은 자동으로 CKB의 보안 예산을 높여 더 많은 채굴 자원을 유치하여 플랫폼의 보안성을 강화하고 플랫폼의 본질적 가치를 높일 수 있습니다. 이는 플랫폼을 지속 가능하게 만드는 것뿐만 아니라, 플랫폼의 본질적 가치의 성장 경로를 제공합니다. 플랫폼이 더욱 안전하면 고가치 자산에 더욱 매력적이기 때문에 수요가 증가하고, 이는 더 많은 수요를 생성합니다. 물론 이는 최종적으로 블록체인 공간으로 이동할 총 투자 금액에 의해 제한되지만, 우리는 CKB가 이러한 수요의 상당한 부분을 확보할 것이라 믿습니다.

시간이 지남에 따라, 우리는 CKB의 경제 밀도가 증가할 것으로 예상합니다. CKByte는 고가의 자산 보관에 사용되며, 저가의 자산은 CKB에 연결된 블록체인(예: 레이어 2 사이드체인)으로 이동할 것입니다. CKB는 직접 자산을 보호하는 대신, 몇 백 바이트의 암호화 증명을 통해 전체 사이드체인 생태계를 보호하는 신뢰 루트로 사용될 수 있습니다. 이러한 증명의 경제적 밀도는 극도로 높으며, CKByte의 가격이 크게 상승함에 따라 저장 공간 수요 곡선을 더 욱 더 많이 지원합니다. 이는 작은 토지 조각이 초고층 빌딩을 지원함으로써 경제적 밀도를 크게 높이는 것과 유사합니다.

마지막으로, NervosDAO와 "인플레이션 쉘터" 기능의 설계를 통해, 장기적인 토큰 홀더들은 항상 총 발행액의 일정 비율을 보유하게 되어, 네이티브 토큰 자체가 우수한 가치 저장 수단이 됩니다.

6.6 규제 간극 연결

퍼미션리스 블록체인은 자산 발행 및 거래에서 완전한 탈중앙화를 가능하게 합니다. 이것이 그들이 가치 있는 이유이지만, 동시에 실세계 금융 및 사법 체계와 호환되지 않는 이유입니다.

계층 구조가 등장함으로써, 규제를 받지 않는 퍼미션리스 블록체인의 규정 준수 부분을 생성할 수 있는 기회가 제공됩니다. 예를 들어, 사용자는 레이어 1에 분산화 된 자산을 저장하고 이러한 자산의 절대적인 소유권을 누리며, 규제 및 법률 제약 조건에 따라 레이어 2에서 실제 비즈니스를 처리할 수 있습니다.

암호화폐 거래소가 대표적인 예입니다 - 일본과 싱가포르와 같은 국가들은 거래소에 라이선스를 발급하고 규제 요건을 만들어내고 있습니다. 규제 준수형 거래소나 글로벌 거래소의 지점은 레이어 2 거래 체인을 구축하여 사용자 ID 및 자산을 가져오고 지역 규제 요건에 따라 합법적인 비즈니스를 진행할 수 있습니다.

실제 세계 자산의 발행 및 거래는 계층화된 블록체인 구조 내에서 가능해집니다. 규제된 레이어 2 사이드체인을 통해 실제 세계 자산이 블록체인 생태계로 유입되어 무제한으로 조합이 가능한 탈중앙화 금융 서비스 생태계에 접근하고 가치를 극대화할 수 있게 됩니다.

앞으로 Nervos Network는 이와 같은 레이어 2 사이드 체인 및 응용 프로그램을 대규모 사용자 채용의 기초로 사용하며 이 공간의 선도 기업들과 협력합니다.

레퍼런스

[1] Satoshi Nakamoto. "비트코인: P2P 전자 화폐 시스템". 2008년 10월 31일, https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin. "이더리움 화이트 페이퍼: 다음 세대 스마트 계약 및 탈중앙화 애플리케이션 플랫폼". 2013년 11월, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] 평균 비트코인 거래 크기가 250바이트인 경우: (2 * 250 * 7,500,000,000) / (24 * 6) = 26,041,666,666 바이트 블록 (10분마다); 26,041,666,666 * (24 * 6) = 3,750,000,000,000 바이트 (블록체인의 일일 성장); 3,750,000,000,000 * 365.25 = 1,369,687,500,000,000 바이트 (블록체인의 연간 성장)

[4] Gur Huberman, Jacob Leshno, Ciamac C. Moallemi. "비트코인 지불 시스템의 경제학적 분석: 독점자 없는 독점". 핀란드 은행 연구 논문 27/2017. 2017년 9월 6일, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032375

[5] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, Arvind Narayanan. "블록 보상 없이 비트코인의 불안정성". 2016년 10월, https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf

[6] Lewis Gudgeon, Perdo Moreno-Sanchez, Stefanie Roos, Patrick McCorry, Arthur Gervais. "SoK: Off The Chain Transactions". 2019년 4월 17일, https://eprint.iacr.org/2019/360.pdf

[7] Joseph Poon, Vitalik Buterin. "플라즈마: 확장 가능한 자율적 스마트 계약". 2017년 8월 11일, https://plasma.io/plasma.pdf

[8] Vitalik Buterin. "대량 거래 유효성 검사를 통한 체인 상 확장 가능성 ~500 tx/sec까지". 2018년 9월 22일, https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477