



LOS CONTRATOS SÍ CAMBIAN DE CÓDIGO CONTRATOS METAMÓRFICOS



PRESENTADO POR

Lee Marreros

Computer Programmer
Blockchain Bites Founder

01 de Diciembre del 2023

Mecanismos para actualizar contratos

EL PATRÓN DIAMANTE

CONTRATOS ACTUALIZABLES (UUPS, TRANSPARENT)

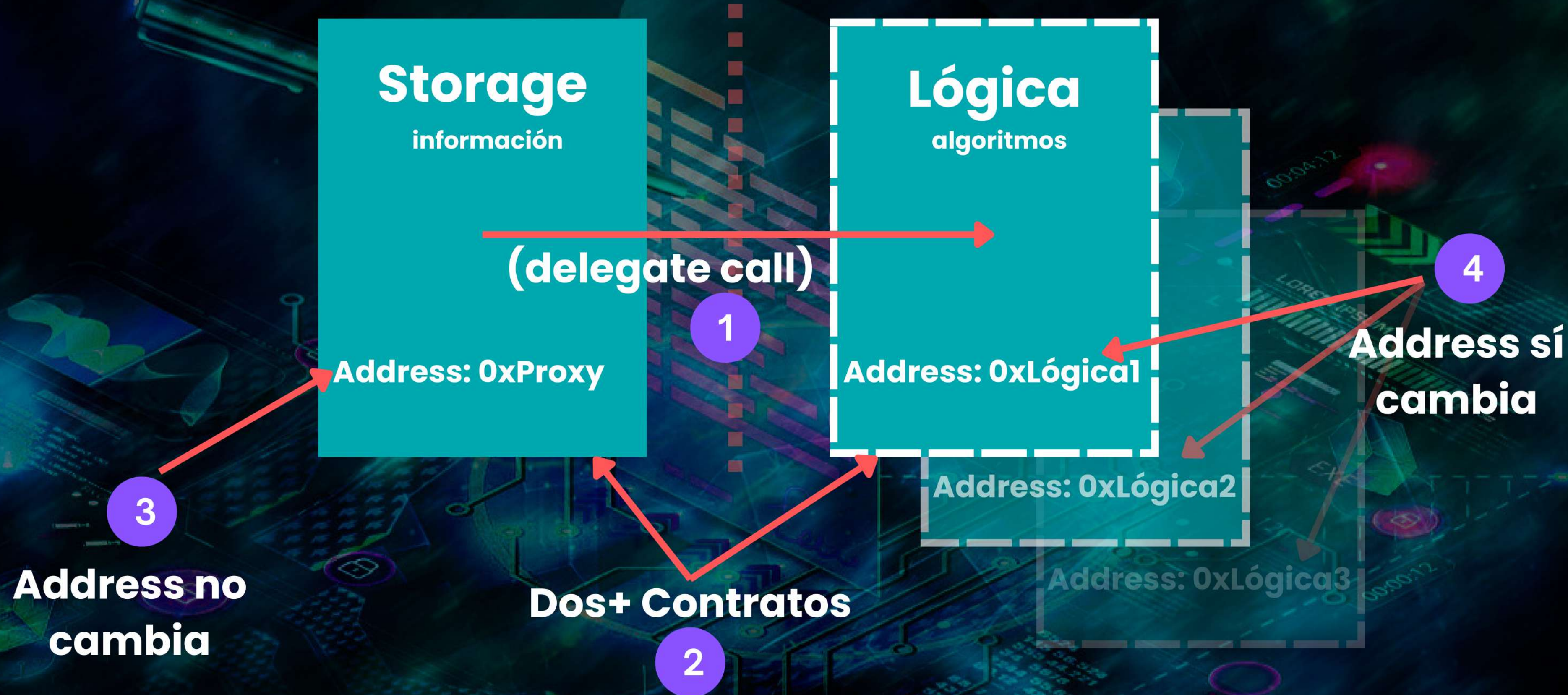
ETERNAL STORAGE

G1

CONTRATOS METAMÓRFICOS

G2

Actualización de Contratos G1



Actualización de C. Metamórficos



Construyendo un C. Metamórfico

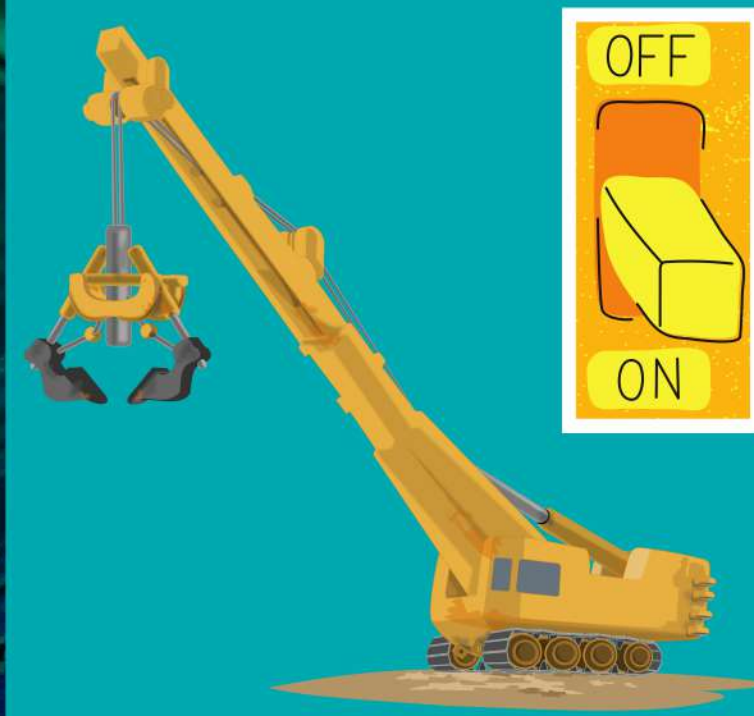
Conductor



2

CREATE2

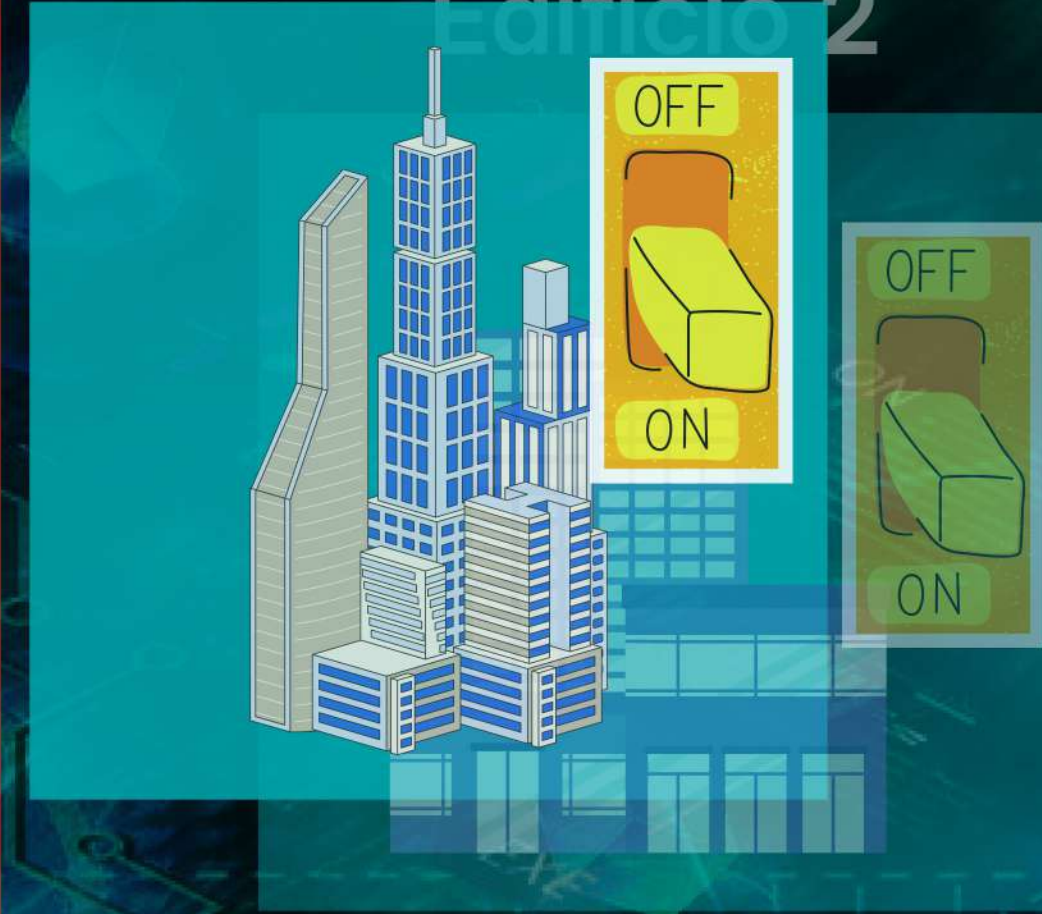
Grúa



1

CREATE

Edificio 1



Conductor
crea el contrato
Grúa

Grúa crea
el contrato
Edificio 1

Actualización

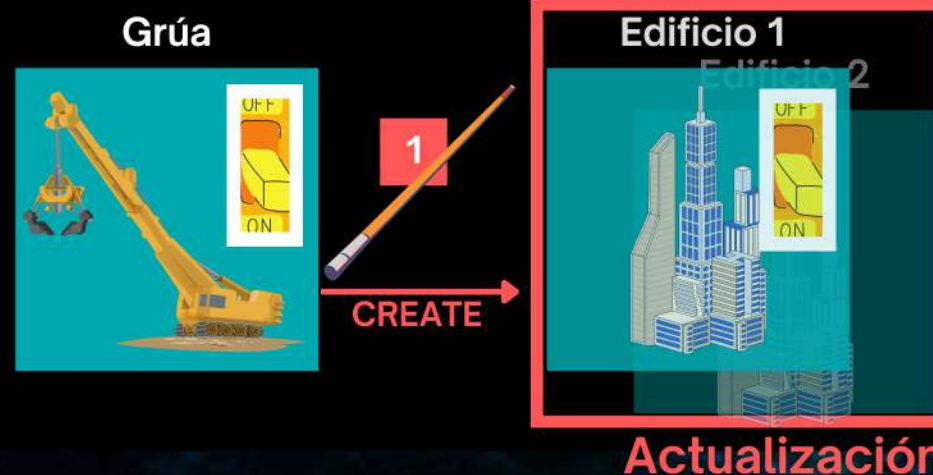
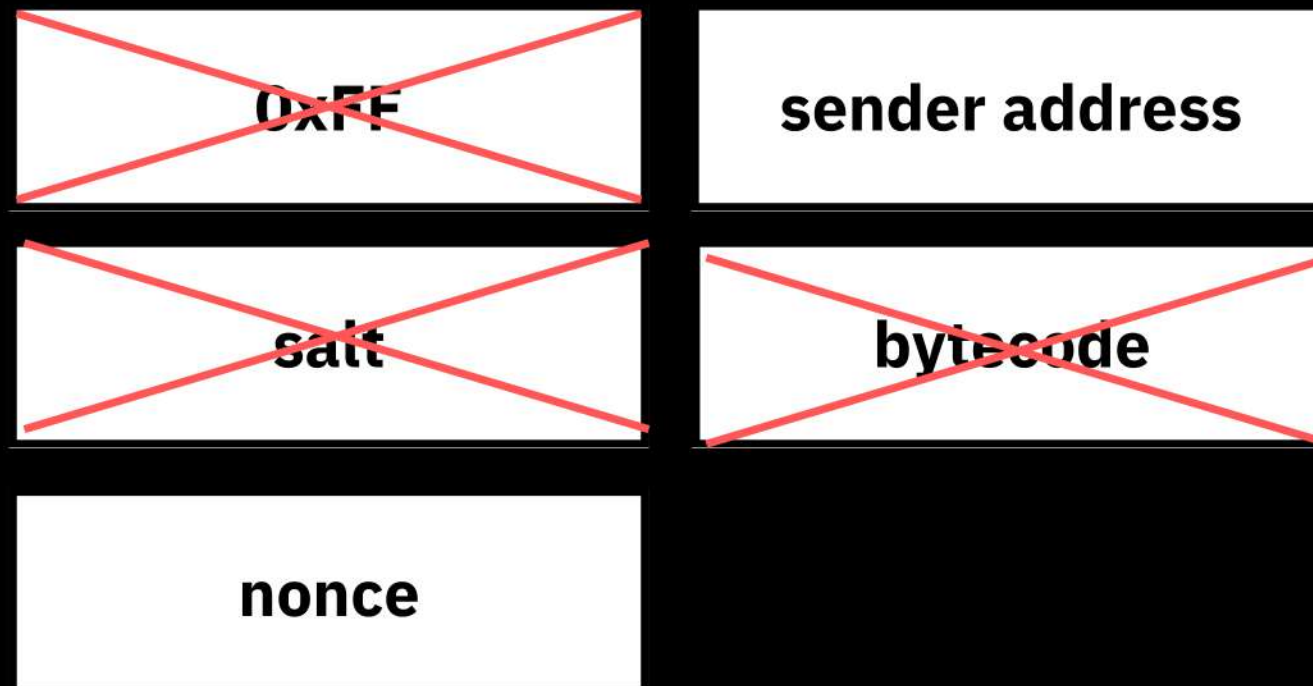
Explicando el opcode **CREATE**



1

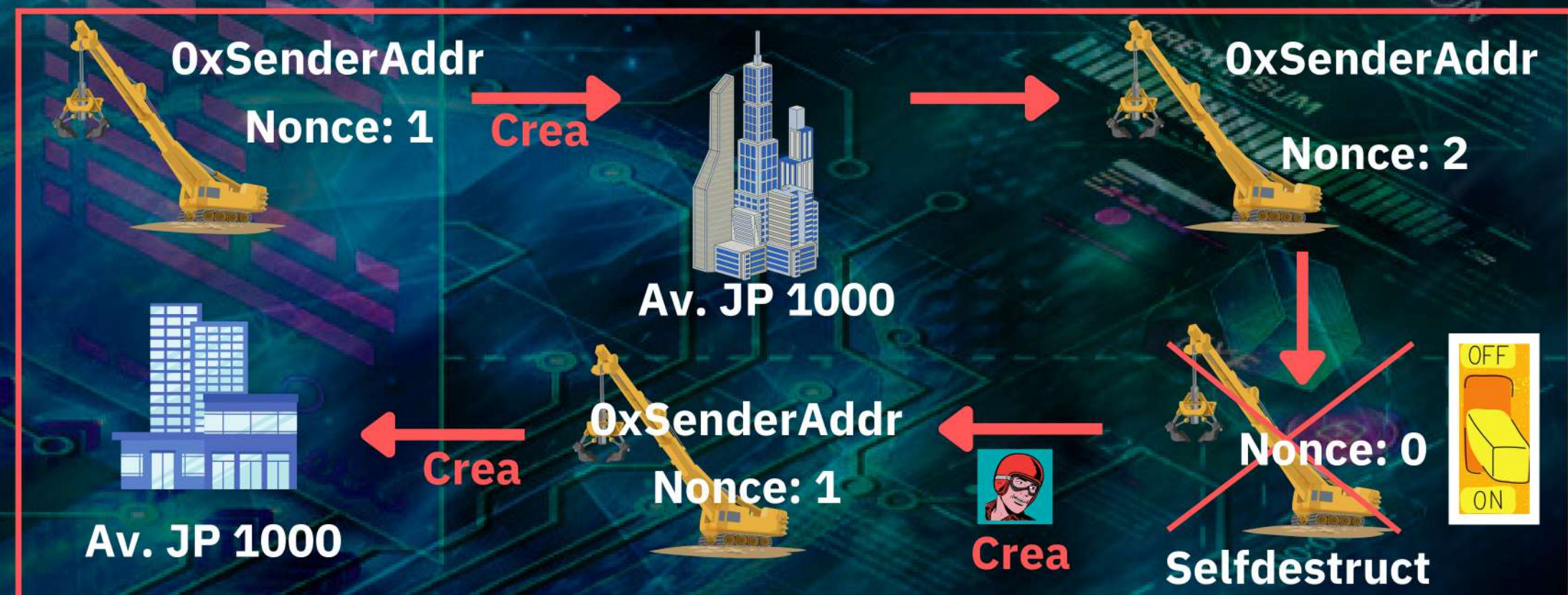
CREATE

Crea Contrato. Se puede resetear.
Protocolo calcula el address

INPUTS



Sender Address	Sender Nonce	Contract Address
 0xSenderAddr	1	Av. JP 1000
 0xSenderAddr	2	Av. ARQ 200



¿Quién se encarga de crear a la Grúa? **El Conductor**
Diferente Edificio en la misma address



Explicando el opcode **CREATE**

Con **CREATE**, podemos publicar diferente código en una misma address siempre y cuando se pueda resetear el **NONCE** del publicante

Explicando el opcode **CREATE2**

2

CREATE2

Crea Contrato. Se puede resetear.
Calcula address determinística

INPUTS



0xFF

sender address

salt

bytecode

~~nonce~~

Conductor

Grúa

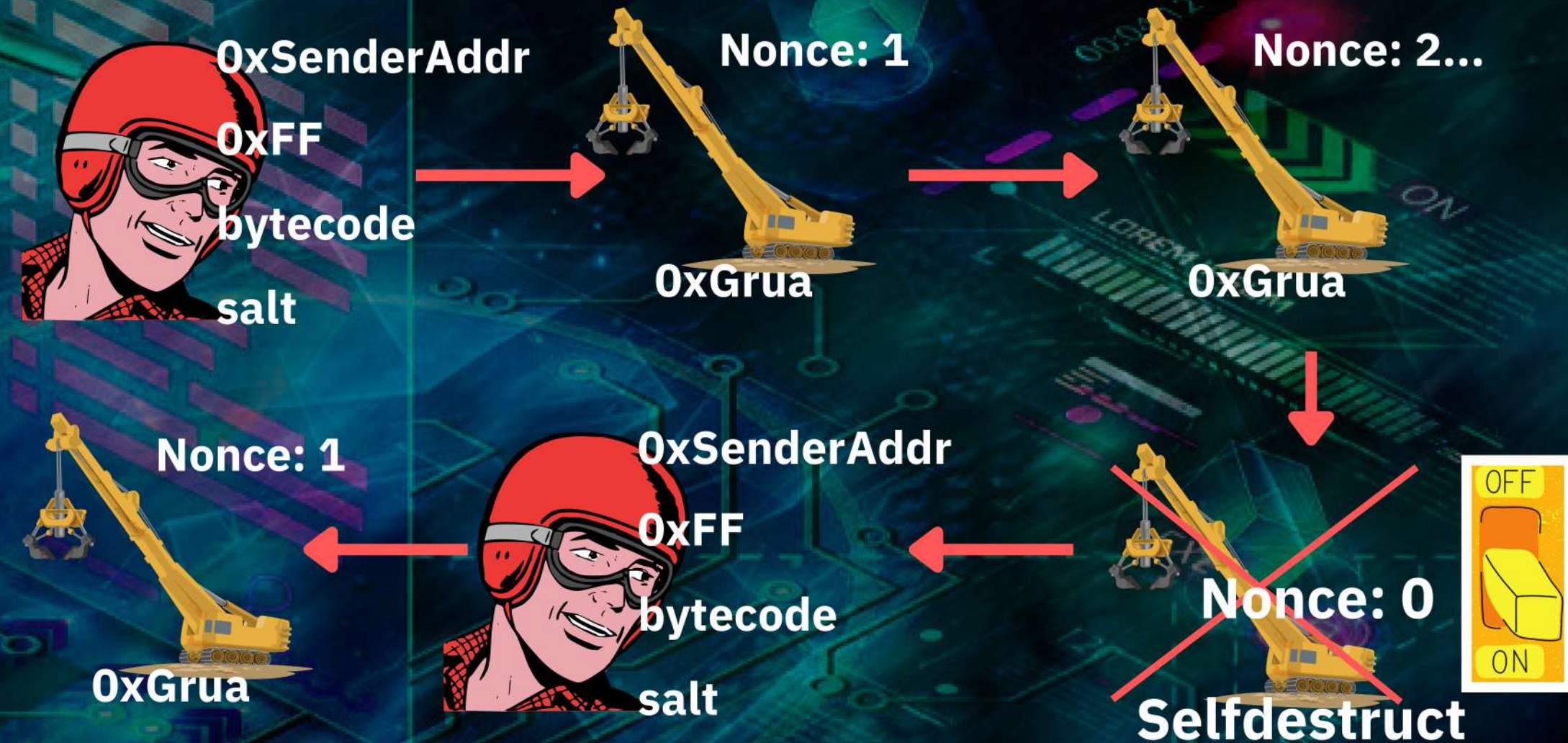


2

CREATE2



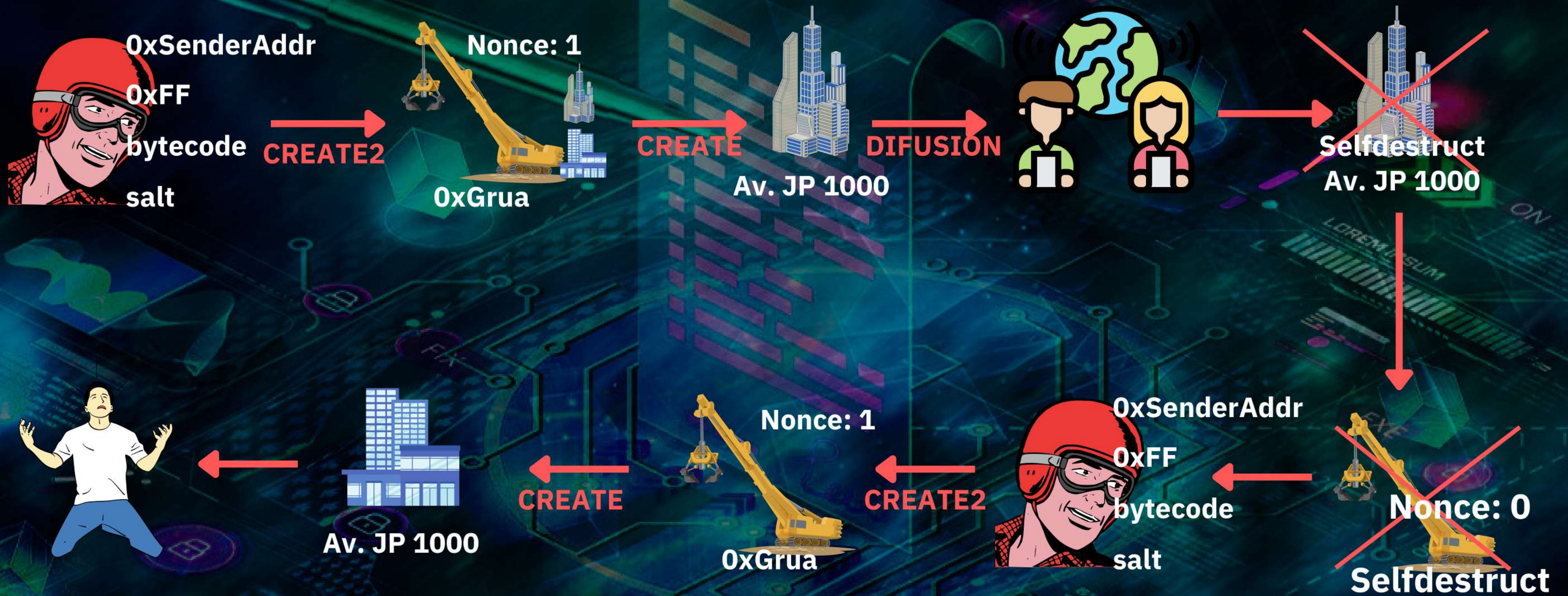
Aquí **no importa el nonce** del sender



Explicando el opcode **CREATE2**

Con **CREATE2**, podemos publicar el mismo código en una misma address siempre y cuando dicha address haya sido reseteada

Ataque de un C. Metamórfico



Repositorio, Artículo, Resumen, Slides



**BLOCKCHAIN
BITES** SCHOOL FOR WEB3
PROGRAMMERS

Especialización en

Programación Blockchain

Doble Certificado | 14 semanas | 03-2024

El programa más completo en todo LATAM



<https://tally.so/r/nrok92>