

CRIPTO · SERIE 2 · PARTE 02 / 04

PRUEBA DE TRABAJO Y PRUEBA DE PARTICIPACIÓN

Dos formas de hacer caro mentir. El modelo de amenaza de cada una, el funcionamiento de Gasper en Ethereum (ranuras, épocas, finalidad de Casper FFG), las penalizaciones por trampa tras Pectra y lo que cuesta atacar cada sistema.

Complemento técnico de la guía «¿Trabajo o participación?»
<https://amstech.dev/guias/bitcoin-s2/02-trabajo-o-participar/>

@ams_tech

ÍNDICE

1 Resumen

2 El problema y el ataque Sybil

3 La seguridad de la prueba de trabajo

4 Ethereum: Gasper

5 Penalizaciones (especificación Electra, desde Pectra)

6 Comparación del coste de un ataque

7 Lo que el vídeo simplifica

8 Referencias

1. RESUMEN

Una blockchain pública necesita que miles de participantes anónimos acuerden el orden de los bloques aunque algunos mientan. La **prueba de trabajo** (PoW) lo consigue haciendo que proponer bloques cueste energía. La **prueba de participación** (PoS), que haciendo trampa se pierda un depósito.

Este dossier:

- plantea el problema del consenso y por qué sin un coste es imposible (§2);
- resume la seguridad de PoW (§3);
- describe con detalle el protocolo de Ethereum desde *The Merge* (15/09/2022): selección de proponentes, comités, finalidad con Casper FFG y su garantía de **seguridad responsable** (§4);
- cuantifica las penalizaciones vigentes tras la actualización Pectra (§5) y compara el coste de atacar los dos sistemas (§6).

2. EL PROBLEMA Y EL ATAQUE SYBIL

En una red abierta, cualquiera puede crear identidades sin coste. Si el consenso se decidiera **por mayoría de identidades**, un atacante crearía millones y ganaría todas las votaciones: es el **ataque Sybil** [1]. Cualquier consenso abierto necesita, por tanto, un **recurso escaso** que no se pueda multiplicar gratis y que pondere la influencia de cada participante:

	RECURSO ESCASO	INFLUENCIA PROPORCIONAL A...
Prueba de trabajo	cálculo (y energía)	la fracción del hashrate
Prueba de participación	moneda bloqueada en depósito	la fracción del depósito total

3. LA SEGURIDAD DE LA PRUEBA DE TRABAJO

En PoW (series 1 y 2), el derecho a proponer un bloque se gana resolviendo la preimagen parcial (dossier 4 de la serie 1), y los nodos siguen la cadena válida con más trabajo acumulado. Sus propiedades:

- **Coste continuo.** El trabajo se gasta aunque nadie ataque; es el «precio» que se paga por bloque ($\approx 3,6$ GWh en Bitcoin, dossier anterior).
- **Umbral del 50 %.** Un atacante con más de la mitad del hashrate puede reescribir bloques recientes. Por debajo, su probabilidad de éxito decrece exponencialmente con las confirmaciones [2].

- **Finalidad probabilística.** Ningún bloque es definitivo al 100 %: solo cada vez más improbable de revertir.
- **Coste externo del ataque.** Hay que conseguir hardware y energía fuera del sistema. Tras un ataque fallido, el hardware sigue siendo del atacante.

4. ETHEREUM: GASPER

Desde *The Merge*, Ethereum usa **Gasper** [3]: la combinación de una regla de elección de cadena (LMD-GHOST) y un mecanismo de finalidad (Casper FFG [4]).

4.1 TIEMPO: RANURAS Y ÉPOCAS

UNIDAD	DURACIÓN	QUÉ OCURRE
Ranura (<i>slot</i>)	12 s	como máximo un bloque, de un proponente sorteado
Época (<i>epoch</i>)	32 ranuras = 6,4 min	cada validador vota (<i>atesta</i>) una vez
Finalidad	≈ 2 épocas = 12,8 min	los bloques quedan irreversibles salvo que se destruya ≥ 1/3 del depósito

4.2 VALIDADORES Y SELECCIÓN DEL PROPONENTE

Un **validador** es una clave con un depósito mínimo de **32 ETH**. Desde Pectra (mayo de 2025), un validador puede llegar a 2.048 ETH de **saldo efectivo** (EIP-7251 [5]). En cada ranura, el protocolo elige un proponente con probabilidad **proporcional a su saldo efectivo**, usando una semilla aleatoria (RANDAO) que construyen entre todos los proponentes anteriores.

Como ilustración, con un millón de validadores de 32 ETH hay unas $2,63 \cdot 10^6$ ranuras al año y cada validador espera

$$\lambda = \frac{2,63 \cdot 10^6}{10^6} \approx 2,6 \text{ propuestas al año,} \quad P(\text{ninguna en un año}) = e^{-\lambda} \approx 7\%. \quad (1)$$

Un validador con 2.048 ETH efectivos (64 veces más) tendría unas 168 propuestas al año: la influencia es proporcional al depósito, que es justamente la crítica de «premia a quien más tiene».

4.3 ATESTACIONES Y COMITÉS

En cada época, los validadores se reparten aleatoriamente en **comités**, uno por ranura, y cada uno firma una **atestación** que contiene dos votos:

1. **LMD-GHOST:** cuál considera la cabeza de la cadena. Sirve para elegir entre bifurcaciones en tiempo real.

2. **Casper FFG**: un voto de **enlace** entre dos *checkpoints*, los bloques de inicio de época: «de la fuente s al destino t ».

Las firmas son **BLS**, que se pueden **agregar**: miles de firmas de un comité se combinan en una sola de 96 bytes, verificable de una vez. Sin agregación, el protocolo no podría manejar cientos de miles de votos por época.

4.4 FINALIDAD CON CASPER FFG

Un *checkpoint* queda **justificado** cuando lo respaldan enlaces que suman al menos **2/3 del saldo total**, y **finalizado** cuando además el siguiente *checkpoint* se justifica a partir de él [4]. Para que el sistema funcione, los validadores honestos no deben firmar nunca dos votos que violen estas dos **reglas de castigo**:

- (I) **doble voto**: dos votos distintos con el mismo destino t ;
 - (II) **voto envolvente**: $s_1 < s_2 < t_2 < t_1$ (un voto «rodea» a otro).
- (2)

4.5 LA GARANTÍA: SEGURIDAD RESPONSABLE

El teorema central de Casper FFG [4] dice: si se finalizan dos *checkpoints* en conflicto, entonces validadores que suman **al menos 1/3 del saldo total** han violado (I) o (II), y la prueba (sus propias firmas) está en la cadena. La idea:

- Cada finalización necesita 2/3 del saldo.
- Dos conjuntos de 2/3 se solapan en al menos $\frac{2}{3} + \frac{2}{3} - 1 = \frac{1}{3}$.
- Ese tercio común ha votado a los dos lados, cosa imposible sin violar una regla.

Esto se llama **seguridad responsable** (*accountable safety*): un fallo de seguridad no puede ocurrir sin que se identifique y se castigue a los culpables.

5. PENALIZACIONES (ESPECIFICACIÓN ELECTRA, DESDE PECTRA)

Cuando se presenta la prueba de una violación de (2), el validador es **slashed** («recortado»): se le expulsa y pierde parte de su saldo en dos fases [5][6]:

$$\text{inicial} = \frac{B}{4096}, \quad \text{correlación} \approx B \cdot \min\left(\frac{3S}{T}, 1\right), \quad (3)$$

donde B es su saldo efectivo, S el saldo total de los validadores castigados en una ventana de unos 36 días y T el saldo total del sistema. La penalización por correlación se aplica a mitad de esa ventana. Para un validador de 32 ETH:

FRACCIÓN CASTIGADA A LA VEZ	INICIAL	POR CORRELACIÓN
solo él ($\approx 0\%$)	0,0078 ETH	≈ 0
1 %	0,0078 ETH	0,96 ETH
10 %	0,0078 ETH	9,6 ETH
$\geq 1/3$	0,0078 ETH	32 ETH (todo)

El diseño es deliberado. Un error aislado (por ejemplo, la misma clave funcionando en dos servidores) cuesta poco, pero un ataque coordinado, que necesita como mínimo $1/3$ del saldo por la sección anterior, **destruye el depósito completo** de todos los participantes. Antes de Pectra, la penalización inicial era $B/32$. Se redujo porque los validadores grandes que permite EIP-7251 sufrirían de forma desproporcionada por un fallo aislado.

6. COMPARACIÓN DEL COSTE DE UN ATAQUE

	PRUEBA DE TRABAJO (BITCOIN)	PRUEBA DE PARTICIPACIÓN (ETHEREUM)
Para reescribir bloques recientes	$> 50\%$ del hashrate	controlar la elección de cabeza de cadena durante varias ranuras
Para revertir lo «definitivo»	rehacer todo el trabajo posterior (probabilístico)	$\geq 1/3$ del saldo, que se pierde por (3)
Para paralizar la finalidad	— (no hay finalidad explícita)	$> 1/3$ del saldo que deje de votar
Después de un ataque	el atacante conserva su hardware	el depósito del atacante se destruye
Coste sin ataques	energía continua	casi nulo ($-99,95\%$ en <i>The Merge</i> [7])

Ninguna es estrictamente mejor. La PoS cambia el coste energético por **riesgo económico interno** y finalidad explícita, pero introduce otros problemas: la concentración del depósito en grandes proveedores, la complejidad del protocolo y los **ataques de largo alcance**. Este último es el riesgo de que alguien compre claves antiguas de validadores que ya retiraron su depósito para fabricar una historia alternativa. Se mitiga con la **subjetividad débil**: los nodos nuevos arrancan desde un *checkpoint* reciente que obtienen de una fuente de confianza.

7. LO QUE EL VÍDEO SIMPLIFICA

EN EL VÍDEO	CON PRECISIÓN
«La red sortea quién propone»	Selección ponderada por saldo efectivo con aleatoriedad RAND, una por ranura de 12 s
«Cuanto más bloqueas, más veces te toca»	Proporcional al saldo efectivo, hasta 2.048 ETH por validador
«Pierde parte de su fianza»	$B/4096$ más una penalización por correlación que llega al 100 % si participa $\geq 1/3$ del saldo
«Recortó su consumo un 99,95 %»	Estimación de la Fundación Ethereum para <i>The Merge</i>

8. REFERENCIAS

- [1] J. R. Douceur. «The Sybil Attack». *IPTPS 2002*, LNCS 2429, Springer.
- [2] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, sección 11. 2008. <https://bitcoin.org/bitcoin.pdf>
- [3] V. Buterin et al. «Combining GHOST and Casper». arXiv:2003.03052, 2020.
- [4] V. Buterin, V. Griffith. «Casper the Friendly Finality Gadget». arXiv:1710.09437, 2017.
- [5] M. Neuder et al. *EIP-7251: Increase the MAX_EFFECTIVE_BALANCE*. <https://eips.ethereum.org/EIPS/eip-7251>
- [6] Ethereum. *consensus-specs: Electra beacon chain*. <https://github.com/ethereum/consensus-specs/blob/master/specs/electra/beacon-chain.md>
- [7] Ethereum.org. *Consumo energético de Ethereum*. <https://ethereum.org/es/energy-consumption/>
- [8] B. Edgington. *Upgrading Ethereum: a technical handbook on Ethereum's move to proof of stake*. <https://eth2book.info>

Los tiempos, la probabilidad de propuesta de (1) y la tabla de penalizaciones se han calculado con un script propio a partir de los parámetros de la especificación.