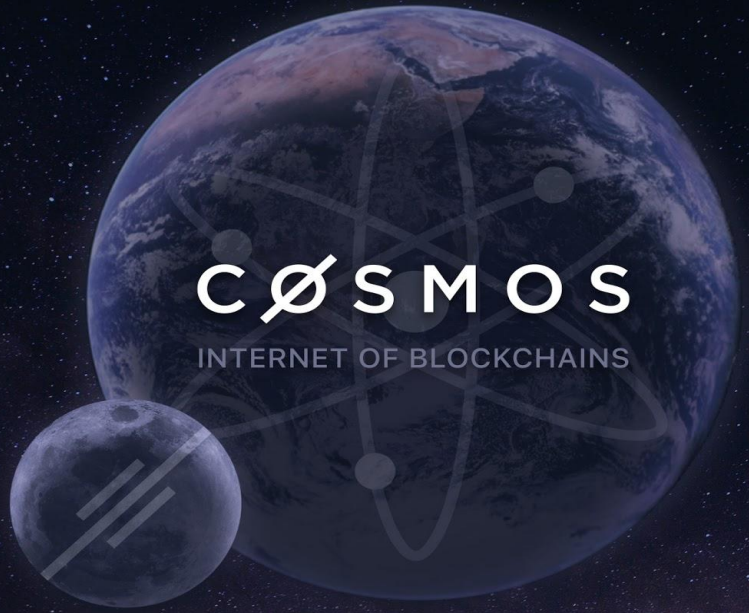


Federico Kunze

Blockchain Summit LATAM ‘18

Objetivos del Internet

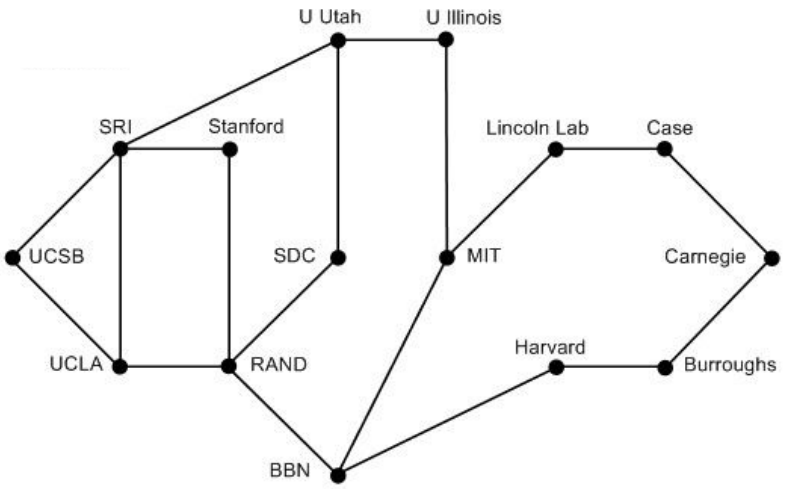
✓ Conectar múltiples servidores separados en una **única red**.

✓ **Escalar** en términos de rendimiento y geografía

✓ Capacidad de tolerar y **recuperarse de fallas**

ARPANET

ABRIL 1971

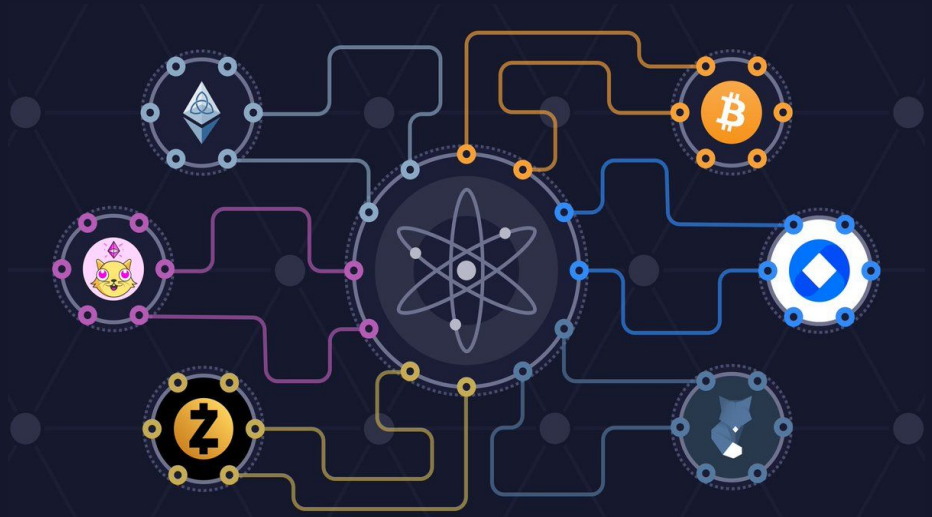


Objetivos de un Internet de *Blockchains*

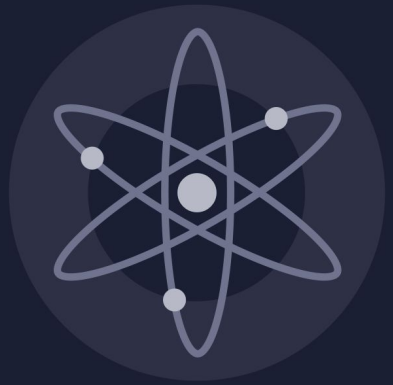
✓ Conectar múltiples ~~servidores~~ *blockchains* separados en una **única red de *blockchains***.

✓ **Escalar** en términos de rendimiento y geografía

✓ Capacidad de tolerar y **recuperarse de fallas**




COSMOS
INTERNET OF BLOCKCHAINS
https://cosmos.network
by @zcpeng



COSMOS

✓ Permitir la **transferencia de valor** entre *blockchains* con IBC y Peg-Zones

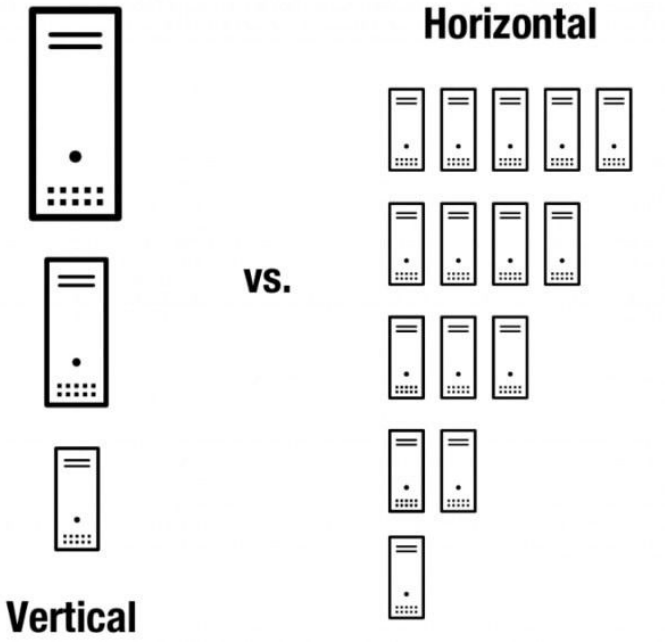
✓ Hacer las aplicaciones de *blockchain* **escalables**

✓ **Facilitar el desarrollo** de *blockchains*

Escalabilidad

1. **Escalabilidad Vertical**: Cuantas *tps* puede tolerar un *blockchain*

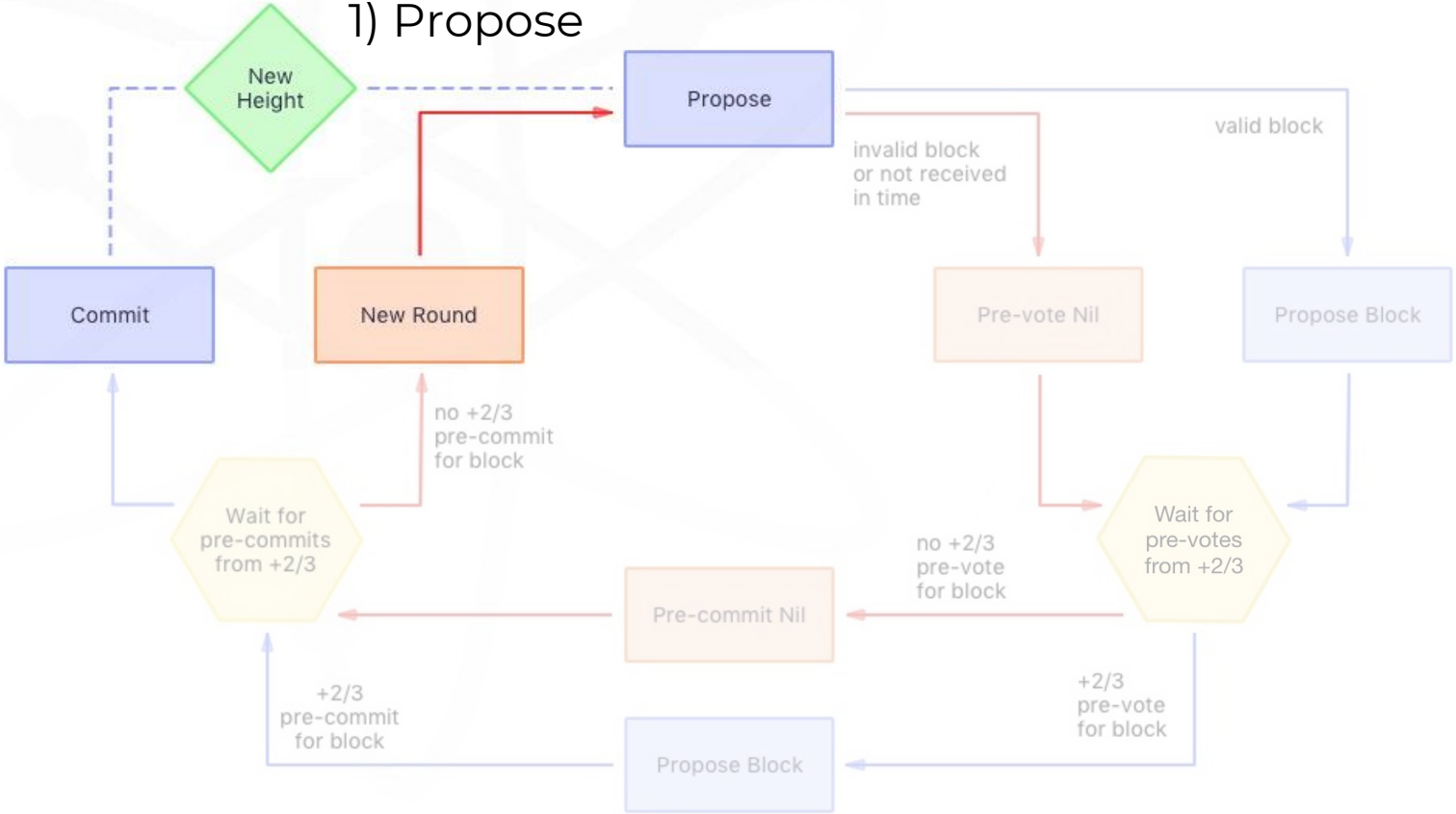
2. **Escalabilidad Horizontal**: Varios *blockchains* separados y especializados que interactúan eficientemente a través de una red

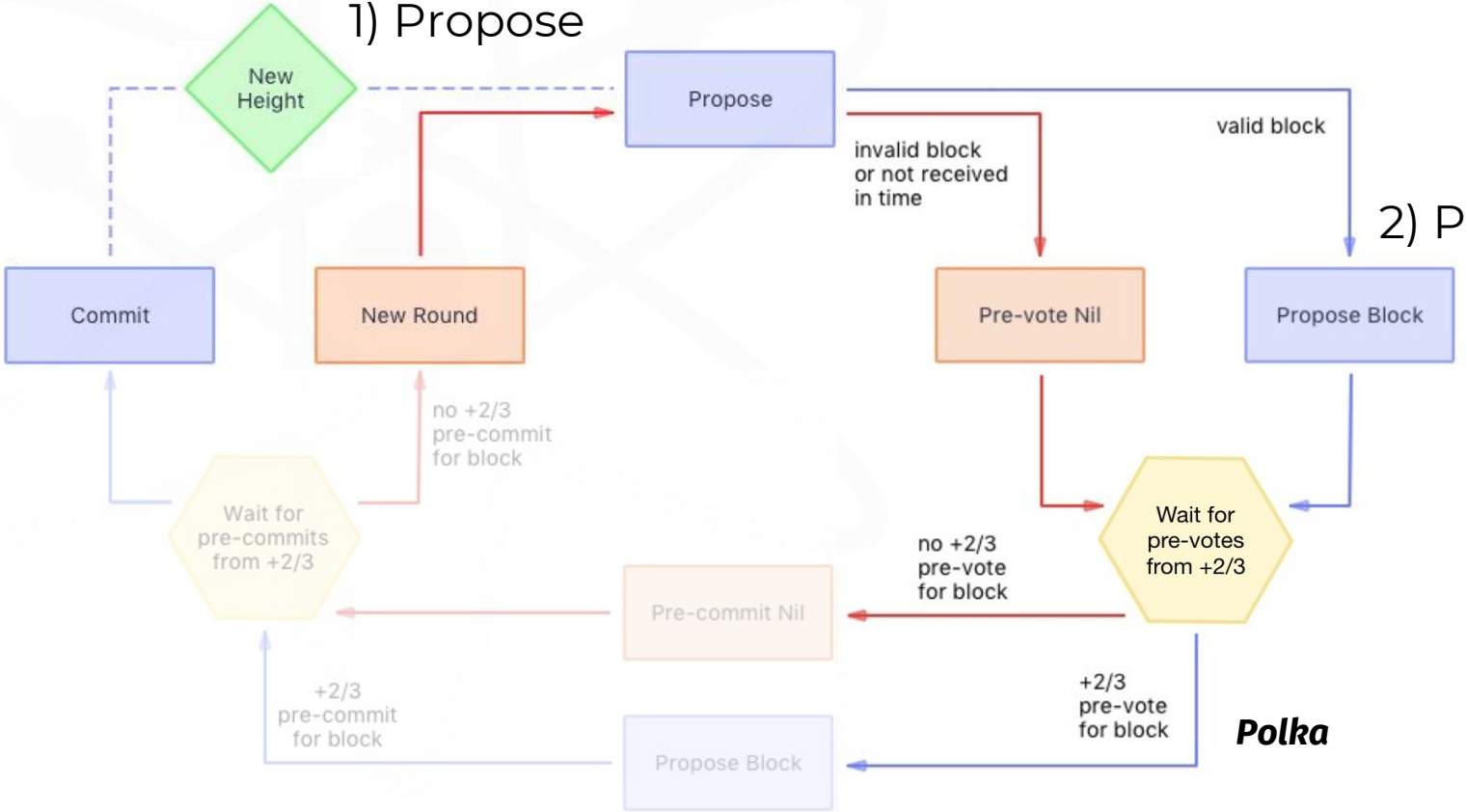


Escalabilidad Vertical

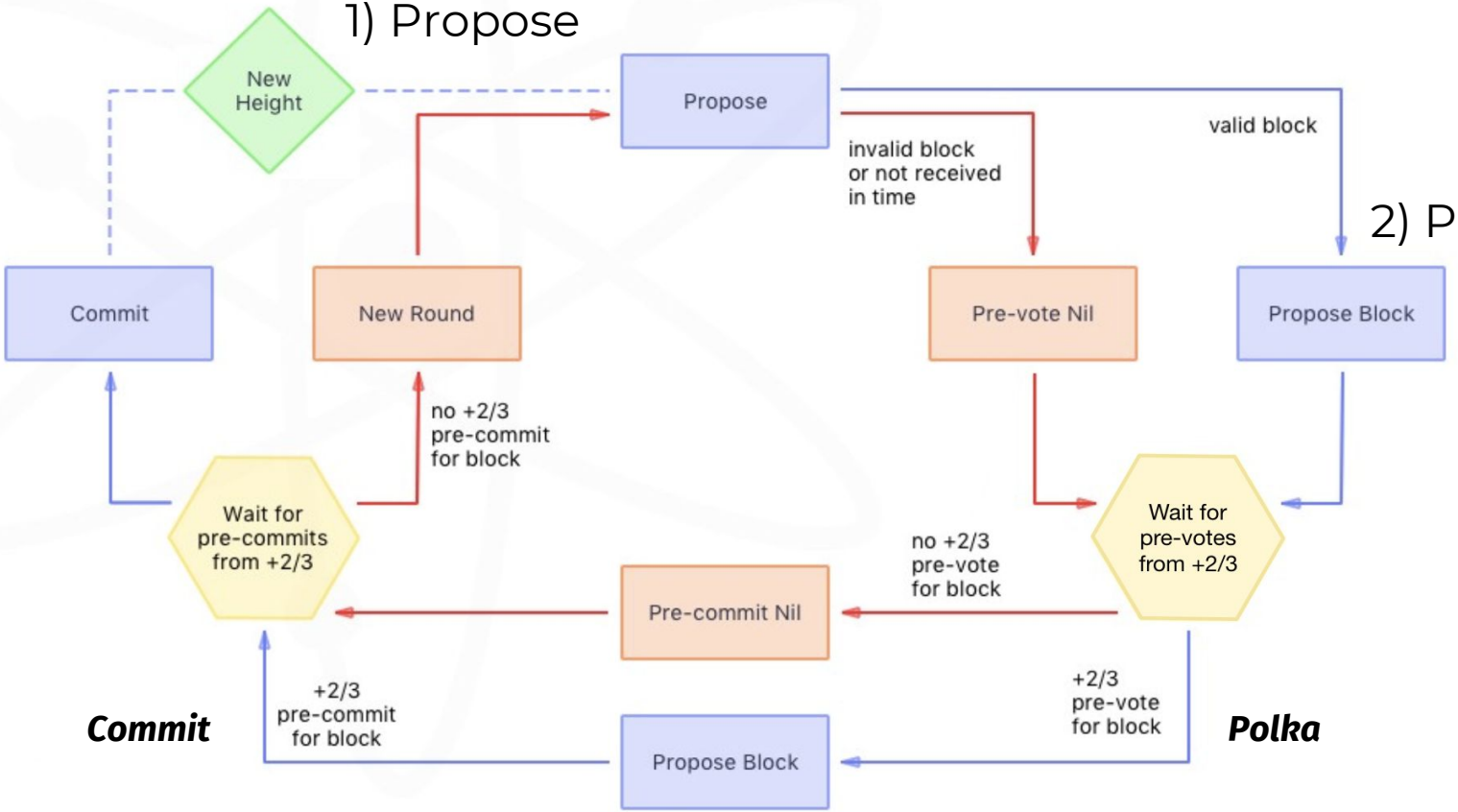
Tendermint

1) Propose


New Height
Propose
invalid block or not received in time
valid block
Commit
New Round
Pre-vote Nil
Propose Block
no +2/3 pre-commit for block
Wait for pre-commits from +2/3
Wait for pre-votes from +2/3
no +2/3 pre-vote for block
Pre-commit Nil
+2/3 pre-commit for block
+2/3 pre-vote for block
Propose Block

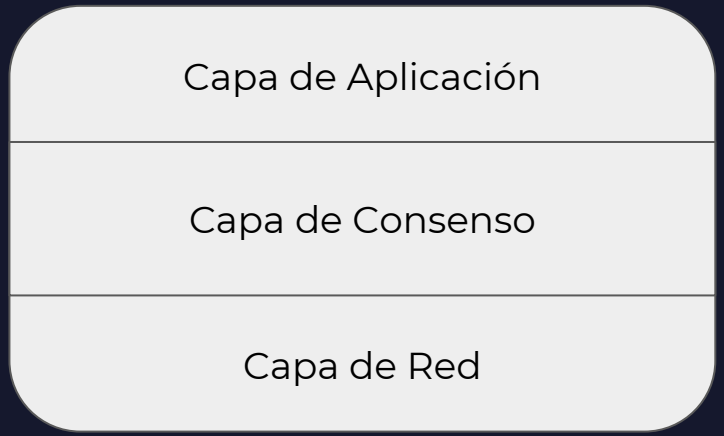


Tendermint BFT Consensus

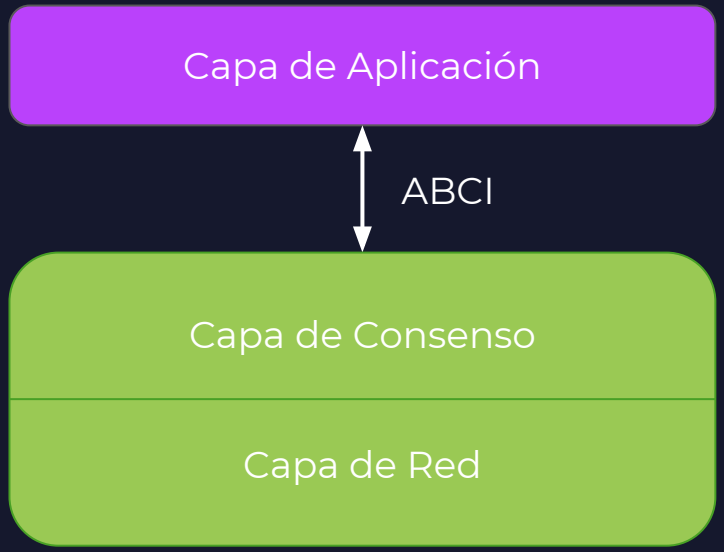


Tendermint BFT Consensus

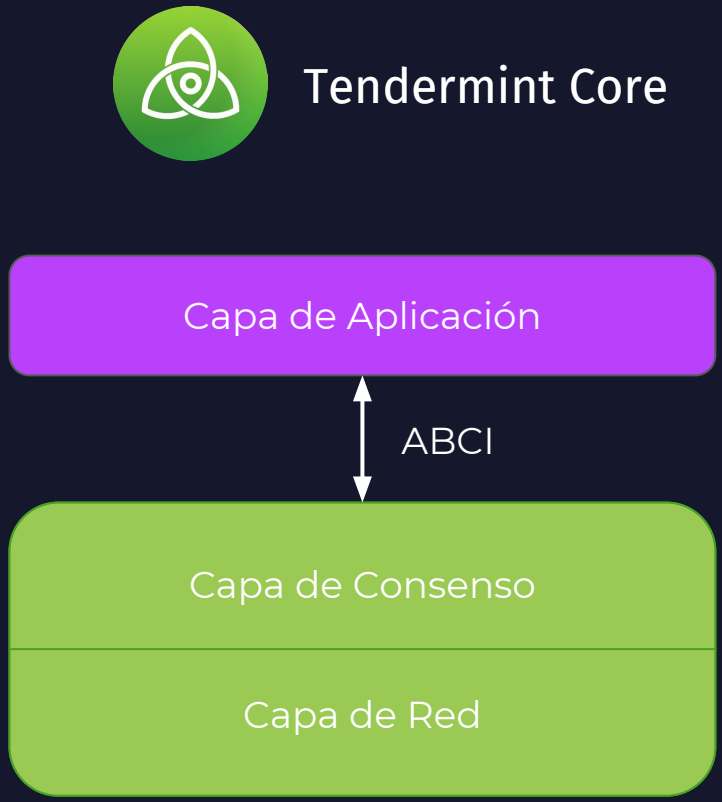
Las capas de un *blockchain*



Tendermint Core



- Consistencia por sobre disponibilidad
- **Umbral de seguridad:** ⅓ del total de poder de validadores
- Compatible con *blockchains* **Públicos/privados**
- **Finalidad instantánea**: 1–3 s dependiendo del número de validadores
- **Optimización** para cada caso de uso

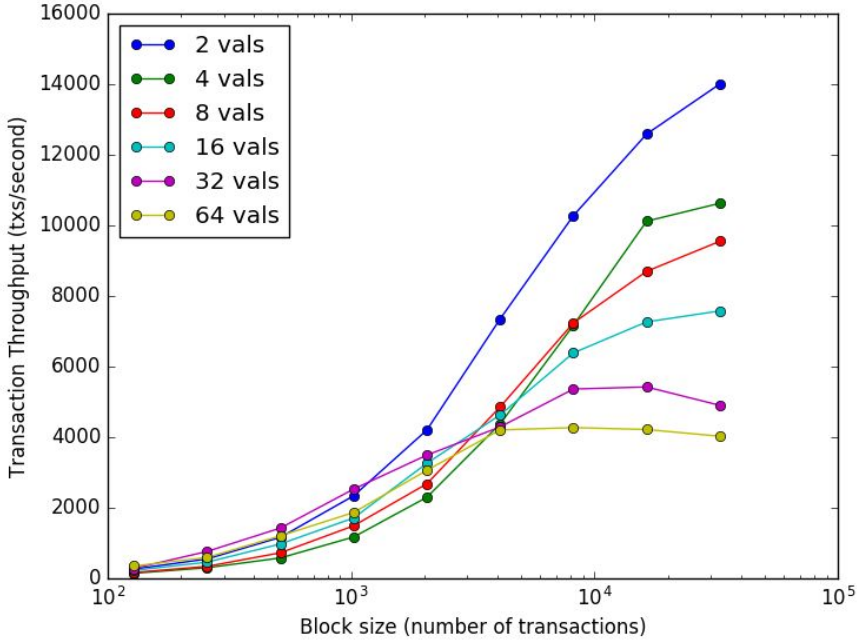



Ethermint
ethereum
ABCI
Capa de Consenso
Capa de Red
Chainmint
Chain
ABCI
Capa de Consenso
Capa de Red

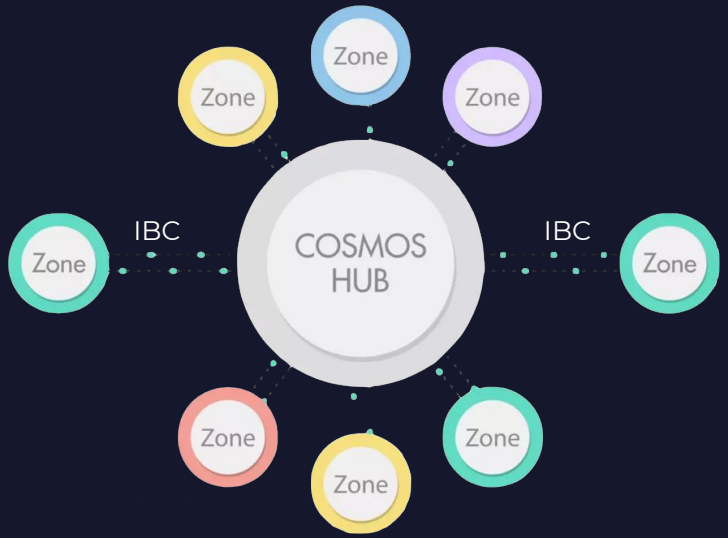
Rendimiento

	Máximo rendimiento (*tps*)
Bitcoin	3,2
Ethereum	15
Ethermint	**200**
Tendermint	**~14.000***
Visa	56.000

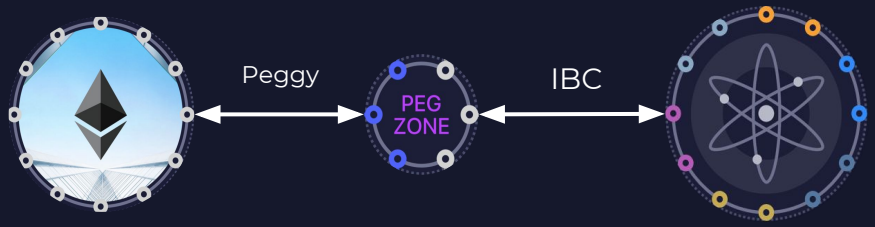
* Depende del # de validadores



Escalabilidad Horizontal



Protocolo IBC



Peg-zones

Interoperabilidad

- **Raíz de confianza** bidireccional para **prevenir *double-spending***:
  - **Set de validadores** de la otra cadena
  - ***Genesis block*** o ***Header* firmado** por una supermayoría
- *Light clients*: registran los cambios en el set de validadores

Opción 1: Conectar cada blockchain con el resto (***Handshake***)

- Alto número de conexiones: n(n-1)/2
- Alto requerimiento de confianza

Opción 2: Arquitectura de ***Spanning tree***

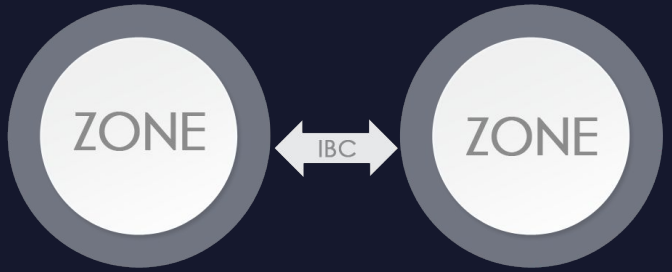
- Zonas Multi-token que conectan otras zonas

Cosmos Hub

- Multi-token **PoS *blockchain***
- **Registra el balance** total de tokens de cada zona al mantener ***light clients***
- Aísla a las demás zonas en caso de falla de una de ellas
- Comunicación con otras zonas independientes mediante un **protocolo IBC**
- Cualquiera de las zonas puede convertirse en un ***hub***

El Protocolo IBC

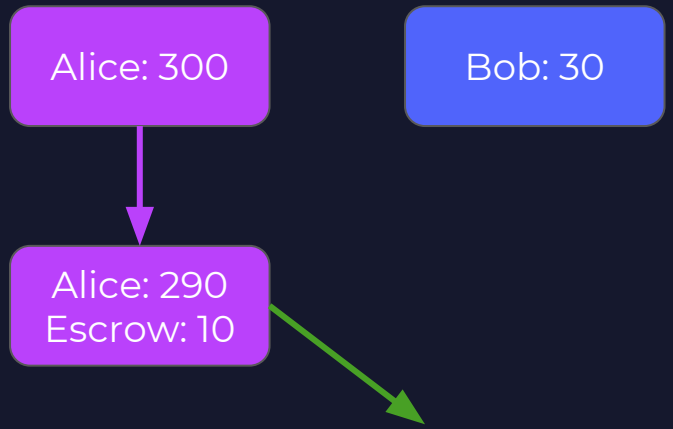
- ***IBC Protocol***: Paquetes de información transferidos de una zona a otra
- ***Merkle-proofs*** como evidencia de que la información fue enviada y recibida
  - *Block-hash* más reciente
  - Paquete ha sido publicado (*ACK*)
- **TCP/IP** para blockchains
- *Tokens* pueden ser transferidos entre zonas de forma segura y rápida sin necesidad de liquidez de intercambio entre ellas



Inter-blockchain *tx*

Zona A ⟶ **Cosmos Hub**

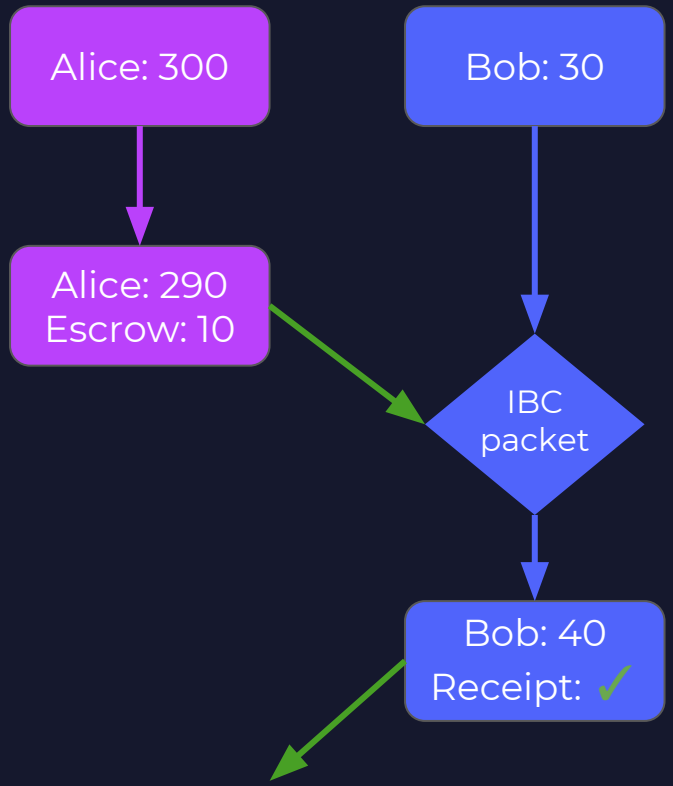
1. Alice envía 10 Atoms a la dirección de Bob en el Cosmos Hub
2. Paquete almacenado en la cola de una lista de ***outbound***
3. La tx se envía a un ***escrow*** y se realiza un *commit* al estado
4. El ***Merkle root*** se transmite al *block-hash*
5. Block-hash se propaga a los validadores
6. +⅔ validadores hacen ***commit*** del bloque con sus firmas



Inter-blockchain *tx*

Cosmos Hub

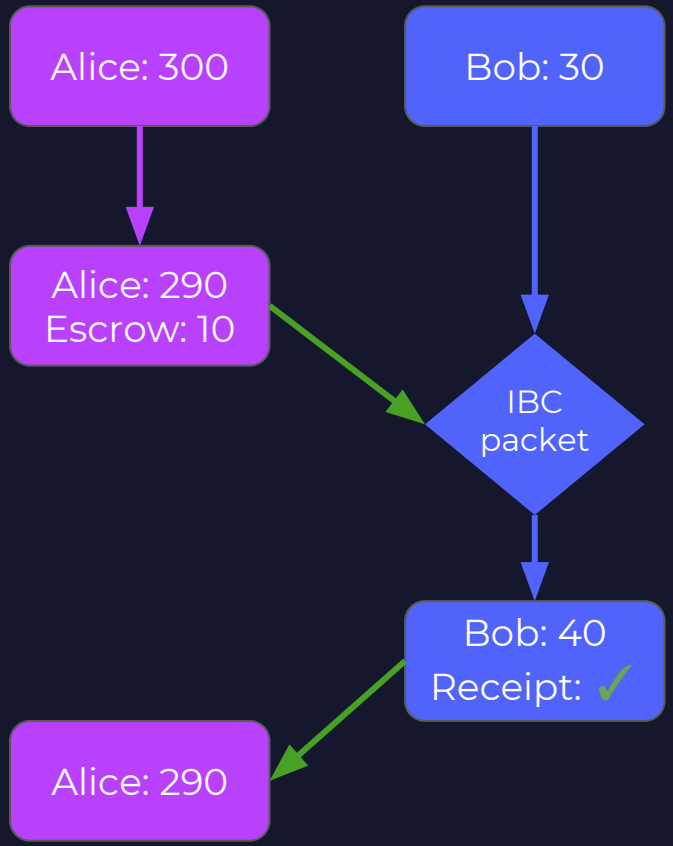
1. El paquete entra en la cola de la lista ***inbound***
2. Se comprueba si el **paquete** es **válido**:
   a. Zona A no puede enviar más Atoms de los que posee
   b. Dirección de Alice y Bob deben estar **registradas** en las cadenas
   c. ***Header*** firmado por los validadores registrados
   d. ***Merkle-proof*** válido
3. Bob recibe los 10 Atoms (si corresponde)
4. Se emite un **recibo** de la transacción



Inter-blockchain *tx*

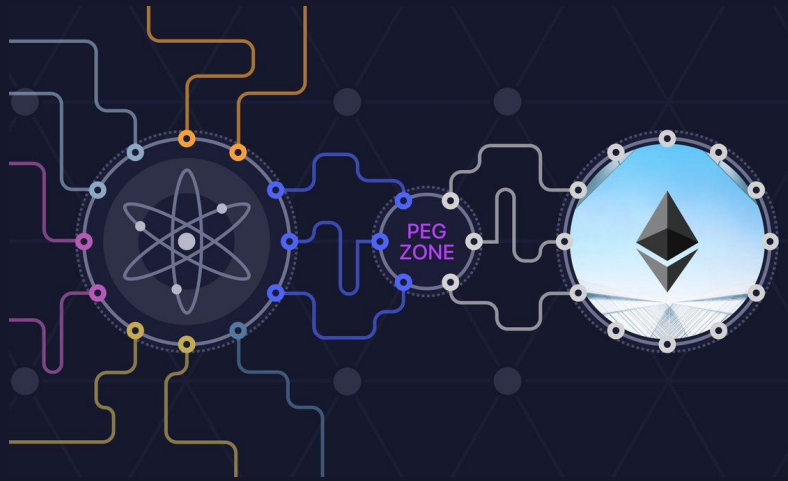
Cosmos Hub → **Zona A**

1. Zona A obtiene el **recibo** de la transacción (*ReceiptTx*) en su lista *inbound*
2. Se **verifica** la ReceiptTx con un *Merkle-proof* del Cosmos Hub
3. Se **actualiza el balance** de Alice (si corresponde)

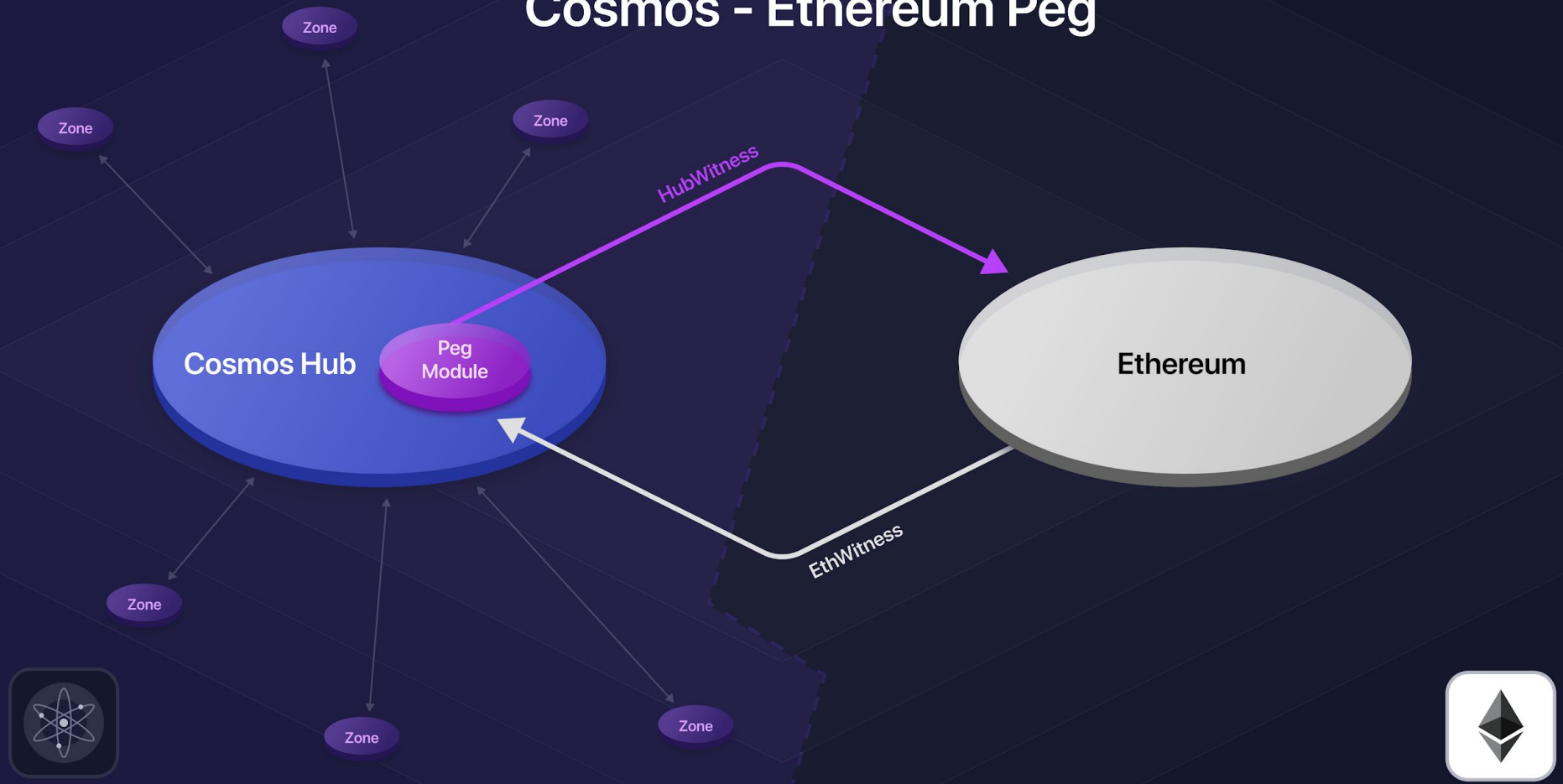


Peg Zones

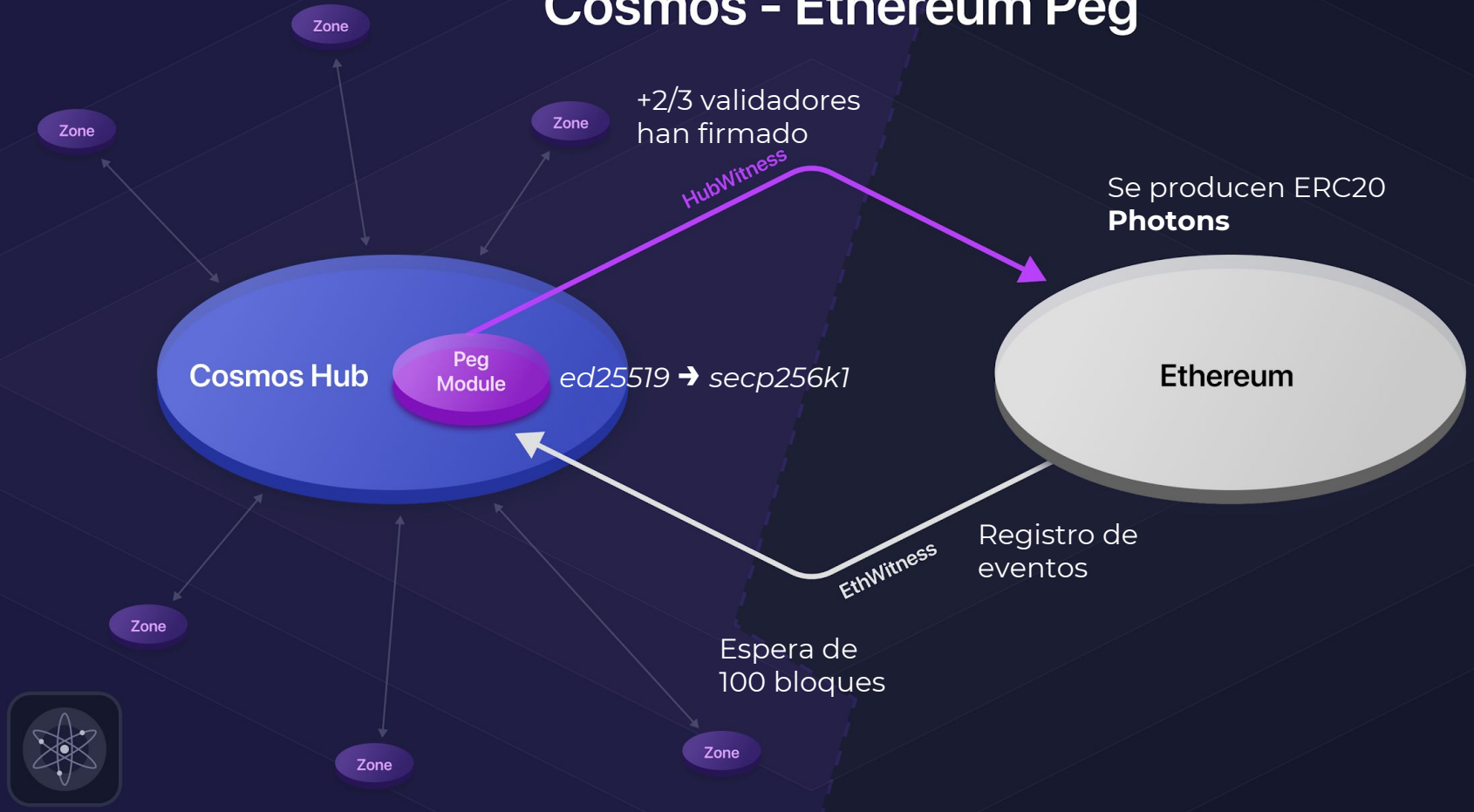
- Cadenas con finalidad probabilística
- Bitcoin y Ethereum **no tienen garantías de finalidad**
- ***Peg-zone***: *blockchain* que **conecta zonas** al imponer un umbral de finalidad a un número arbitrario de bloques para conseguir *pseudo-finalidad*
- EVM **no es compatible** con IBC: serialización, firmas y estructuras de datos



Cosmos - Ethereum Peg



Cosmos - Ethereum Peg




Escalabilidad
Diversidad
COSMOS
INTERNET OF BLOCKCHAINS
Soberanía
Seguridad
Gobernación

Soberanía

- Mantener la soberanía de cada zona de acuerdo con sus **valores e intereses**
- Cada zona tiene sus propios validadores
- Mayor seguridad que solo incentivos económicos
- *Blockchains* privados pueden interoperar con cadenas públicas

Gobernación

- Cada zona tiene su propia **constitución y mecanismo de gobernación**
- Validadores y delegantes **votan propuestas**
- **Votar enmiendas** a la constitución que define las políticas del Cosmos Hub

Seguridad

- **BFT**: Tolera hasta ⅓ nodos maliciosos
- **Seguridad acumulada**: validadores son castigados en todas las zonas que pertenecen
- ***Slashing***: doble firma, no disponible, no vota
- **Congelado de depósitos**: ataques de largo alcance
- **Recompensa de hackeo**: incentivo para hackear validadores

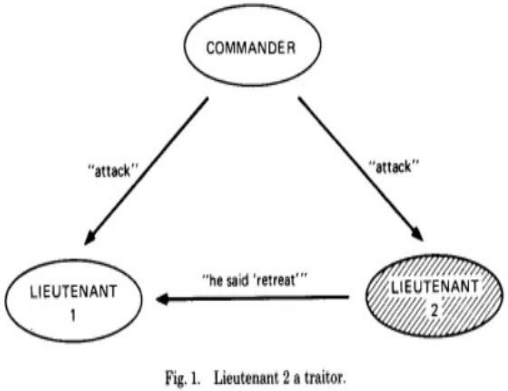


Fig. 1. Lieutenant 2 a traitor.

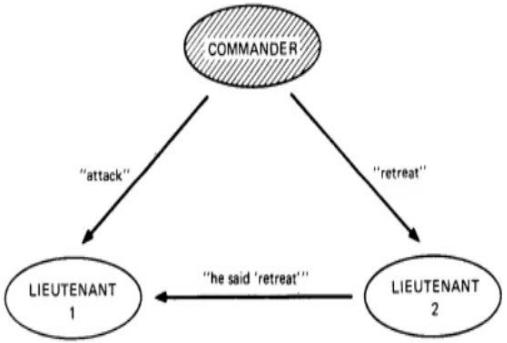
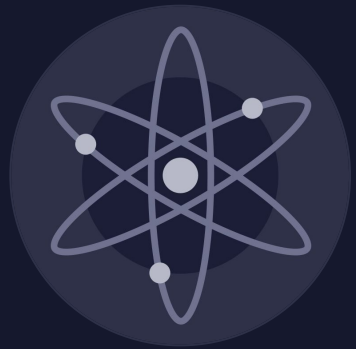


Fig. 2. The commander a traitor.

Seguridad

- La utilidad económica de un PoS *token* es doble: ***staking* y transaccional**
- Un *token* ➔ menos incentivos para *staking*
- **Menor seguridad de la red**
- Solución: dos *tokens* diferentes para *staking* y comisiones



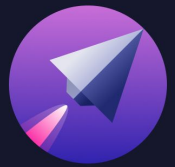
Herramientas de desarrollo

COSMOS
Hub

COSMOS
SDK

Ethermint

Tendermint
Core

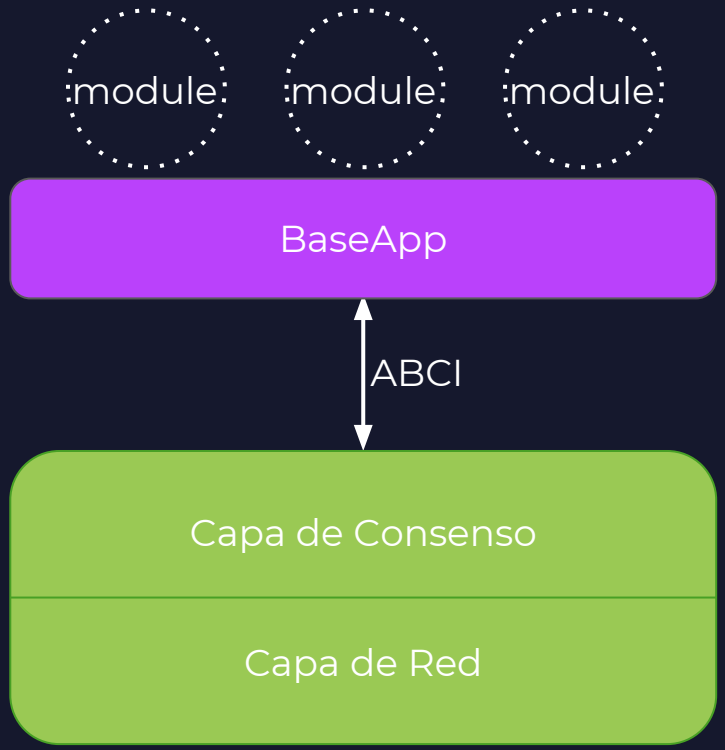


COSMOS
Voyager

lotion

Cosmos-SDK

- Plataforma para construir *multi-token* PoS *blockchains*
- **Apps personalizadas** fáciles de programar en el ecosistema Cosmos
- *Framework*: "`npm` para ***blockchains***"
- **Módulos** definen funcionalidades, lógica, estado de la app y transiciones
- Actualmente en el lenguaje **Go**



Módulos disponibles

✓ **Auth**: cuentas y autenticación de firmas

✓ **Bank**: transferencia de tokens

✓ **Governance**: propuestas y votaciones

✓ **Staking**: PoS, *bonding*, comisiones, inflación, *etc.*

✓ **IBC**: interoperabilidad

lotion

- Crear apps de blockchain en **Javascript**
- **Tendermint BFT** mediante protocolo ABCI
- **Interoperable** con otros *blockchains*
- **Tutorial**: https://www.pscp.tv/w/1lDxLajgldRKm

Making a cryptocurrency

Let's make a new coin on lotion.

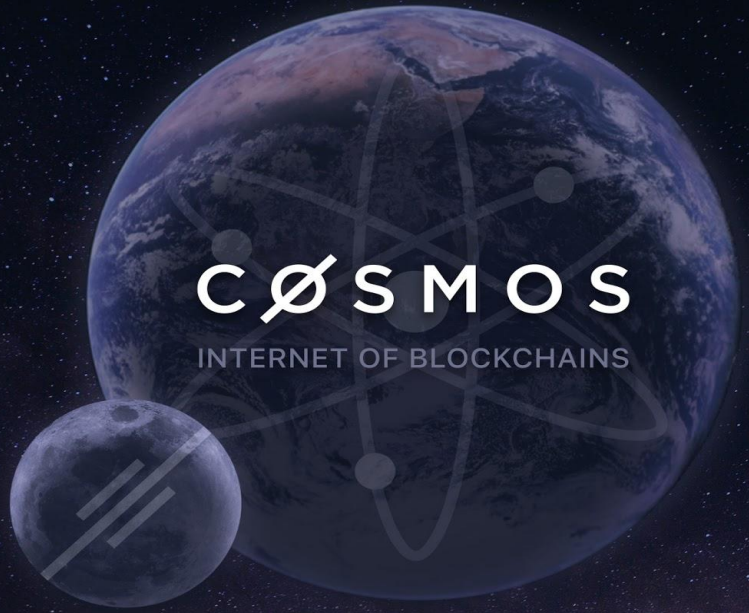
Here's the code we're going to end up with:

```
let secp256k1 = require('secp256k1')
let { randomBytes } = require('crypto')
let createHash = require('sha.js')
let vstruct = require('varstruct')
let axios = require('axios')

let TxStruct = vstruct([
  { name: 'amount', type: vstruct.UInt64BE },
  { name: 'senderPubKey', type: vstruct.Buffer(33) },
  { name: 'senderAddress', type: vstruct.Buffer(32) },
  { name: 'receiverAddress', type: vstruct.Buffer(32) },
  { name: 'nonce', type: vstruct.UInt32BE }
])
```

To the Cosmos

To the Cosmos



federico@tendermint.com

https://cosmos.network

https://tendermint.com