

Ethereum merge

Lorenzo Zaccagnini 26/10/2022 @JODI



Lorenzo Zaccagnini

Founder of Devoleum

Psychology MSc

Blockchain developer @Kaaja

Contatti

Lorenzo Zaccagnini LinkedIn

Github

<https://github.com/LorenzoZaccagnini>

La fusione della Beacon Chain

Fonte: <https://ethereum.org/en/upgrades/merge/>

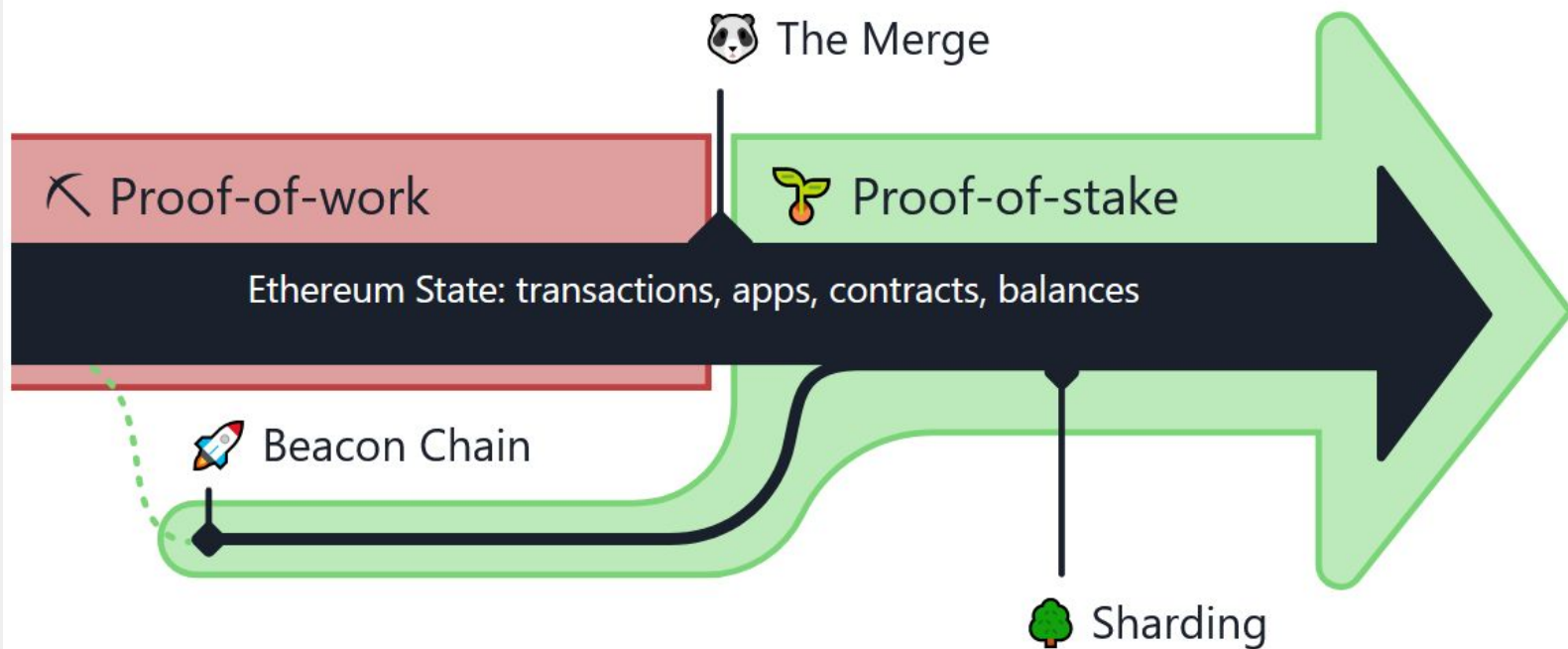
Inizialmente, la Beacon Chain veniva usata separatamente dalla Mainnet.

Ethereum Mainnet, con tutti i suoi account, bilanci, smart contract e stati della blockchain ha continuato a essere protetta dalla Proof-of-Work.

La Beacon Chain funzionava in parallelo utilizzando la Proof-of-Stake.

La fusione è avvenuta quando questi due sistemi si sono finalmente uniti e il proof-of-work è stato permanentemente sostituito dal Proof-of-Stake.

Passaggio da PoW a PoS



Un po' di storia

La Proof-of-Work ha assicurato Ethereum Mainnet dalla genesi fino al merge. Ciò ha consentito alla blockchain di Ethereum di nascere a luglio 2015 con tutte le sue caratteristiche familiari: transazioni, smart contract, account, ecc.

Nel corso della storia di Ethereum, gli sviluppatori si sono preparati per un'eventuale transizione dal Proof-of-Work al Proof-of-Stake.

Il 1° dicembre 2020, la Beacon Chain è stata creata come blockchain separata da Mainnet, in esecuzione in parallelo.

La Beacon Chain non stava originariamente elaborando le transazioni Mainnet. Invece, stava raggiungendo il consenso sul proprio stato concordando sui validatori attivi e sui saldi dei loro account. Dopo numerosi test, è arrivato il momento per la Beacon Chain di raggiungere il consenso sui dati del mondo reale. Dopo il merge, la Beacon Chain è diventato il motore (layer) del consenso.


Cosa era la Beacon Chain

La Beacon Chain era il nome della blockchain Proof-of-Stake originale lanciata nel 2020.

È stata creata per garantire che la logica del consenso Proof-of-Stake fosse solida e sostenibile prima di abilitarla su Ethereum Mainnet. Pertanto, funzionava insieme all'originale Ethereum Proof-of-Work.

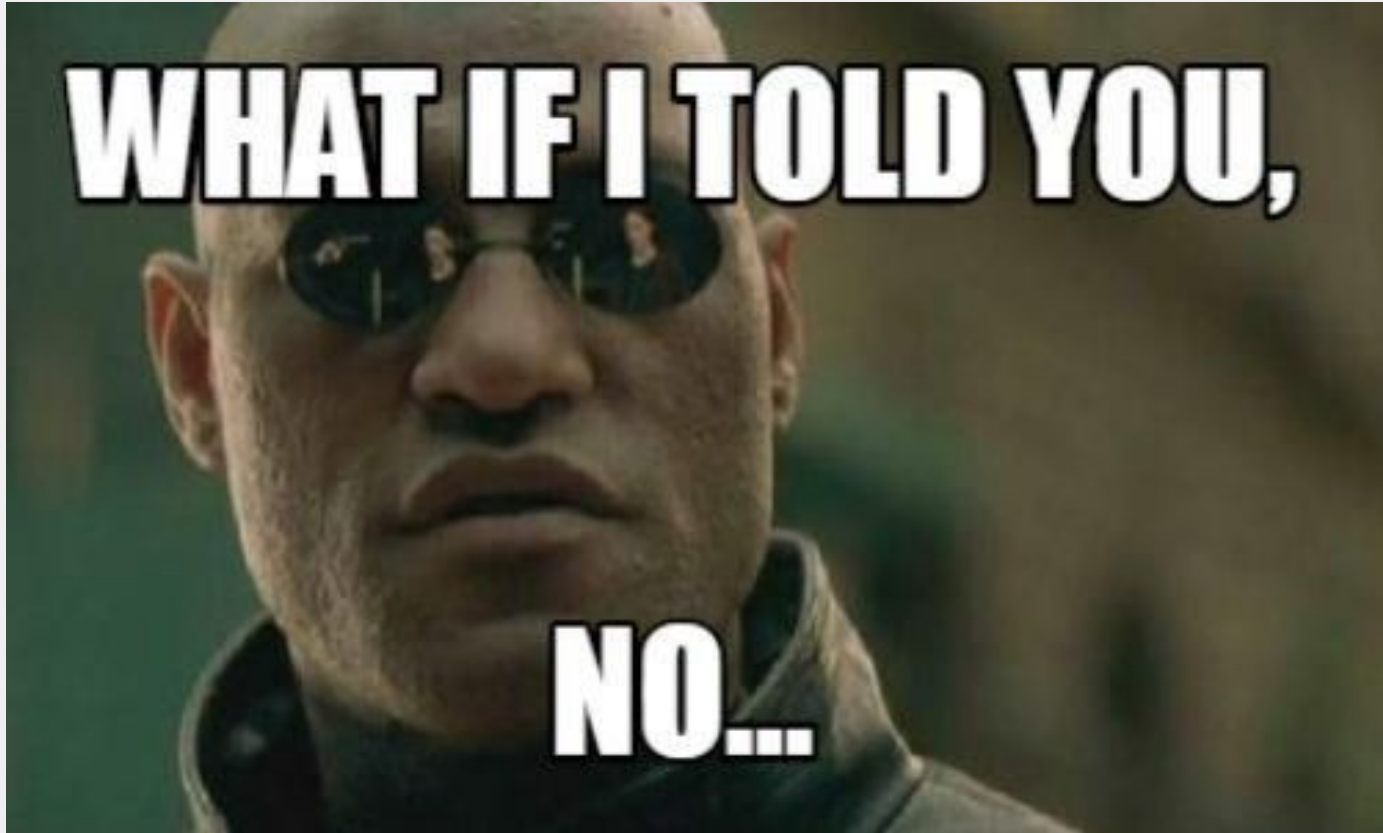
La disattivazione del Proof-of-Work e l'attivazione del Proof-of-Stake su Ethereum hanno richiesto alla Beacon Chain di accettare le transazioni dalla catena originale di Ethereum, raggrupparle in blocchi e quindi organizzarle in una blockchain utilizzando un Proof-of-Stake basato sul meccanismo di consenso. Nello stesso momento, i client originali di Ethereum hanno disattivato il mining, la propagazione dei blocchi e la logica del consenso, consegnando tutto alla Beacon Chain.

Questo evento era noto come "The Merge". Una volta avvenuto, non c'erano più due blockchain; c'era solo una blockchain di Ethereum Proof-of-Stake.

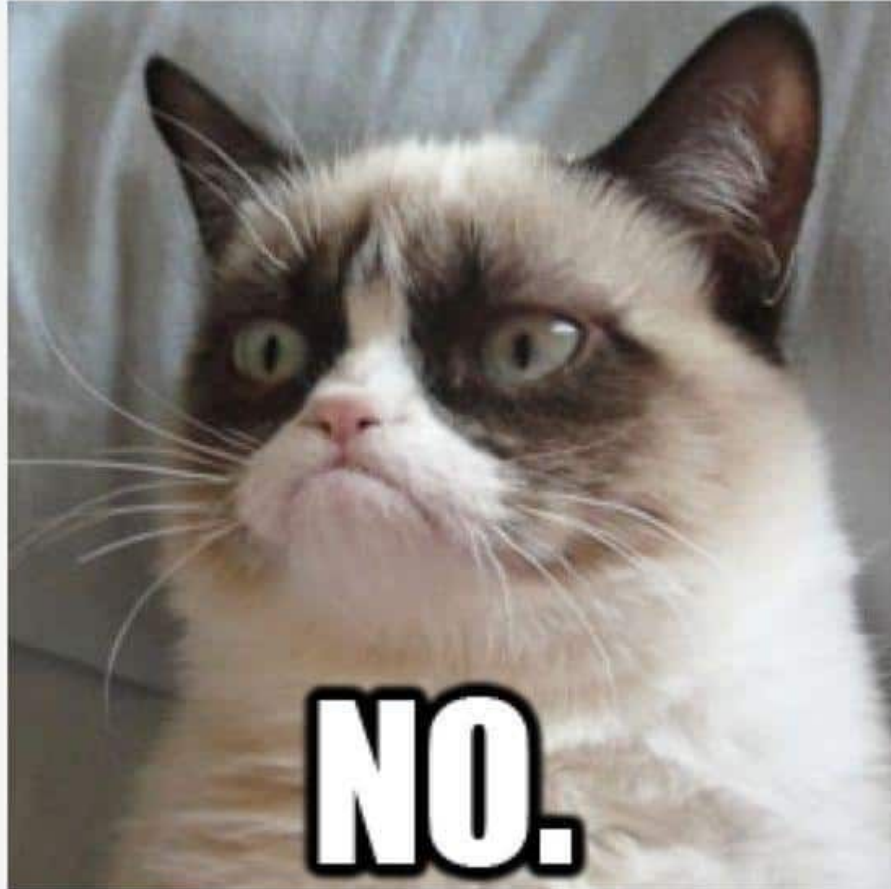
The background is a solid dark blue color. In the top right corner, there is a decorative pattern of overlapping triangles in various shades of blue, including a lighter blue and a darker blue, creating a geometric, abstract design.

**Il merge è avvenuto il 15
settembre 2022
E quindi...**

Minori costi per le transazioni?



Transazioni più veloci?



Sarà aumentata la scalabilità?





**Hanno implementato
il Proof of Stake**

Il Merge doveva avvenire dopo lo Sharding

Inizialmente, il piano prevedeva di lavorare sullo sharding prima del merge per affrontare la scalabilità. Tuttavia, con il boom delle soluzioni di layer 2 (Polygon, Optimism, Arbitrum), la priorità è passata allo scambio di Proof-of-Work con Proof-of-Stake.

I piani per implementare lo sharding sono in rapida evoluzione, ma data l'ascesa e il successo delle tecnologie per scalare l'esecuzione delle transazioni nel layer 2, i piani di sharding sono passati alla gestione dei rollup contract, consentendo una crescita esponenziale della capacità di rete. Ciò non sarebbe stato possibile senza prima passare al Proof-of-Stake.

Cos'è lo Sharding

- Lo sharding è un aggiornamento multifase per migliorare la scalabilità e la capacità di Ethereum.
- Lo sharding fornisce una distribuzione sicura dei requisiti di archiviazione dei dati, consentendo ai rollup di essere ancora più economici e semplificando il funzionamento dei nodi.
- Consente alle soluzioni di livello 2 di offrire commissioni di transazione basse sfruttando la sicurezza di Ethereum.

Lo sharding è il processo di divisione orizzontale di un database per distribuire il carico: è un concetto comune nell'informatica. In un contesto Ethereum, lo sharding funzionerà in sinergia con i rollup di livello 2 suddividendo l'onere della gestione della grande quantità di dati necessari per i rollup sull'intera rete. Ciò continuerà a ridurre la congestione della rete e ad aumentare le transazioni al secondo.

Cosa sono le layer 2

Layer 2 è un termine collettivo per le soluzioni scalabili di Ethereum che gestiscono le transazioni al di fuori della layer 1 di Ethereum sfruttando comunque la solida sicurezza decentralizzata della layer 1 di Ethereum.

Una layer 2 è dunque una blockchain separata che estende Ethereum.

Le layer 2 comunica regolarmente con Ethereum (inviando pacchetti di transazioni) per garantire che abbia garanzie di sicurezza e decentralizzazione simili. Tutto ciò non richiede modifiche al protocollo di layer 1 (Ethereum). Ciò consente alla layer 1 di gestire la sicurezza, la disponibilità dei dati e la decentralizzazione, mentre la layer 2 gestisce il ridimensionamento. Le layer 2 sottraggono il carico transazionale alla layer 1 e le inviano le prove finalizzate.

Rimuovendo questo carico di transazione dalla layer 1, la layer di base diventa meno congestionato e tutto diventa più scalabile.

Cosa è il Proof of Stake

Il Proof-of-Stake è alla base di alcuni meccanismi di consenso utilizzati dalle blockchain per ottenere un consenso distribuito.

Nel Proof-of-Work, i minatori dimostrano di avere un capitale a rischio spendendo energia.

Ethereum utilizza il Proof-of-Stake, in cui i validatori investono esplicitamente il capitale sotto forma di ETH in uno smart contract su Ethereum. Questo ETH in staking funge quindi da garanzia che può essere distrutta tutta o in parte se il validatore si comporta in modo disonesto o va offline. Il validatore dunque è responsabile del controllo che i nuovi blocchi propagati sulla rete siano validi.

I vantaggi

Il Proof-of-Stake include una serie di miglioramenti all'ormai deprecato sistema di Proof-of-Work:

- migliore efficienza energetica: non è necessario utilizzare molta energia per i calcoli Proof-of-Work
- barriere all'ingresso inferiori, requisiti hardware ridotti: non è necessario hardware d'élite
- rischio di centralizzazione ridotto: il Proof-of-Stake dovrebbe portare a più nodi che proteggono la rete
- a causa del basso fabbisogno energetico è necessaria una minore emissione di ETH per incentivare la partecipazione
- le sanzioni economiche per comportamento scorretto rendono il 51% degli attacchi di stile esponenzialmente più costosi per un attaccante rispetto al Proof-of-Work

Dai minatori ai validatori













Per partecipare come validatore, un utente deve depositare minimo 32 ETH nel contratto di deposito ed eseguire tre software separati: un client di esecuzione, un client di consenso e un validatore.

Al momento del deposito del proprio ETH, l'utente si unisce a una coda di attivazione che limita il tasso di nuovi validatori che si uniscono alla rete.

Una volta attivati, i validatori ricevono nuovi blocchi dai peer sulla rete Ethereum. Le transazioni consegnate nel blocco vengono rieseguite e la firma del blocco viene verificata per garantire che il blocco sia valido. Il validatore invia quindi un voto (chiamato attestato) a favore di quel blocco attraverso la rete.

Smart contract di staking

<https://etherscan.io/address/0x00000000219ab540356cbb839cbe05303d7705fa>

Txn Hash	Method ⓘ	Block	Age	From	To	Value	Txn Fee
 0x7d1cabd83d14223dd5...	Deposit	15812038	44 mins ago	0x579820a987b6a7e57d...	 Beacon Deposit Contract	32 Ether	0.00114628 
 0xf37781224494804602...	Deposit	15811674	1 hr 57 mins ago	Kraken: Eth2 Depositor	 Beacon Deposit Contract	32 Ether	0.00075698 
 0x576331d8dcead776cd...	Deposit	15811483	2 hrs 36 mins ago	Kraken: Eth2 Depositor	 Beacon Deposit Contract	32 Ether	0.0006729 
 0x5b51e1ddba2ca70968...	Deposit	15810846	4 hrs 44 mins ago	0x25ce1a59cf91ad5636...	 Beacon Deposit Contract	32 Ether	0.00121578 

E la mining difficulty?

E la gestione del tempo?

Mentre con la Proof-of-Work, la tempistica dei blocchi è determinata dalla difficoltà di mining, con la Proof-of-Stake il tempo è fisso.

Il tempo nel PoS Ethereum è diviso in slot (12 secondi) ed epoche (32 slot).

Un validatore viene selezionato casualmente per essere un proponente di blocco in ogni slot.

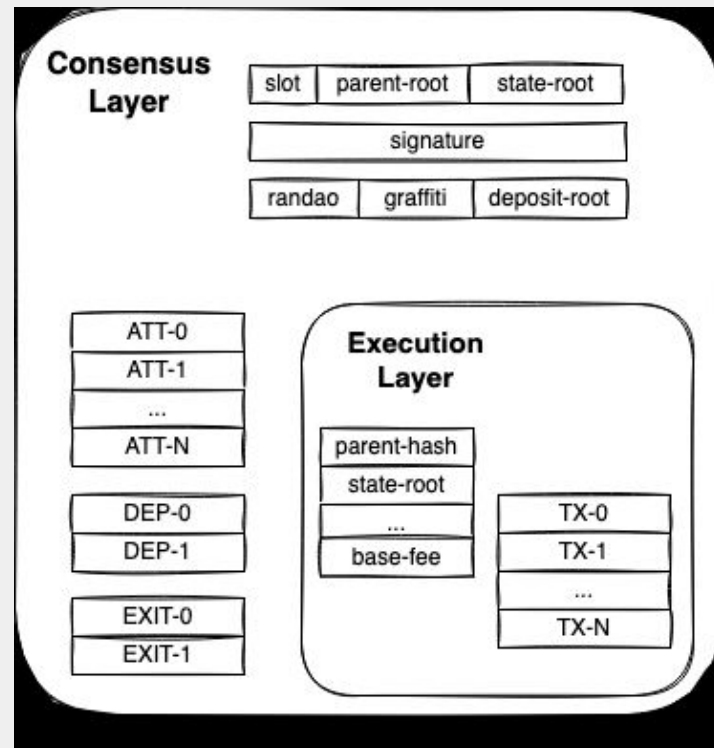
Questo validatore è responsabile della creazione di un nuovo blocco e dell'invio ad altri nodi della rete. Inoltre in ogni slot viene scelto casualmente un comitato di validatori, i cui voti sono utilizzati per determinare la validità del blocco proposto.

Block	Age	Txn
15812284	12 secs ago	155
15812283	24 secs ago	76
15812282	36 secs ago	140
15812281	48 secs ago	157
15812280	1 min ago	171
15812279	1 min ago	102
15812278	1 min ago	167
15812277	1 min ago	205

Struttura dati del blocco dopo PoS

Poiché il proof-of-stake non produce naturalmente ommer (ovvero uncle blocks) come il proof-of-work, l'elenco di questi in ogni blocco (ommers) sarà vuoto e l'hash di questo elenco (ommersHash) diventerà il RLP-hash codificato di una lista vuota. Allo stesso modo, poiché la difficoltà e il nonce sono caratteristiche della proof-of-work, questi verranno impostati a 0

mixHash, un altro campo relativo al mining, non sarà impostato su 0 ma conterrà invece il valore RANDAO della catena di beacon.



Cosa sono le epoche

Nelle blockchain, un'epoca è un periodo di tempo che stabilisce quando si verificheranno determinati eventi. Gli esempi includono la velocità con cui vengono distribuiti i premi o quando verrà assegnato un nuovo gruppo di validatori per convalidare le transazioni. I protocolli Blockchain che utilizzano epoche variano in quale periodo di tempo definisce un'epoca.

Con PoS Ethereum, si verifica un'epoca ogni 32 slot (6,4 minuti). Ogni slot in un'epoca rappresenta un tempo stabilito per un comitato di validatori (gruppi di almeno 128 validatori) per proporre e attestare (votare) la validità di nuovi blocchi.

Cosa sono le epoche

Questo significa che in ogni epoca ci sono 32 gruppi di comitati. Dopo che un comitato è stato assegnato a un blocco, una persona a caso su 128 nel comitato viene selezionata come proponente del blocco.

Quella persona è l'unica che può proporre un nuovo blocco di transazioni mentre le altre 127 persone votano la proposta e attestano le transazioni. Una volta che la maggioranza è d'accordo, il blocco viene aggiunto alla blockchain e il validatore che ha proposto il blocco riceve una quantità variabile di ETH sulla base di un calcolo formulario.

Validatori selezionati “casualmente”

I validatori vengono selezionati tramite un processo pseudocasuale tramite RANDAO. Poiché RANDAO fa parte dell'infrastruttura dell'ecosistema Ethereum, la premessa di base è che in ogni epoca, RANDAO assegna i proponenti di blocchi a ciascuno slot e rimescola i validatori in diversi comitati.

RANDAO teoricamente può essere soggetto a potenziali distorsioni o manipolazioni. Ethereum potrebbe integrare in futuro quella che è nota come VDF che rende il tempo di calcolo più lungo, più difficile da prevedere. Ogni validatore dovrebbe avere esattamente la stessa vincita prevista e la stessa probabilità di essere selezionato per i compiti.

Penalità

Esistono tre modi in cui un validator può essere sanzionato, che equivalgono tutti alla proposta disonesta o all'attestazione di blocchi:

- Proponendo e firmando due blocchi diversi per lo stesso slot
- Attestando un blocco che "circonda" un altro (cambiando di fatto la storia)
- Per "doppio voto" attestando due candidati per lo stesso blocco

Se vengono rilevate queste azioni, il validator viene sanzionato. Ciò significa che $\frac{1}{32}$ del loro eth in staking (fino a un massimo di 1 eth) viene immediatamente bruciato, quindi inizia un periodo di rimozione di 36 giorni. Durante questo periodo di rimozione il bilancio a stake dei validatori viene diminuito tramite uno stillicidio. A metà (Giorno 18) viene applicata una penalità aggiuntiva la cui magnitudo scala con l'eth totale di tutti i validatori puniti nei 36 giorni prima dell'evento malevolo. Ciò significa che quando vengono puniti più validatori, l'entità della sanzione aumenta. La sanzione massima è il saldo effettivo completo di tutti i validatori puniti.

Inattività

Se i validatori che rappresentano più di $1/3$ del totale dei validatori vanno offline o non presentano le attestazioni corrette, non è possibile che una supermaggioranza di $2/3$ finalizzi i voti e proponga i nuovi blocchi. La perdita di inattività attiva uno stillicidio graduale del bilancio a stake dei validatori inattivi fino a quando non controllano meno di $1/3$ della puntata totale, consentendo ai rimanenti validatori attivi di riprendere il controllo della gestione dei blocchi

Il design di ricompense, penalità e sanzioni della Beacon Chain incoraggia i singoli validatori a comportarsi correttamente. Tuttavia, da queste scelte progettuali emerge un sistema che incentiva fortemente la distribuzione equa dei validatori tra più clienti e dovrebbe fortemente disincentivare il dominio del singolo cliente

Consumo energetico PoW

Il consenso con la PoW richiede ai minatori di utilizzare il proprio hardware per risolvere un enigma, consumando energia nel processo.

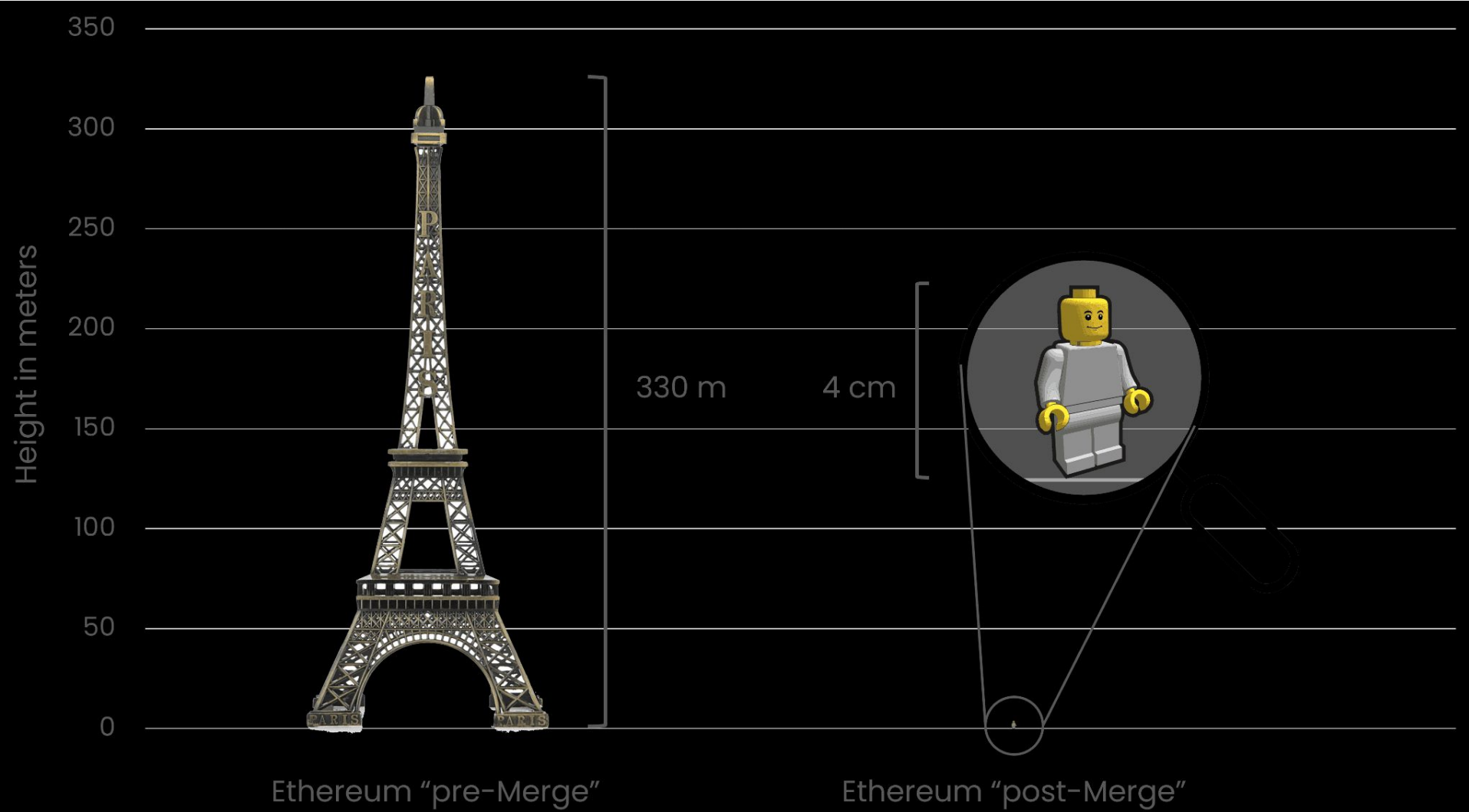
La soluzione del puzzle dimostra che l'energia è stata spesa dal minatore, investendo valore nel mondo reale per ottenere il diritto di aggiungere un blocco alla blockchain.

Il consumo totale di energia di Ethereum ha raggiunto il picco nel febbraio 2022 a poco meno di 94 TWh/anno. Nell'estate prima del passaggio al PoS, il consumo di energia era più vicino a 60 TWh/anno, paragonabile a quello dell'Uzbekistan, con un'emissione di carbonio equivalente a quella dell'Azerbaijan (33 MT/anno).

Consumo energetico PoS vs PoW

CCRI ha esaminato l'impatto del passaggio di Ethereum dal Proof-of-Work al Proof-of-Stake; i risultati hanno evidenziato l'impatto significativo della modifica del protocollo di consenso: il consumo di energia elettrica annualizzato è stato ridotto da 22.900.320 MWh a 2.601 MWh e quindi di oltre il 99,988%.

Allo stesso modo, l'impronta di carbonio di Ethereum è stata ridotta di circa il 99,992% (da 11.016.000 a 870 tonnellate di CO₂e). Rappresentato metaforicamente, ciò corrisponde a una riduzione delle emissioni dall'altezza della Torre Eiffel a un piccolo giocattolo di plastica, come mostrato nella figura della slide seguente.



**La sincronizzazione dei nodi richiede
comunque di scaricare GB di dati 24
ore al giorno**

Sicurezza degli smart contract

Per esempio con PoS se controlli lo 0,015% di tutti i validatori ETH, potresti proporre due blocchi di fila circa ogni 62 giorni. È possibile conoscere il produttore del blocco fino a 12,8 minuti in anticipo, questo invece non era possibile con PoW.

Unendo questi due aspetti si aprono nuovi scenari di attacco agli oracoli dei prezzi, i quali non richiedono zero costi ma il possesso di ingenti capitali (<35M\$).

Manipolando due blocchi di seguito è possibile ingannare gli oracoli che prezzano i token con danni devastanti, come visto negli attacchi flashloan o quello di Terra Luna.

Blockchain Sigint

Tutte le risorse sono gratuite e accessibili sulla repository Github della nostra open academy Blockchain Sigint: <https://github.com/blockchainsigint/slides>

