

Analysis

지분증명방식 블록체인 네트워크의 개방성 수준 비교 분석

요약

이 분석 보고서는 지분 증명(Proof of Stake) 합의 기반으로 동작하는 열한 개의 블록체인 네트워크를 선별하고, 다섯 가지 지표를 활용하여 이 네트워크들의 개방성 수준을 제공합니다. 개방성 수준 지표 중에는 밸리데이터 수와 자본의 집중성과 같은 탈중앙 수준 측면 지표와, 참여를 위해 필요한 자본 및 경제적 관점에서의 네트워크 안정성과 같은 참여 가능성 측면의 지표 등이 있으며, 이를 통해 지분 증명 합의 기반 블록체인 네트워크들의 개방성을 측정하고 특징을 분석합니다.

개방성이 높은 블록체인 네트워크로는 솔라나, 아발란체 등이 있으며, 개방성이 낮은 블록체인 네트워크로는 BNB 체인, 클레이튼, 폴리곤 등이 있습니다.

이더리움은 참여자 수와 체인 운영 비용 등에서 높은 개방성 수준을 보였으나, 유통량 중 스테이크 된 지분의 비율이 상대적으로 적고, 지분의 상당수가 리도와 같은 스테이킹 풀 내에 있어 자본 집중도 및 스테이킹 비율 면에서 낮은 점수를 받았습니다.

허가형 블록체인인 클레이튼과 폴리곤은 낮은 수준의 개방성을 보이고 있으며, 이들이 무허가형 블록체인으로 변화하기 위해서는 개방성 수준을 함께 고려해야 할 것으로 보입니다.

1. 서론

이 글에서는 지분 증명(Proof of Stake, PoS) 합의 기반으로 동작하는 여러 블록체인의 네트워크의 개방성 수준을 비교하고 장단점을 파악하여 블록체인 네트워크의 개방성을 높일 수 있는 방안을 제시해 보고자 합니다.

지분 증명 방식은 스테이킹 된 자산의 양에 따라 블록을 생성하고 합의를 이루는 방식입니다. 일반적으로 이 방식은 지분에 비례한 합의 방식(지분 비례 방식)을 사용하여, 더 많은 지분을 가진 밸리데이터가 블록 생성 및 합의 과정에서 더 큰 영향력을 행사할 수 있습니다. 이 방식은 일부의 지분이 많은 검증자의 영향력이 강해질 수 있는 문제가 있습니다. 이 문제를 완화하기 위해, 일부 네트워크에서는 지분 사용을 밸리데이터 자격 조건으로만 제한하고, 밸리데이터 수에 비례하여 합의를 이루는 방식(밸리데이터 수 비례 방식)을 사용하는 경우도 있습니다. 이런 네트워크에서는 일단 밸리데이터가 되면 지분의 크기와 관계 없이 다른 밸리데이터와 동등하게 합의 과정에 참여합니다.

블록체인의 개방성은 탈중앙성과 어느 정도 연관된 맥락을 갖지만, 완전히 같은 것은 아닙니다. 먼저, 개방성은 블록체인의 네트워크 참여 접근성에 초점이 맞추어져 있습니다. 누구나 밸리데이터로 참여하여 블록 생성과 검증에 할 수 있는지, 각각의 네트워크 참여자가 얼마나 많은 기여를 할 수 있는지 등을 중요하게 여기면서, 동시에 잠재적인 공격으로부터 얼마나 신뢰성 있게 네트워크 운영이 가능한지를 확인합니다. 이런 요소를 통해 네트워크의 개방성을 측정할 수 있습니다.

탈중앙성은 블록체인의 네트워크 참여자들 사이에 권력이 얼마나 고르게 분산되어 있는지에 초점이 맞추어져 있습니다. 즉, 개방성은 탈중앙성의 개념을 일부 포함하면서도 좀더 넓은 의미를 가지고 있습니다.

블록체인의 개방성 수준을 측정할 수 있는 표준은 없지만, 네트워크 참여자 수, 의미 있는 참여자 수와 같은 탈중앙적인 요소와, 경제적 측면의 접근성 및 지속 가능성, 그리고 경제적 관점에서의 네트워크 보안성과 같은 참여 가능성 측면 등을 고려해 볼 수 있습니다. 본 글에서는 다음 다섯 가지 지표를 통해 블록체인의 개방성 수준을 비교하고자 합니다.

- 1) 밸리데이터 수 측면: 밸리데이터 수는 블록체인의 네트워크에 직접 참여하여 블록을 생성하고 검증하는 노드의 수를 나타내며, 이는 개방성의 중요한 지표 중 하나로 작용할 수 있습니다. 일반적으로 개방형 블록체인의 밸리데이터 수는 허가형 블록체인의 밸리데이터 수보다 많습니다.
- 2) 참여를 위해 필요한 자본 측면: 참여를 위해 필요한 자본은 블록체인의 개방성과 밀접한 관련이 있습니다. 참여를 위한 자본 요구량이 낮은 네트워크는 경제적 측면에서 접근성이 높아지게 됩니다. 이는 밸리데이터 운영에 참여하는 사용자의 범위를 확대에 도움이 될 수 있습니다.
- 3) 자본 집중도 측면: 스테이킹 된 자본이 고르게 분포된 블록체인은 많은 수의 밸리데이터 합의를 통해 높은 보안성을 유지할 수 있습니다. 지분증명 방식 블록체인은 스테이킹 지분에 비례하여 합의를 결정하는 경우가 많습니다. 만약 특정 밸리데이터에 너무 많은 지분이 몰려 있으면, 소수의 몇몇 밸리데이터들의 합의만으로도 블록이 생성될 수 있으며 이는 개방된 네트워크에는 적절하지 않습니다. 따라서, 스테이킹 된 자본이 고르게 분포되어 있을수록 블록체인의 개방성이 높다고 이야기 할 수 있습니다.
- 4) 운영 비용 측면: 밸리데이터를 운영하는 비용이 낮을수록, 더 많은 사용자들이 지속적으로 밸리데이터로 참여하는 데 도움을 줄 수 있습니다.
- 5) 경제적인 관점에서의 네트워크 안정성 측면: 블록체인의 경제적 안정성은 외부 공격자로부터 네트워크를 보호하는 데 중요한 역할을 합니다. 네트워크 안정성에는 다음과 같은 두 가지 요소를 고려해야 합니다.
 - a) 스테이킹 비율: 유통 물량 중 스테이킹 된 지분 비율이 높을수록 네트워크의 안정성이 향상됩니다. 스테이킹 비율이 높을수록 공격자가 네트워크에 문제를 일으키기 위해 필요한 네이티브 토큰을 확보하기 어렵게 만들 수 있습니다.

- b) 공격 비용: 공격자가 네트워크에 문제를 일으키기 위해 필요한 비용은 네트워크 안정성에 중요한 요소입니다. 공격 비용이 높을수록 네트워크 공격이 경제적으로 불리해지며, 공격자가 공격을 시도할 가능성이 줄어들 수 있습니다.

이번 글에서는 아홉 곳의 무허가 블록체인 네트워크와, 점진적으로 개방형 네트워크로 변화를 계획하고 있는 허가형 블록체인 네트워크 두 곳을 조사하여 각각의 개방성 수준을 측정 및 분석합니다.

2. 개방성 수준 측정

1) 밸리데이터 수 측면

먼저, 밸리데이터 수를 살펴보겠습니다. 네트워크에 참여하는 밸리데이터 수가 많을수록, 더 많은 참여자들의 의견이 반영될 수 있어 개방성이 높아진다고 이야기할 수 있습니다. 일반적으로, 개방형 블록체인 네트워크는 누구나 참여할 수 있는 구조로 이루어져 있으므로 허가형 블록체인 네트워크보다 밸리데이터 수가 더 많을 것이라고 예상할 수 있습니다. 예를 들어, 개방된 블록체인 중 하나인 비트코인의 노드 수는 약 [17,000개](#)입니다. 반면, 허가형 블록체인 중 하나인 EOS의 밸리데이터 수는 [21개](#)에 불과합니다.

[표 1] 2023년 3월 말 기준 블록체인 네트워크 별 밸리데이터 수

개방형/허가형	블록체인 네트워크	밸리데이터 수	최대 밸리데이터 수*
개방형 블록체인	Algorand	183 (추정)**	제한 없음 / 5,000
	Aptos	104	104 / 1,000
	Avalanche	1,200	제한 없음 / 5,000
	BNB Chain	29	29 / 100
	Celo	110	110 / 200
	Cosmos Hub	175	175 / 300
	Ethereum	9,700 (클라이언트 수)***	제한 없음 / 100,000
	Near	213	213 / 400
	Solana	2,000	제한 없음 / 10,000
허가형 블록체인	Klaytn	31	허가 필요
	Polygon	100	허가 필요

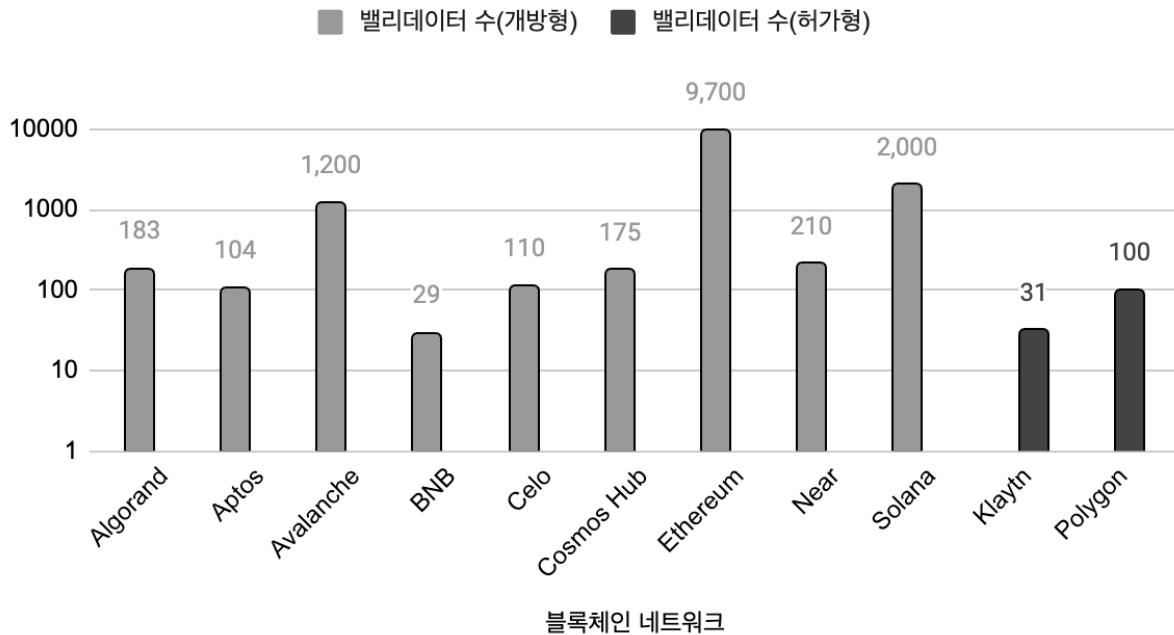
* A / B - A: 2023년 3월 기준 해당 네트워크의 정책, B: 2023년 3월 기준 기술적 최대 수치 표기. 기술적 최대 수치는 자체 분석

** 알고랜드는 밸리데이터의 전체 수를 공개하고 있지 않음

*** 이더리움의 경우, 밸리데이터 수는 50만 이상이나, 하나의 클라이언트에서 여러 밸리데이터를 가동할 수 있으므로, 밸리데이터 수 대신 클라이언트 수를 표기함

data from [Staking Rewards](#), [TheCelo](#), [Chainparrot](#), [Avalanche Explorer](#), [NEAR Explorer](#), [Algorand Developer Portal](#), [Aptos explorer](#), [Polygon Scan](#), [cosmos chain explorer](#), [Solana Beach](#), [Klaytn Scope](#), [Ethereum Node Tracker](#), [BscScan](#)

체인 별 밸리데이터 수



[표 1]을 통해, 개방형 블록체인과 허가형 블록체인의 밸리데이터 수 차이를 확인할 수 있습니다. 또한, 개방형 블록체인 사이에서도 밸리데이터 수의 차이가 발생하는 것을 볼 수 있습니다. 이는 밸리데이터 참여 조건 및 최대 밸리데이터 수 제한 등의 요소가 다르기 때문입니다.

예를 들어, BNB 체인은 개방형 블록체인이지만 최대 밸리데이터 수를 29개로 제한하고 있습니다. BNB 체인과 같이, 개방형 블록체인 중에서도 개방성을 일부 제한하더라도 안정성을 높이기 위해 최대 밸리데이터 수를 제한하는 전략을 사용하는 경우도 많습니다.

이더리움과 같이 단일 클라이언트 내에서 여러 밸리데이터가 동작하는 블록체인의 경우, 개방성을 평가할 때 클라이언트 내에서 작동하는 여러 밸리데이터를 여러 개체로 볼 것인지, 한 개로 볼 것인지를 고려해야 합니다. 이 글에서는 단일 클라이언트 내에서 동작하는 모든 밸리데이터들을 하나의 밸리데이터로 간주하였습니다. 이는, 하나의 클라이언트가 어떤 이유로 정지되면, 해당 클라이언트와 연결된 모든 밸리데이터들이 동시에 정지될 수 있기 때문입니다. 따라서, 이 글에서는 이더리움의 밸리데이터 개수 대신 클라이언트 개수를 표기하였습니다.

2) 참여를 위해 필요한 자본 측면

참여에 필요한 자본은 블록체인의 개방성에 큰 영향을 미칩니다. 초기 자본 비용이 낮을수록 참여 장벽이 낮아지고 더 많은 사용자가 밸리데이터로 참여할 기회를 얻을 수 있어 개방성이 높아집니다. 그러나, 초기 자본 요구량이 낮을수록 악의적 행위의 위험 또한 증가할 수 있습니다. 악의적 행위를 제재하는 주요 방법 중 하나로 자본 삭감(슬래싱)이 있지만, 삭감할 자본이 부족하면 제재의 효과가 약해질 수 있으며, 악의적 공격자가 낮은 기회 비용으로 공격을 시도할 수 있습니다.

[표 2] 2023년 3월 말 기준 블록체인 네트워크 별 최소 스테이킹 요구량

블록체인 네트워크	요구되는 스테이킹 수량	USD 환산
Algorand	0.1 ALGO	0.1
Solana	0.01 SOL*	0.2
Cosmos Hub	0.1 ATOM	1
Celo	10,000 CELO	6,000
Polygon	10,000 MATIC	11,000
Avalanche	2,000 AVAX	36,000
Near	25,200 Near	50,400
Ethereum	32 ETH	57,600
Aptos	10,000 APT	130,000
Klaytn	5,000,000 KLAY	1,150,000
BNB	10,000 BNB	3,300,000

* Solana는 최소 스테이킹 수량을 정하지 않았지만, 합의 과정에 가스비를 사용하며, 이 양은 하루에 약 1.1SOL입니다.

[표 2]를 통해, 각 블록체인 네트워크의 밸리데이터 참여에 필요한 최소 자본 요구량이 다양하다는 것을 확인할 수 있으며, 이를 통해 블록체인 네트워크의 개방성 수준을 일부 파악할 수 있습니다.

BNB 체인은 최소 자본 요구량을 상대적으로 높게 설정하여, 다른 블록체인에 비해 개방성보다는 선별된 운영주체에 대한 신뢰도를 더욱 중요시하고 있다고 분석할 수 있습니다. 코스모스 허브나 알고랜드는 최소 스테이킹 요구량이 없으므로, 최소 스테이킹 요구량 측면에서 개방성이 높다고 볼 수 있습니다.

솔라나의 경우, 밸리데이터에 참여하기 위해 정해진 최소 자본 요구량은 없지만, 합의 과정에서 발생하는 트랜잭션 가스비를 고려해야 하는 독특한 구조를 가지고 있습니다. 솔라나는 이런 전략을 통해 초기에 대량의 자본을 예치해야 하는 진입장벽을 없앴습니다.

[표 3] 2023년 3월 말 기준 밸리데이터 순위에 들기 위한 최소 자본

밸리데이터 수 제한	블록체인 네트워크	최소 스테이킹 요구량	가장 적게 스테이킹한 밸리데이터의 수량	USD 환산
제한 없음	Algorand	0.1 ALGO	0.1 ALGO	0.1
	Avalanche	2,000 AVAX	2,000 AVAX	36,000
	Ethereum	32 ETH	32 ETH	57,600
	Solana	0.01 SOL*	10,000 SOL	230,000
최대 밸리데이터 수 제한 있음	Near	25,200 Near	25,200 Near	50,400
	Polygon	10,000 MATIC	58,000 MATIC	66,700
	Celo	10,000 CELO	1,350,000 CELO	837,000
	Cosmos Hub	0.1 ATOM	82,000 ATOM	984,000
	Klaytn	5,000,000 KLAY	5,000,000 KLAY	1,150,000
	Aptos	10,000 APT	1,010,000 APT	13,130,000
	BNB	10,000 BNB	182,500 BNB	60,225,000

* Solana는 최소 스테이킹 요구량은 없지만, 합의 과정에 가스비를 사용하며, 이 양은 하루에 약 1.1SOL입니다.

[표 3]은 각 네트워크에 참여 중인 밸리데이터 중에서 가장 적은 자본을 담보로 맡긴 밸리데이터의 자본량을 조사한 것입니다. 이 자료를 통해 밸리데이터로 참여하기 위해 어느 정도의 자본이 필요한지를 확인할 수 있습니다.

BNB 체인과 앵토스와 같은 블록체인 네트워크에서 밸리데이터로 참여하기 위해서는 제한된 밸리데이터 순위 내에 들어야 하며, 순위 내에 들기 위해서는 최소 스테이킹 요구량보다 훨씬 많은 자본을 필요로 합니다. 즉, 밸리데이터로 참여하기 위해서는 최소 스테이킹 요구량보다 훨씬 많은 수량의 자본을 스테이킹해야 하는 구조입니다. 이렇게 큰 자본을 요구하는 블록체인 네트워크에 일반 사용자들이 밸리데이터로 참여하기는 어려우며, 재단이나 다른 기관의 도움이 필요할 수 있습니다.

아발란체, 이더리움, 솔라나와 같은 네트워크들은 밸리데이터 수에 제한을 두지 않으므로, 최소 스테이킹 수량만 충족하면 누구나 밸리데이터로 참여할 수 있습니다. 이런 네트워크에서는 상대적으로 적은 양을 스테이킹한 밸리데이터가 많습니다. 이러한 구조는 더 많은 사용자들이 밸리데이터로 참여할 수 있는 기회를 제공하므로 개방성을 높이는 데 도움을 줍니다.

이더리움은 최소 및 최대 스테이킹 수량이 동일한 32 ETH로 설정되어 있습니다. 이더리움의 밸리데이터 수가 많은 이유는, 많은 자본을 가진 그룹들이 여러 개의 밸리데이터를 운영하면서 각 밸리데이터마다 32 ETH씩 스테이킹하고 있기 때문입니다.

3) 자본 집중도 측면

블록체인 네트워크의 개방성은 스테이킹 된 자본의 분포와 관련이 있습니다. 특히, 스테이킹 지분에 비례하여 합의를 결정하는 블록체인 네트워크에서는 소수의 밸리데이터에 지분이 집중되어 있는 경우,

특정 밸리데이터들이 합의 과정에서 너무 큰 영향력을 행사할 수 있습니다. 이런 상황은 네트워크의 개방성을 낮추고 중앙화된 권력을 형성할 수 있게 됩니다. 스테이킹 된 자본이 고르게 분포되어 있을수록 밸리데이터들의 균형이 유지되어 개방성이 높다고 이야기 할 수 있습니다.

밸리데이터 수에 비례하는 합의 방식을 사용하는 네트워크에서는 밸리데이터간의 영향력이 고르게 분포되며, 합의를 위해 더 많은 밸리데이터가 필요하게 됩니다. 따라서, 이런 네트워크들은 집중도 측면에서 상대적으로 높은 개방성을 제공할 수 있습니다.

[표 4] 블록체인 네트워크 별 합의에 중요한 영향을 미치는 밸리데이터의 수

합의 방식	블록체인 네트워크	밸리데이터 수	나카모토 계수* (체인 정지에 필요한 밸리데이터 수)	블록 합의에 필요한 밸리데이터 수
지분에 비례	Algorand	183(추정)****	?	?
	Aptos	104	13	27
	Avalanche	1,200	29	80
	Cosmos hub	175	7	27
	Ethereum	9,700(클라이언트 수)**	2	3,200 (클라이언트 수, 추정치)***
	Near	210	7	28
	Polygon	100	4	12
	Solana	2,000	33	132
밸리데이터 수에 비례	BNB	29	8	20
	Celo	110	37	74
	Klaytn	31	11	21

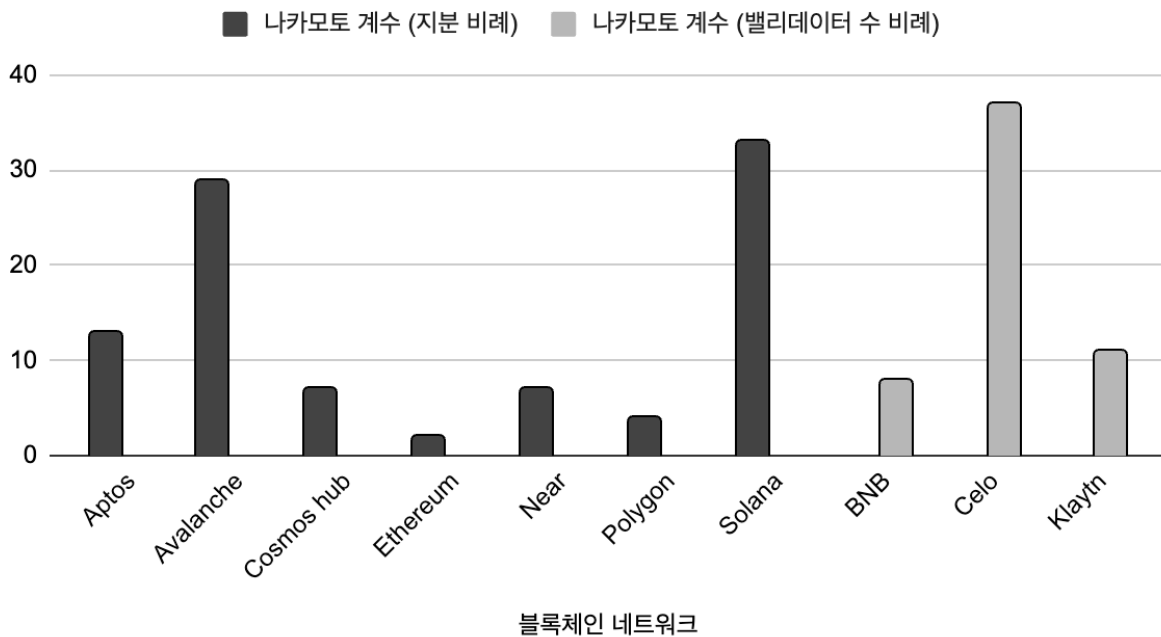
*[Nakamoto Coefficients](#) 를 인용하였으며, 일부 네트워크는 자체 분석

** 이더리움의 경우, 밸리데이터 수는 50만 이상이나, 하나의 클라이언트에서 여러 밸리데이터를 가동할 수 있으므로, 밸리데이터 수 대신 클라이언트 수를 표기함. 나카모토 계수 측정 시, 하나의 그룹이 여러 클라이언트를 운영할 경우 1개로 간주함

*** 두 그룹이 1/2 이상의 지분을 가지고 있으므로 전체 클라이언트 수의 1/2 미만으로 추정됨

**** 알고랜드는 밸리데이터의 전체 수를 공개하고 있지 않음

블록체인 별 나카모토 계수



[표 4]를 통해, 지분에 비례하는 합의 방식을 사용하는 블록체인 네트워크의 나카모토 계수가 밸리데이터 수에 비례하는 네트워크의 계수보다 상대적으로 낮다는 것을 확인할 수 있습니다. 지분에 비례하는 합의 방식에서 소수의 밸리데이터가 많은 지분을 가지고 있으면 이들이 네트워크에 큰 영향력을 행사하며, 이들의 동작에 문제가 발생하면 체인 정지를 유발할 수 있습니다. 예를 들어, 이더리움의 경우 지분의 상당수가 [리도](#)와 같은 스테이킹 풀 내에 있어, 소수의 그룹에 1/3 이상의 자본이 집중되어 있는 것으로 보입니다. 반면, 밸리데이터 수에 비례하는 합의 방식을 사용하는 블록체인은 모든 밸리데이터가 동등한 수준의 투표권을 행사하기 때문에, 적은 밸리데이터 수에서도 상대적으로 더 높은 수준의 분산성을 제공할 수 있습니다.

합의를 이루기 위한 밸리데이터 수를 살펴봐도 크게 다르지 않은 모습을 볼 수 있습니다. 솔라나의 밸리데이터 수는 2,000개에 달하지만, 합의를 위해 필요한 밸리데이터 수는 전체의 7% 정도인 130여 개로 이루어집니다. 지분에 비례하는 합의 방식을 사용하는 네트워크에 많은 수의 밸리데이터가 참여하는 것처럼 보이지만, 실제로는 적은 수의 밸리데이터의 합의만으로도 네트워크가 운영될 수 있음을 확인할 수 있습니다. 단, 이더리움의 경우에는 블록 합의를 위해 충분히 많은 수의 클라이언트가 필요할 것으로 예상합니다.

4) 운영 비용 측면

밸리데이터 운영 비용은 네트워크의 개방성에 많은 영향을 줄 수 있습니다. 운영 비용이 낮을수록 참여를 위한 장벽이 낮아져 개방성을 높일 수 있습니다. 운영 비용이 높을수록 밸리데이터 유지 비용이 높아지므로 참여가 어려워질 수 있습니다. 또한, 운영 비용을 상쇄하기 위해 밸리데이터들은 보상으로 주어지는 토큰을 현금화하려는 압력이 커질 수 있습니다. 이는 토큰 공급 증가로 이어지며, 토큰 가격에 영향을 줄 수 있습니다.

[표 5] 밸리데이터 최소 사양 및 월별 하드웨어 비용* (단위: US 달러)

블록체인 네트워크	컴퓨팅 성능	스토리지 크기	컴퓨팅 비용	스토리지 비용	총 비용
Algorand	8 vCPU (AWS c5.2xlarge)	100GB SSD	280	10	290
Aptos	AWS c6i.8xlarge	2TB SSD (io2)	1,110	260	1,370
Avalanche	8 vCPU (AWS c5.2xlarge)	1TB SSD	280	90	370
BNB	AWS M5zn.3xlarge	2TB SSD	880	180	1,060
Celo	8 vCPU (AWS c5.2xlarge)	256GB SSD	280	20	300
Cosmos hub	32GB RAM (m5.2xlarge)	2TB SSD	340	180	520
Ethereum	4 vCPU (AWS m6i.xlarge)	2TB SSD	170	180	350
Klaytn	AWS m6i.8xlarge	3TB SSD	1,360	280	1,640
Near	AWS m5.2xlarge	1TB SSD	340	90	430
Polygon	AWS c5.4xlarge	2.5TB SSD	550	230	780
Solana**	GCP n2-standard-32	2TB SSD (NVMe)	1,430	410	1,840

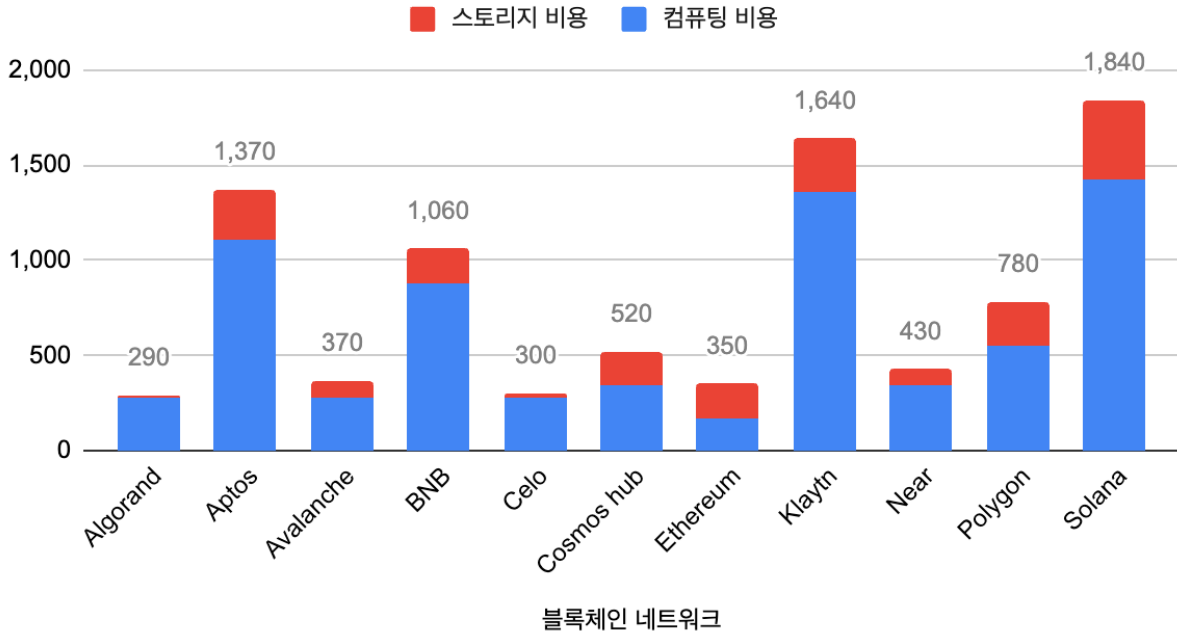
* 하드웨어 비용은 1개의 밸리데이터 노드 비용이 포함되어 있습니다. 네트워크 전송 비용은 포함되어 있지 않습니다.

** 솔라나의 경우, 운영을 위해 하드웨어 비용 이외에도 합의 과정에 필요한 비용이 추가적으로 필요합니다.

[표 5]는 여러 블록체인 네트워크의 밸리데이터 최소 사양에 따른 월간 하드웨어 비용을 AWS EC2 기준으로 나타낸 것입니다. 하드웨어 사양은 각 네트워크의 홈페이지에서 제공하는 요구 사양을 기재하였습니다. 이 표를 통해 블록체인 네트워크마다 밸리데이터 운영을 위해 필요한 하드웨어 사양이

다르고, 이에 따른 비용도 다르다는 것을 확인할 수 있습니다. 이를 통해 각 네트워크에서 밸리데이터로 참여하기 위한 운영 비용이 대략적으로 어느 정도인지 비교할 수 있습니다.

월별 하드웨어 비용 (US 달러)



고성능 블록체인 네트워크들은 높은 처리량 및 빠른 응답에 최적화되어 있기 때문에 운영 비용이 상대적으로 높게 나타나게 됩니다. 더 많은 CPU 코어 및 메모리가 필요하고, 블록 당 트랜잭션 수가 상대적으로 많기 때문에 블록의 크기가 커지므로 저장 공간도 더 많이 필요하게 됩니다. 따라서 전체적인 운영 비용이 증가하게 됩니다. 차트를 통해 고성능 블록체인으로 분류되는 애플토스, 클레이튼, 솔라나와 같은 네트워크들의 운영 비용이 상대적으로 높다는 것을 확인할 수 있습니다. 이는 고성능 블록체인이 개방성 측면에서 상대적인 약점을 가질 수 있음을 보여줍니다. 또한, 고성능 블록체인은 일반적으로 블록 타임이 짧고, 블록 당 많은 트랜잭션을 처리하므로, 밸리데이터 사이에서 빠른 시간 내에 많은 데이터를 전송하고 동기화해야 합니다. 이에 따라 네트워크 전송 비용도 상대적으로 더 높을 가능성이 높습니다.

그렇다면, 밸리데이터를 운영하면서 받는 보상을 통해 운영 비용을 충당하기 위해서는 어느 정도의 초기 자본이 필요한지도 예상해 볼 수 있을 것입니다. 만약 이 비용이 낮고 보상이 충분하다면 밸리데이터로 참여하기 위한 인센티브가 될 수 있습니다. 물론, 이 예상치는 현재 시점의 보상 수준 및 네이티브 토큰 가격을 기준으로 한 것으로, 언제든지 변경될 수 있습니다.

[표 6] 2023년 3월 기준 밸리데이터 운영 비용을 충당할 수 있는 초기 투자 비용* (단위: US 달러)

블록체인 네트워크	APR(예상치)	연간 운영 비용** (예상치)	BEP를 위한 초기 투자 비용*** (예상치)	100만 달러 투자 시 기대 이익 (예상치)
Algorand	5.6%	16,000	280,000	40,000

Aptos	7.0%	29,000	410,000	41,000
Avalanche	8.5%	17,000	200,000	68,000
BNB****	2.5%	25,000	990,000	300
Celo	4.2%	16,000	380,000	26,000
Cosmos Hub	21.4%	19,000	90,000	195,000
Ethereum	4.6%	17,000	360,000	29,000
Klaytn	13.5%	32,000	240,000	103,000
Near	9.5%	18,000	185,000	78,000
Polygon	4.8%	22,000	450,000	26,000
Solana	7.5%	49,000*****	655,000	26,000

* 예상치이며, 실제와 다를 수 있음

** 1 개의 노드 운영 비용과 월 1,000달러에 상당하는 운영비 포함. 프록시 노드 등의 비용은 포함하지 않음

*** 최소 스테이킹 수량 제한을 적용하지 않음

**** BNB 체인은 블록 생성 및 검증 보상을 제공하지 않고, 블록에 담긴 트랜잭션 가스비로 보상 제공. 밸리데이터에 따라 보상 수준이 다를 수 있음

***** 솔라나는 운영 비용에 네트워크 합의 과정에 필요한 비용 포함(약 400 SOL/년)

[표 6]은 각 네트워크 밸리데이터를 운영할 때 예상되는 초기 투자 비용 및 연간 보상 비율을 나타낸 것입니다. 이 표에서 단일 노드를 밸리데이터로 간주하고, 노드 운영에 필요한 프록시 노드 등의 비용은 제외하였습니다. 클레이튼과 같은 일부 네트워크는 밸리데이터 운영에 반드시 프록시 노드를 설치해야만 참여가 가능하게 구성되어 있지만, 이 표에서는 단일 노드로 운영할 때의 비용을 계산했기 때문에 실제 운영 비용과 차이가 발생할 수 있으며, 연간 보상 수준도 달라질 수 있습니다.

코스모스 허브와 클레이튼의 경우, 연 이율 10%가 넘는 보상을 제공하는 것으로 조사되었으며, 다른 체인들은 그보다 적은 수준의 보상을 제공하고 있습니다. 초기 투자 비용 면에서는, 대부분의 체인에서 수십만 달러 정도의 자본을 스테이킹해야 밸리데이터 운영 비용 대비 이익을 낼 것으로 예상됩니다.

이더리움의 경우, 밸리데이터 당 스테이킹할 수 있는 양이 정해져 있으므로(32 ETH), 단일 클라이언트에서 여러 대의 밸리데이터를 실행해야만 운영 비용을 넘어서는 이익을 낼 수 있을 것으로 예상됩니다.

5) 경제적인 관점에서의 네트워크 안정성 측면

일반적으로 지분증명방식의 블록체인은 스테이킹에 필요한 높은 비용 때문에 작업증명방식의 블록체인에 비해 이중 지불 공격을 위해 필요한 비용이 더 높다고 여겨집니다. 지분증명방식 블록체인에서 이중 지불 공격을 시도하려면, 공격자가 스테이킹 된 네이티브 토큰의 과반수 이상을 보유해야 하는데, 이 비용이 매우 높기 때문입니다. 또한, 스테이킹 비율이 높은 블록체인은 공격자가 공격에 필요한 네이티브 토큰을 얻기 어려워지므로, 상대적으로 높은 보안성을 갖춘 네트워크로 여길 수 있습니다.

네트워크의 가치는 네이티브 토큰 유통량에 비례한다고 생각할 수 있습니다. 유통량이 많을수록 네트워크가 활발하다고 여겨지기 때문입니다. 그런데, 어떤 무허가형 블록체인의 유통량 대비 스테이킹 비율이 낮다면, 공격자는 유통 중인 토큰을 대량으로 구입하여 네트워크를 공격할 수 있는 가능성이 있습니다. 예를 들어, 지분에 비례하여 합의를 이루는 지분증명방식 블록체인의 경우, 공격자가 합의를 위해 필요한 수량인 총 스테이킹 지분의 ⅓를 확보하면 이중 지불 공격이 가능합니다. 한편, 밸리데이터 수에 비례하는 합의 방식을 사용하는 블록체인 네트워크는 합의를 위해 필요한 스테이킹 지분이 ⅓ 보다 적을 수 있습니다. 스테이킹 량을 오름차순으로 정렬한 밸리데이터 수의 ⅓ 이 모이면 합의에 이를 수 있기 때문입니다. 따라서, 공격자는 상대적으로 적은 비용으로 공격을 시도할 수 있는 가능성이 존재합니다.

공격에 대비한 네트워크 저항성을 비교하기 위해, [표 7]에서 각 네트워크별 거래 가능 물량 대비 합의에 필요한 스테이킹 양을 계산해 보았습니다. 거래 가능 물량의 정의가 네트워크마다 조금씩 다르기 때문에, 정상적인 거래를 통해 확보 가능한 물량을 거래 가능 물량으로 정의합니다. 여기에서는 발행량(total supply) 또는 유통량(circulating supply)을 거래 가능 물량으로 정의하며, 이미 발행되었지만 리저브로 정의된 물량 또는 소각된 물량은 거래 가능 물량에서 제외됩니다.

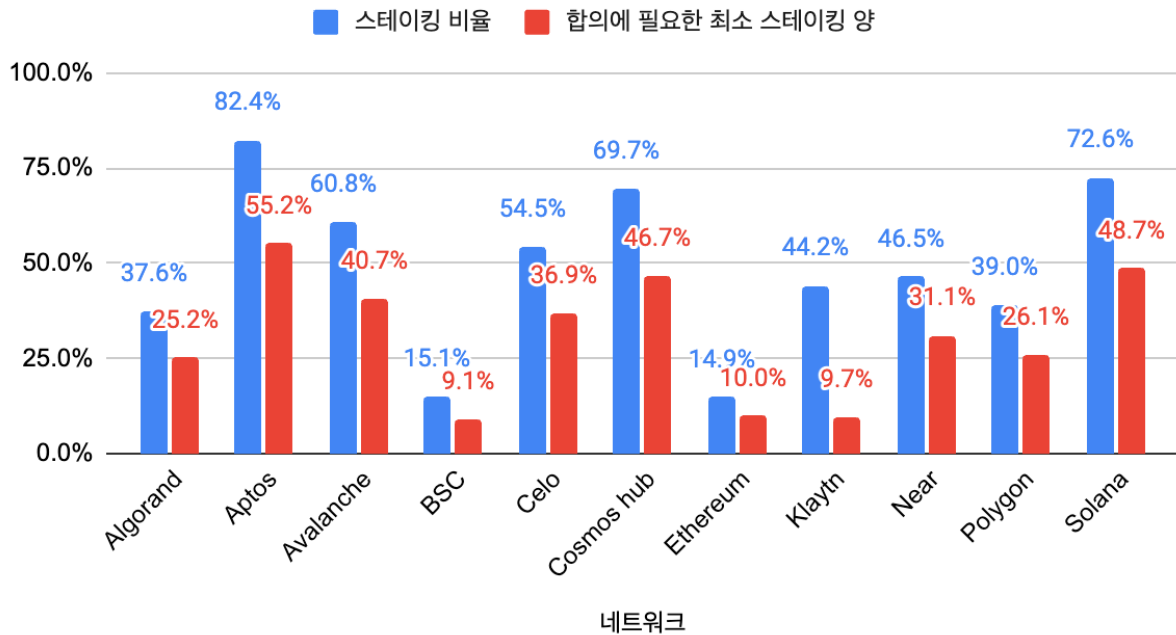
[표 7] 2023년 4월 21일 기준 전체 유통량 대비 합의에 필요한 스테이킹 수량

네트워크	전체 물량	전체 스테이킹 양	스테이킹 비율	합의에 필요한 최소 스테이킹 양 / 전체 유통량
Algorand*	7,230,202,491	2,719,284,958	37.6%	25.2%
Aptos**	1,030,430,527	848,799,394	82.4%	55.2%
Avalanche**	422,765,487	256,902,450	60.8%	40.7%
BSC	155,864,769	23,571,835	15.1%	9.1%
Celo	494,976,084	269,794,726	54.5%	36.9%
Cosmos hub**	339,703,187	236,814,410	69.7%	46.7%
Ethereum	120,428,889	17,915,419	14.9%	10.0%
Klaytn	3,087,221,664	1,364,046,125	44.2%	9.7%
Near	1,131,342,100	525,738,078	46.5%	31.1%
Polygon	9,219,469,069	3,591,201,401	39.0%	26.1%
Solana**	545,758,273	396,316,007	72.6%	48.7%

* Aptos는 circulating supply를 total supply에서 스테이킹 량을 제외한 값을 사용하고 있어, total supply를 전체 유통량으로 정의했습니다.

** Cosmos hub, Solana는 미유통 물량의 일부가 스테이킹에 포함되어 있어 total supply를 전체 유통량으로 정의했습니다.

스테이킹 비율과 합의에 필요한 스테이킹 양



[표 7]은 각 네트워크별 전체 유통량과 합의에 필요한 최소 스테이킹량을 전체 유통량으로 나눈 수량을 보여줍니다. 만약 네트워크 내에 네이티브 토큰 유통량이 많고 스테이킹량이 적으면, 공격자가 공격 성공 시 많은 수익을 얻을 수 있습니다. 이런 경우, 많은 공격 비용을 감수하고서라도 이중 지불 공격을 시도할 수 있습니다. 이러한 관점에서, 스테이킹 비율이 높은 애플토스, 코스모스 허브, 솔라나와 같은 블록체인들은 이중 지불 공격에 상대적으로 안전하다고 생각할 수 있습니다.

앞서 설명한 바와 같이, 밸리데이터 수에 비례하는 합의 방식을 채택한 네트워크는 합의에 필요한 네이티브 토큰의 양이 스테이킹 양의 ⅓ 보다 적을 수 있습니다. 알고랜드, BNB 체인, 클레이튼은 합의에 필요한 네이티브 토큰의 양이 상대적으로 적어서, 공격자가 유통 물량 중 10% 정도를 확보하게 되면 이중 지불 공격 등의 네트워크를 장악할 수 있는 공격을 시도할 수 있습니다. 그러나, 이러한 공격을 시도하기 위해서는 공격자가 충분한 수의 밸리데이터를 확보할 수 있다는 가정이 필요하며, 그렇지 않으면 공격이 불가능합니다.

셀로 블록체인은 밸리데이터 수에 비례하는 합의 방식을 사용하지만, 합의에 필요한 네이티브 토큰 수량이 상대적으로 많습니다. 이는 밸리데이터들의 스테이킹 양이 상대적으로 고르게 분포되어 있음을 의미합니다. 셀로 네트워크는 경제적인 관점에서의 공격에 대한 저항성이 상대적으로 높다고 할 수 있습니다.

이번에는, 실제로 공격자가 네트워크에 문제를 일으키기 위해 필요한 자본의 양이 어느 정도인지를 분석해 보겠습니다. 이를 통해 공격을 위해 얼마나 많은 자본을 필요로 하는지 예상해 볼 수 있으며, 블록체인 네트워크의 공격 저항력을 평가하는 데 도움이 될 수 있습니다.

공격자가 스테이킹 된 물량을 건드리지 못한다고 가정하면, 공격자는 공격에 필요한 양의 네이티브 토큰을 시장에서 구매하고 스테이킹해야 합니다. 이 때 필요한 네이티브 토큰의 양은, 지분 비례 합의 방식 기준으로 현재 스테이킹 양의 50% 이상이 됩니다. 현재 스테이킹 양의 절반을 공격자가 스테이크 하는 순간, 공격자의 지분이 총 스테이킹 양의 1/3 이 되기 때문입니다. 네이티브 토큰의 가격과 스테이킹 양을 알고 있다면, 공격자가 체인을 공격하기 위해 필요한 자본을 대략적으로 추정할 수 있습니다.

[표 8] 2023년 4월 21일 기준 체인을 공격하는 데 필요한 네이티브 토큰의 수량 및 자본

	네트워크	현재 유통량	현재 스테이킹 양	유통량 대비 공격에 필요한 코인 비율*	USD 환산**
지분에 비례	Algorand	7,230,202,491	2,719,284,958	?***	?***
	Aptos	1,030,430,527	848,799,394	40.8%	4,200,000,000
	Avalanche	422,765,487	256,902,450	30.7%	2,210,000,000
	Cosmos hub	155,864,769	236,814,410	77.0%	1,320,000,000
	Ethereum	120,428,889	17,915,419	8.3%	18,600,000,000
	Near	1,131,342,100	525,738,078	23.0%	520,000,000
	Polygon	9,219,469,069	3,591,201,401	19.5%	1,800,000,000
	Solana	545,758,273	396,316,007	36.6%	4,400,000,000
밸리데이터 수에 비례	BNB	155,864,769	23,571,835	2.5%	1,320,000,000
	Celo	494,976,084	269,794,726	18.4%	54,600,000
	Klaytn	3,087,221,664	1,364,046,125	2.6%	20,000,000

* 지분 비례 합의 방식의 체인을 멈추기 위해서는, 공격자가 추가로 확보한 스테이킹 양이 총 스테이킹 양의 1/3 이상이 되어야 합니다. 이는 현재 스테이킹 양의 50% 이상으로 표현할 수 있습니다. 밸리데이터 수에 비례하는 합의 방식의 체인을 멈추기 위해서는, 공격자가 추가로 확보한 밸리데이터 수가 총 밸리데이터 수의 1/3 이상이 되어야 합니다. 이는 현재 밸리데이터 수의 50% 이상으로 표현할 수 있습니다. 밸리데이터 수에 비례하는 합의 방식을 공격하는 데 필요한 네이티브 토큰 수량은 해당 네트워크에서 가장 적게 스테이크 한 밸리데이터의 스테이킹 수량에 공격에 필요한 밸리데이터 수를 곱하여 계산하였습니다.

** 네이티브 토큰 1개 가격에 공격에 필요한 양을 곱한 액수입니다. 공격자는 이보다 높은 가격을 지불해야 필요한 지분을 확보할 수 있습니다.

*** 알고랜드는 실제 밸리데이터 수를 공개하지 않고 있습니다.

[표 8]을 통해, 각 블록체인 네트워크의 경제적인 공격 저항성이 어느 정도인지를 대략적으로 알 수 있습니다. 지분에 비례하는 블록체인 네트워크의 경우, 공격자가 체인에 문제를 일으키기 위해서는 매우 큰 자본이 필요하다는 것을 알 수 있습니다. 이는 지분 증명 기반의 블록체인 네트워크가 높은 수준의 공격 저항성을 가지고 있다는 것을 확인해 줍니다. 이더리움의 경우, 공격에 드는 비용이 최소 180억 달러 이상으로 평가 되었으며, 분석 대상 중 가장 높은 저항성을 가지고 있음을 확인하였습니다.

한편, 밸리데이터 수에 비례하여 합의를 이루는 네트워크는 상대적으로 공격 저항성이 낮은 수준을 보이고 있습니다. 이는, 공격에 필요한 수량이 가장 적은 수량을 스테이킹하고 있는 밸리데이터에 비례하고 있기 때문입니다. 따라서, 이 네트워크들은 공격 저항성을 높이기 위해 최대 밸리데이터 수의 제한을 두거나,

최소 스테이킹 수량 조건을 높일 필요가 있습니다. 이렇게 하여 네트워크의 참여 접근성과 네트워크 안정성 및 신뢰성을 적절히 유지할 수 있습니다.

실제 공격 비용은 시장 상황 및 가격 변동 등 다양한 요인에 따라 달라질 수 있으므로, 이 분석 결과는 대략적인 지표로 생각하는 것이 좋습니다.

3. 정리: 개방성 수준 비교

[표 9] 블록체인 네트워크 별 상대적 개방성 수준 비교 (최저 1점, 최대 5점)

블록체인 네트워크	밸리데이터 수(5)	초기 자본 비용(5)	나카모토 계수(5)	스테이킹 비율(5)	운영 비용(5)	총점(25)
Algorand	3(추정)*	5	3(추정)*	3	5	19(추정)*
Aptos	3	1	2	5	2	13
Avalanche	4	5	3	4	5	21
BNB	1	1	1	1	3	7
Celo	3	3	3	3	5	17
Cosmos Hub	3	3	1	4	4	15
Ethereum	5	4	1	2	5	17
Klaytn	1	3	2	1	2	9
Near	3	4	1	3	5	16
Polygon	2	4	1	3	3	13
Solana	5	4	3	4	1	17

* 알고랜드는 밸리데이터 수를 공개하고 있지 않음

[표 9]는 이번에 조사한 열한 가지 블록체인 네트워크의 상대적인 개방성 수준을 점수화한 것입니다. 지표마다 5점에 가까울수록 상대적으로 개방성 수준이 높고, 1점에 가까울수록 개방성 수준이 낮습니다.

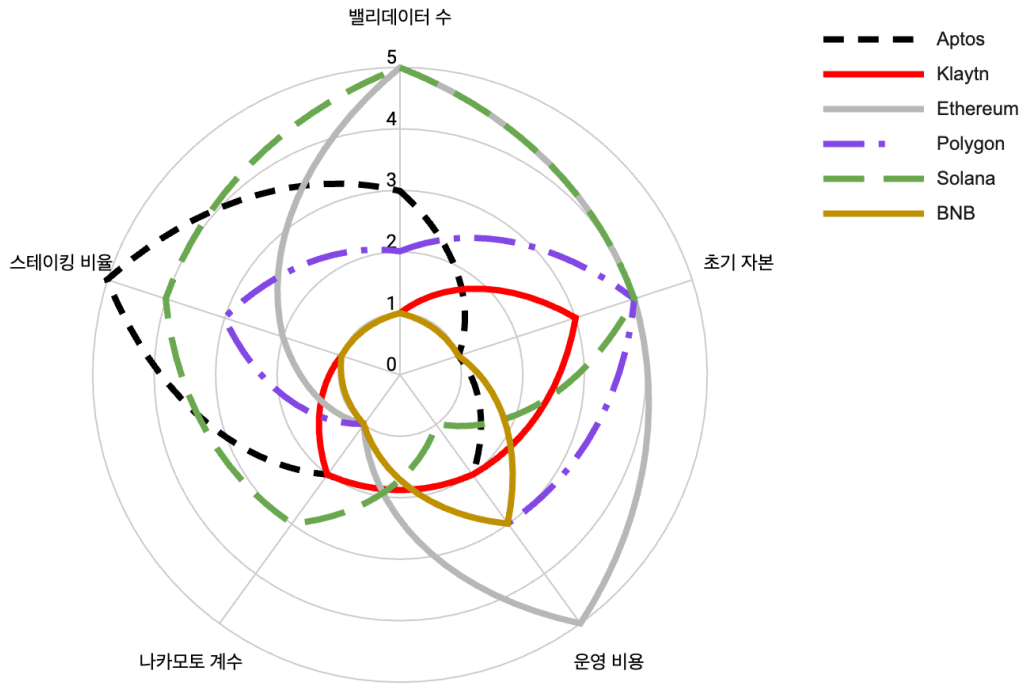
솔라나와 아발란체 네트워크가 높은 개방성을 보이고 있음을 확인할 수 있었습니다. 이들은 밸리데이터 수 및 초기 자본 비용, 자본 집중도 등에서 상대적으로 높은 점수를 보였습니다. 이러한 요소들이 결합되어 해당 블록체인 네트워크의 개방성을 높이는 데 기여하였습니다.

알고랜드는 정확한 밸리데이터 수를 공개하고 있지 않아 정확한 결과를 알기는 어렵지만, 여러 자료를 종합하여 추정해 보면 높은 수준의 개방성을 보일 것으로 추정됩니다.

이더리움은 여러 지표에서 높은 점수를 얻었지만, 자본의 집중도 및 네트워크 안정성 부분에서 낮은 점수를 받았으며, 이는 이더리움 네트워크의 개방성에 일부 제한이 있음을 나타냅니다.

애포스 및 BNB 체인은 초기 자본 비용 및 권력 분산도 등에서 낮은 점수를 받았으며, 총점 역시 상대적으로 낮은 수준을 기록했습니다. 클레이튼과 폴리곤은 허가형 블록체인이기에 개방성 점수의 의미가 크지 않지만, 현 상태에서 개방된 블록체인으로 전환된다면 낮은 개방성을 나타낼 것으로 예상됩니다.

개방성 수준 차트



위 레이더 차트는 비교 대상 11종 블록체인 네트워크 중 6종을 선택하여 개방성 수준을 시각화한 것입니다. 개방성이 상대적으로 높은 이더리움과 솔라나는 상대적으로 큰 영역을 차지하고 있는 반면, BNB 체인과 클레이튼은 상대적으로 좁은 영역을 차지하고 있다는 것을 알 수 있습니다. 이 차트를 통해 비교 대상 네트워크들의 개방성 수준을 한눈에 비교하고 평가할 수 있습니다.

4. 결론

이 글에서는 다양한 지분증명방식 블록체인 네트워크의 개방성 수준을 비교하며 아래와 같은 흥미로운 결과를 도출했습니다.

- 지분증명방식 네트워크는 지분 비례 합의 방식과 밸리데이터터 수 비례 합의 방식으로 나눌 수 있습니다.

- 지분 비례 방식을 사용하는 네트워크는 많은 밸리데이터 수를 가지고, 자본이 집중될 가능성이 높지만 상대적으로 높은 네트워크 안정성을 지닙니다.
- 밸리데이터 수 비례 방식을 사용하는 네트워크는 자본 집중도 측면에서 상대적으로 높은 개방성을 제공하지만, 스테이킹 양의 편차가 클 경우 네트워크 공격에 취약할 수 있습니다.
- 일부 블록체인 네트워크는 초기 자본 요구량이 매우 높아, 재단의 지원 없이는 밸리데이터로 참여하기 어려운 구조를 가지고 있습니다.
- 고성능 블록체인은 높은 수준의 하드웨어 사양을 요구하여 상대적으로 많은 운영 비용이 필요합니다.
- 알고랜드, 아발란체, 셀로, 솔라나의 개방성은 높은 수준을 보여줍니다.
- 코스모스 허브, 이더리움, 니어 프로토콜은 중간 정도의 개방성을 가지고 있습니다.
- 이더리움은 밸리데이터 수, 초기 자본, 운영 비용 등 많은 지표에서 높은 점수를 기록했지만, 자본 집중도 및 스테이킹 비율에서 낮은 점수를 기록했습니다.
- 개방형 네트워크 중 매우 높은 초기 자본을 요구하는 네트워크의 개방성은 허가형 네트워크와 큰 차이가 없음을 확인할 수 있었습니다.

이 분석 결과를 통해 블록체인 네트워크의 개방성과 안정성이 어떻게 상호 작용하는지 이해를 도울 수 있고, 무허가형 네트워크들이 개방성을 높이기 위해 어떤 전략을 사용해야 하는지를 확인할 수 있습니다.

한편, 허가형 블록체인 네트워크를 효과적인 무허가형 블록체인으로 전환하려면, 아래와 같은 점들을 고려해 볼 수 있습니다.

- 지분 비례 합의 방식과 밸리데이터 수 비례 합의 방식 중에서 네트워크에 적합한 방식 선택하기
- 알맞은 수의 밸리데이터 수, 초기 자본 비용, 운영 비용 정하기
- 네트워크의 신뢰성을 유지하기 위한 자본 집중도, 유통량 대비 스테이킹 비율 수준 정하기

이러한 사항을 바탕으로, 개방성 수준을 만족시키면서 동시에 신뢰성을 유지할 수 있는 방법을 설계하면, 허가형 블록체인이 무허가형 블록체인으로 전환되는 과정에 도움이 될 수 있을 것이라 생각합니다. 이 글이 무허가형 블록체인을 설계할 때 도움이 되길 바랍니다.