



Chainlink

Moneda Digital Descentralizada (72.89)

Grupo 1

Atar, Ariel

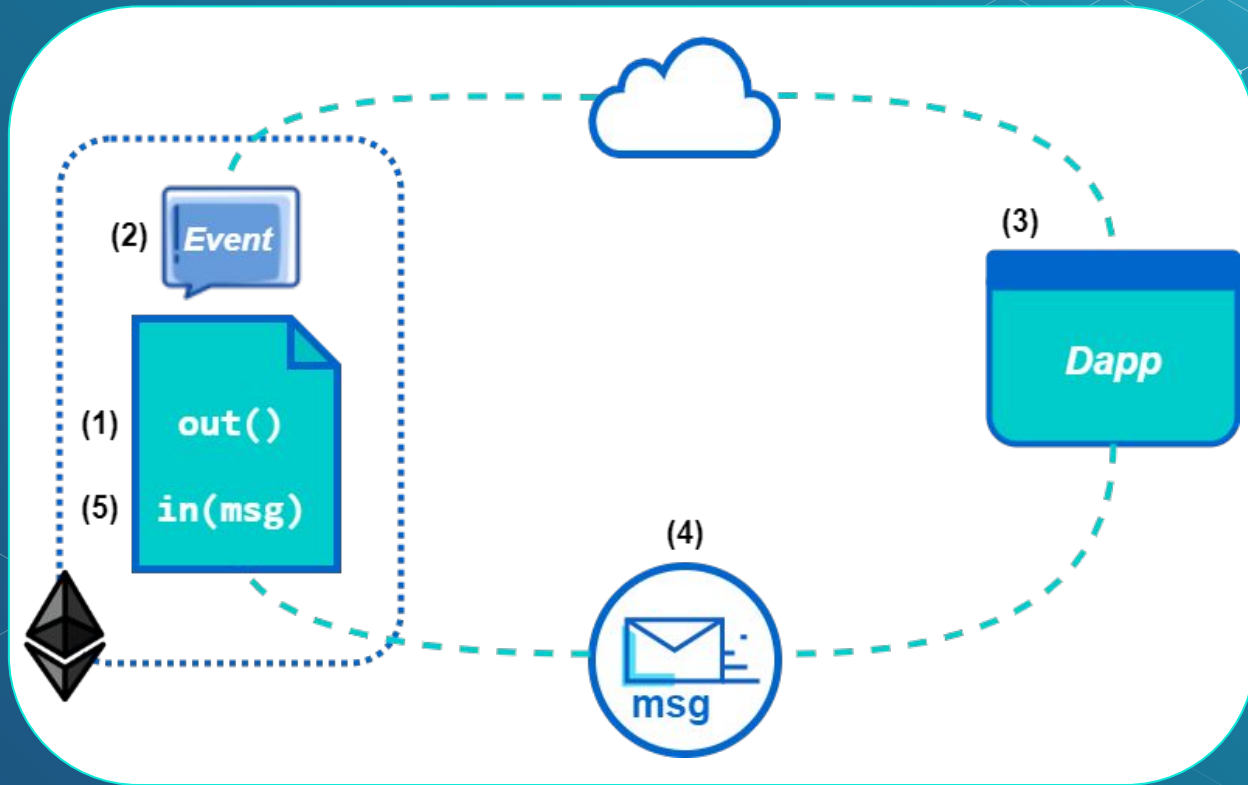
Balfour, Oliver

Golmar, Agustín

INTRODUCCIÓN

- ◇ Para realizar smart contracts **más complejos** se necesita **consultar fuentes externas** a la blockchain.
- ◇ Los **canales de comunicación** entre lo que sucede on-chain y lo que sucede off-chain son **limitados** (la blockchain es un sistema cerrado).
- ◇ **Aumentar las capacidades** de los smart contracts **aceleran su adopción** en la economía actual.

ARQUITECTURA

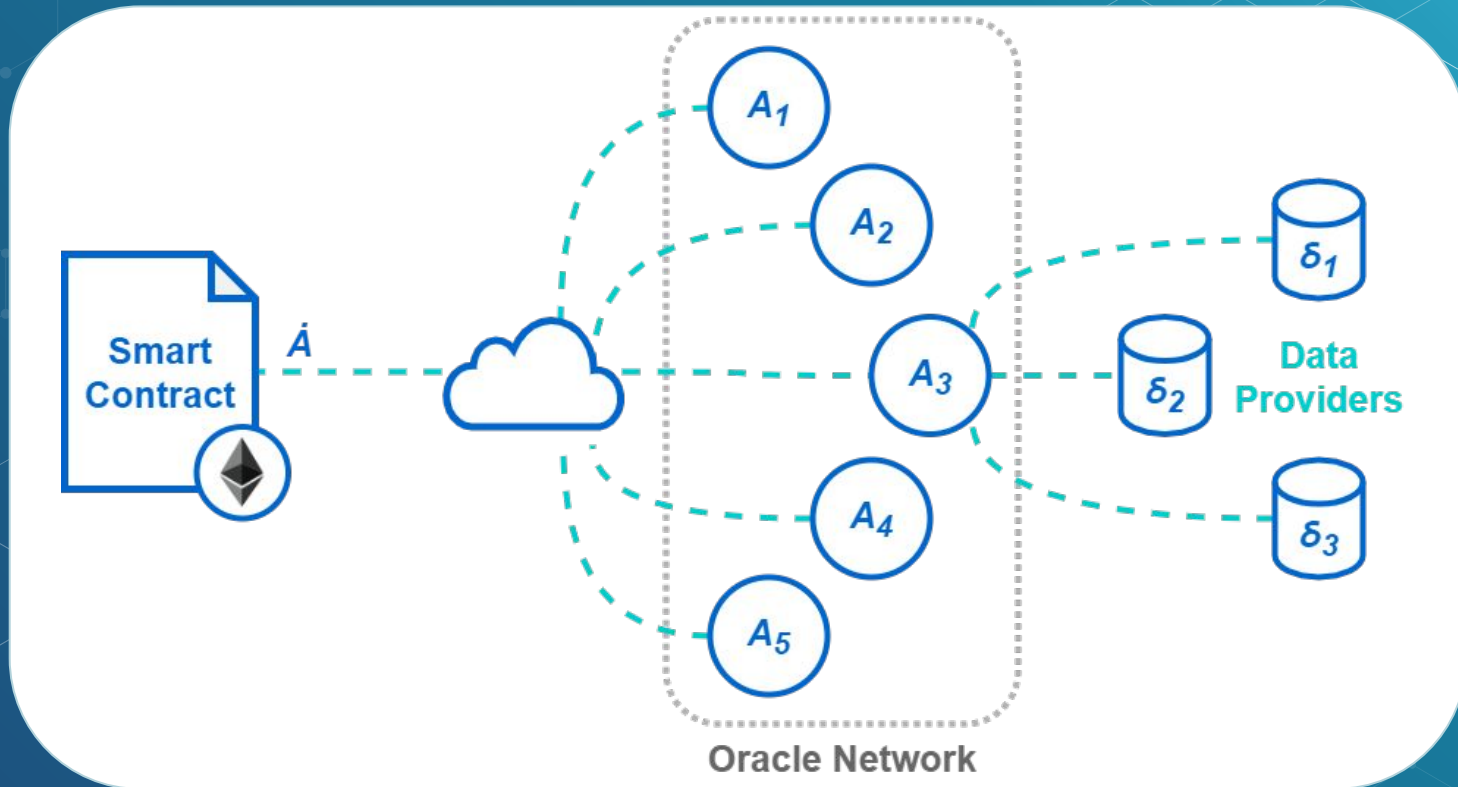


EL PROBLEMA

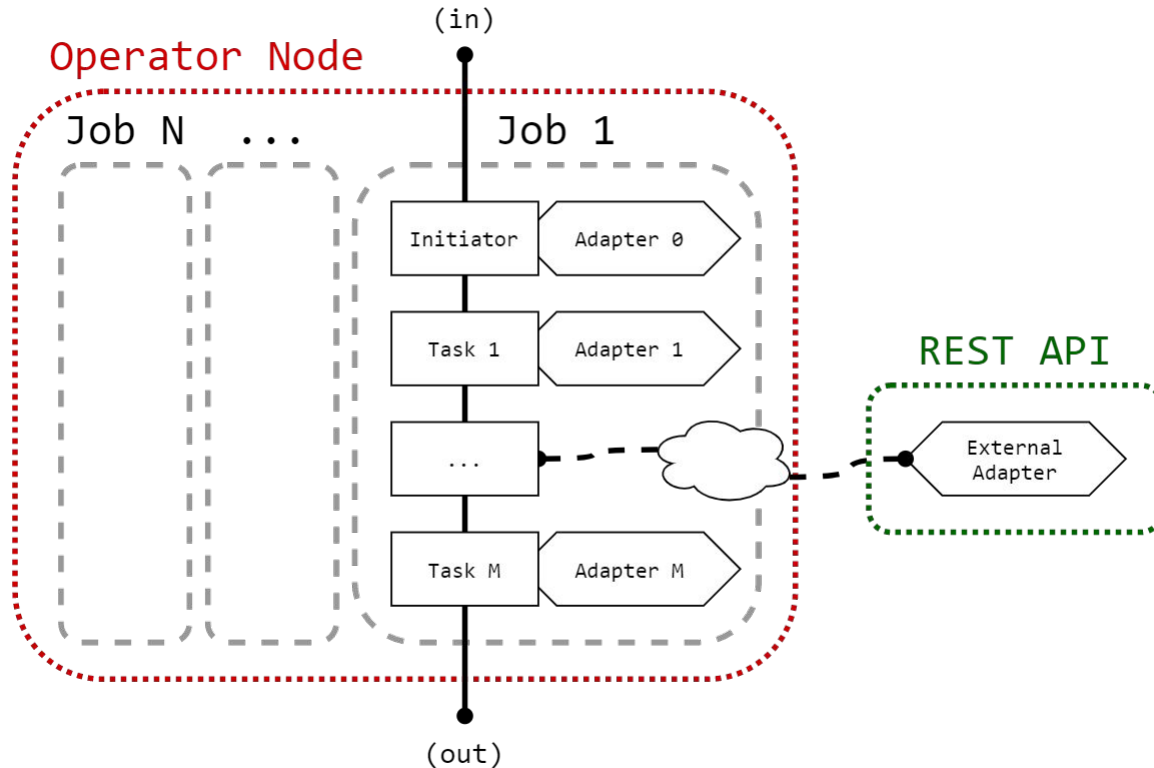
- ◇ La blockchain no solo debe operar en forma **descentralizada** sino también asumir que las operaciones son realizadas en un **ambiente hostil** (fallas bizantinas).
- ◇ Además, los servicios externos deben garantizar la propiedad de **pseudo-anonimidad**.

El **middleware** debe utilizar una **tecnología similar** a la de la **blockchain** para garantizar estas propiedades (consenso + zero trust).

LA APUESTA DE CHAINLINK



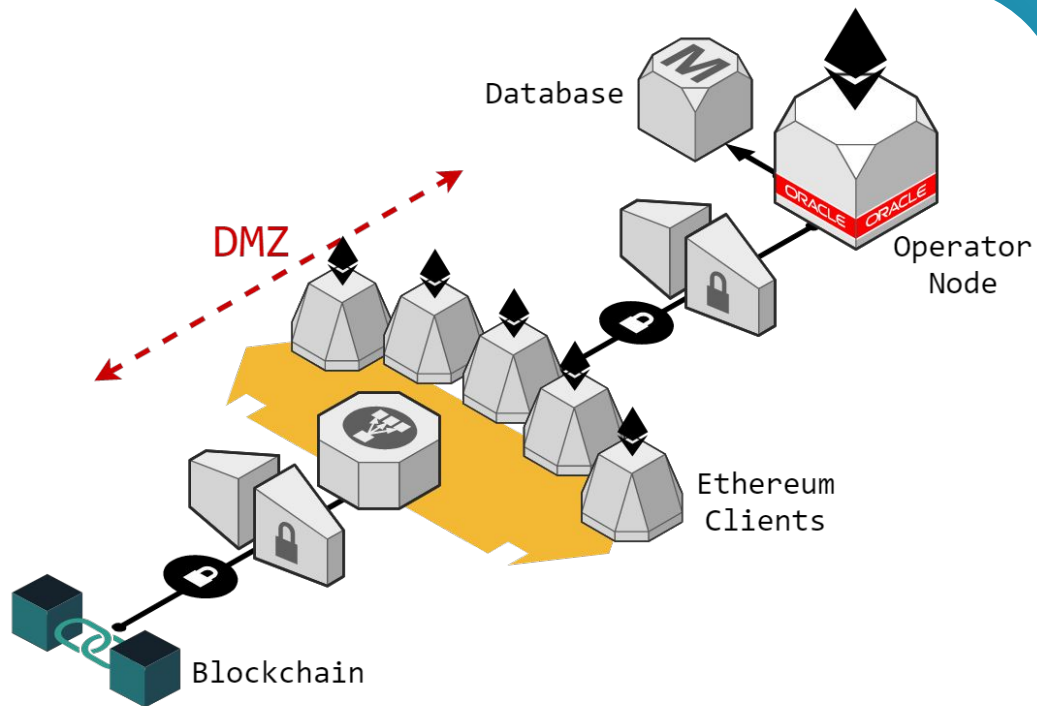
BAJO ACOPLAMIENTO



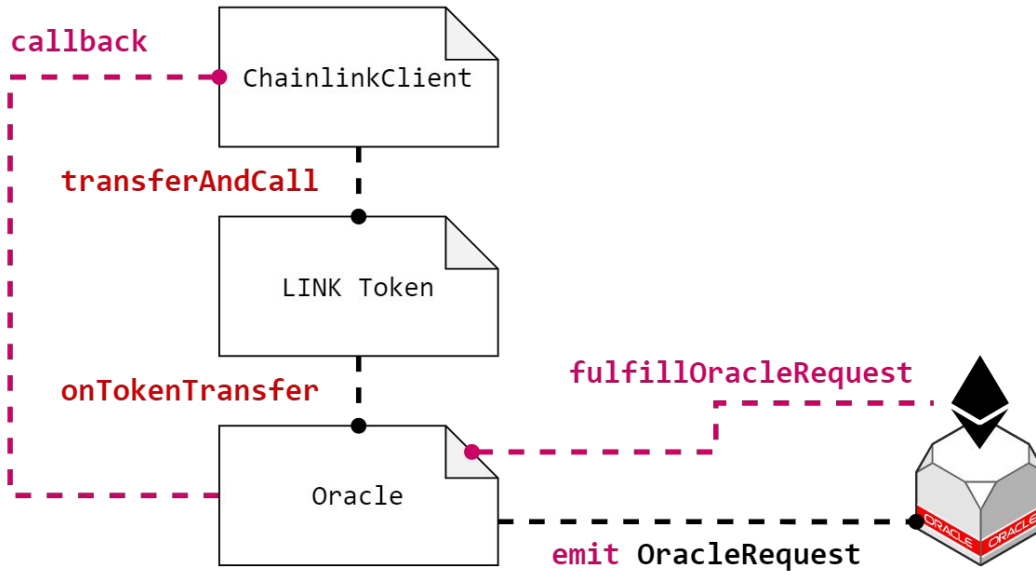


SEGURIDAD

INFRAESTRUCTURA



BAJO NIVEL: CRIPTOGRAFÍA

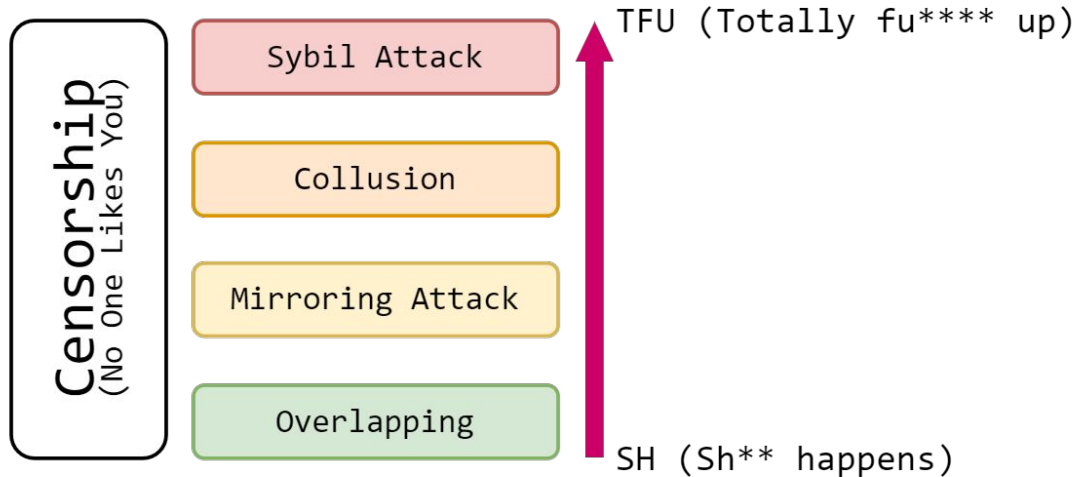


DISPONIBILIDAD

INTEGRIDAD

CONFIDENCIALIDAD

ALTO NIVEL: TAMPER-PROOF RESISTANCE



FREELADING

COMMIT-AND
REVEAL

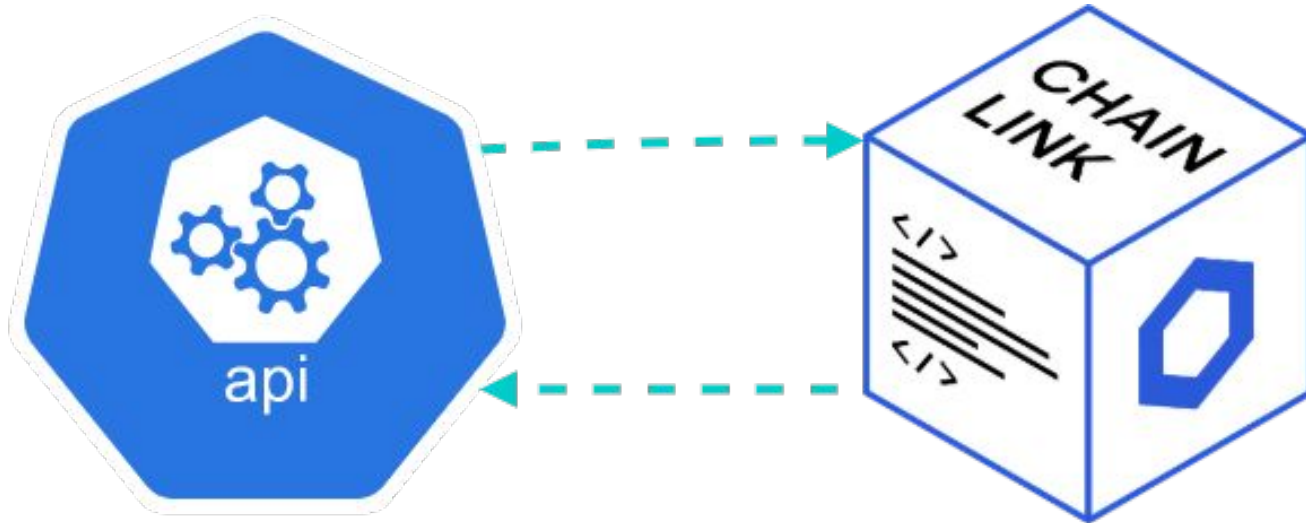
OCA (OFF-CHAIN
AGGREGATION)



SERVICIOS

Que nos ofrece Chainlink

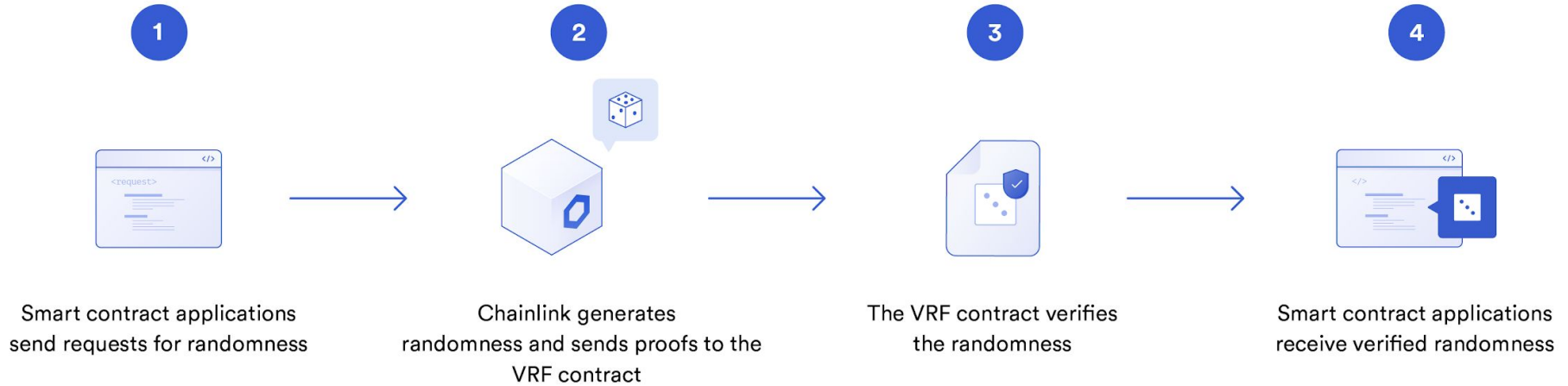
CONECTARSE A UNA API



ORÁCULOS MÚLTIPLES: PRICE FEEDS



VRF (FUNCIÓN ALEATORIA VERIFICABLE)





CRYPTO POKES

Probando las funcionalidades
de Chainlink en una D-App.

→ <https://obalfour.github.io/CryptoPokes/>

GRACIAS

¿ALGUNA CONSULTA?

