Interoperability of BlockChain (인터체인)

김재욱(cmdhema@gmail.com)
전창석(jcs191072@gmail.com)

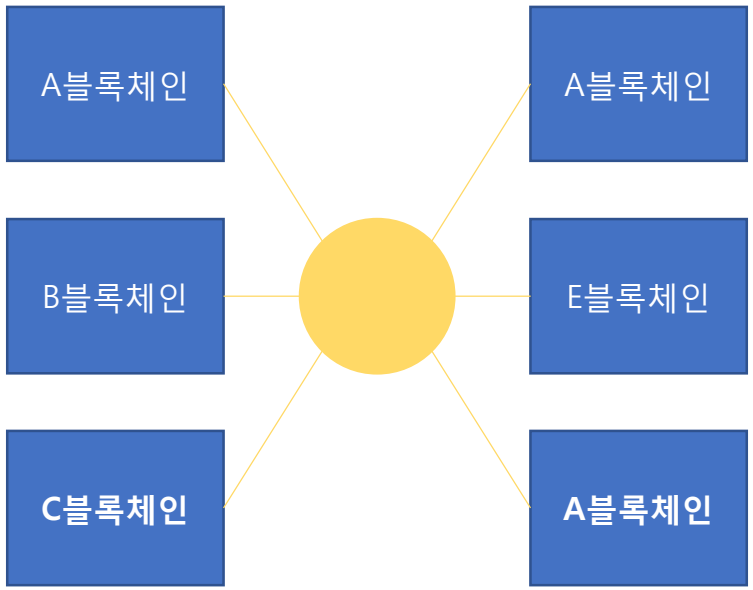
Agenda

이더리움 연구회
korea ethereum study group

- InterChain OverView(김재욱)
- InterChain Project DeepDive(전창석)
  - Cosmos

인터체인의 개요

인터체인이란?



- 여러 개의 블록체인간 정보를 교환하고 공유할 수 있는 기술, 네트워크 혹은 블록체인 이다.
- 독립된 네트워크를 하나로 연결한 인터넷, TCP/IP와 비슷한 개념으로 불리고있다.
- A 블록체인에서 통용되는 화폐를 B블록체인에서 사용할 수 있도록 한다.
- E블록체인에 기록된 데이터를 C블록체인에서 조회할 수 있도록 한다.
- A블록체인의 트렌젝션을 다른 A체인들이 나눠서 처리한다.

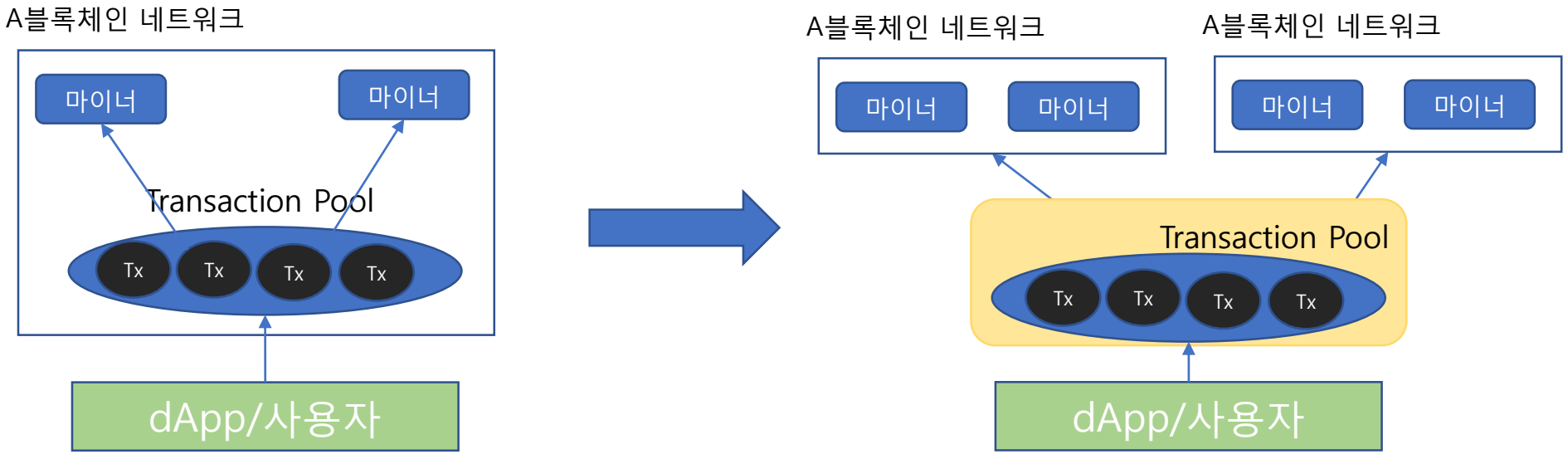
인터체인의 개요

인터체인으로 해결 할 수 있는 Issue

- 블록체인의 Scalability 향상의 대안중 하나가 될 수 있다.

  - 블록체인은 Consensus라는 특성이 존재하기 때문에, 단순히 마이너를 추가한다고 해서 TPS가 올라가지않는다.

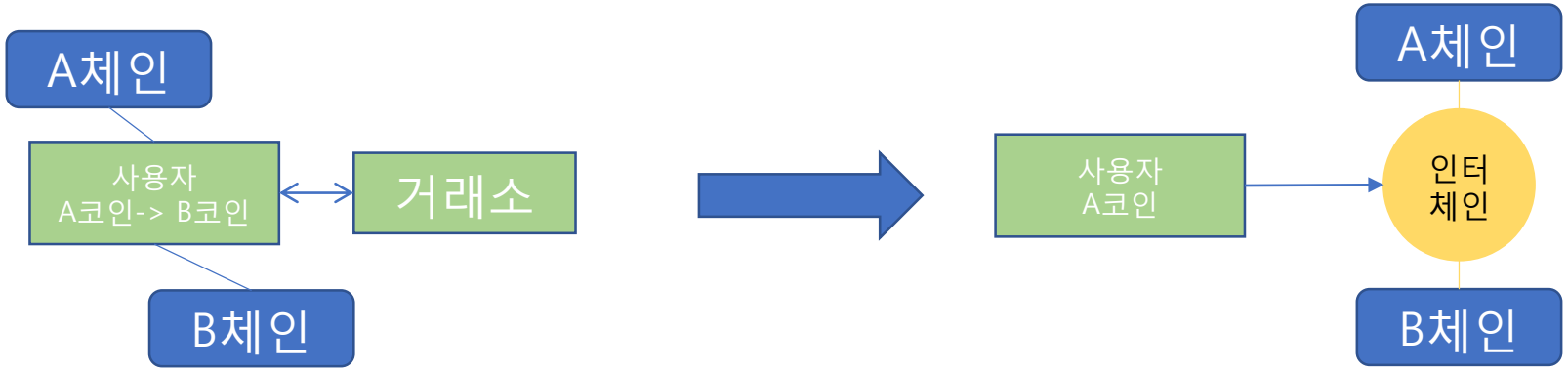
  - 인터체인 네트워크에 마이너가 아닌 동일 블록체인 네트워크를 추가하여 TPS를 올릴 수 있다.



인터체인의 개요

인터체인으로 해결 할 수 있는 Issue

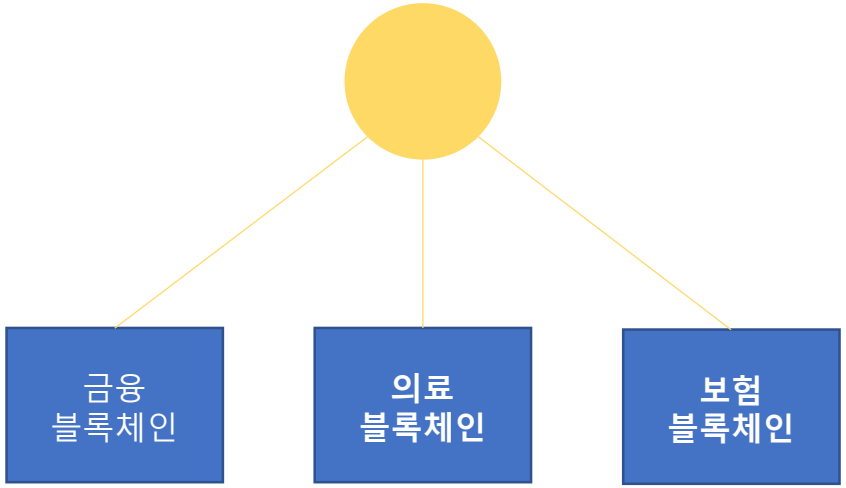
- 특정 블록체인의 암호화폐는 다른 블록체인에 사용할 수 없는 문제의 해결책 중 하나가 될 수 있다.
  - A블록체인의 a암호화폐로 B블록체인의 dApp을 사용하기 위해서 현재는 거래소에서 a화폐를 특정 통화로 팔고 그 통화로 B블록체인의 화폐를 구입해야한다.
  - 그 과정에서 이중 수수료 부과(판매, 구입), 거래소 이용의 부담(거래 채결 시간, 안정성, 화폐 거래 목록 확인 등)이 있을 수 있다.
  - 인터체인에 연결된 블록체인끼리는 인터체인 자체의 화폐 혹은 참여 블록체인의 화폐로 모든 블록체인을 이용할 수 있다.



인터체인의 개요

인터체인으로 해결 할 수 있는 Issue

- 독립된 블록체인끼리 데이터를 주고받을 수 있는 방법중 하나가 될 수 있다.
  - 특히 Private 블록체인끼리는 정보를 전혀 주고받을 수가 없다.
  - 인터체인은 참여한 블록체인 끼리 공통의 원장을 공유하므로 조회가 가능하다.
  - 각각의 블록체인은 억지로 데이터를 모을 필요가 없기 때문에 시너지 효과가 발생할 수 있다.

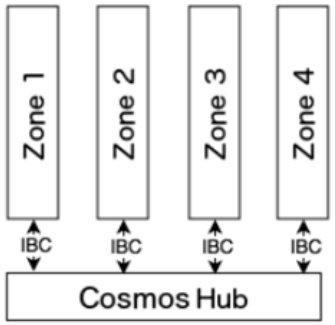


인터체인의 개요

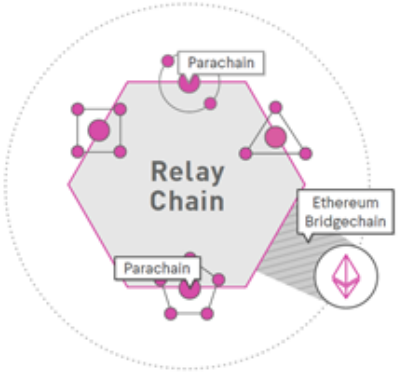
인터체인 동작 방식

◆ 어떻게 블록체인끼리 연결할 것인가?

- 연결을 위해 인터체인 프로젝트들은 브릿지, 릴레이 등과 같은 이름으로 연결할 수 있는 수단을 제공한다.
- 인터체인 별로 Source BlockChain에서 Destination 블록체인으로 트랜잭션을 보내는 프로토콜은 다르다.
- 필요에 따라 체인별 SmartContract를 만들거나, Public BlockChain을 연결할 경우 싱크하는 Full Client, Light Client가 필요할 수 있다.



From Cosmos White paper



From PolkaDot White paper

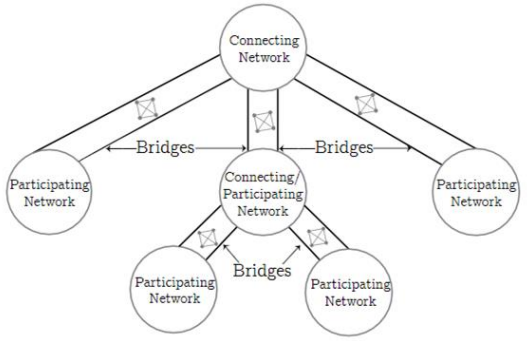


Figure 5: High level overview of bridge to connecting network relationship

From AION White paper

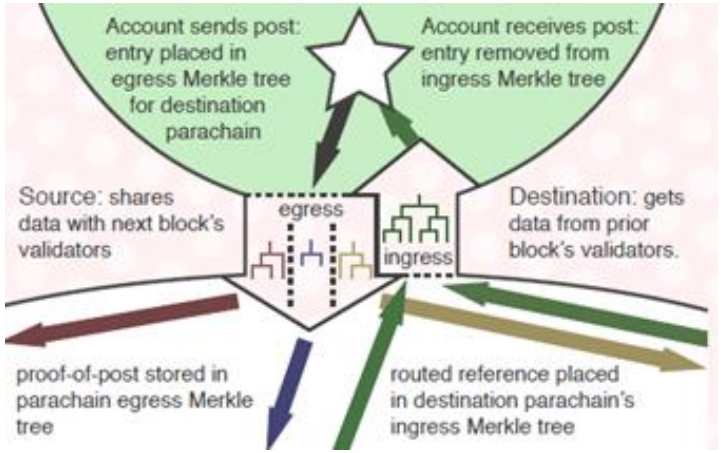
인터체인의 개요

인터체인 동작 방식

◆ 블록체인-블록체인의 데이터 교환
- A Zone에서 B Zone으로 보낸 트랜잭션을 직접적으로 확인하지 않고, 중간에 허브에서 거쳐서 전송된다.
- 허브에서는 A Zone에서 온 트랜잭션의 유효성을 검사하고 검증이 완료되면 B Zone으로 트랜잭션을 보낸다.
- B Zone에서는 허브에서 온 트랜잭션이 유효한지 검사한다.
- 각 단계에서 트랜잭션이 유효한지에 대한 여부는 머클 트리를 활용한 머클 증명을 사용한다.
- 머클트리는 각 블록체인별로 가지고 있을 수 있고, 허브에서 전역 머클 트리를 가지고 있을 수 있다.

```
receive(P{type, sequence, source, destination, data}, M_kvh) ⇒ success | failure
```

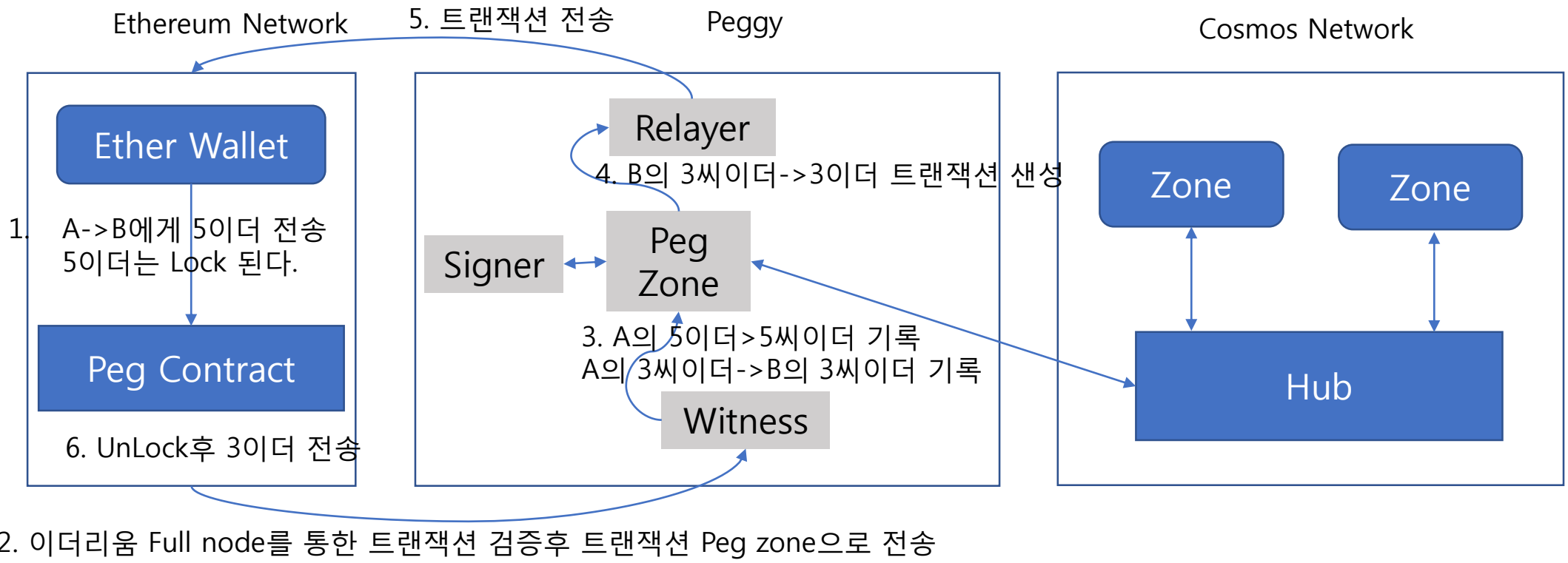
```
case
  incoming_B == nil ⇒ fail with "unregistered sender"
  destination /= (B, connection, channel) ⇒ fail with "wrong destination"
  sequence /= head(Incoming_B) ⇒ fail with "out of order"
  H_h not in T_A ⇒ fail with "must submit header for height h"
  valid(H_h, M_kvh) == false ⇒ fail with "invalid Merkle proof"
  otherwise ⇒
    set result = f_type(data)
    push(incoming_B, R{tail(incoming_B), (B, connection, channel), (A, connection, channel), result})
    success
```



인터체인의 개요

인터체인 동작 방식

◆ 블록체인-블록체인의 가치(코인, 토큰 교환)
- Two Way Pegging이란 사이드 체인과 유사한 기술을 사용할 수 있다. 코스모스 체인은 Peg-zone 이라는 기존 코인에 해당하는 '가치 ' 를 zone에 저장한다.
- 가치를 보내는 블록체인은 보내는 사람의 가치를 동결하고, 가치를 받는 체인에서는 동결이 확인되면 보낸 사람의 동일한 가치에 해당하는 '동일 가치'를 발행한다. '가치'를 받은 사람은 그걸 소비하면 '동일 가치 ' 는 소멸되고 동결된 원래의 가치의 동결이 풀리며 소비된다.

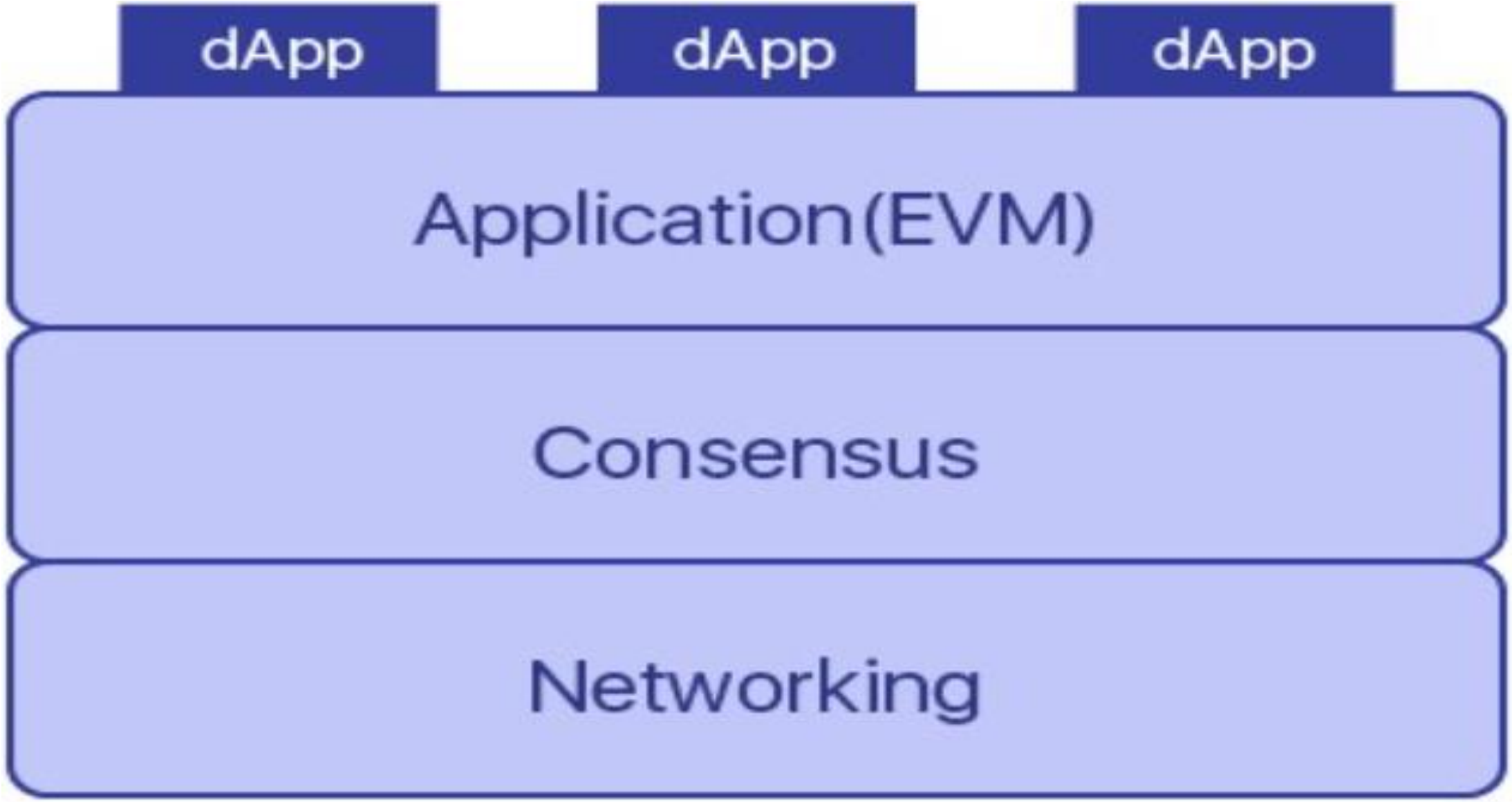


	이더	씨이더
A	0	2
B	3	0

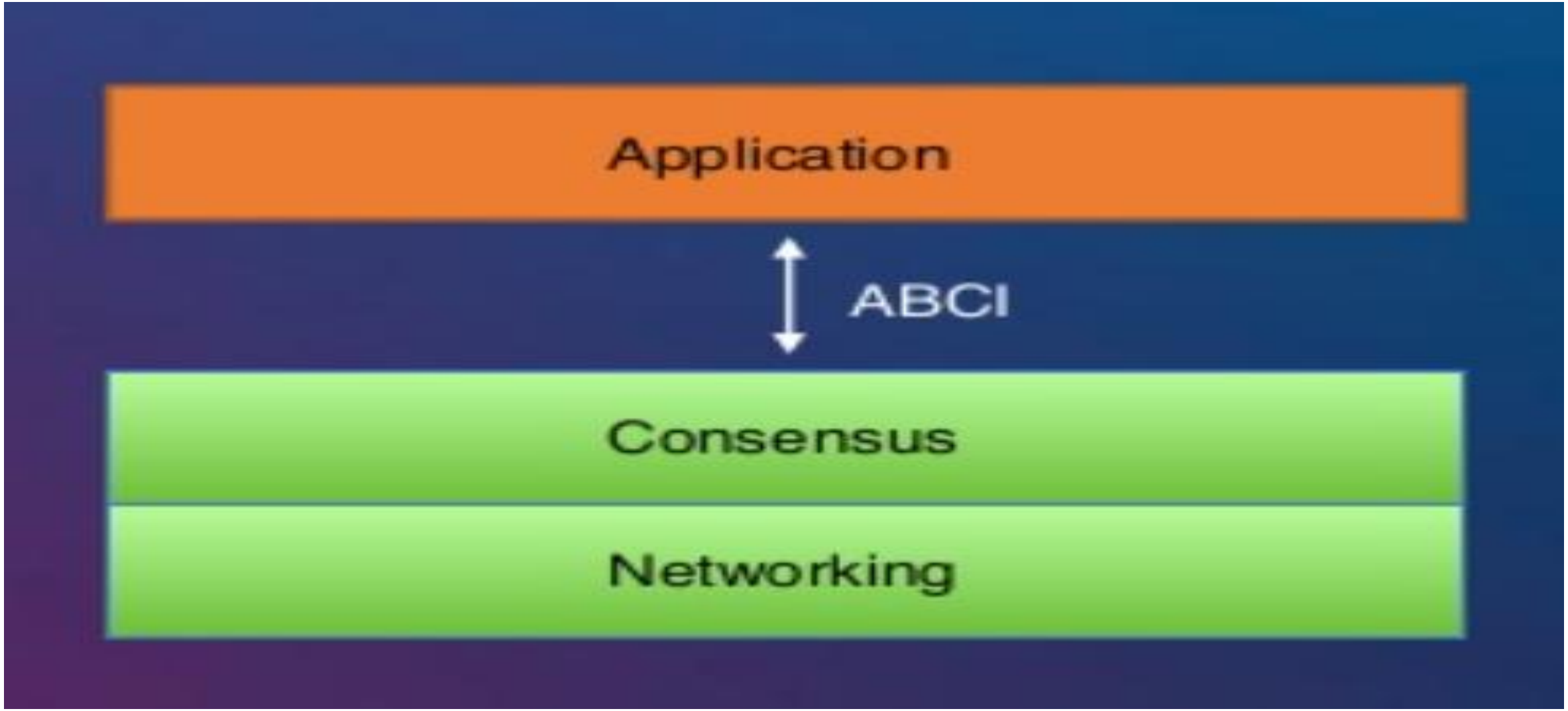

COSMOS
INTERNET OF BLOCKCHAINS

Where is a Killer dApp?

Ethereum

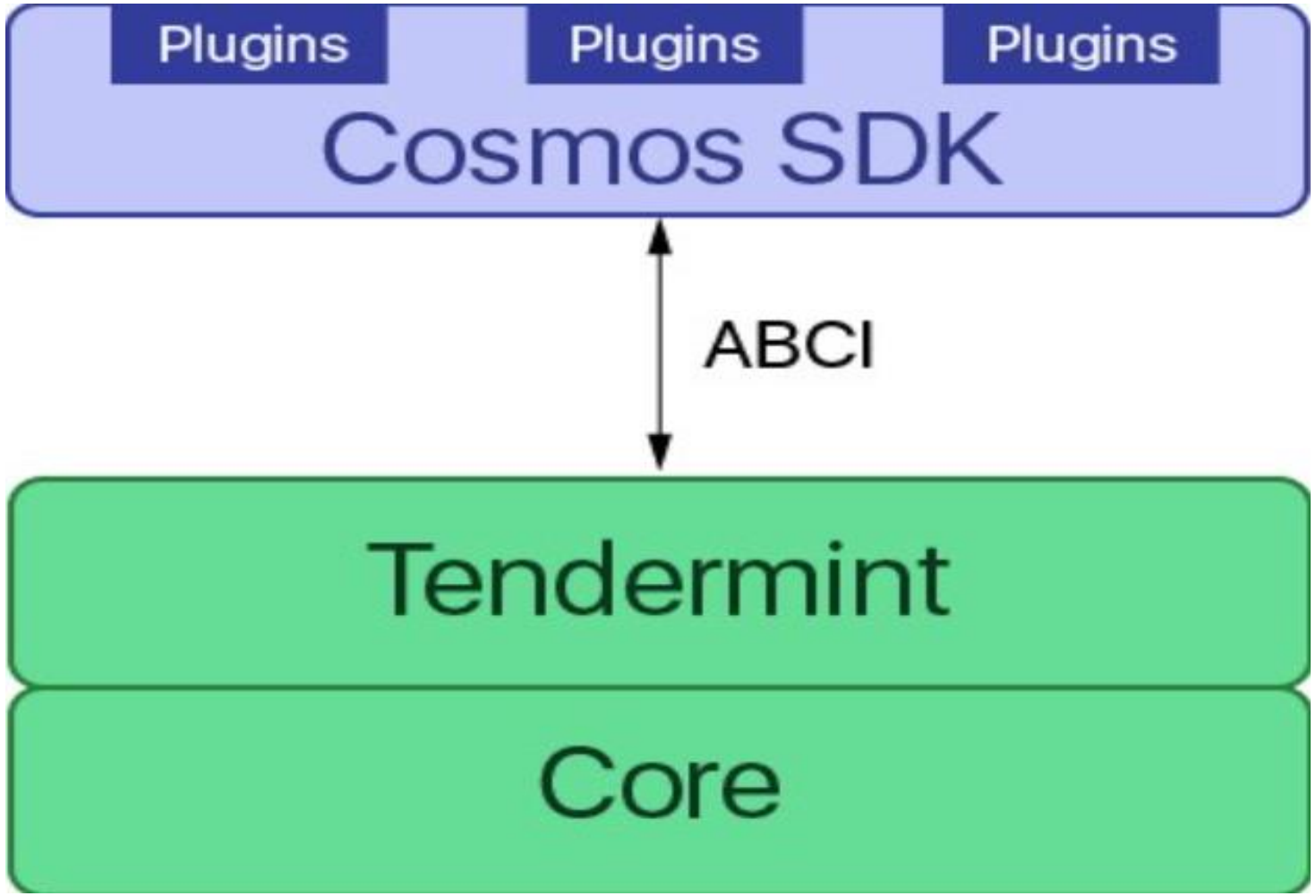


Application-Specific Blockchain
1dApp = 1 Blockchain



The benefits of Application-Specific Blockchain

- Performance
- Security
- Sovereignty
- Flexibility



Tendermint BFT “Blockchain Engine”

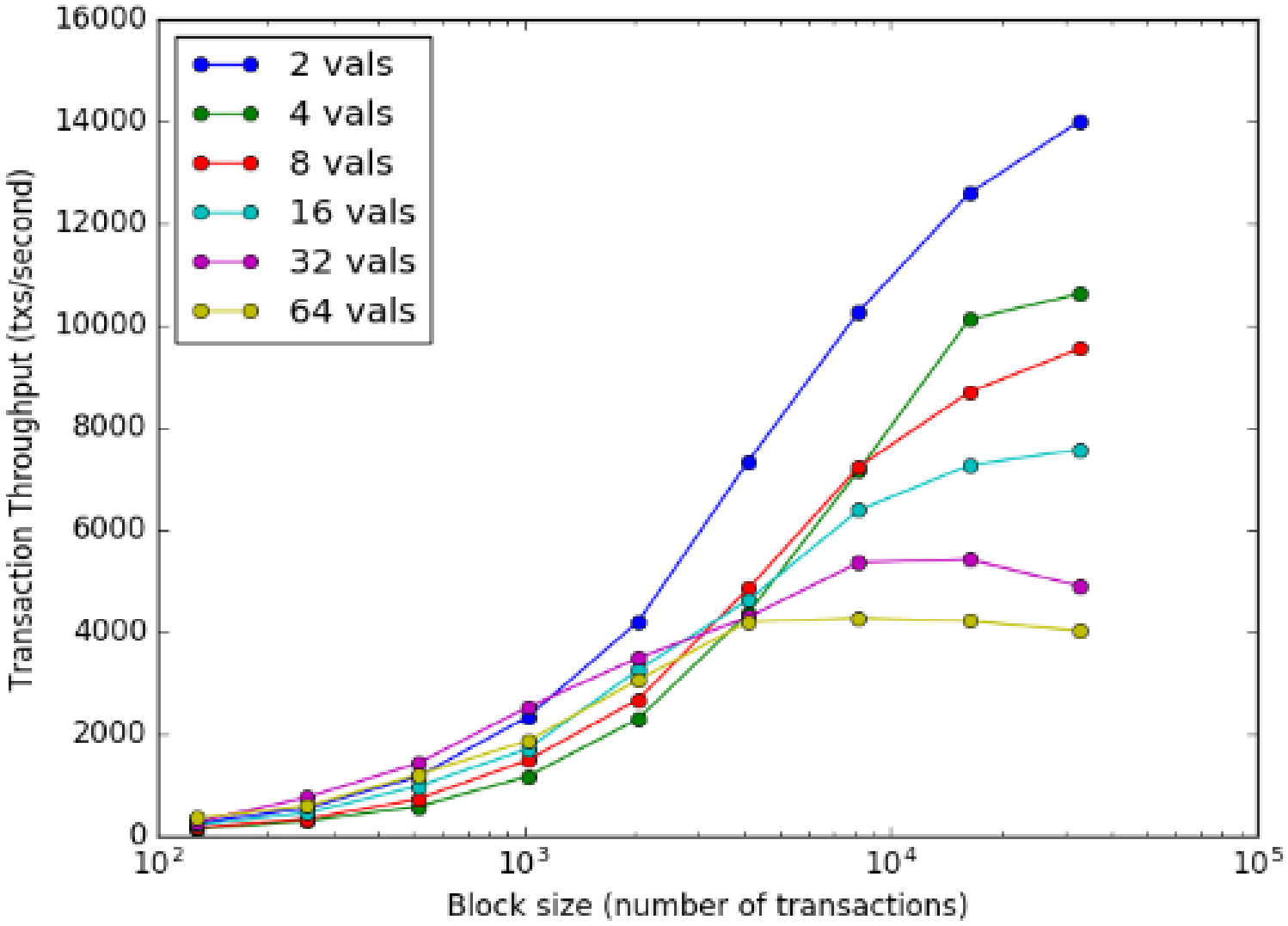
- Public or Private blockchain capable – PoS or POA
- Instant finality
- High throughput
- Fault tolerance
- Fork accountability
- Open-Source

Scalability

이더리움 연구회
korea ethereum study group

- **Vertical Scalability**

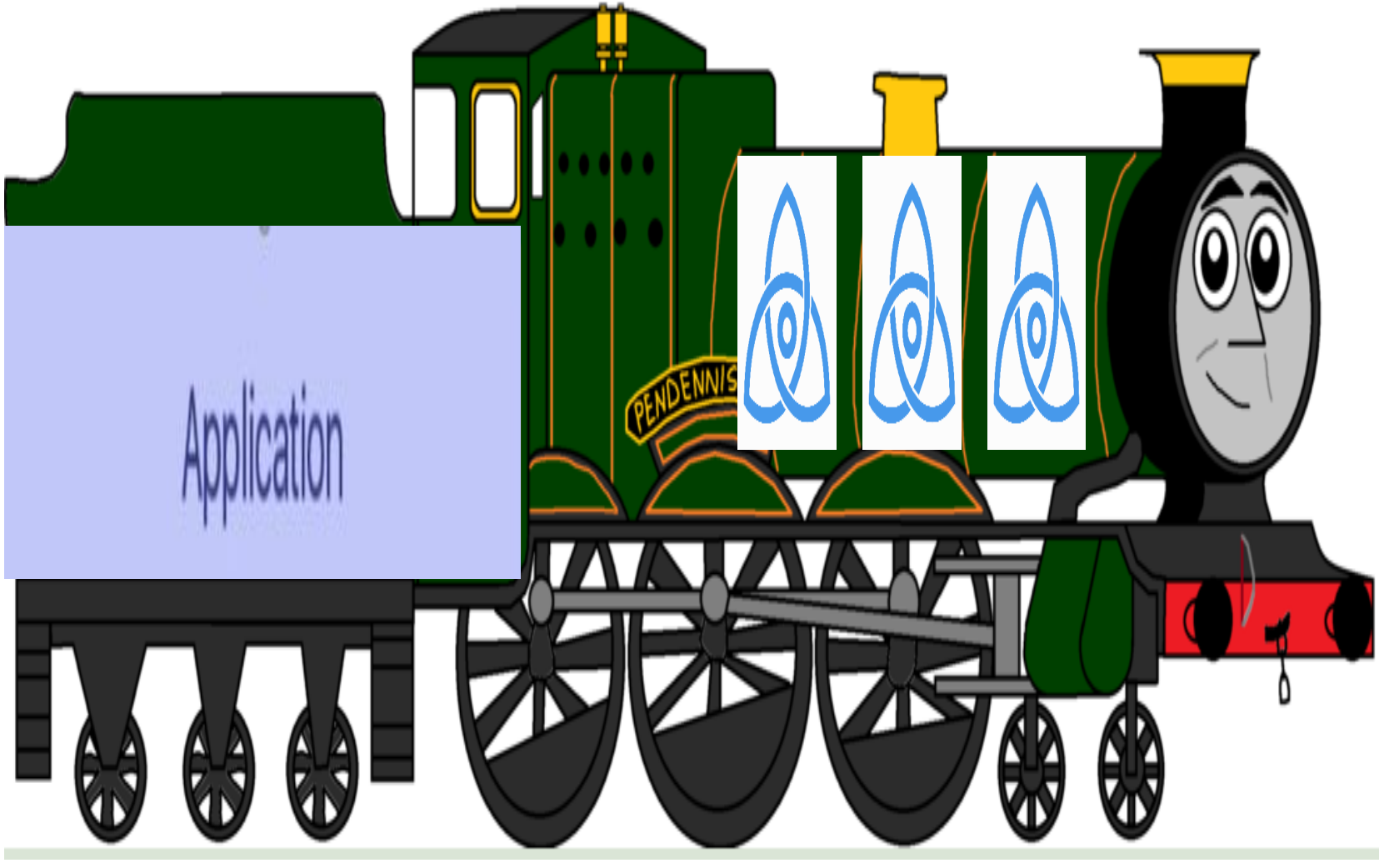
Tendermint Core can process 1000 TPS with over 100 validators on 5 different continents.



Scalability

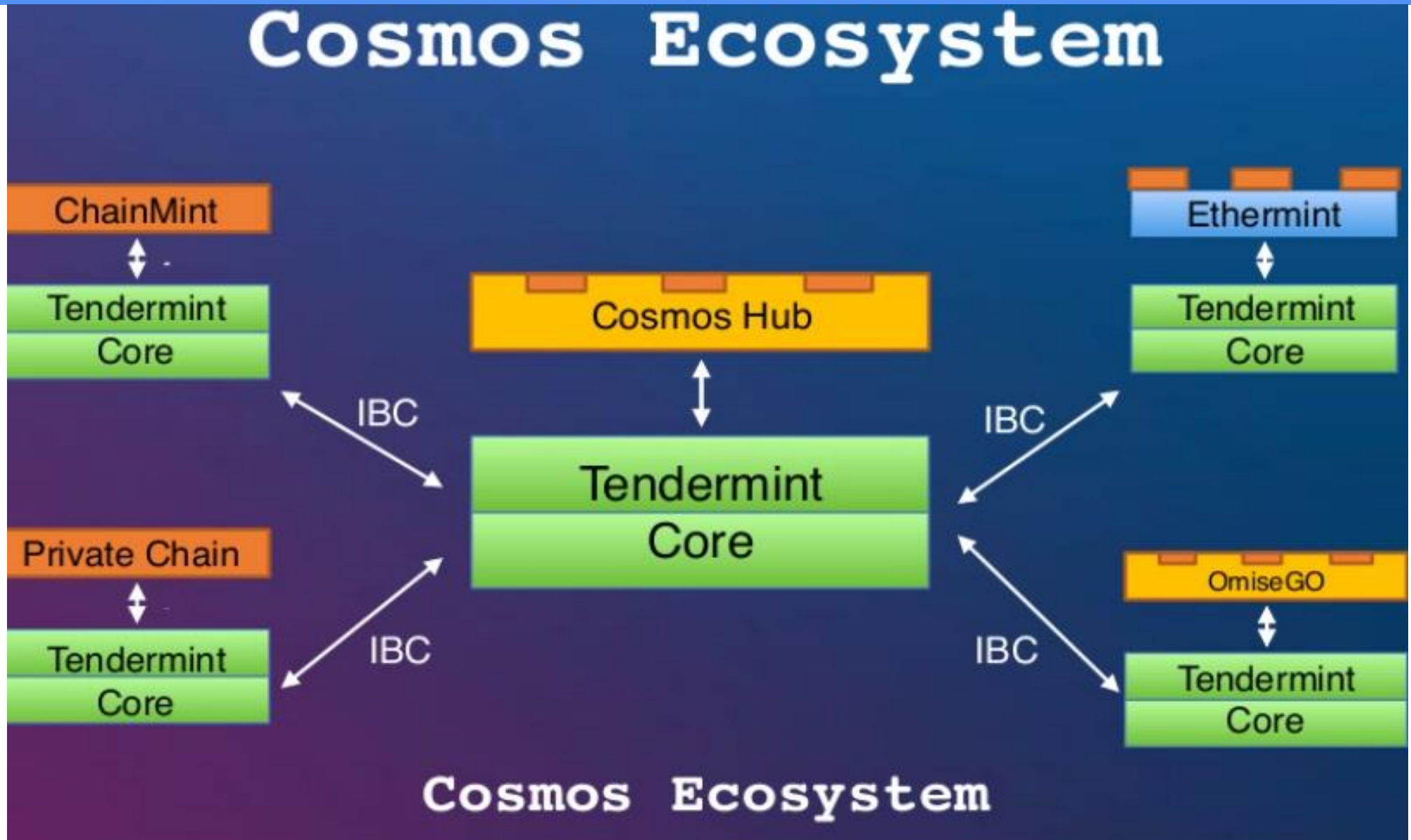
- **Horizontal Scalability**

-Multiple parallel chains running the same application and operated by a common validator set, making blockchains theoretically **indefinitely scalable**.



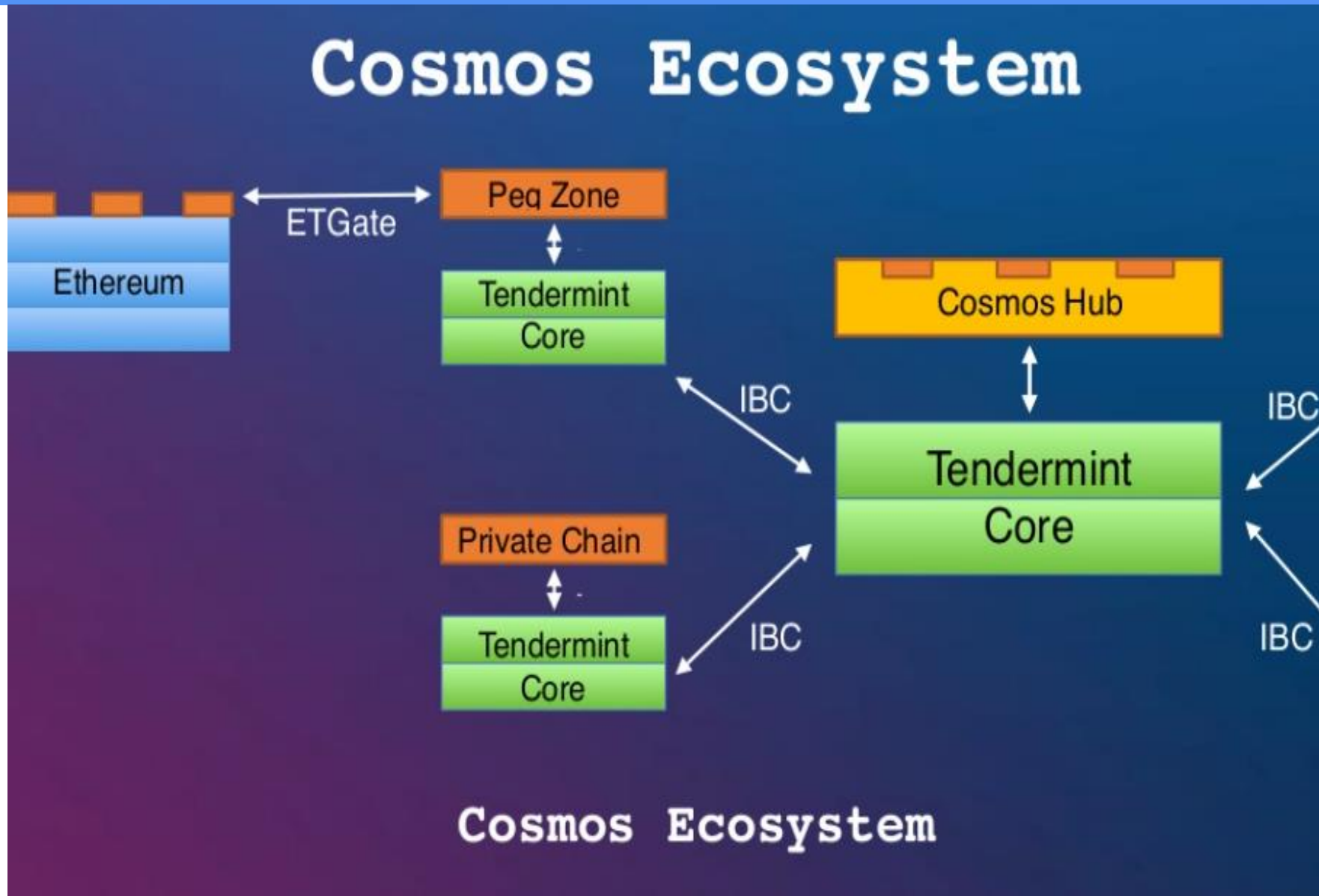
Cosmos Ecosystem

Ethermint
-Hardspoon
Omisego
Private
Chain



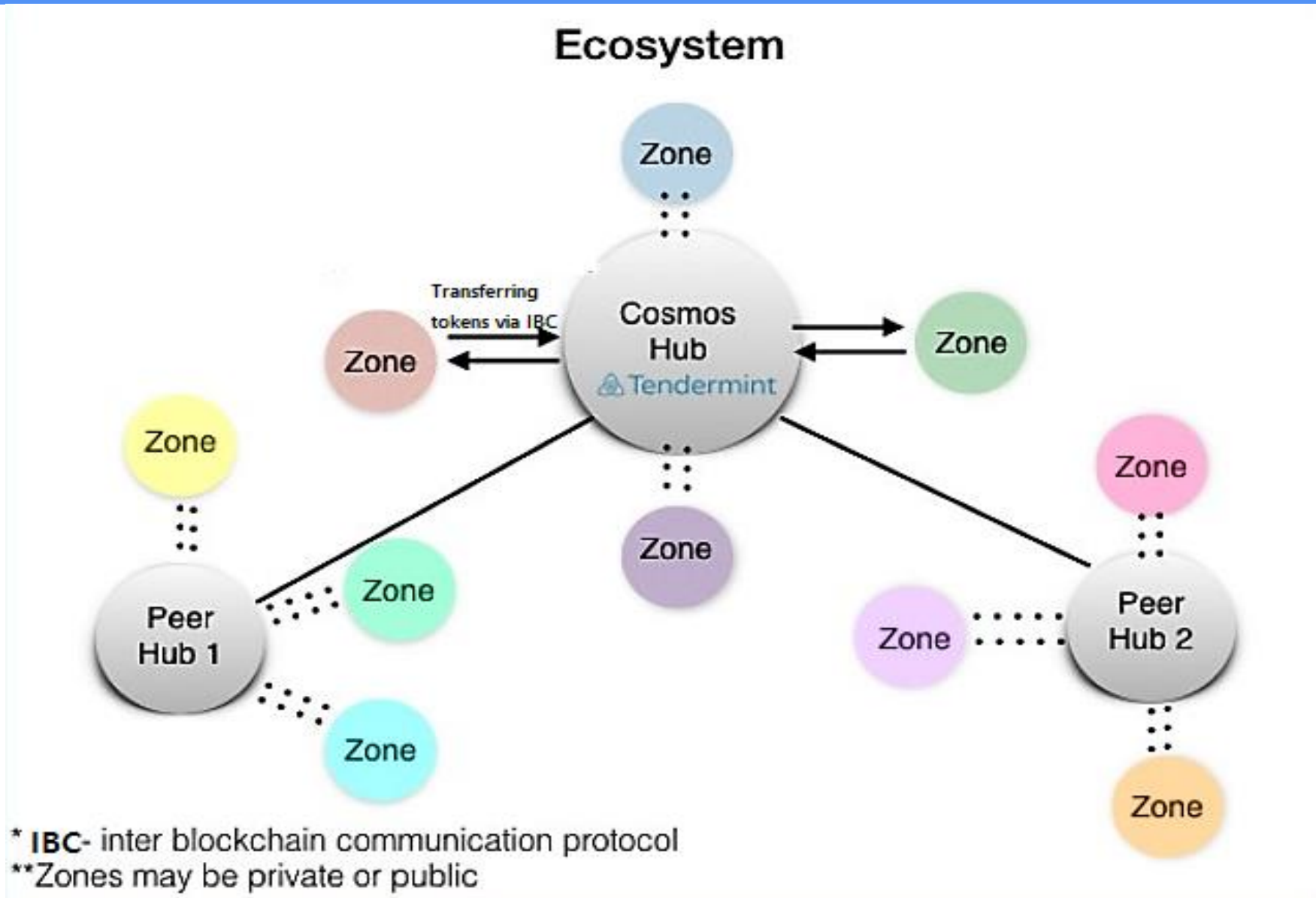
Peg Zone(Bridge Zone)

Ethereum
-Peg Zone(Bridge Zone)



Cosmos Hub & Peer Hubs

- The importance of Hub
- Interoperable(token transfer)
- Never fork; use smart contract in any language
- Each governance & constitution



Staking Token: Atom

The benefit of holding Atoms

1) (Vote)
2) (Validation)
3) (Delegation)

Validator

1) 100>>>300 over the 10 years(13%)
2) Revenue: Validator>Delegator
3) Governance
4) Slashing conditions
   -Double Spending
   -Unavailability
   -Non-voting

*Unintentional or not available

Due to regional network disruptions, power failure, or other reasons

lose “ValidatorTimeoutPenalty” (DEFAULT 1%) of its stake.

Governance

이더리움 연구회
korea ethereum study group

1. **Yea**
2. **YeaWithForce**
3. **Nay**
4. **NayWithForce**
5. **Abstain**

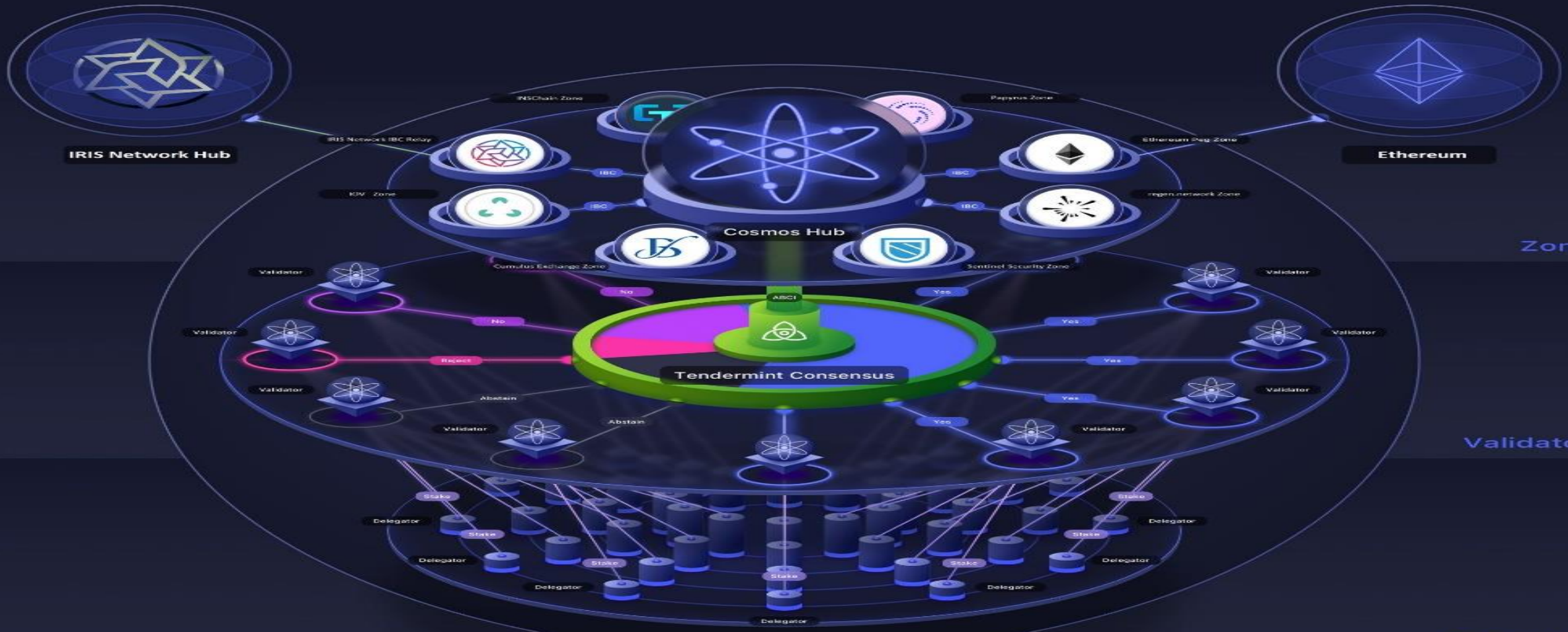
A strict majority of Yea or YeaWithForce votes required for the proposal to be decided as passed

But 1/3+ can veto the majority decision by voting "with force".

>> Everyone punished by losing **VetoPenaltyFeeBlocks** (DEFAULT 1 day's worth of blocks)

>> The party that vetoed the majority decision additionally punished by losing **VetoPenaltyAtoms** (DEFAULT 0.1%) of its atoms.

Internet of Blockchains



Testnet

이더리움 연구회
korea ethereum study group

Gaia-1000 / Oct 19 2017
Token Transaction
-코스모스 허브에서 사용자들이 토큰을 서로에게 전송 가능해짐

Gaia-2000 / Jan 31 2018
Dynamic Peer Discovery
-풀노들들과 검증인들은 PEX 리액터를 통해 연결된 피어들을 업데이트 진행

Gaia-3000 / Apr 20 2018
Decentralized Genesis
-커뮤니티가 생성한 최초의 트랜잭션이 모든 네트워크의 제네시스 파일에 추가 됨

Gaia-4000
Asynchronous Candidacy
-풀노드 운영자들은 최상위 100개의 검증인이 되어 새로운 블록을 제안할 수 있게 됨

Gaia-5000 / May 02 2018
Block Reward
-테스트넷의 검증인들은 매 블록마다 토큰 보상을 받게 됨. 검증인의 커미션을 위한 최초 지원

Gaia-6000 / June 08 2018
Liveness Slashing
-검증인이 새로운 블록을 생성하지 못하면 해당 검증인은 스테이킹한 토큰을 영구히 잃는 슬래싱 단계

Gaia-7000 / July 16 2018
Governance Testing
-테스트넷을 통한 거버넌스 버그를 찾음. 검증인 후보자들은 테스트넷에 참여하여 DDos 공격 및 방어 등 메인넷이 전 다양한 작업 진행

Present

Thank you