

코스모스(COSMOS)

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

코스모스 백서 (Cosmos Whitepaper)

초기의 비전인 “인터체인(The Interchain)” — 주권 블록체인들의 상호 연결된 네트워크는 2016년, 코스모스 프로젝트의 창립자인 **Ethan Buchman**과 **Jae Kwon**이 발표한 백서에서 처음 소개되었습니다.

이 문서는 인터체인의 원래 비전과 Cosmos SDK, IBC, CometBFT와 같은 인터체인 스택 구성 요소의 근본적인 역할을 이해하는 데 유용한 가이드로 남아 있습니다.

현재 인터체인 스택 제품의 현황에 대해 더 알아보려면 아래를 참고하세요:

- IBC
- Cosmos SDK
- CometBFT
- Interchain Security

Introduction (소개)

오픈소스 생태계, 탈중앙화 파일 공유, 그리고 공개 암호화폐의 결합된 성공은 **탈중앙화 인터넷 프로토콜이 사회경제적 인프라를 근본적으로 개선할 수 있다**는 인식을 불러일으켰습니다.

우리는 Bitcoin (암호화폐), Zerocash (프라이버시 중심 암호화폐), Ethereum (범용 스마트 계약 플랫폼)과 같은

특화된 블록체인 응용 프로그램을 보아왔습니다. 또한 Augur (예측 시장), TheDAO (투자 클럽) 등 Ethereum Virtual Machine (EVM)을 기반으로 한 수많은 분산 애플리케이션(dApp)들이 등장했습니다.

니다.

그러나 지금까지 이러한 블록체인들은 다음과 같은 여러 가지 문제를 겪어왔습니다.

- 심각한 에너지 비효율성 (Gross Energy Inefficiency)
- 낮은 성능 또는 제한된 처리량 (Poor or Limited Performance)
- 미숙한 거버넌스 메커니즘 (Immature Governance Mechanisms)

Bitcoin의 거래 처리량을 확장하기 위한 제안들 — 예: Segregated Witness 및 BitcoinNG — 은 여전히 단일 물리적 기계의 처리 한계에 의해 제한되어 있습니다. Lightning Network는 일부 거래를 원장 (ledger) 밖에서 처리하여

마이크로 결제 및 프라이버시 중심 결제에는 적합하지만, 보다 일반적인 확장성 요구를 충족시키기에는 적합하지 않을 수 있습니다.

이상적인 솔루션은 여러 병렬 블록체인이 **보안 속성을 유지하면서 상호 작용(interoperate)** 할 수 있게 하는 것입니다.

그러나 작업 증명(Proof-of-Work) 시스템에서는 이것을 구현하기 어렵거나 거의 불가능합니다.

예를 들어, 병합 채굴(Merged Mining)은 부모 체인의 작업을 자식 체인에서 재사용할 수 있도록 허용하지만, 여전히 각 노드가 거래를 순서대로 검증해야 하며, 부모 체인에서 충분한 해시 파워가 유지되지 않으면 공격에 취약할 수 있습니다.

여기에서 우리는 Cosmos를 소개합니다. Cosmos는 위의 모든 문제를 해결하는 새로운 블록체인 네트워크 아키텍처입니다.

Cosmos는 **여러 개의 독립적인 블록체인(Zone)**으로 구성된 네트워크입니다. 이 Zone들은 **Tendermint Core**에 의해 구동되며, 고성능 (High Performance), 일관성 (Consistency), 보안성 (Security)을 제공합니다.

Tendermint Core는 **PBFT 유사 합의 엔진(PBFT-like Consensus Engine)**을 기반으로 하며, 엄격한 포크 책임성(Fork Accountability) 보장을 통해 악의적인 행위자의 행동을 제어할 수 있습니다.

이 Tendermint Core의 BFT 합의 알고리즘은 공개형 지분증명(Proof-of-Stake) 블록체인을 확장하는 데 적합하며, 작업 증명(Proof-of-Work)을 사용하는 블록체인인 Ethereum과 Bitcoin도 어댑터 존(Adapter Zone)을 통해 Cosmos 네트워크에 연결할 수 있습니다.

Cosmos의 첫 번째 Zone은 **Cosmos Hub**라고 불립니다. Cosmos Hub는 다중 자산 지분증명 (Multi-Asset Proof-of-Stake) 암호화폐로, 간단한 거버넌스 메커니즘을 통해 네트워크가 적응하고 업그레이드할 수 있도록 합니다.

또한 Cosmos Hub는 다른 Zone을 연결함으로써 확장될 수 있습니다.

Cosmos 네트워크의 허브와 존들은 **IBC (Inter-Blockchain Communication) 프로토콜**을 통해 상호 통신합니다. 이는 블록체인을 위한 가상의 UDP 또는 TCP 프로토콜과 유사합니다.

토큰은 한 존에서 다른 존으로 교환 유동성(Exchange Liquidity) 없이 안전하고 빠르게 전송될 수 있습니다.

모든 존 간 토큰 전송은 Cosmos Hub를 통해 이루어지며, 허브는 각 존이 보유한 전체 토큰 수량을 추적합니다.

또한 허브는 한 존의 실패가 다른 존에 영향을 주지 않도록 격리합니다. 누구나 새로운 존을 Cosmos Hub에 연결할 수 있으며, 이 구조는 새로운 블록체인 혁신과의 미래 호환성(Future Compatibility)을 제공합니다.

Cosmos를 통해 블록체인 간 상호운용성(Interoperability)이 실현될 수 있습니다. 이로써 “가치의 인터넷(Internet of Value)”이 가능해지며, 다른 검증자 세트에 의해 관리되는 자산들이 신뢰할 수 있는 제3자 없이도 자유롭게 이동하고 교환될 수 있습니다.

텐더민트 (Tendermint)

이 섹션에서는 **Tendermint 합의 프로토콜(Tendermint Consensus Protocol)**과 이를 기반으로 애플리케이션을 구축하기 위한 인터페이스를 설명합니다. 자세한 내용은 부록(Appendix)을 참고하십시오.

검증자 (Validators)

고전적인 **비잔틴 장애 허용(Byzantine Fault-Tolerant, BFT)** 알고리즘에서는 모든 노드가 동일한 가중치(Weight)를 갖습니다. 그러나 Tendermint에서는 노드마다 **투표 권한(Voting Power)**의 양이 다를 수 있습니다. 양의 투표 권한을 가진 노드는 **검증자(Validator)**라고 불립니다. 검증자들은 **암호 서명(Cryptographic Signatures)** 또는 **투표(Votes)**를 브로드캐스트하여 다음 블록을 합의(Consensus)로 결정하는 과정에 참여합니다.

검증자의 투표 권한은

- 제네시스 블록(Genesis)에서 결정되거나,
- 애플리케이션에 따라 블록체인 상에서 **결정론적으로 변경(deterministically changed)**됩니다.

예를 들어, **Cosmos Hub**와 같은 지분증명(Proof-of-Stake, PoS) 시스템에서는 검증자의 투표 권한이 **스테이킹(Staking)된 토큰의 양**에 따라 결정됩니다.

참고: $\frac{2}{3}$, $\frac{1}{3}$ 등의 분수는 전체 검증자 수가 아닌
총 투표 권한의 비율을 의미합니다.

- “ $>2/3$ ”는 “ $2/3$ 초과”
 - “ $\geq 1/3$ ”은 “ $1/3$ 이상”을 뜻합니다.
-

합의 (Consensus)

Tendermint는 부분 동기식(**partially synchronous**) BFT 합의 프로토콜로, **DLS 합의 알고리즘**에서 파생되었습니다.

Tendermint는 **단순성(Simple Design)**, **성능(Performance)**, 그리고 **포크 책임성(Fork-Accountability)**으로 주목받습니다.

이 프로토콜은 **고정된 검증자 집합(Fixed Set of Validators)**을 필요로 하며, 각 검증자는 **공개 키(Public Key)**로 식별됩니다.

검증자들은 **한 번에 하나의 블록**에 대해 합의에 도달하려고 시도하며, 각 블록은 **트랜잭션의 리스트(List of Transactions)**로 구성됩니다.

블록에 대한 합의 투표(Voting for Consensus)는 여러 **라운드(Rounds)**에 걸쳐 진행됩니다. 각 라운드에는 **라운드 리더(Round Leader)** 또는 **제안자(Proposer)**가 있으며, 그가 새로운 블록을 제안합니다.

그 후 검증자들은 여러 단계(Stage)에 걸쳐 해당 블록을 **수용(Accept)** 할지, 아니면 **다음 라운드로 넘어갈지** 투표합니다.

각 라운드의 제안자는 검증자들의 정렬된 목록에서 **투표 권한(Voting Power)** 비율에 따라 **결정론적(Deterministic)**으로 선택됩니다.

프로토콜의 전체 세부사항은 [여기\(here\)](#)에 설명되어 있습니다.

Tendermint의 보안성 (Security)

Tendermint의 보안성은 **슈퍼다수(super-majority, $>2/3$)** 투표 및 **락킹 메커니즘(Locking Mechanism)**을 사용하는 최적의 **비잔틴 장애 허용(Byzantine Fault Tolerance)** 설계에서 비롯됩니다.

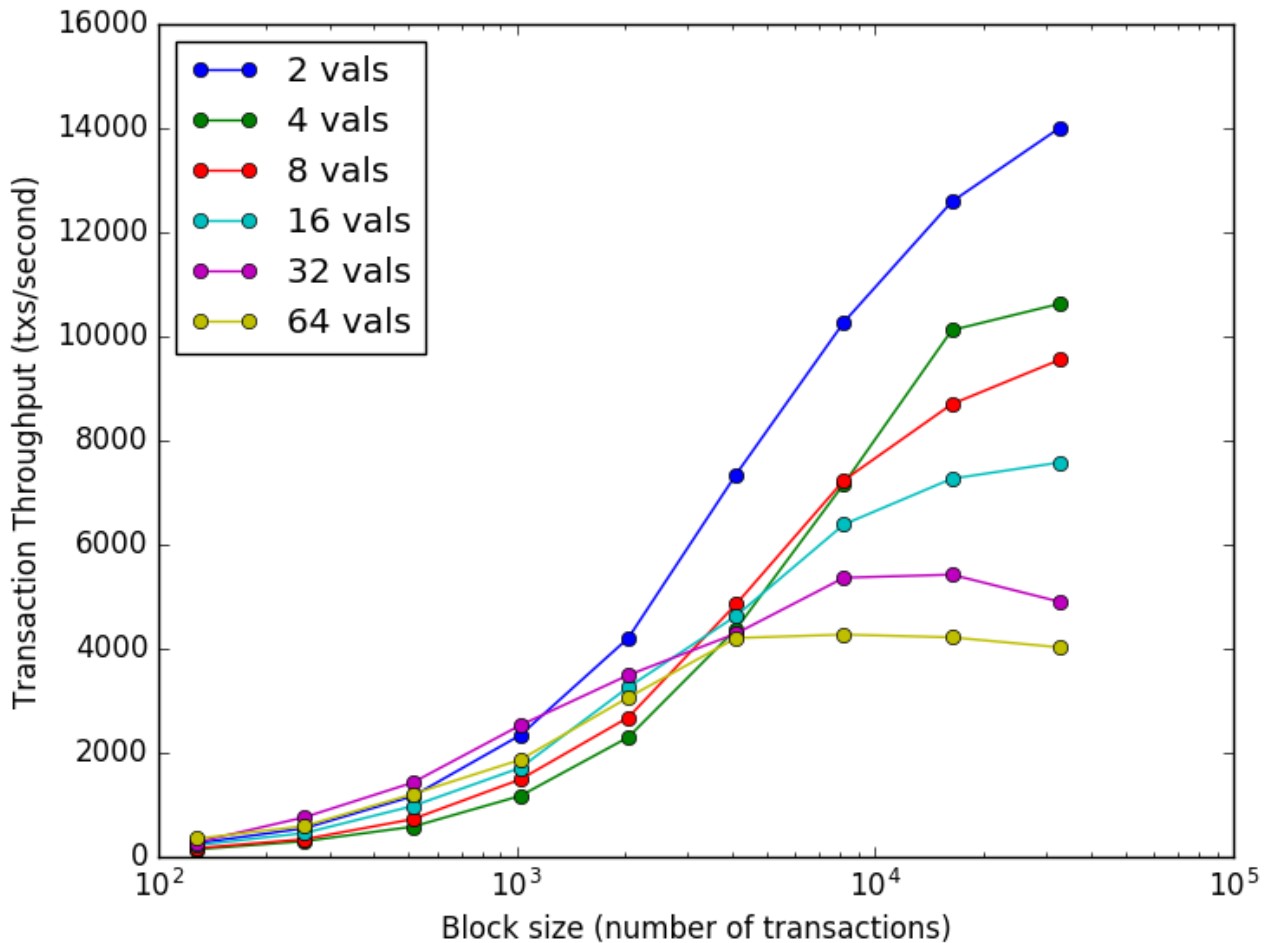
이 시스템은 다음을 보장합니다:

- 안전성이 위반되기 위해서는 최소 **$1/3$ 이상의 투표 권한($\geq 1/3$ voting power)**이 비잔틴(Byzantine) 상태여야 하며, 두 개 이상의 값이 동시에 커밋되는 상황이 발생해야 합니다.
- 만약 어떤 검증자 집단이 안전성을 위반하거나 시도한다면, **프로토콜이 이를 식별할 수 있습니다.** (이는 상충되는 블록에 투표하거나, 부당한 투표를 전송하는 행위 모두 포함)

강력한 보안 보장을 유지하면서도, Tendermint는 탁월한 **성능(Performance)**을 제공합니다.

64개의 노드가 5대륙에 분산된 7개 데이터센터에 배포된 벤치마크 결과에 따르면, Tendermint 합의는 **일반적인 클라우드 인스턴스(Commodity Cloud Instance)**에서도 초당 수천 건의 거래 (Transactions per Second, TPS)를 처리할 수 있습니다.

커밋 지연 시간(Commit Latency)은 약 **1~2초 수준**이며, 노드가 장애를 일으키거나 악의적인 투표를 브로드캐스트하는 등의 **가혹한 조건(Adversarial Conditions)**에서도 **초당 1,000건 이상의 거래 처리 속도**를 안정적으로 유지합니다. 자세한 내용은 아래 그래프(Figure)에서 확인할 수 있습니다.



라이트 클라이언트 (Light Clients)

Tendermint 합의 알고리즘의 주요 이점 중 하나는 **간소화된 라이트 클라이언트 보안 모델(Simplified Light Client Security)**입니다.

이 특성 덕분에 Tendermint는 **모바일(Mobile)** 및 **사물인터넷(IoT)** 환경에 이상적인 솔루션으로 평가됩니다.

비트코인 라이트 클라이언트의 경우, 체인의 블록 헤더를 동기화하고 가장 많은 작업 증명(Proof of Work)을 가진 체인을 찾아야 합니다.

그러나 Tendermint 라이트 클라이언트는 단지 **검증자 집합(Validator Set)**의 변경 사항을 추적하고, 최신 블록의 **2/3 이상(>2/3) 사전 커밋(PreCommit)** 을 검증함으로써 현재 상태를 결정할 수 있습니다.

또한, **간결한 라이트 클라이언트 증명(Succinct Proofs)** 은 **인터블록체인 통신(Inter-Blockchain Communication, IBC)** 을 가능하게 합니다.

공격 방지 (Preventing Attacks)

Tendermint는 특정한 악의적 공격을 방지하기 위한 보호 메커니즘을 갖추고 있습니다. 이러한 공격 방지 기법들은 부록(Appendix)에서 더 자세히 설명됩니다.

ABCI (Application Blockchain Interface)

Tendermint의 합의 알고리즘은 **Tendermint Core**라는 프로그램으로 구현됩니다.

Tendermint Core는 **애플리케이션 독립형 합의 엔진(Application-Agnostic Consensus Engine)** 으로,

어떠한 결정론적 애플리케이션(Deterministic Application)이라도 분산 복제 블록체인(Distributedly Replicated Blockchain)으로 전환할 수 있습니다.

Tendermint Core는 **ABCI(Application Blockchain Interface)** 를 통해 블록체인 애플리케이션과 연결됩니다.

따라서 ABCI를 사용하면, **합의 엔진이 작성된 프로그래밍 언어와 관계없이** 어떠한 언어로도 블록체인 애플리케이션을 개발할 수 있습니다.

또한 ABCI는 **기존 블록체인 스택의 합의 레이어를 손쉽게 교체(Swap Out)** 할 수 있도록 합니다.

비유하자면, **비트코인(Bitcoin)** 을 예로 들 수 있습니다.

비트코인은 모든 노드가 **UTXO(Unspent Transaction Output)** 데이터베이스를 완전히 감사(Audited) 가능한 형태로 유지하는 암호화폐 블록체인입니다.

만약 ABCI 위에 비트코인 유사 시스템을 구축한다면, **Tendermint Core**는 다음 역할을 담당합니다.

- 노드 간 블록 및 트랜잭션 공유 (Sharing Blocks and Transactions)
- 트랜잭션의 불변/표준 순서 확립 (Immutable Order of Transactions)

한편, **ABCI 애플리케이션**은 다음을 담당합니다:

- UTXO 데이터베이스 유지 (Maintaining the UTXO Database)
- 트랜잭션 암호 서명 검증 (Validating Cryptographic Signatures)

- 존재하지 않는 자금 사용 방지 (Preventing Spending of Non-Existent Funds)
- 클라이언트의 UTXO 데이터베이스 조회 허용 (Allowing Clients to Query)

결국 Tendermint는

애플리케이션 프로세스와 합의 프로세스 간에 단순하고 강력한 API를 제공함으로써, 블록체인 설계를 모듈화(Modularize) 하는 것을 가능하게 합니다.

코스모스 개요 (Cosmos Overview)

Cosmos는 Tendermint와 같은 고전적인 BFT(비잔틴 장애 허용) 합의 알고리즘으로 구동되는 독립적이고 병렬적인 블록체인 네트워크(Network of Independent Parallel Blockchains)입니다.

이 네트워크의 첫 번째 블록체인은 **Cosmos Hub**가 될 것입니다. Cosmos Hub는 새로운 **인터블록체인 통신 프로토콜(Inter-Blockchain Communication Protocol, IBC)** 을 통해 다른 여러 블록체인(또는 “Zones”)과 연결됩니다.

Cosmos Hub는 다양한 **토큰 유형(Token Types)** 을 추적하며, 각 연결된 Zone 내의 **총 토큰 수(Total Number of Tokens)** 를 기록합니다.

토큰은 **Zone 간 교환소(Liquid Exchange)** 없이도 Cosmos Hub를 통해 빠르고 안전하게 전송될 수 있습니다.

즉, 모든 Zone 간 전송은 Cosmos Hub를 경유하게 됩니다.

이 아키텍처는 오늘날 블록체인 산업이 직면한 여러 문제 — 예를 들어 **응용 프로그램 간 상호운용성(Application Interoperability)**, **확장성(Scalability)**, **무중단 업그레이드(Seamless Upgradability)** — 를 해결합니다.

예를 들어, Bitcoin, Go-Ethereum, CryptoNote, ZCash 등 기존 블록체인 시스템에서 파생된 Zone들도 Cosmos Hub에 연결될 수 있습니다.

이러한 Zone 구조는 Cosmos가 **글로벌 거래 수요(Global Transaction Demand)** 를 충족하기 위해 무한히 확장(Scale Infinitely)할 수 있도록 하며, **분산형 거래소(Distributed Exchange)** 에도 적합합니다.

Cosmos는 단일한 분산 원장(Distributed Ledger)이 아닙니다. 그리고 Cosmos Hub는 “폐쇄된 생태계(Walled Garden)”나 “Cosmos의 중심(Center of its Universe)”이 아닙니다.

우리는 **암호학(Cryptography)**, **건전한 경제학(Sound Economics)**, **합의 이론(Consensus Theory)**, **투명성(Transparency)**, **책임성(Accountability)** 에 기반한 **개방형 분산 원장 네트워크(Open Network of Distributed Ledgers)** 를 설계하고 있습니다.

이 네트워크는 **미래 금융 시스템(Future Financial Systems)**의 새로운 기반이 될 수 있는 프로토콜로 기능하도록 설계되었습니다.

텐더민트-BFT (Tendermint-BFT)

Cosmos Hub는 Cosmos 네트워크의 첫 번째 퍼블릭 블록체인으로, Tendermint의 BFT(비잔틴 장애 허용) 합의 알고리즘에 의해 구동됩니다.

Tendermint 오픈소스 프로젝트는 **2014년에 시작되었으며**, 비트코인의 작업 증명(Proof-of-Work, PoW) 합의 알고리즘이 가진 **속도, 확장성, 환경적 문제(Speed, Scalability, Environmental Issues)**를 해결하기 위해 만들어졌습니다.

Tendermint 팀은 **1988년 MIT에서 개발된 검증된 BFT 알고리즘**을 기반으로 발전시켰으며, **1세대 지분증명(Proof-of-Stake)** 암호화폐들이 겪었던 **Nothing-at-Stake** 문제를 해결한 **새로운 형태의 PoS 암호화폐 구조**를 처음으로 제시한 팀입니다. 대표적인 예로는 **NXT** 및 **BitShares 1.0**이 있습니다.

오늘날 대부분의 **비트코인 모바일 지갑(Bitcoin Mobile Wallet)**은 **신뢰된 서버(Trusted Server)**를 통해 거래 검증(Transaction Verification)을 수행합니다. 그 이유는 **PoW 시스템에서는 많은 수의 블록 확인(Confirmations)**이 완료되어야만 거래가 되돌릴 수 없게 확정(Irreversibly Committed)되기 때문입니다.

이미 **이중 지불(Double-Spend)** 공격은 **Coinbase**와 같은 서비스에서도 실증되었습니다.

다른 블록체인 합의 시스템과 달리, **Tendermint는 즉각적이고 검증 가능한 보안성을 가진 모바일 결제 검증(Provably Secure Mobile-Client Payment Verification)**을 제공합니다. Tendermint는 **포크(Fork)**가 발생하지 않도록 설계되어 있기 때문에, 모바일 지갑은 즉시 **거래 확정(Instant Transaction Confirmation)**을 받을 수 있습니다.

이는 신뢰할 수 없는(Trustless) 환경에서도 **스마트폰 기반 실시간 결제(Practical Payments)**가 가능하게 하며, **사물인터넷(Internet of Things, IoT)** 응용 프로그램에도 중요한 의미를 가집니다. Cosmos의 **검증자(Validators)**는 비트코인의 채굴자(Miners)와 유사한 역할을 수행하지만, 블록 생성 대신 **암호 서명(Cryptographic Signatures)**을 통해 **투표(Vote)**를 진행합니다.

검증자는 **블록 커밋(Committing Blocks)**을 담당하는 **보안성이 높은 전용 머신(Secure Dedicated Machines)**이며, **비검증자(Non-Validators)**는 자신의 스테이킹 토큰(Atoms)을 검증자에게 **위임(Delegate)**하여 블록 수수료 및 Atom 보상(Reward)의 일부를 받을 수 있습니다.

그러나, 만약 위임받은 검증자가 해킹되거나 프로토콜을 위반하면, **슬래싱(Slashing, 벌금형)**이 적용되어 스테이킹 자산이 감소할 위험이 있습니다.

Tendermint BFT 합의의 입증된 안전성(Proven Safety Guarantees) 과 검증자 및 위임자의 담보 스테이킹 구조(Collateral Deposit Structure) 는 노드와 라이트 클라이언트 모두에게 정량적이고 측정 가능한 보안성(Quantifiable Security) 을 제공합니다.

거버넌스 (Governance)

분산 퍼블릭 원장(Distributed Public Ledgers)은 헌법(Constitution) 과 거버넌스 시스템 (Governance System) 을 가져야 합니다. 비트코인은 Bitcoin Foundation과 채굴(mining)을 통해 업그레이드를 조율하지만, 이는 매우 느린 과정입니다.

예를 들어, 이더리움(Ethereum) 은 TheDAO 해킹 사건 이후, ETH와 ETC로 하드포크(Hard Fork) 되었는데, 이는 이러한 결정을 내릴 사회적 합의(Social Contract) 나 결정 메커니즘 (Mechanism) 이 존재하지 않았기 때문입니다.

Cosmos Hub의 검증자(Validators) 와 위임자(Delegators) 는 다음과 같은 제안(Proposals)에 대해 투표(Vote) 할 수 있습니다. 시스템의 사전 설정 매개변수 변경 (예: 블록 가스 한도, Block Gas Limit)

- 업그레이드 조율(Coordinate Upgrades)
- Cosmos Hub의 정책을 규정하는 인간이 읽을 수 있는 헌법(Human-Readable Constitution) 수정안

이 헌법은 이해관계자 간의 결속(Cohesion) 을 강화하여, 도난(Theft) 및 버그(Bug) 와 같은 문제(예: TheDAO 사건) 해결을 더 빠르고 명확하게 수행할 수 있게 합니다.

각 Zone 또한 자체적인 헌법과 거버넌스 메커니즘 을 가질 수 있습니다.

예를 들어, Cosmos Hub는 불변성(Immutability) 을 유지하기 위한 헌법을 가질 수 있습니다. (즉, 롤백(Roll-back) 은 허용되지 않으며, 단지 Hub 노드의 버그에 한해 예외가 허용됨)

반면, 각 Zone은 롤백 정책(Policy on Roll-backs) 을 독자적으로 설정할 수 있습니다.

Cosmos 네트워크는 이처럼 다양한 정책을 가진 Zone 간 상호운용성(Interoperability) 을 가능하게 함으로써, 사용자에게 최고 수준의 자유(Freedom) 와 허가 없는 실험(Permissionless Experimentation) 의 기회를 제공합니다.

허브와 존 (The Hub and Zones)

여기서는 **탈중앙화(Decentralization)** 및 **확장성(Scalability)** 의 새로운 모델을 설명합니다.

Cosmos는 **Tendermint**에 의해 구동되는 다수의 블록체인 네트워크(**Network of Many Blockchains**) 로 구성됩니다.

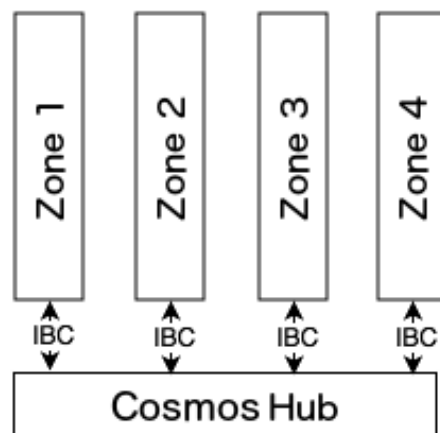
기존 제안들이 **글로벌 단일 거래 순서를 가진 단일 블록체인(Single Blockchain)** 을 구축하려는 반면, Cosmos는 **서로 독립적이지만 상호운용 가능한 블록체인(Many Concurrent Blockchains)** 들이 병렬로 실행될 수 있도록 허용합니다.

Cosmos의 기반에서, **Cosmos Hub**는 여러 개의 **독립 블록체인(Independent Blockchains)**, 즉 **Zone** 들을 관리합니다. (Zone은 데이터베이스 샤딩 기법에서 유래된 **Shards**로 불리기도 함)

각 Zone에서 발생한 블록 커밋(Block Commit)은 Hub에 지속적으로 게시(Post)되어, Hub가 각 Zone의 상태(State)를 추적할 수 있도록 합니다.

마찬가지로, 각 Zone은 Hub의 상태를 동기화하지만, Zone 간에는 Hub를 거치지 않고는 직접 통신하지 않습니다. Zone 간의 정보는 **머클 증명(Merkle-Proof)** 형태로 전달되며, 이 증명은 데이터가 **송신 및 수신되었음을 입증(Evidence)** 합니다.

이러한 메커니즘은 **인터블록체인 통신(Inter-Blockchain Communication)** 으로 불리며, 약칭으로 **IBC** 라고 합니다.



모든 존(Zone)은 자체적으로 **허브(Hub)** 가 되어 비순환 그래프(Acyclic Graph) 형태의 네트워크를 형성할 수 있습니다.

그러나 설명의 명확성을 위해, 여기서는 **단일 허브(Single Hub)** 와 **여러 비허브 존(Non-Hub Zones)** 으로 구성된 단순한 구조만을 다루겠습니다.

허브 (The Hub)

Cosmos Hub는 다중 자산 분산 원장(Multi-Asset Distributed Ledger)을 호스팅하는 블록체인으로, 토큰은 개별 사용자(Individual Users) 또는 존(Zones) 자체가 보유할 수 있습니다.

이 토큰들은 **IBC 패킷(IBC Packet)** 이라 불리는 특수한 전송 단위, 즉 “**코인 패킷(Coin Packet)**” 을 통해 한 존에서 다른 존으로 이동할 수 있습니다.

Hub는 모든 존에서 각 토큰의 총량(Global Invariance of Token Supply) 을 보존하는 역할을 합니다. 따라서 IBC 코인 패킷 거래는 송신자(Sending Zone), 허브(Hub), 수신자(Receiving Zone) 블록체인 모두에 의해 커밋되어야 합니다.

Cosmos Hub는 시스템 전체의 중앙 원장(Central Ledger) 역할을 하기 때문에, 그 보안(Security)은 가장 중요한 요소입니다.

각 Zone은 소수(예: 4개)의 검증자(Validators)만으로도 Tendermint 기반의 BFT 보안을 유지할 수 있지만, Hub는 전 세계적으로 분산된 검증자 집합(Globally Decentralized Set of Validators)에 의해 보호되어야 합니다.

이 검증자 집합은 대륙 단위 네트워크 분할(Continental Network Partition) 또는 국가 차원의 공격(Nation-State Sponsored Attack) 과 같은 가장 심각한 공격 시나리오에도 견딜 수 있어야 합니다.

존 (The Zones)

Cosmos Zone은 허브(Hub)와 IBC 메시지(IBC Messages) 를 교환하는 독립적인 블록체인(Independent Blockchain) 입니다.

허브의 관점에서 각 Zone은 다중 자산 동적 멤버십 멀티시그 계정(Multi-Asset Dynamic-Membership Multi-Signature Account) 으로 간주됩니다. 이 계정은 IBC 패킷을 통해 토큰을 송수신(Send and Receive)할 수 있습니다.

암호화폐 지갑과 마찬가지로, Zone은 자신이 보유한 양보다 더 많은 토큰을 보낼 수 없지만, 다른 Zone으로부터는 토큰을 수신할 수 있습니다.

특정 Zone은 “소스(Source)” 존 으로 지정될 수 있으며, 이는 해당 Zone이 하나 이상의 토큰 종류의 공급을 인플레이션(Inflate) 시킬 수 있는 권한을 갖는다는 의미입니다.

Cosmos Hub의 아톰(Atom) 토큰은 허브에 연결된 Zone의 검증자들에 의해 스테이킹(Staking)될 수 있습니다.

Zone에서 이중 지출(Double-Spend) 공격이 발생할 경우, Tendermint의 포크 책임성(Fork Accountability) 메커니즘에 따라 해당 검증자의 아톰은 슬래싱(Slashing, 삭감) 됩니다.

하지만 Zone에서 $\frac{2}{3}$ 이상의 투표 권한이 비잔틴(Byzantine) 이 될 경우, 잘못된 상태(Invalid State)가 기록될 위험이 있습니다.

Cosmos Hub는 개별 Zone에서 수행된 거래를 직접 검증하거나 실행하지 않으므로, 사용자들은 신뢰할 수 있는 Zone으로 토큰을 전송해야 합니다.

향후 Cosmos Hub의 거버넌스 시스템(Governance System)은 Zone의 장애나 공격을 고려한 Hub 개선 제안(Hub Improvement Proposals)을 통과시킬 수 있습니다. 예를 들어, 일부(또는 전체) Zone으로부터의 아웃바운드 토큰 전송(Outbound Token Transfers)을 제한(Throttle)하여, 공격이 탐지될 경우 비상 회로 차단(Emergency Circuit-Breaking) — 즉, 일시적으로 토큰 전송을 중단하는 — 기능이 활성화될 수 있습니다.

인터블록체인 통신 (Inter-blockchain Communication, IBC)

이제 허브(Hub)와 존(Zones)이 서로 어떻게 통신하는지를 살펴보겠습니다. 예를 들어, 세 개의 블록체인 "Zone1", "Zone2", 그리고 "Hub"가 있다고 가정합니다. 만약 "Zone1"에서 "Zone2"로 데이터를 전송하려면, 그 패킷(Packet)은 “Hub”를 통해 전달됩니다.

IBC 패킷 전송 과정

한 블록체인에서 다른 블록체인으로 패킷을 이동시키기 위해, 수신 체인(Receiving Chain)에 증명(Proof)이 게시됩니다.

이 증명은 송신 체인(Sending Chain)이 특정 목적지(Destination)를 향해 패킷을 게시(Publish)했다는 사실을 명시합니다.

수신 체인이 이 증명을 검증하기 위해서는 송신 체인의 블록 헤더(Block Headers)를 지속적으로 동기화해야 합니다.

이 메커니즘은 사이드체인(Sidechains)에서 사용되는 방식과 유사합니다. 즉, 상호 작용하는 두 체인은 양방향 데이터 스트림(Bidirectional Stream)을 통해 서로의 존재를 인식하고, 존재 증명 데이터그램(Proof-of-Existence Datagrams, 즉 트랜잭션)을 교환합니다.

IBC 트랜잭션 유형

IBC 프로토콜은 기본적으로 두 가지 트랜잭션 유형으로 정의됩니다.

1. IBCBlockCommitTx

- 블록체인이 **가장 최근 블록 해시(Most Recent Block-Hash)** 를 모든 관찰자(Observer)에게 증명(Prove)할 수 있게 합니다.

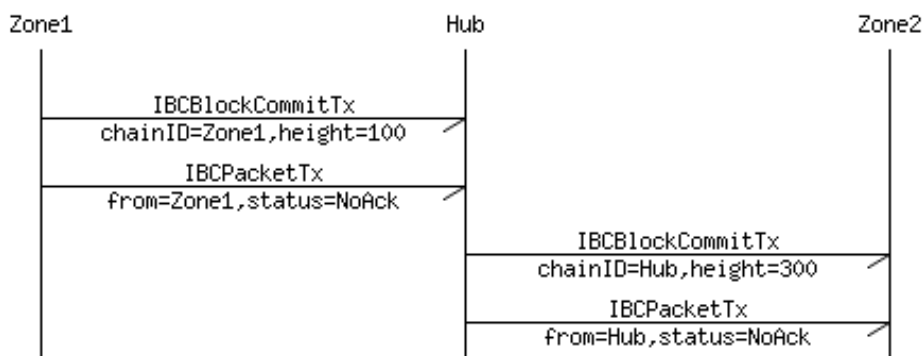
2. IBCPacketTx

- 블록체인이 **특정 패킷(Packet)** 이 송신자의 애플리케이션에서 실제로 게시되었음을 머클 증명(Merkle-Proof)을 통해 증명할 수 있게 합니다.

IBC의 거래 구조 및 자유도

IBC 메커니즘을 두 개의 독립된 트랜잭션으로 분리함으로써, 수신 체인의 **수수료 시장 메커니즘(Fee Market Mechanism)** 이 어떤 패킷이 커밋(Commit, 즉 승인)될지를 결정하게 됩니다.

동시에, 송신 체인은 **아웃바운드 패킷(Outbound Packets)** 을 얼마나 많이 보낼지를 자유롭게 결정할 수 있습니다.



예시 (Example), "Zone1"에서 "Zone2"로 패킷을 보내기 위해서는 "Hub"에 "Zone1"의 블록 해시(Block-Hash)를 포함하는 IBCBlockCommitTx 트랜잭션이 게시되어야 합니다. 반대로 "Hub"의 블록 해시를 "Zone2"에 업데이트하려면 "Zone2"에 동일한 IBCBlockCommitTx가 게시되어야 합니다.

참고:

자세한 내용은 IBCBlockCommitTx 및 IBCPacketTx의 섹션에서 확인할 수 있습니다.
이 두 가지는 IBC의 핵심 트랜잭션 유형입니다.

활용 사례 (Use Cases)

분산형 거래소 (Distributed Exchange)

비트코인이 분산되고 대규모로 복제된 원장(Distributed, Mass-Replicated Ledger) 덕분에 더 높은 보안을 가지는 것처럼, 거래소를 블록체인 위에서 운영함으로써 내부 또는 외부 해킹에 대한 취약성을 줄일 수 있습니다. 이를 분산형 거래소(Distributed Exchange) 라고 합니다.

기존의 탈중앙화 거래소 (Atomic Cross-Chain, AXC)

오늘날 암호화폐 커뮤니티에서 “탈중앙화 거래소(Decentralized Exchange)”라고 부르는 개념은 원자적 교차 체인 거래(Atomic Cross-Chain Transactions, AXC)에 기반하고 있습니다.

AXC 트랜잭션을 통해 두 사용자는 서로 다른 블록체인 상에서 두 개의 전송 거래를 동시에(또는 전혀 하지 않거나, 즉 원자적으로) 수행할 수 있습니다.

예를 들어, 비트코인과 이더리움이 직접 연결되어 있지 않더라도, AXC를 통해 두 사용자가 **비트코인을 이더로 교환**할 수 있습니다.

AXC의 장점은 사용자들이 서로를 신뢰할 필요가 없고, 거래 중개 서비스(Trade-Matching Service)가 필요하지 않다는 점입니다.

그러나 단점은 두 사용자가 모두 온라인 상태여야만 거래가 진행될 수 있다는 점입니다.

블록체인 기반 분산형 거래소 (Mass-Replicated Distributed Exchange)

또 다른 형태의 탈중앙화 거래소는 자체 블록체인에서 운영되는 대규모 복제 거래소(Mass-Replicated Exchange)입니다.

이 형태에서는 사용자가 지정가 주문(Limit Order)을 제출한 후 컴퓨터를 꺼도 거래가 자동으로 실행될 수 있습니다.

블록체인이 거래를 매칭하고, 사용자를 대신해 거래를 완료합니다.

중앙화 거래소와의 비교 (Centralized Exchange vs Decentralized Exchange)

중앙화 거래소는

깊은 주문 장(Order Book)을 구축할 수 있기 때문에 더 많은 유동성과 트레이더를 유치할 수 있습니다.

예를 들어, 현재 주요 거래소로는 **Poloniex**(24시간 거래량 약 \$20M)과 **Bitfinex**(약 \$5M)가 있습니다.

이처럼 강력한 네트워크 효과(Network Effect)를 가진 중앙화 거래소와 경쟁하기 위해서는, 탈중앙화 거래소 또한 **깊은 주문 장과 지정가 주문 지원**이 필요합니다. 이러한 기능은 **블록체인 기반의 분산형 거래소**에서만 구현 가능합니다.

Tendermint의 역할 (Tendermint's Contribution)

Tendermint는 빠른 거래 확정(Fast Transaction Commit)과 일관성(Consistency)을 유지하면서도 **신속한 결제(Finality)**를 제공하는 장점을 지닙니다.

Cosmos의 각 Zone은 **거래 주문 트랜잭션**과 **IBC 토큰 전송** 모두에서 빠른 확정을 수행할 수 있습니다.

Cosmos의 응용 (Cosmos as a Distributed Exchange)

현재 암호화폐 거래 환경에서,
Cosmos는 **분산형 거래소(Distributed Exchange)** 또는 **Cosmos DEX**로서 이상적인 응용 사례입니다.

Cosmos의 **트랜잭션 처리량(Throughput)**과 **확정 지연 시간(Commit Latency)**은 중앙화 거래소 수준에 근접할 수 있습니다.

트레이더는 온라인 상태가 아니더라도 **지정가 주문(Limit Orders)**을 제출하고 실행할 수 있으며, Tendermint, Cosmos Hub, 그리고 IBC**를 통해 토큰을 빠르고 안전하게 다른 Zone과 거래소 간에 이동할 수 있습니다.

다른 암호화폐와의 브리징 (Bridging to Other Cryptocurrencies)

특정 **특권 존(Privileged Zone)**은 다른 암호화폐의 **브리징 토큰(Bridged Token)** 발행 원천으로 작동할 수 있습니다.

이 **브리지(Bridge)**는 Cosmos의 허브(Hub)와 존(Zone) 간 관계와 유사합니다. 양쪽 모두 최신 블록 정보를 유지하며, 토큰이 한 체인에서 다른 체인으로 이동했음을 검증할 수 있어야 합니다.

Cosmos 네트워크 상의 **브리지 존(Bridge-Zone)**은 허브뿐 아니라 연결된 외부 암호화폐 네트워크(예: Bitcoin, Ethereum 등)와도 동기화됩니다.

이러한 **간접 연결(Indirection)**을 통해, 허브는 외부 블록체인의 합의 구조(예: 비트코인의 작업증명 PoW)로부터 독립적인 단순하고 블록체인 불가지론적(Agnostic)인 구조를 유지할 수 있습니다.

Cosmos Hub로 토큰 전송 (Sending Tokens to the Cosmos Hub)

각 **브리지 존 검증자(Bridge-Zone Validator)**는 특수한 **ABCI 브리지 애플리케이션(ABCI Bridge-App)**을 탑재한 Tendermint 기반 블록체인과, 해당 암호화폐의 **풀 노드(Full Node)**를 함께 운영합니다.

새 블록이 원본 체인(Origin)에서 채굴될 때, 브리지 존의 검증자들은 서명(Signing)과 블록 헤더 공유를 통해 새 블록 커밋(Committed Block)에 합의합니다.

예를 들어, 브리지 존이 이더리움(Ethereum) 또는 비트코인(Bitcoin) 같은 PoW 체인에서 지불을 수신하고 충분한 컨펌(Confirmation)이 완료되면, 해당 금액과 동일한 계정이 브리지 존 내에 생성됩니다.

Ethereum 사례

Ethereum의 경우, 브리지 존은 Cosmos Hub와 동일한 **검증자 집합(Validator Set)** 을 공유할 수 있습니다.

이더리움 측(Origin Side)에서는 **브리지 컨트랙트(Bridge Contract)** 가 존재하며, 이더 보유자는 이 컨트랙트에 이더를 전송함으로써 Cosmos 네트워크의 브리지 존으로 자산을 이동시킬 수 있습니다.

이더가 브리지 컨트랙트에 입금되면, 해당 이더는 브리지 존에서 적절한 IBC 패킷을 수신하기 전까지 출금이 불가능합니다.

이더리움 브리지 컨트랙트는 브리지 존의 검증자 세트를 추적하며, 이는 Cosmos Hub의 검증자 세트와 동일할 수도 있습니다.

Bitcoin 사례

비트코인의 경우 개념은 유사하지만, 단일 브리지 컨트랙트 대신 **P2SH 멀티시그(Multisignature P2SH)** 스크립트가 사용됩니다.

각 UTXO는 개별 서브스크립트(Subscript)에 의해 제어되며, P2SH 시스템의 제약으로 인해 서명자는 Cosmos Hub의 검증자 세트와 완전히 동일할 수는 없습니다.

Cosmos Hub에서 토큰 인출 (Withdrawing Tokens from Cosmos Hub)

브리지 존의 이더(Bridged Ether)는 Hub로 전송되었다가 다시 이더리움 네트워크의 지정된 출금 주소(Withdrawal Address)로 파괴(소각)될 수 있습니다.

이때 브리지 존에서 해당 트랜잭션이 발생했음을 증명하는 **IBC 패킷(IBC Packet)** 이 이더리움의 브리지 컨트랙트에 게시되어야 하며, 이를 통해 출금이 승인됩니다.

비트코인의 경우, 제한된 스크립팅 시스템으로 인해 IBC 코인 전송 메커니즘을 완전히 반영하기 어렵습니다.

각 UTXO는 독립적인 서브스크립트를 가지고 있으므로, 새로운 비트코인 에스크로 서명자 집합이 형성될 때마다 모든 UTXO가 새로운 주소로 이전되어야 합니다.

이 문제를 해결하기 위한 한 가지 방법은 필요 시 **UTXO 세트를 압축(Compress)** 또는 **해제(Decompress)** 하는 것입니다.

브리지 존의 책임성 (Total Accountability of Bridge Zones)

이러한 브리징 구조의 주요 위험은 **악의적인 검증자 집합(Rogue Validator Set)** 입니다.

$\frac{1}{3}$ 이상의 비잔틴 투표권이 존재할 경우, 이더리움 브리지 컨트랙트에서 이더를 인출하면서 브리지 존에 있는 브리징된 이더를 그대로 보관하는 포크(Fork)가 발생할 수 있습니다.

더 나아가 $\frac{2}{3}$ 이상의 비잔틴 투표권이 존재하면, 브리지 존의 원래 논리를 벗어나 이더를 직접 탈취할 수도 있습니다.

해결책: 완전한 검증 가능 설계

이 문제는 브리지를 **완전 검증 가능(Totally Accountable)** 하게 설계함으로써 해결할 수 있습니다.

예를 들어, 모든 허브와 원본 체인의 IBC 패킷은 브리지 존의 승인을 요구하도록 설계할 수 있습니다.

이때 브리지 존의 상태 변화를 허브나 원본의 브리지 컨트랙트 중 어느 쪽에서든 효율적으로 검증할 수 있습니다. 또한 허브와 원본 체인은 브리지 존의 검증자들이 **담보(Collateral)** 를 게시하도록 요구하고, 토큰 출금은 일정한 **언본딩 기간(Unbonding Period)** 이후에만 가능하도록 지연시킬 수 있습니다.

이 시스템의 구체적인 명세 및 구현은 **Cosmos 개선 제안(Cosmos Improvement Proposal)** 으로 제시될 수 있으며, **Cosmos Hub 거버넌스 시스템** 을 통해 승인될 예정입니다.

이더리움 확장 (Ethereum Scaling)

이더리움의 확장성 문제(Scaling Problem)는 여전히 미해결 과제입니다. 현재 이더리움 노드는 모든 거래를 직접 처리하며, 모든 상태(State) 데이터를 저장해야 합니다.

Tendermint는 비트코인의 작업 증명(Proof-of-Work)보다 훨씬 빠르게 블록을 커밋할 수 있기 때문에, Tendermint 합의로 구동되는 EVM 존(EVM Zones)은 브리징된 이더(Bridged Ether)를 통해 이더리움 블록체인에 더 높은 성능을 제공합니다.

또한, Cosmos Hub와 IBC 패킷 메커니즘은 任의의 스마트 계약 로직 실행은 지원하지 않지만, 여러 존에서 실행 중인 이더리움 계약 간의 **토큰 이동(Token Movement)** 을 조정할 수 있습니다. 이로써 **토큰 중심의 이더리움 샤딩(Token-Centric Ethereum Sharding)** 기반 확장의 토대를 제공합니다.

다중 애플리케이션 통합 (Multi-Application Integration)

Cosmos 존은 任의의 애플리케이션 로직을 실행할 수 있습니다. 이는 존이 생성될 때 정의되며, 거버넌스를 통해 시간이 지나면서 업데이트될 수도 있습니다.

이러한 유연성 덕분에 Cosmos 존은 이더리움이나 비트코인 같은 다른 암호화폐의 브리지로 작동할 수 있으며, 해당 블록체인의 파생체(Derivative) 또한 동일한 코드베이스를 사용하면서 다른 검증자 집합(Validator Set)과 초기 분배 구조를 가질 수 있습니다.

이로써 이더리움, Zerocash, 비트코인, CryptoNote 등의 기존 암호화폐 프레임워크들이 Tendermint Core와 함께 사용할 수 있습니다. Tendermint Core는 고성능 합의 엔진(High-Performance Consensus Engine)을 갖춘 공통 네트워크를 제공하므로, 플랫폼 간 상호운용성(Interoperability)을 위한 큰 기회를 열어줍니다.

또한 Cosmos는 다중 자산 블록체인(Multi-Asset Blockchain)으로, 단일 거래에 여러 입력(Input)과 출력(Output)을 포함할 수 있으며, 각 입력은 任의의 토큰 유형이 될 수 있습니다. 이를 통해 Cosmos는 탈중앙화 거래소 플랫폼으로 직접 활용될 수 있습니다.

대안적으로, Cosmos 존은 **분산형 내결함성 거래소(Distributed Fault-Tolerant Exchange)** 역할을 할 수도 있으며, 이는 시간이 지남에 따라 해킹의 위험이 높은 기존 중앙화 거래소보다 더 나은 개선책으로 평가됩니다.

Cosmos 존은 또한 기업(Enterprise)이나 정부 시스템(Government Systems)의 블록체인 기반 버전으로도 활용될 수 있습니다.

기존에는 특정 기관이나 조직 그룹이 관리하던 서비스가 이제는 특정 존에서 **ABCI 애플리케이션**으로 운영될 수 있습니다. 이 방식은 퍼블릭 Cosmos 네트워크의 보안성과 상호운용성을 상속받으면서도, 서비스에 대한 통제권(Control)을 유지할 수 있도록 합니다.

따라서 Cosmos는 **블록체인 기술을 활용하면서도 완전한 탈중앙화에 대한 우려를 갖는 조직에게** 양쪽 세계의 장점을 모두 제공할 수 있습니다.

네트워크 분할 완화 (Network Partition Mitigation)

일부에서는 Tendermint와 같은 합의 알고리즘이
네트워크 분할(Network Partition) 상황에서
2/3 이상의 투표권을 가진 파티션이 존재하지 않으면
합의가 중단(Halt)된다고 비판합니다.

Cosmos의 아키텍처는
글로벌 허브(Global Hub)와 **지역 자율 존(Regional Autonomous Zones)** 구조를 통해
이 문제를 완화할 수 있습니다.

각 존의 투표권은 **공통 지리적 지역(Geographic Region)**에 따라 분산되어 있으며,
예를 들어 각 도시나 지역이 독립적인 존을 운영하면서도
공통 허브(Cosmos Hub)를 공유할 수 있습니다.

이를 통해 일시적인 네트워크 분할이 발생하더라도
허브가 중단되거나 정지되더라도
지역 활동(Municipal Activity)은 계속 유지될 수 있습니다.

이 접근법은
지리적, 정치적, 네트워크 토폴로지적 요소를 반영하여
강력한 연합형 내결함성 시스템(Federated Fault-Tolerant System) 설계에 기여합니다.

연합형 이름 해석 시스템 (Federated Name Resolution System)

NameCoin은 **비트코인 블록체인 기반**으로 이름 해석(Name Resolution) 문제를 해결하려는
최초의 시도 중 하나였지만, 여러 한계를 드러냈습니다.

예를 들어 NameCoin에서는
특정 시점에 @satoshi가 어떤 공개키에 등록되었는지 증명할 수 있지만,
그 이후 공개키가 변경되었는지는
그 이름의 마지막 업데이트 이후 모든 블록을 다운로드해야만 확인할 수 있습니다.

이는 비트코인의 UTXO 모델에서
거래(Transaction)만 머클화되고,
애플리케이션 상태(Application State)는 머클화되지 않기 때문입니다.
따라서 우리는 “존재(Existence)”는 증명할 수 있지만,
“변경되지 않음(Non-Existence of Updates)”은 증명할 수 없습니다.

결국 이름의 최신값을 확실히 알기 위해서는
전체 노드(Full Node)를 신뢰하거나,
전체 블록체인을 다운로드해야 하며,
이 과정은 상당한 대역폭(Bandwidth)을 필요로 합니다.

심지어 머클화된 탐색 트리(Merkleized Search Tree)를 구현하더라도,
PoW 의존성으로 인해 라이트 클라이언트(Light Client) 검증이 어렵습니다.
라이트 클라이언트는 모든 블록의 헤더를 다운로드해야 하며,
이 대역폭 요구사항은 시간에 비례하여 선형적으로 증가합니다.
또한 비트코인의 경우, 이름 변경은
추가적인 PoW 확인 블록(Confirmation Blocks)을 기다려야 하며,
이 과정은 최대 한 시간까지 걸릴 수 있습니다.

Tendermint에서는
검증자 투표권 기반의 **쿼럼 서명(Quorum Signature)** 과
현재 이름 값에 대한 **머클 증명(Merkle Proof)** 만 있으면 충분합니다.
이 방식은 **짧고(Succinct), 빠르고(Quick), 안전한(Secure)**
라이트 클라이언트 검증을 가능하게 합니다.

Cosmos에서는 이 개념을 확장할 수 있습니다.
각 이름 등록 존(Name-Registration Zone)은
.com이나 .org 같은 **최상위 도메인(Top-Level Domain, TLD)** 을 가질 수 있으며,
각 존은 독자적인 **거버넌스(Governance)** 와 **등록 규칙(Registration Rules)** 을 유지할 수 있습니다.

발행 및 인센티브 (Issuance and Incentives)

아톰 토큰 (The Atom Token)

Cosmos Hub는 다중 자산 분산 원장(Multi-Asset Distributed Ledger)이지만,
Atom이라는 특별한 네이티브 토큰이 존재합니다.

Atoms는 Cosmos Hub의 **유일한 스테이킹 토큰(Staking Token)** 으로, 보유자는 이를 통해 **투표(Vote)**, **검증(Validate)** 또는 **위임(Delegate)** 할 수 있습니다.

이더리움의 이더(Ether)처럼, Atom은 **스팸 방지를 위한 거래 수수료(Transaction Fee)** 로도 사용됩니다. 추가로 발생하는 인플레이션성 아톰(Inflationary Atoms)과 블록 트랜잭션 수수료는 검증자(Validators)와 위임자(Delegators)에게 분배됩니다.

BurnAtomTx 트랜잭션은 예비 풀(Reserve Pool)에서 비례적인 양의 토큰을 회수하는 데 사용될 수 있습니다.

기금 조성 (Fundraiser)

제네시스(Genesis) 시점의 아톰 토큰 및 검증자 분배는 **Cosmos Fundraiser**의 기부자들에게 다음 비율로 분배됩니다.

- Fundraiser 기부자: 75%
- 주요 기부자(Lead Donors): 5%
- Cosmos Network Foundation: 10%
- ALL IN BITS, Inc: 10%

제네시스 이후부터 매년 전체 Atom의 1/3이 **본딩된 검증자(Bonded Validators)** 및 **위임자(Delegators)**에게 보상으로 지급됩니다.

자세한 내용은 **Cosmos Plan**을 참고하십시오.

검증자 수 제한 (Limitations on the Number of Validators)

비트코인이나 다른 작업증명(Proof-of-Work) 블록체인과 달리, Tendermint 기반 블록체인은 검증자 수가 많아질수록 통신 복잡도가 증가하여 속도가 느려집니다.

다행히도 Cosmos는 충분한 수의 검증자를 지원하여 **글로벌 분산 블록체인(Global Distributed Blockchain)**을 구축할 수 있습니다. 이를 통해 매우 빠른 트랜잭션 확정 시간(Transaction Confirmation Time)을 제공하며, 향후 대역폭, 저장공간, 병렬 연산 능력의 증가에 따라 더 많은 검증자를 지원할 수 있게 됩니다.

제네시스 시점의 **최대 검증자 수는 100명**으로 설정되며,
이 수는 **10년 동안 매년 13%씩 증가**하여
최종적으로 **300명**으로 고정됩니다.

제네시스 이후 검증자 되기 (Becoming a Validator After Genesis Day)

아직 검증자가 아닌 Atom 보유자는
BondTx 트랜잭션을 서명 및 제출하여
새로운 검증자가 될 수 있습니다.

제공되는 담보(Collateral)의 Atom 양은 0이 될 수 없습니다.
누구나 언제든지 검증자가 될 수 있지만,
현재의 검증자 집합이 **최대 검증자 수**를 초과할 경우에는 제한됩니다.

이 경우, 거래는 다음 조건을 만족할 때만 유효합니다.

- 새 검증자의 Atom 수가
기존 검증자 중 가장 적은 Atom 수보다 많을 때

이때 “유효 Atom(Effective Atoms)”에는
위임된 Atom이 포함됩니다.

새로운 검증자가 기존 검증자를 대체하면,
기존 검증자는 비활성화 상태로 전환되며,
해당 검증자와 위임된 Atom들은 **언본딩(Unbonding)** 상태로 진입합니다.

검증자에 대한 벌칙 (Penalties for Validators)

검증자는 **의도적(Intentional)** 또는 **비의도적(Unintentional)** 으로
프로토콜을 위반할 경우 벌칙(Penalty)을 받게 됩니다.

즉시 적용 가능한 위반 증거로는 다음이 있습니다.

- 동일한 블록 높이(Height) 및 라운드(Round)에서 **이중 서명(Double Sign)**
- “**Prevote-the-Lock**” 규칙 위반 (Tendermint 합의 프로토콜의 규칙)

이러한 증거가 발견되면,
해당 검증자는 신뢰 상태(Good Standing)를 잃고
본딩된 Atom과 예비 풀의 비례 지분(Stake)이 삭감(Slashed)됩니다.

검증자가 네트워크 장애, 정전, 기타 이유로 인해
일정 기간 동안 트랜잭션을 커밋하지 못하는 경우에도
자동으로 비활성화됩니다.

- ValidatorTimeoutWindow 블록 동안
커밋이 누락되고,
 - 누락 횟수가 ValidatorTimeoutMaxAbsent 이상일 경우
 - 검증자는 비활성화 상태로 전환되고,
ValidatorTimeoutPenalty (기본 1%)의 스테이크가 삭감됩니다.
-

일부 악의적 행위(Malicious Behavior)는
명백한 블록체인 증거로 식별되지 않을 수도 있습니다.
이 경우, 다른 검증자들이 **슈퍼다수합의(Supermajority Consensus)** 로
해당 악의적 검증자의 타임아웃(Timeout)을 강제할 수 있습니다.

Cosmos Hub가
1/3 이상의 투표권이 오프라인 상태가 되거나,
1/3 이상의 연합이 악의적 증거를 검열(Censorship)하는 경우
Hub는 **하드 포크 복구 제안(Hard-Fork Reorg-Proposal)** 을 통해 회복해야 합니다.

자세한 내용은 “Forks and Censorship Attacks” 항목을 참조하십시오.

거래 수수료 (Transaction Fees)

Cosmos Hub의 검증자(Validators)는 거래 처리 수수료로 받을 수 있는 토큰 종류 또는 그 조합을 자유롭게 정할 수 있습니다.

각 검증자는 원하는 **환율(Exchange Rate)** 과 원하는 **거래 유형(Transaction Type)** 을 선택할 수 있으며,
단 BlockGasLimit을 초과하지 않아야 합니다.

수집된 수수료는 아래 명시된 세금을 제외하고, 본딩된 Atom 비율에 따라 이해관계자(Stakeholders)에게 분배됩니다.

이 분배 주기는 ValidatorPayoutPeriod(기본값: 1시간)입니다.

수집된 거래 수수료 중 ReserveTax(기본값 2%)는 예비 풀(Reserve Pool)에 적립되어 네트워크의 보안성과 가치(Value)를 강화하는 데 사용됩니다. 또한 거버넌스 시스템(Governance System)의 결정에 따라 이 자금은 다양한 용도로 재분배될 수 있습니다.

Atom 보유자가 투표권을 다른 검증자에게 위임(Delegate)할 경우, 위임 수수료(Commission)를 지불해야 하며, 이 비율은 각 검증자가 직접 설정할 수 있습니다.

해커 보상 시스템 (Incentivizing Hackers)

Cosmos Hub의 보안(Security)은 기본 검증자들의 안정성(Security of Validators)과 위임자(Delegators)의 선택(Delegation Choice)에 의해 결정됩니다.

잠재적인 취약점(Vulnerability)을 조기에 발견하고 보고하도록 장려하기 위해, Cosmos Hub는 해커들이 ReportHackTx 트랜잭션을 통해 성공적인 해킹 정보를 공개하도록 유도합니다.

이 트랜잭션은 “이 검증자가 해킹되었습니다. 이 주소로 보상금을 보내주세요.”라는 메시지를 포함합니다.

해킹이 보고되면, 해당 검증자와 위임자는 비활성화(Inactive) 상태가 되고, HackPunishmentRatio(기본값 5%) 비율만큼 모든 Atom이 삭감(Slashed)됩니다.

반면, HackRewardRatio(기본값 5%) 비율만큼의 Atom은 해커의 보상 주소(Bounty Address)로 전송됩니다.

검증자는 백업 키(Backup Key)를 사용하여 남은 Atom을 복구해야 합니다.

이 기능이 악용되어 미본딩(Unvested) Atom이 부당하게 이동되는 것을 방지하기 위해, ReportHackTx 실행 전후의 본딩(Vested) 및 미본딩(Unvested) Atom의 비율은 동일하게 유지됩니다. 따라서 해커의 보상에는 미본딩 Atom이 일부 포함될 수도 있습니다.

거버넌스 명세 (Governance Specification)

Cosmos Hub는 명확하게 정의된 **거버넌스 메커니즘(Governance Mechanism)** 을 기반으로 운영 됩니다.

이는 시스템 변수(Parameter) 조정, 소프트웨어 업그레이드(Software Upgrade), 헌법 개정 (Constitutional Amendments) 등을 조정하기 위함입니다.

모든 검증자는 모든 제안(Proposal)에 대해 투표할 책임이 있습니다. 정해진 시간 내에 투표하지 않으면, 검증자는 `AbsenteeismPenaltyPeriod`(기본값: 1주) 동안 비활성화됩니다.

위임자(Delegator)는 위임한 검증자의 투표를 자동으로 상속하지만, 원할 경우 수동으로 재설정할 수 있습니다. 언본딩(Unbonded) 상태의 Atom은 투표권이 없습니다.

각 제안은 `MinimumProposalDeposit` 만큼의 토큰을 예치해야 하며, 이는 Atom을 포함한 한 개 이상의 토큰 조합으로 구성될 수 있습니다.

투표자 과반수가 예치금을 몰수(Deposit Forfeiture)하기로 결정하면 (예: 스팸 제안으로 판단될 경우), 예치금은 예비 풀(Reserve Pool)로 이전되며, 소각(Burn)된 Atom은 제외됩니다.

투표 옵션 (Voting Options)

- `Yea`
 - `YeaWithForce`
 - `Nay`
 - `NayWithForce`
 - `Abstain`
-

가결 및 거부 조건

제안이 통과되거나 기각되기 위해서는 **`Yea/YeaWithForce` 또는 `Nay/NayWithForce`** 투표 중 단순 과반(Simple Majority)이 필요합니다.

다만, $\frac{1}{3}$ 이상의 투표권이 “`WithForce`”로 행사될 경우, 과반 결정이 **거부(Veto)** 될 수 있습니다.

Veto가 발생하면, 모든 참여자는 `VetoPenaltyFeeBlocks`(기본값: 하루치 블록 수수료)만큼의 수수료를 잃게 되며, 거부를 실행한 당사자는 추가로 `VetoPenaltyAtoms`(기본값: Atom의 0.1%)을 잃습니다.

매개변수 변경 제안 (Parameter Change Proposal)

정의된 매개변수(Parameter)는 `ParameterChangeProposal`을 통과시킴으로써 변경할 수 있습니다.

보상 제안 (Bounty Proposal)

Atom의 발행(Inflation) 및 예비 풀(Reserve Pool) 자금 사용은 `BountyProposal`을 통해 승인될 수 있습니다.

텍스트 제안 (Text Proposal)

프로토콜 업그레이드(Protocol Upgrade) 등 기타 모든 제안은 일반적인 `TextProposal`을 통해 조정됩니다.

로드맵 (Roadmap)

자세한 일정 및 계획은 [Plan](#) 문서를 참조하십시오.